Future X Communications

FXC9024XG Management Guide

2016 年 4 月 Ver.2.1

FXC株式会社

本マニュアルについて

- 本マニュアルでは、FXC9024XG の各種設定およびシステムの監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末接続して、CLI （コマンドラインインタフェース）または Web ブラウザで行います。
- 本マニュアルに記載している機能は、ファームウェアバージョン 2.3.0.0 以降の製品に対応しています。

製品取り扱い時のご注意

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

・下記事項は、安全のために必ずお守りください。

● 安全のための注意事項を守る

注意事項をよくお読みください。製品全般の注意事項が記載されています。

● 故障したら使わない

すぐに販売店まで修理をご依頼ください。

● 万一異常が起きたら

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

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

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

● 電源ケーブルや接続ケーブルを傷つけない

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

● 内部に水や異物を入れない

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

● 内部をむやみに開けない

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

● 落雷が発生したらさわらない

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

● 油煙、湯気、湿気、ほこりの多い場所には設置しない

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

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

● ぬれた手で電源プラグやコネクタに触らない

感電の原因となります。

● 指定された電源コードや接続ケーブルを使う

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

● 指定の電圧で使う

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

● コンセントや配線器具の定格を超えるような接続はしない

発熱による火災の原因となります。

● 通風孔をふさがない

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

・毛足の長いジュウタンなどの上に直接設置しない。

・布などでくるまない。

● 移動させるときは、電源ケーブルや接続ケーブルを抜く

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

目次

目次

目次

目次

1. イントロダクション

1.1 主な機能

本機はレイヤ 2 スイッチングおよびレイヤ 3 ルーティングの、豊富な機能を提供します。

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 ー HTTPS Telnet ー SSH SNMPv1/2c －コミュニティ名 SNMPv3 － MD5 、SHA パスワード Port － IEEE802.1x 認証、MAC アドレスフィルタリング
Access Control Lists	最大 128 の IP ACL、96 の MAC ルールをサポート
DHCP Client	サポート
DNS	クライアントおよびプロキシサービス
Port Configuration	スピード、通信方式、フローコントロール
Rate Limiting	ポートごとの入力・出力帯域制御
Port Mirroring	1 つの分析ポートに対する 1 つまたは複数ポートのミラーリング
Port Trunking	Static 及び LACP による最大 32 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
IP バージョン 4	IPv4 アドレッシング、マネージメント、QoS サポート
IEEE802.1D Bridge	動的スイッチング及び MAC アドレス学習
Store-and-Forward Switching	ワイヤスピードスイッチング
Virtual LANs	IEEE802.1Q タグ付 VLAN/ ポートベース VLAN/ プロトコルベース VLAN/ プライベート VLAN（最大 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、DSCP、TCP/UDP ポート
Quality of Service	DiffServ サポート
IP ルーティング	RIP、静的ルーティングサポート
ARP	静的、動的アドレス設定、プロキシ ARP サポート
Multicast Filtering	IGMP Snooping、Query

1.2 ソフトウェア機能

本機は多くの機能を有し、それにより、効果的なネットワークの運用を実現します。
ここでは、本機の主要機能を紹介します。

設定のバックアップ及び復元

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

認証 /Authentication

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

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

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

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

ACL/Access Control Lists

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

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

ポート設定 /Port Configuration

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

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

帯域制御 /Rate Limiting

各インタフェースにおいて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 32 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？ Mbit 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。

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。
- プロトコルベース VLAN により、プロトコルタイプに基づいたトラフィックの制限を行うことが可能です。

プライオリティ /Traffic Prioritization

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

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

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

マルチキャストフィルタリング /Multicast Filtering

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

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

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？？？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	Baund Rate	auto
	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	SNMP Agent	Enabled
	Community Strings	“public“(read only) “private“(read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View:default view Group:public(read only) private(read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP(all ports)	Disabled

Broadcaststorm Protection	Status	Enabled(all ports)
	Broadcast Limit Rate	500 packets per second
Address Table	Aging Time	300seconds
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
	Queue Mode	WRR
	Weighted Round Robin	Queue:0 1 2 3 4 5 6 7 Weight:1 2 4 6 8 10 12 14
	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 Relay:Disabled Server:Disabled
	DNS	Client/Proxy:Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout:20 minutes Proxy:Disabled
Unicast Routing	RIP	Disabled
Multicast Filtering	IGMP Snooping	Snooping:Enabled Querier:Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled(but no server defined)
SNTP	Clock Synchronization	Disabled

2. 本機の管理

2.1 本機への接続

2.1.1 設定方法

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

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

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

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

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

- ユーザ名、パスワードの設定
- 管理 VLAN の IP インタフェースの設定
- SNMP パラメータの設定
- 各ポートの有効 / 無効
- 各ポートの通信速度及び Full/Half Duplex の設定
- 帯域制御による各ポートの入力及び出力帯域の設定
- IEEE802.1Q 準拠のタグ付 VLAN (最大 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
- Class of Service (CoS) の設定
- 静的トランク及び LACP 設定 (最大 32)
- 各ポートのブロードキャストストームコントロールの設定
- システム情報及び統計情報の表示

2.1.2 接続手順

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

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

[注意] スタックを設定している場合には、マスタユニットのコンソールポートへ接続をしてください。

手順 :

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

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

（3）パソコンのターミナルソフトウェアの設定を以下の通り行ってください。

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

通信速度 ---------- 9600 ～ 115200 ボー (baud)

データビット -------- 8bit

ストップビット ----- 1bit

パリティ ---------- なし

フロー制御 ---------- なし

エミュレーション -- VT100

（4）上記の手順が正しく完了すると、コンソールログイン画面が表示されます。

[注意] Windows2000 のハイパーターミナルを使用する場合、Windows2000 サービスパック 2 以上がインストールされていることをご確認ください。

[注意] コンソール接続に関する設定の詳細は P270 「Line （ラインコマンド）」を参照して下さい。
CLI の使い方は P233 「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 P242 「コマンドグループ」を参照して下さい。

2.1.3 リモート接続

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

初期設定では本機は DHCP、BOOTP を用いて自動的に IP アドレスを取得します。手動で IP アドレスの設定を行う場合の設定方法は P11 「IP アドレスの設定」を参照して下さい。

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

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

2.2 基本設定

2.2.1 コンソール接続

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

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

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

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

（2）ユーザ名入力画面で "admin" と入力します。

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

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

2.2.2 パスワードの設定

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

パスワードは最大 8 文字の英数字です。大文字と小文字は区別されます。

パスワードの設定方法は以下の通りです。

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

（2）"configure" と入力し <Enter> キーを押します。

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

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

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

```
Username: admin
Password:

      CLI session with the FXC 10/100/1000 is opened.
      To end the CLI session, enter [Exit].

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

2.2.3 IP アドレスの設定

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

IP アドレスの設定は下記のどちらかの方法で行うことができます。

手動設定

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

動的設定

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

手動設定

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

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

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

IP アドレスを設定するための手順は以下の通りです。

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

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

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

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

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

動的設定

"bootp" 又は "dhcp" を選択した場合、BOOTP 又は DHCP からの応答を受け取るまで IP アドレスは有効になりません。IP アドレスを取得するためには "ip dhcp restart client" コマンドを使用してブロードキャストサービスリクエストを行う必要があります。リクエストは IP アドレスを取得するために周期的に送信されます（BOOTP と DHCP から取得する値には IP アドレス、サブネットマスクおよびデフォルトゲートウェイが含まれます）

IP アドレスの取得方法として "bootp" 又は "dhcp" が起動ファイルに設定されている場合、本機は電源投入時に自動的にブロードキャストリクエストを送信します。

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

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

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

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

（3）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 client" 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

\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

2.2.4 SNMP 管理アクセスを有効にする

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

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

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

コミュニティ名（Community Strings）

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

初期設定でのコミュニティ名は以下のとおりです。

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

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

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

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

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

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

トラップ・レシーバ（Trap Receivers）

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

トラップ・レシーバの設定は以下の手順で行います

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

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

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

2.2.5 設定情報の保存

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

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

設定ファイルの保存は以下の手順で行います :

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

（2）起動設定ファイル名前を入力し、<Enter> キーを押します。

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

\Write to FLASH finish.
Success.

Console#
```

2.3 システムファイルの管理

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

3 種類のファイルは以下の通りです。

- **Configuration(設定ファイル)** — このファイルはシステムの設定情報が保存されており、設定情報を保存した際に生成されます。保存されたシステム起動ファイルに設定することができる他、サーバに TFTP 経由でアップロードしバックアップを取ることができます。
  "Factory_Default_Config.cfg" というファイルはシステムの初期設定が含まれており、削除することはできません。
  詳細に関しては P3-17「設定ファイルの保存・復元」を参照して下さい。

- **Operation Code(オペレーションコード)** — 起動後に実行されるシステムソフトウェアでランタイムコードとも呼ばれます。オペレーションコードは本機のオペレーションを行なう他、CLI、Web インタフェースを提供します。
  詳細に関しては 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)。

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

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

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

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

3. Web インタフェース

3.1 Web インタフェースへの接続

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

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

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

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

Web インタフェースを使用する場合は、事前に下記の設定を行って下さい。

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

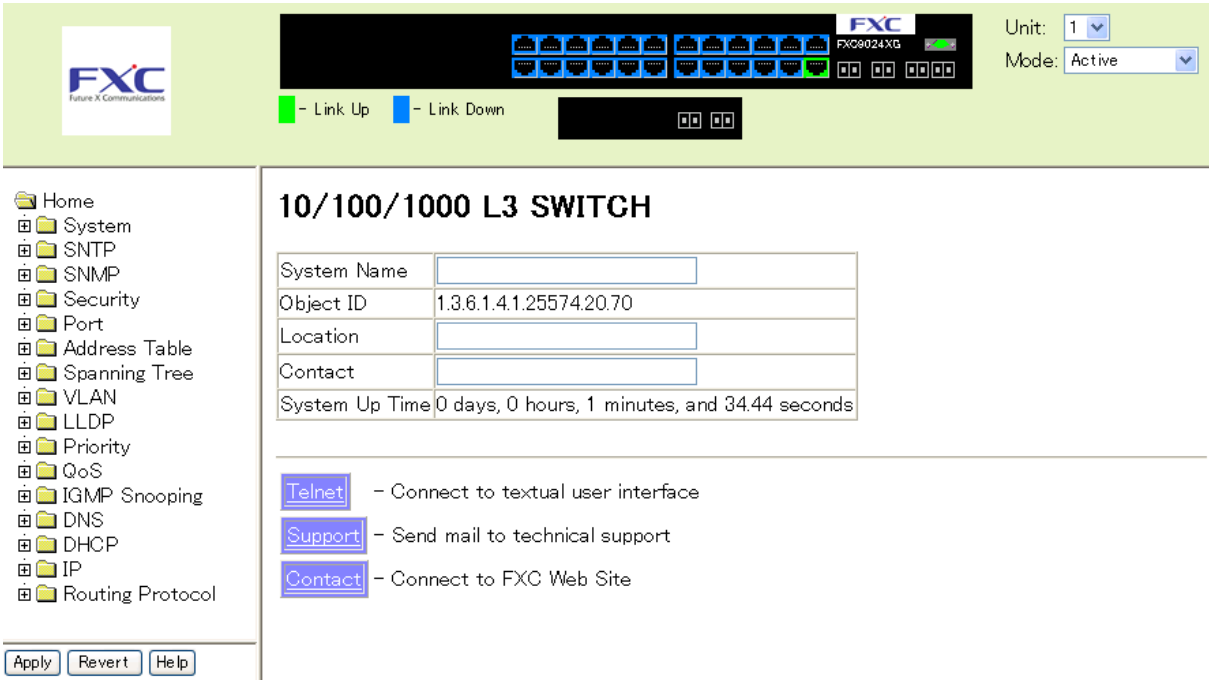
[注意] 管理用 PC と本機の間でスパニングツリーアルゴリズム (STA) が使用されていない場合、管理用 PC に接続されたポートをファストフォワーディングにする（Admin Edge Port の有効化）ことにより、Web インタフェースからの設定に対する本機の応答速度を向上させることができます（詳細は P113 「インタフェース設定」を参照して下さい）

3.2 Web インタフェースの操作方法

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

3.2.1 ホームページ

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



3.2.2 設定オプション

設定パラメータにはダイアログボックスとドロップダウンリストがあります。

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

次の表は Web ページに表示される設定ボタンの内容を解説しています。

表 3-1

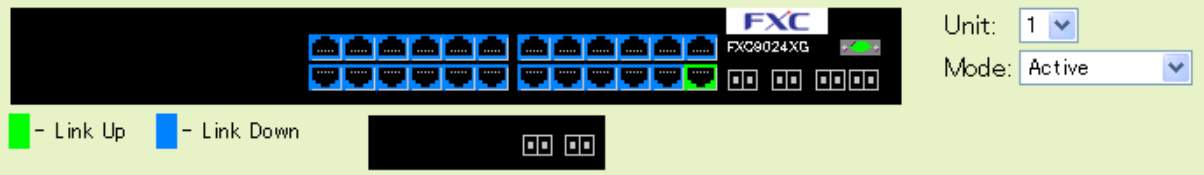
ボタン	操作
Revert	入力した値をキャンセルし、[Apply] 又は [Apply Changes] をクリックする前に表示されていた元の値に戻す
Apply	入力した値を本機に反映させる
Help	Web ヘルプにリンクしています

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

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

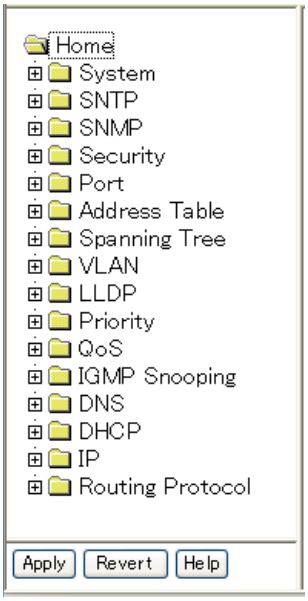
3.2.3　パネルの表示

Web インタフェースではポートの状態が画像で表示されます。各ポートのリンク状態、Duplex、フローコントロールなどの状態を確認することができます。また、各ポートをクリックすることで P86 「インタフェース接続の設定」で解説している各ポートの設定ページが表示されます。



3.2.4　メインメニュー

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



3.3 基本設定

3.3.1 システム情報の表示

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

設定・表示項目

System Name

本機に設定した名前

Object ID

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

Location

本機の設置場所

Contact

管理者のコンタクト情報

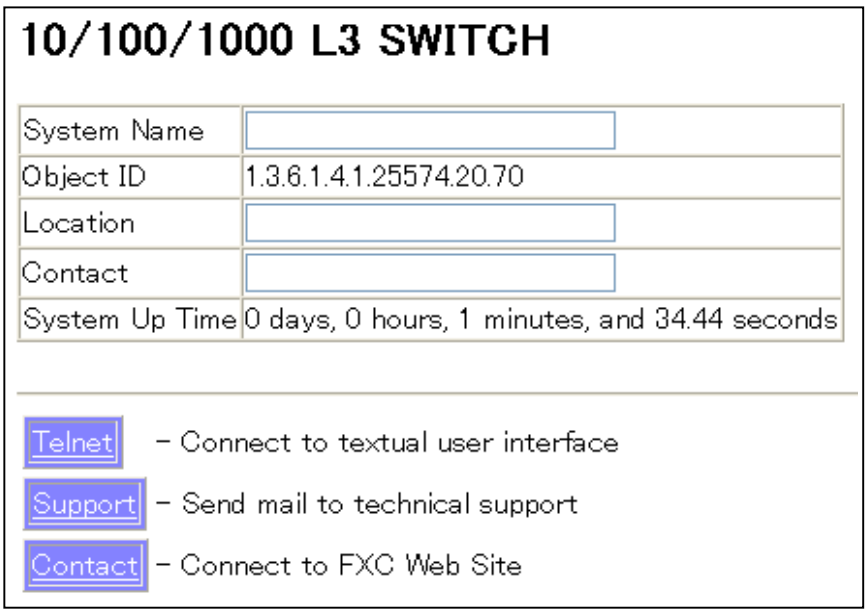
System Up Time

管理システムを起動してからの時間

設定方法

[System] → [System Information] **をクリックします。**system name**（システム名）、**location**（設置場所）及び** Contact**（管理者のコンタクト情報）を入力し、**[Apply] **ボタンをクリックします。**

（このページは Telnet **を利用し** CLI **にアクセスするための** [Telnet] **ボタンがあります）**



3.3.2 ハードウェア及びソフトウェアバージョンの表示

設定・表示項目

[Main Board](ハードウェア本体)

Serial Number

本機のシリアルナンバー

Number of Ports

搭載された RJ － 45 **ポートの数**

Hardware Version

ハードウェアのバージョン

Internal Power Status

内蔵電源のステータス

[Management Software](管理ソフトウェア)

EPLD Version

Electronically Programmable Logic Device Code **のバージョン**

Loader Version

Loader Code **のバージョン**

Boot-ROM Version

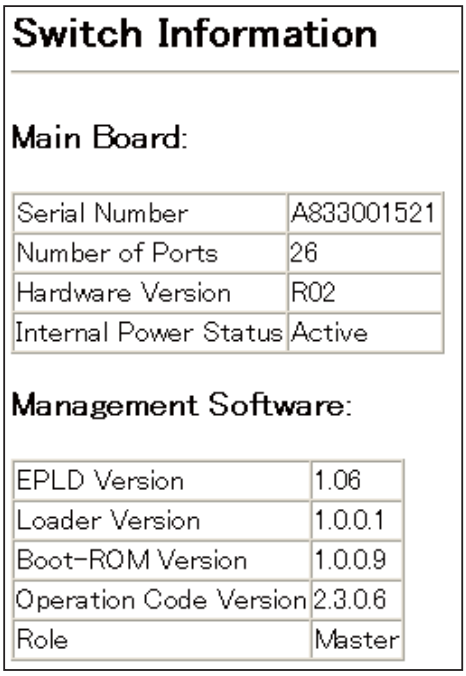
Power-On Self-Test (POST) **及び** boot code **のバージョン数**

Operation Code Version

runtime code **のバージョン**

設定方法

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



3.3.3 ブリッジ拡張機能の表示

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

設定・表示項目

Extended Multicast Filtering Services

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

Traffic Classes

ユーザプライオリティが複数のトラフィッククラスにマッピングされていることを表します。(詳細は、P154 「Class of Service（CoS)」を参照して下さい)

Static Entry Individual Port

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

VLAN Learning

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

Configurable PVID Tagging

本機は各ポートに対して初期ポート VLAN ID（フレームタグで使用される PVID）と、その出力形式（タグ付又はタグなし VLAN）が設定可能であることを表しています（P120 「VLAN」を参照して下さい）

Local VLAN Capable

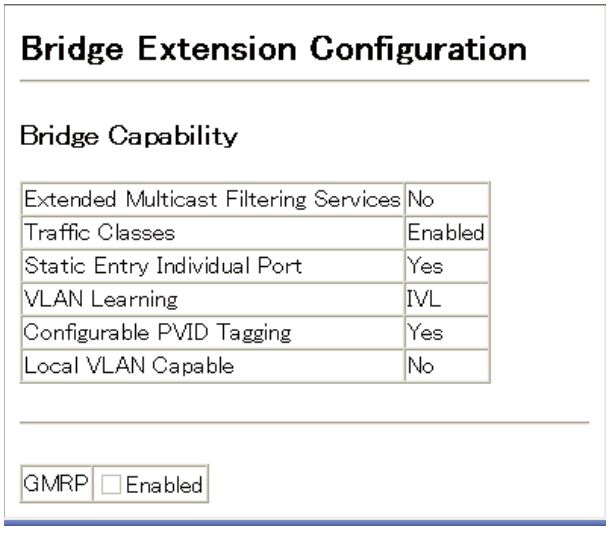
本機は複数のローカルブリッジ (マルチプルスパニングツリー) をサポートしていることを表しています

GMRP

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

設定方法

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



3.3.4 IP アドレスの設定

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

手動で IP アドレスの設定を行う際は、使用するネットワークで利用可能な IP アドレスを設定して下さい。
（手動設定時の初期設定は、IP アドレス :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

VLAN

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

IP Address Mode

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

IP Address

管理アクセスを行うことができる VLAN インタフェースの IP アドレスを設定します。

有効な IP アドレスは、0-255 までの十進数 4 桁によって表現され、それぞれピリオドで区切られます（初期設定：0.0.0.0）

Subnet Mask

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

Default Gateway

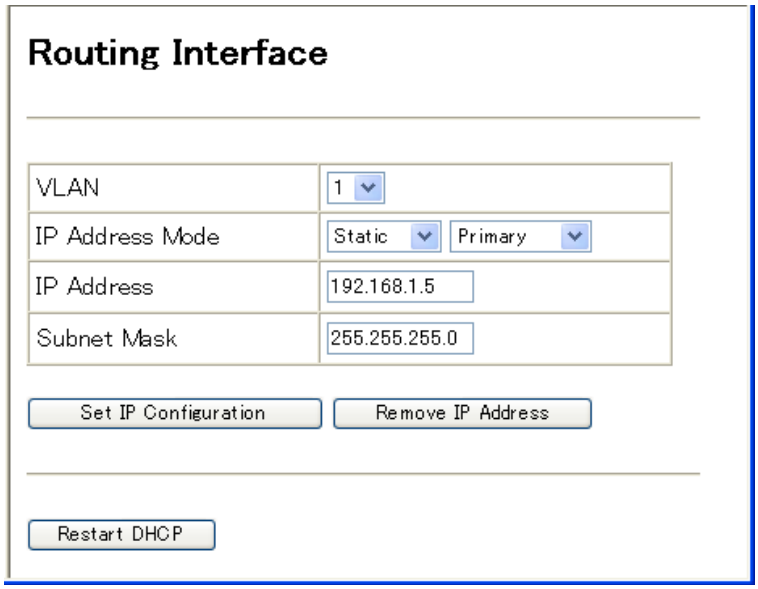
管理端末へのゲートウェイの IP アドレスを設定します。

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）

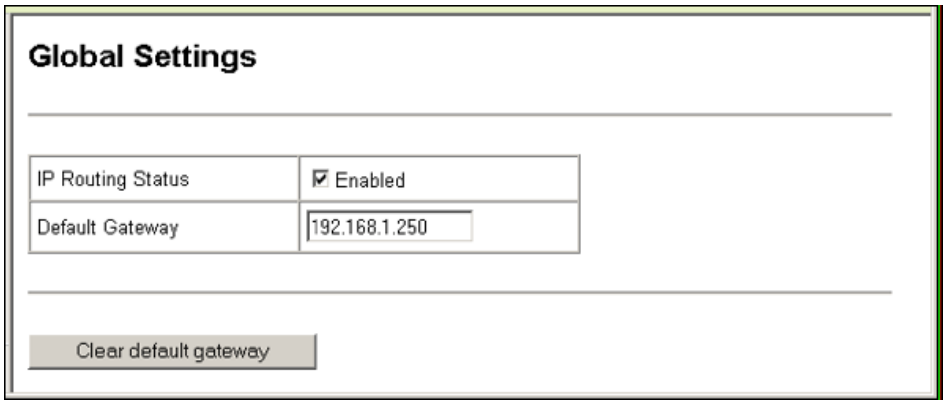
手動での IP アドレスの設定

設定方法

[IP] → [General] → [Routing Interface] をクリックします。



[IP] → Global Setting] をクリックします。スイッチとマネージメントステーションが異なるネットワークに存在する場合、デフォルトゲートウェイを指定します。

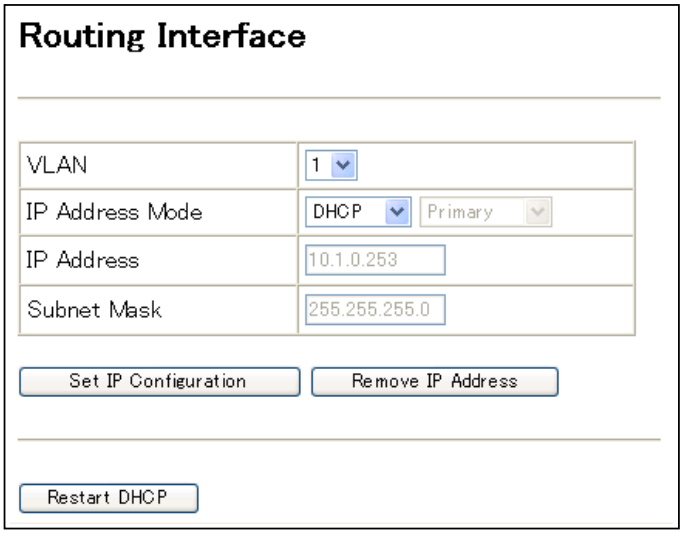


DHCP 又は BOOTP による IP アドレスの設定

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

設定方法

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



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

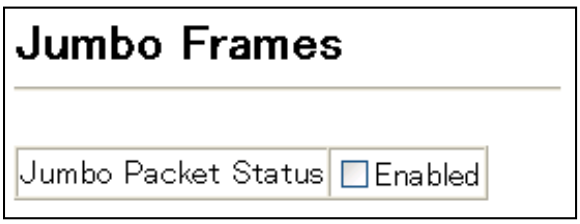
DHCP の更新

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

設定方法

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

3.3.5 ジャンボフレームの設定



3.3.6 ファームウェアの管理

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

設定・表示項目

File Transfer Method

ファームウェアコピーの操作方法。下記のオプションがあります。

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

TFTP Server IP Address

TFTP サーバの IP アドレス

File Name

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

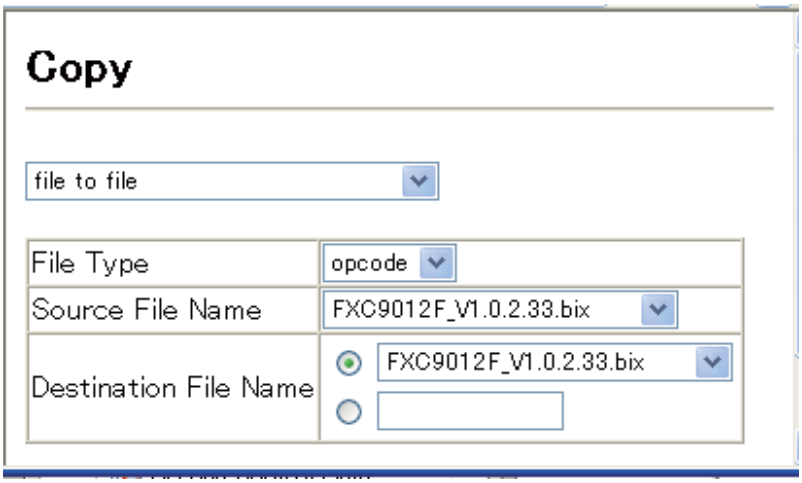
[注意] システムソフトウェアファイルは最大 2 つまでしか保存できません。起動ファイルに指定されているファイルは削除することができません。

システムソフトウェアのダウンロード

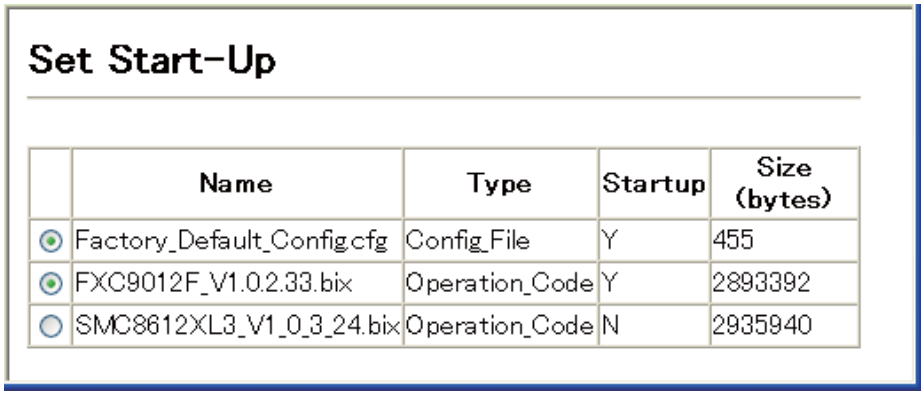
runtime code をダウンロードする場合、現在のイメージと置き換えるために現在のファイルを Destination File Name として指定することができます。また、現在の runtime code ファイルと異なるファイル名を使用し本体にダウンロードし、その後ダウンロードしたファイルを起動ファイルに設定することもできます。

設定方法

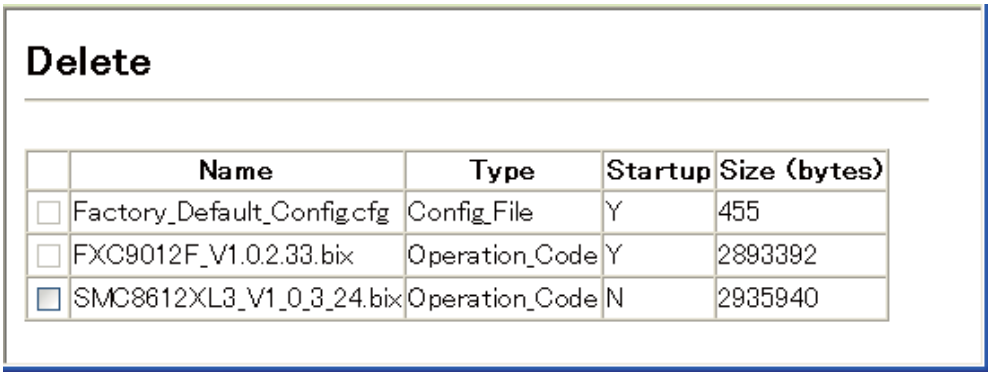
[System] → [File Management] → [Copy Operation] をクリックします。



現在の 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 Operation Code にする必要があります。ドロップダウンボックスから新しいファイル名を選択します。その後、[Apply Changes] をクリックします。新しいファームウェアを使用するためには本機の再起動を行います。



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



3.3.7 設定情報ファイルの保存・復元

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

設定・表示項目

TFTP Server IP Address

TFTP サーバの IP アドレス

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, ".", "-", "_"）

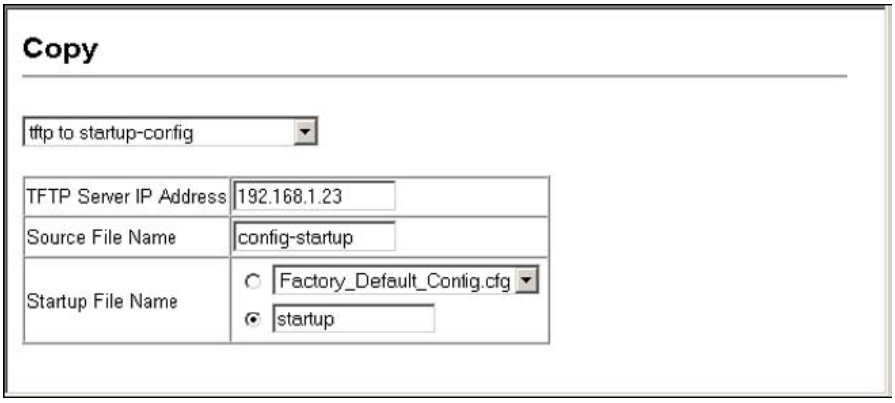
[注意] 本機内に保存可能な設定ファイルの最大数はフラッシュメモリの容量に依存します。

設定情報ファイルのダウンロード

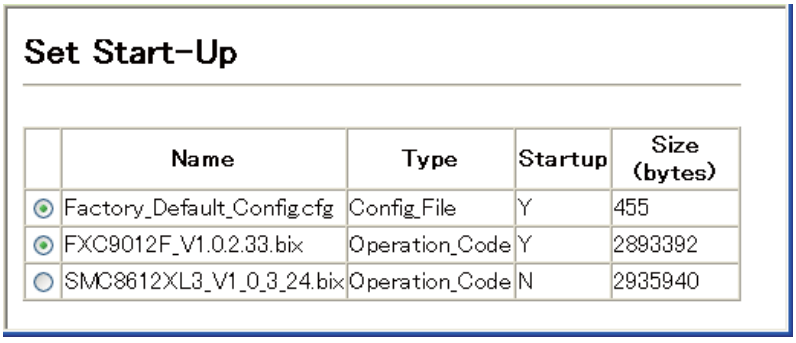
設定ファイルは新しいファイル名で保存し、起動ファイルとして設定できる他に、現在の起動設定ファイルを保存先に指定することで直接起動設定ファイルを置き換えることができます。但し、"Factory_Default_Config.cfg" ファイルは TFTP サーバへコピーすることはできますが、設定ファイルをダウンロードする際に、ダウンロード先のファイル名として指定し、新しいファイルに置き換えることはできません。

設定方法

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



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



3.3.8 コンソールポートの設定

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

設定・表示項目

Login Timeout

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

Exec Timeout

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

Password Threshold

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

Quiet Period

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：30 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）

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）

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、38400baud　初期設定：115200 baud)

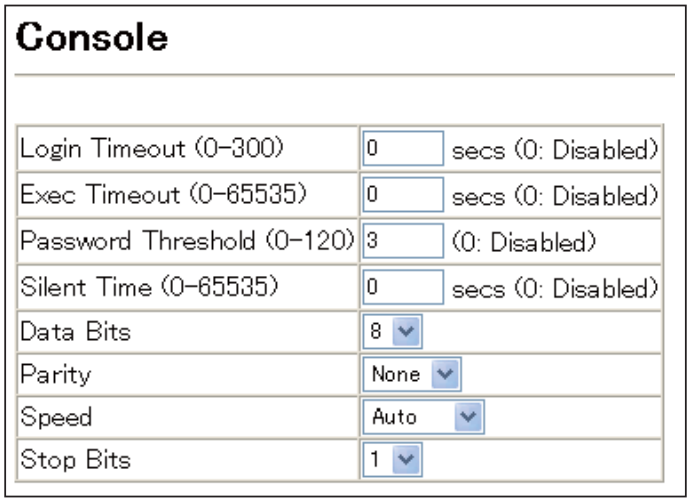
[注意]　コンソール接続のパスワードは CLI からのみ設定出来ます。（P273 「password」を参照）

[注意]　コンソール接続ログインのパスワードチェックは有効または無効に出来ます。（P272 「login」を参照）

[注意]　"password" コマンドで設定されたシングルグローバルパスワードによる認証または、ユーザネームアカウントのために設定されたパスワードによる認証から選択が可能です。スイッチ上に設定されている初期設定はローカルパスワードです。

設定方法

(1) [System] → [Console] をクリックします。
(2) 必要な接続パラメータを指定します。
(3) ＜ Apply ＞をクリックします。



3.3.9 Telnet の設定

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

設定・表示項目

Telnet Status

本機への Telnet 接続の有効 / 無効（初期設定：有効）

TCP Port

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。

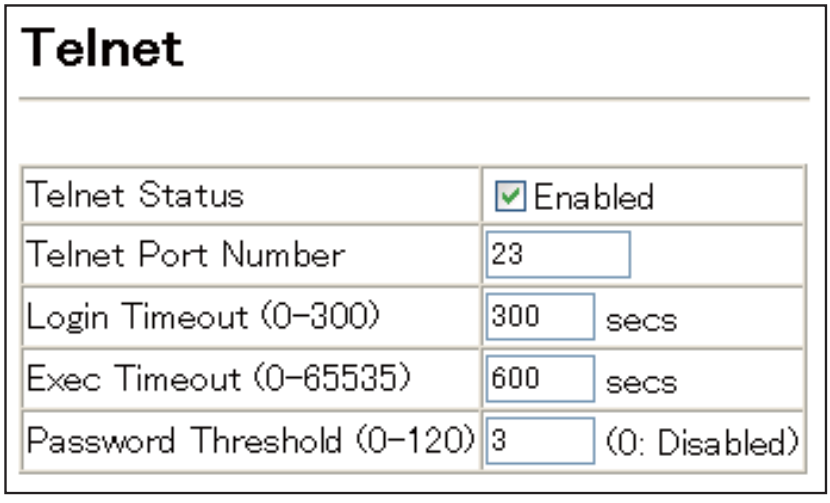
（範囲：0-120 回、初期設定：3 回）

Quiet Period

パスワード入力のリトライ数を超えた場合に、管理インタフェースへのアクセスができなくなる時間（範囲：0-65535 秒、初期設定：30 秒）

設定方法

（1）[System] → [Telnet] をクリックします。
（2）必要な接続パラメータを指定します。
（3）＜ Apply ＞をクリックします。



3.3.10 Event Logging の設定

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

syslog の設定

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

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

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

設定・表示項目

System Log Status

デバッグ又はエラーメッセージのログ保存の有効 / 無効（初期設定：有効）

Flash Level

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

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

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

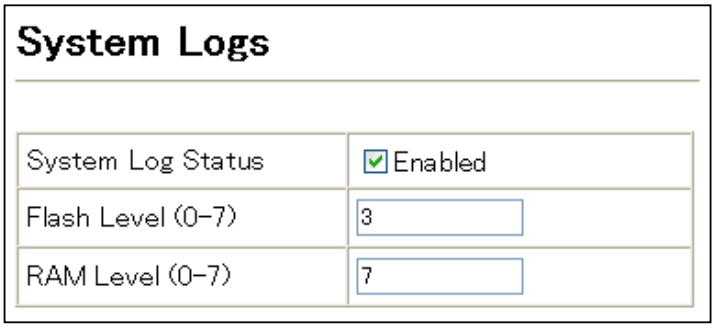
RAM Level

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フラッシュメモリに保存されます（範囲：0-7、初期設定：6）

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

設定方法

[System] → [Log] → [System Logs] をクリックします。"System Log Status" 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 Facility

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

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

Logging Trap

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

Host IP List

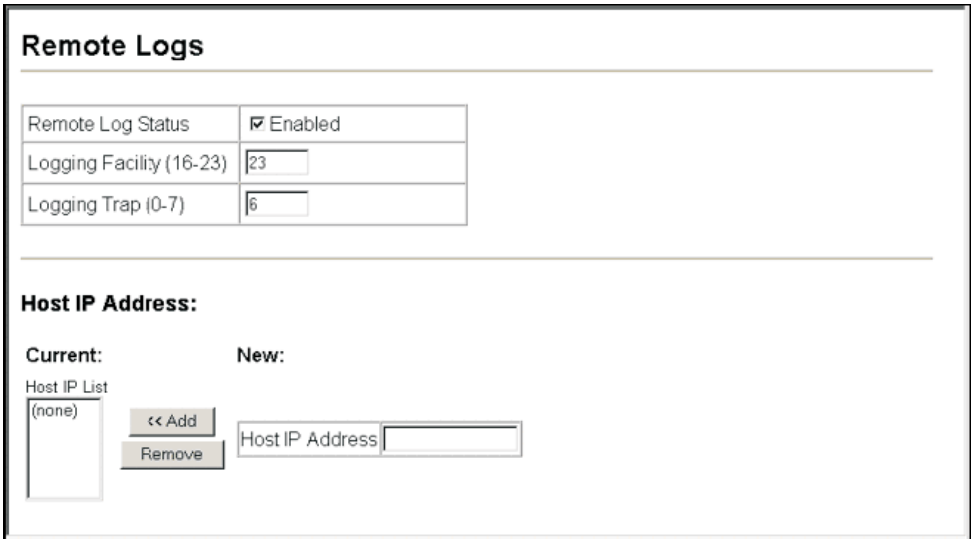
syslog メッセージを受け取るリモート syslog サーバの IP アドレスのリストを表示します。Host IP アドレスの上限は 5 つです。

Host IP Address

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

設定方法

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

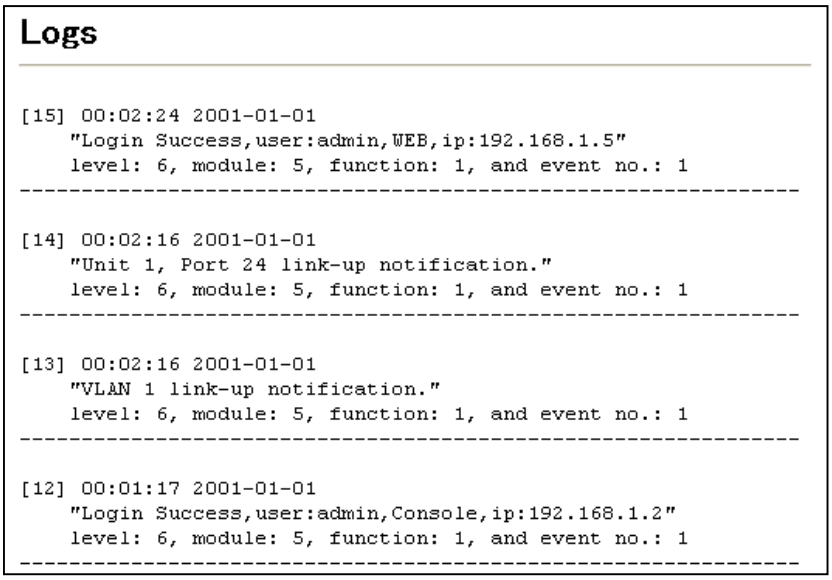


ログメッセージの表示

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

設定方法

[System] → [Log] → [Logs] をクリックします。



SMTP（Simple Transfer Protocol）

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

設定・表示項目

Admin Status

SMTP 機能の有効 / 無効（初期設定：有効）

Email Source Address

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

Severity

アラートメッセージのしきい値。指定したレベルより上のレベルのイベント発生時には、設定したメール受信者あてに送信されます。例えば "7" を指定すると、0-7 のレベルのメッセージがすべて通知されます。レベルについては P33 を参照してください。

SMTP Server List

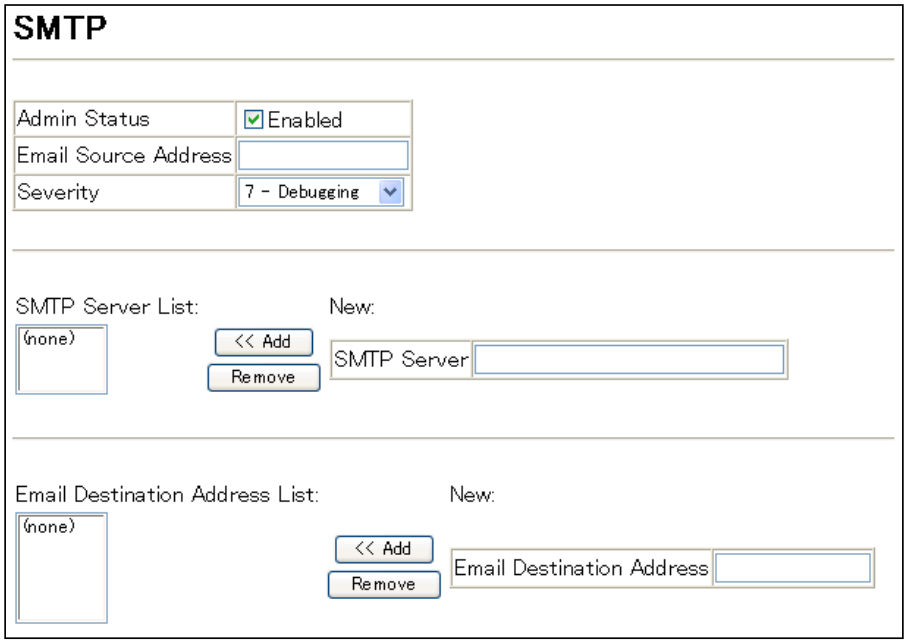
本機からのアラートメッセージを受信する SMTP サーバを指定できます。

Email Destination Address Liet

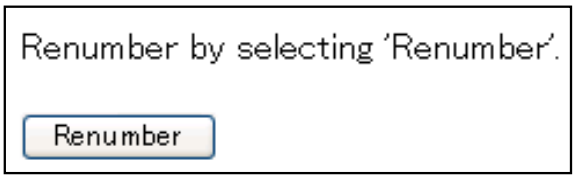
アラートメッセージを受信するアドレス。

設定方法

[System] → [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。



3.3.11 Renumbering the Stack



3.3.12 再起動

設定方法

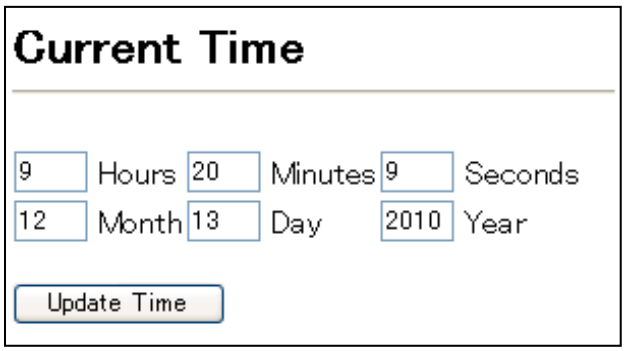
[System] → [Reset] をクリックします。[Reset] ボタンを押して、本機の再起動を行います。再起動の確認を促すプロンプトが表示されたら、確認して実行します。

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

3.3.13　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 P4-61「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。

現在の時刻を設定



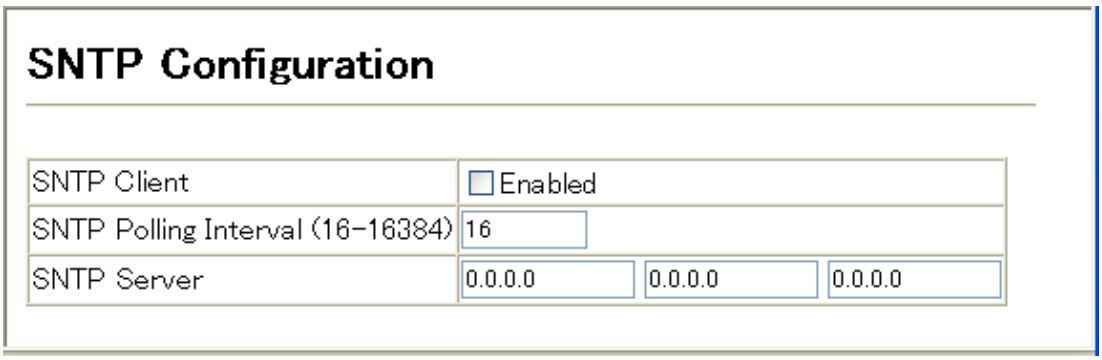
SNTP 設定

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。

[注意]　SNTP 設定は CLI からのみ可能です。設定方法については P38「システムクロック設定」を参照ください。

設定方法

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


SNTP Configuration
SNTP Client
Enabled
SNTP Polling Interval (16-16384)
16
SNTP Server
0.0.0.0
0.0.0.0
0.0.0.0

タイムゾーンの設定

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

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

設定・表示項目

Current Time

現在時刻の表示

Name

タイムゾーンに対する名称を設定します。（設定範囲：1-29 文字）

Hours (0-12)

UTC からの時間の差を設定します。

Minutes (0-59)

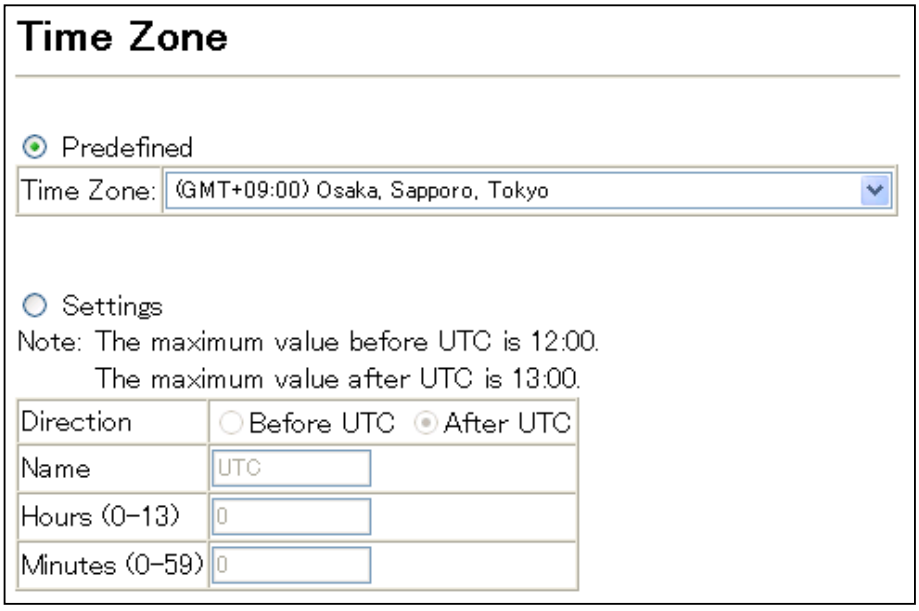
UTC からの時間（分数）の差を設定します。

Direction

UTC からのタイムゾーンの差がプラスかマイナスかを設定します。

設定方法

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

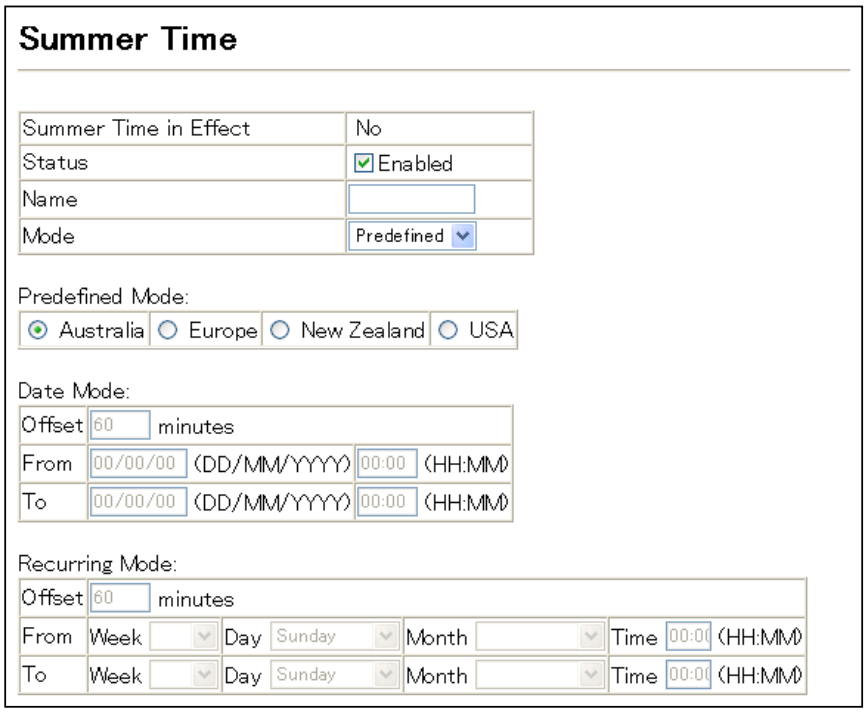


サマータイムの設定

設定・表示項目

設定方法

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



3.4 SNMP

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

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

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

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

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

SNMPv3 セキュリティモデルとレベル

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

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

3.4.1 SNMP エージェントを有効にする

SNMPv3 サービスを有効にします

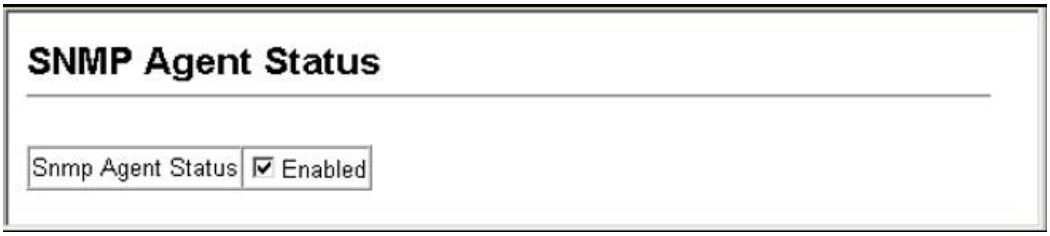
設定・表示項目

SNMP Agent Status

チェックを入れることで、SNMP エージェントが有効になります

設定方法

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



3.4.2 コミュニティ名の設定

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

セキュリティのため、初期設定のコミュニティ名を削除することを推奨します。

設定・表示項目

SNMP Community Capability

本機が最大 5 つのコミュニティ名をサポートしていることを表しています

Current

現在設定されているコミュニティ名のリスト

Community String

SNMP でのアクセスを行う際にパスワードの役割を果たすコミュニティ名

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

Access Mode

コミュニティ名へのアクセス権を設定します :

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

設定方法

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

3.4.3 トラップマネージャ・トラップタイプの指定

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

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

設定・表示項目

Trap Manager Capability

本機が最大 5 つのトラップマネージャをサポートしていることを表しています

Current

登録されているトラップマネージャのリスト

Trap Manager IP Address

トラップを受信するホストの IP アドレス

Trap Manager Community String

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

Trap UDP Port

トラプマネージャが使用する UDP ポートを指定します（初期設定：162）

Trap Version

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

Trap Security Level

トラップセキュリティレベルを指定します

Enable Authentication Traps

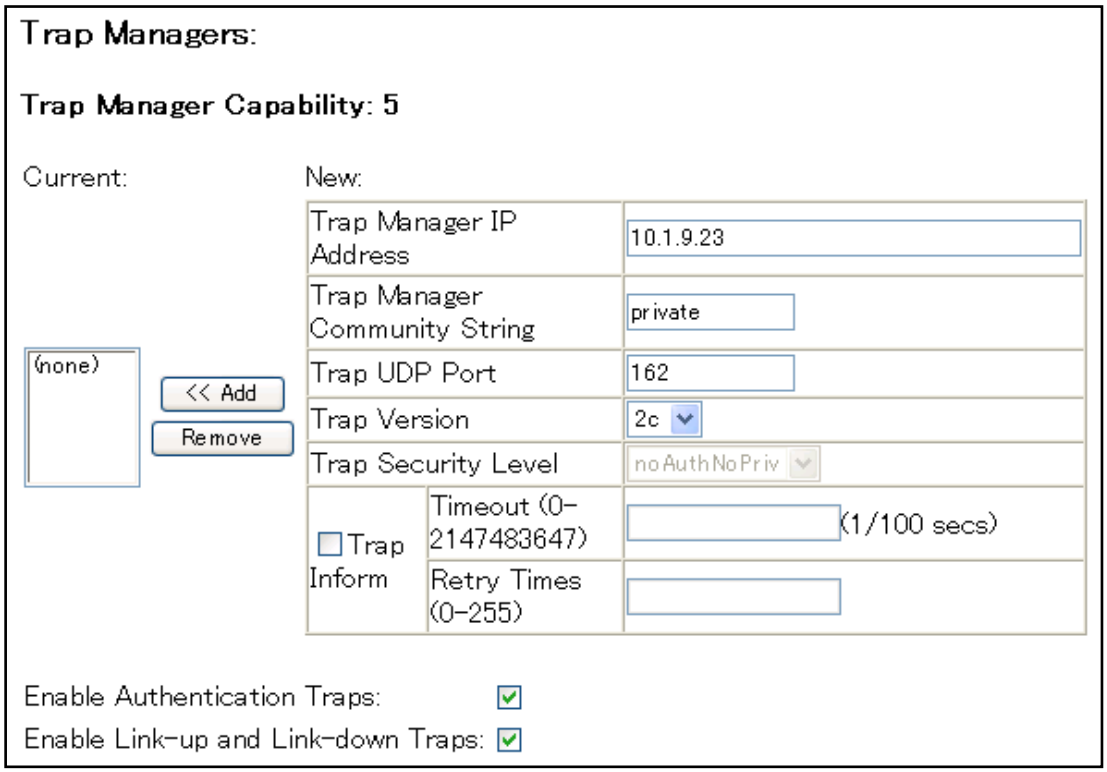
認証時に不正なパスワードが送信された場合にトラップが発行されます
（初期設定：有効）

Enable Link-up and Link-down Traps

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

設定方法

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



3.4.4 SNMPv3 マネージメントアクセスの設定

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

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

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

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

(7) ユーザーを作成し、所属するグループを決定します。

ローカルエンジン ID の設定

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

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

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

エンジン ID は、1 から 26 文字の 16 進数を指定できます。もし 26 文字以下を入力した場合、後に 0 が加えられます。例えば、”1234” は、”1234” の後に 22 個の 0 が追加された値と等しくなります。

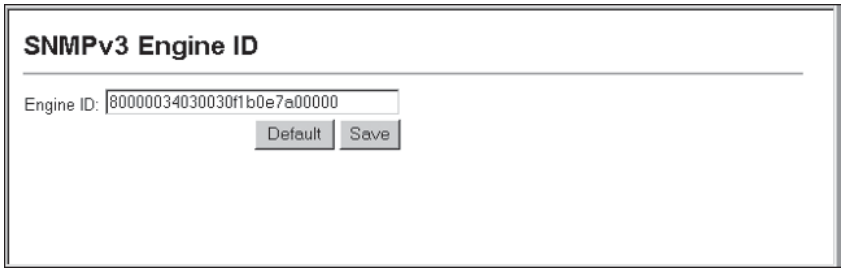
設定・表示項目

Engine ID

エンジン ID を設定します。

設定方法

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



リモートエンジン ID の設定

リモートデバイス上の SNMPv3 ユーザーへインフォームメッセージを送る場合、最初にリモートエンジン ID を設定します。リモートエンジン ID は、リモートホストで認証と暗号化パケットのセキュリティダイジェストを計算するために使用されます。
SNMP パスワードは、信頼できるエージェントのエンジン ID を使用してローカライズされます。インフォームの信頼できる SNMP エージェントはリモートエージェントです。そのため、プロキシリクエストまたはインフォームを送信する前にリモートエージェントの SNMP エンジン ID を設定する必要があります。（詳しくは P44 「トラップマネージャ・トラップタイプの指定」および P45 「SNMPv3 マネージメントアクセスの設定」を参照してください）
いエンジン ID は、1 から 26 文字の 16 進数を指定できます。もし 26 文字以下を入力した場合、後に 0 が加えられます。例えば、”1234” は、”1234” の後に 22 個の 0 が追加された値と等しくなります

設定・表示項目

Remote Engine ID

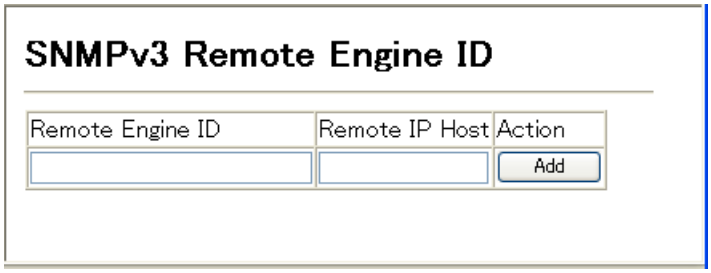
リモートエンジン ID を設定します。

Remote IP Host

リモートデバイスの IP アドレスを設定します。

設定方法

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



SNMPv3 ユーザーの設定

それぞれの SNMPv3 ユーザーは固有の名前を持ちます。

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

設定・表示項目

User Name

SNMPv3 ユーザー名（1-32 文字）

Group Name

既存のグループから選択または新規グループを作成します（1-32 文字）

Model

セキュリティモデルを選択します（v1,v2c,v3　初期設定：v1）

Level

セキュリティレベル

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

Authentication

認証用プロトコルの選択。MD5 または SHA（初期設定：MD5）

Authentication Password

認証用パスワード（最小 8 文字）

Privacy

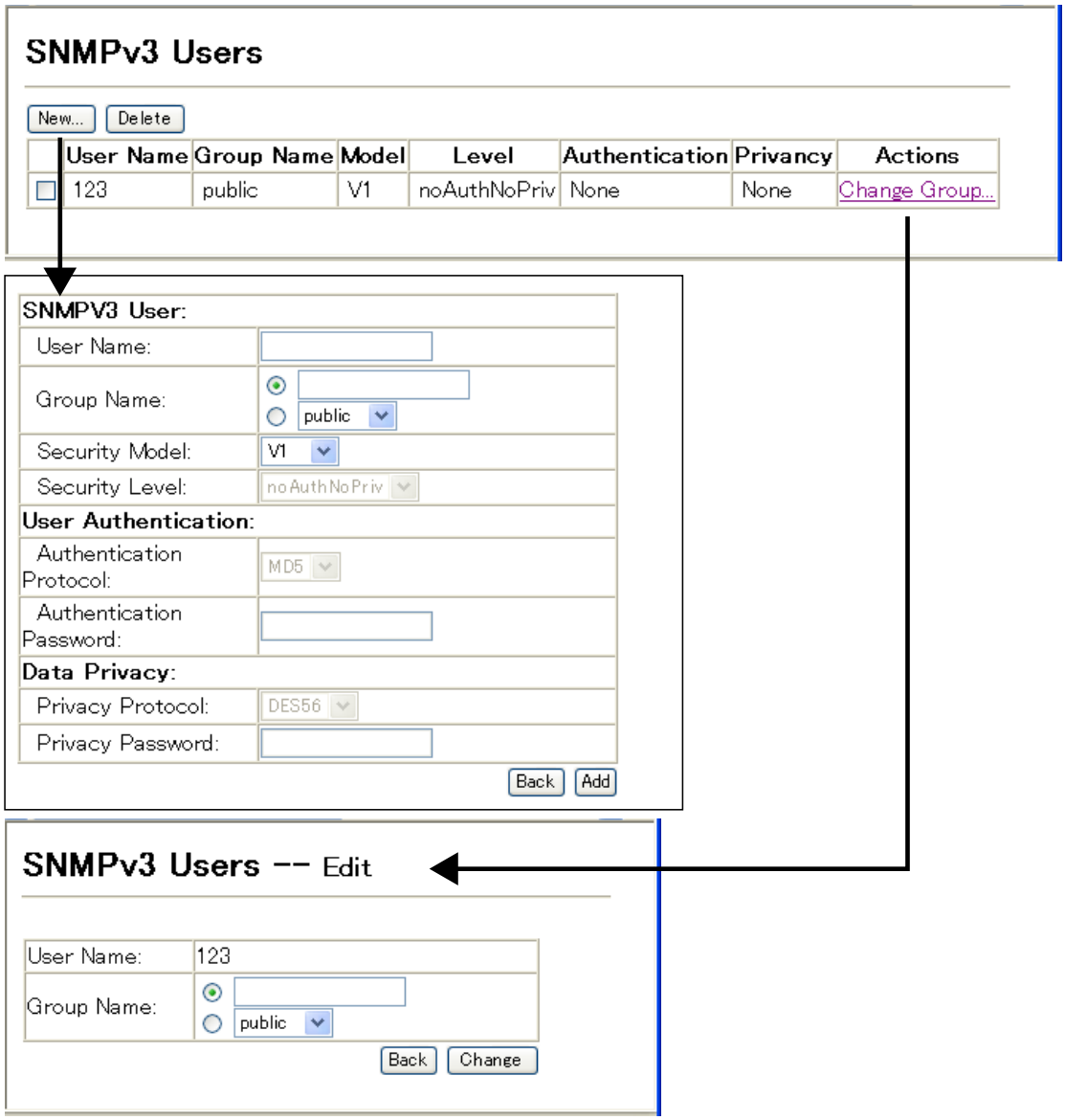
暗号化プロトコル。DES56bit のみ使用可

Actions

ユーザを別の SNMPv3 グループへアサインすることができます。

設定方法

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

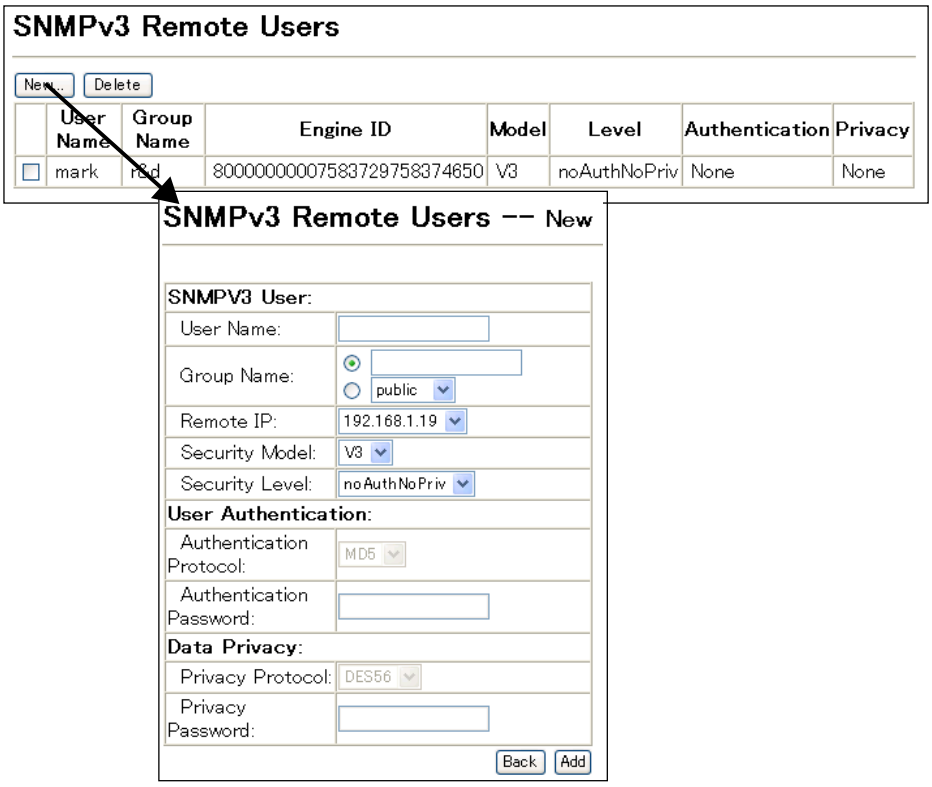


リモート SNMPv3 ユーザの設定

設定・表示項目

設定方法

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



SNMPv3 グループの設定

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

設定・表示項目

Group Name

グループ名（1-32 文字）

Model

セキュリティモデル（1,v2c,v3）

Lebel

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

Read View

Read **アクセスのビューを設定します**

Write View

Wite **アクセスのビューを設定します**

Notify View

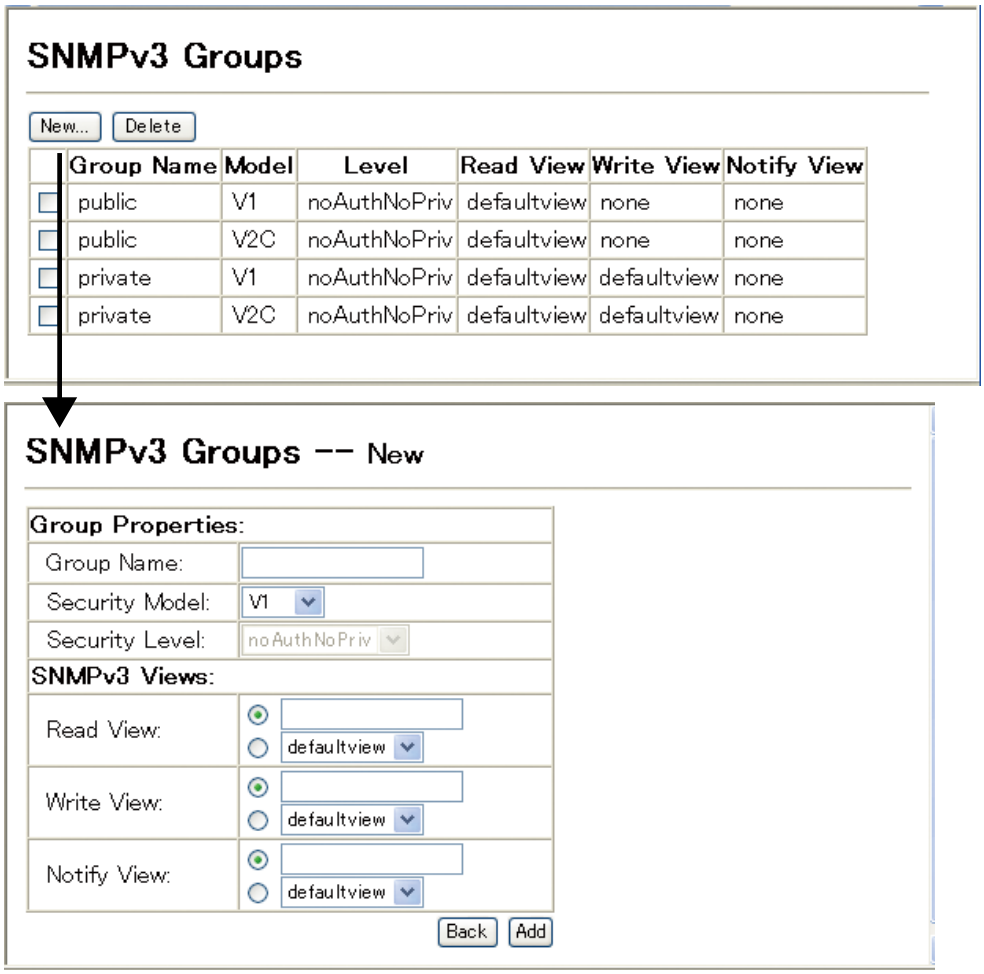
通知ビューを設定します。下表にてサポートする通知メッセージを示します。

表 3-1

Object Label	**Object ID**
RFC1493Traps	
newRoot	1.3.6.1.2.1.17.0.1
topologyChange	1.3.6.1.2.1.17.0.2
SNMPv2 Traps	
coldStart	1.3.6.1.6.3.1.1.5.1
warmStart	1.3.6.1.6.3.1.1.5.2
linkDown	1.3.6.1.6.3.1.1.5.3
linkUp	1.3.6.1.6.3.1.1.5.4
authentication Failure	1.3.6.1.6.3.1.1.5.5
RMON Events(V2)	
risingAlarm	1.3.6.1.2.1.16.0.1
fallingAlarm	1.3.6.1.2.1.16.0.2
Private Traps	
swPowerStatus Change Trap	1.3.6.1.4.1.202.20.56.63.2.1.0.1
swIpFilter RejectTrap	1.3.6.1.4.1.202.20.56.63.2.1.0.40
pethPsePortOnOff Notification	1.3.6.1.4.1.202.20.56.63.2.1.0.43
pethPsePortPower MaintenanceStatus Notification	1.3.6.1.4.1.202.20.56.63.2.1.0.44
pethMainPower Usage OnNotification	1.3.6.1.4.1.202.20.56.63.2.1.0.45
pethMainPower Usage OffNotification	1.3.6.1.4.1.202.20.56.63.2.1.0.46

設定方法

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



SNMPv3 ビューの設定

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

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

設定・表示項目

View Name

SNMP ビュー名（1-64 文字）

View OID Subtrees

ビューの内容が表示されます

Edit OID Subtrees

既存のビューの編集ができます

OID Subtrees

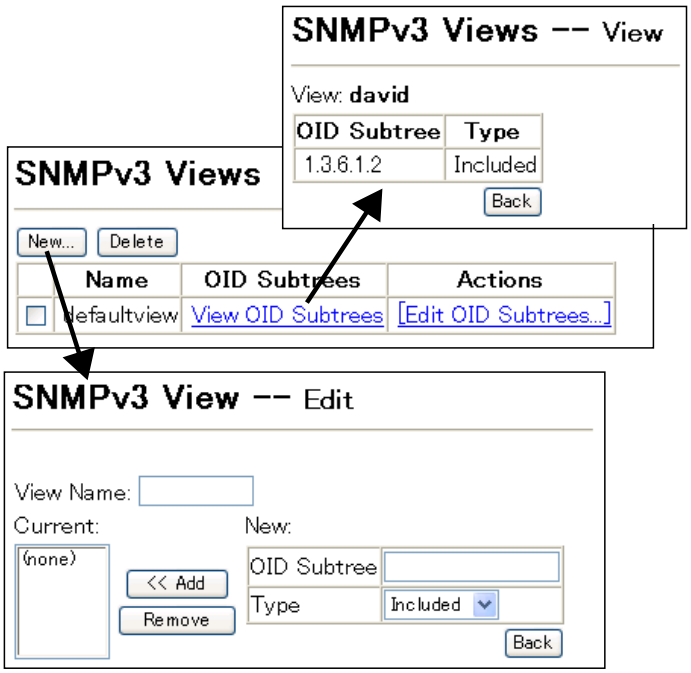
参照可能にする MIB ツリーの OID。ワイルドカードを使用してマスクを設定することも可能です

Type

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

設定方法

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



3.5 ユーザ認証

本機の管理アクセスへは以下の方法により制限を行えます。

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

3.5.1 ユーザアカウントの設定

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

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

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

ユーザ名は CLI を使用した場合のみ利用、変更可能です。

設定・表示項目

Accout List

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

New Account

新たに追加するユーザアカウント情報

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

Change Password

既存ユーザアカウントのパスワードを変更します。

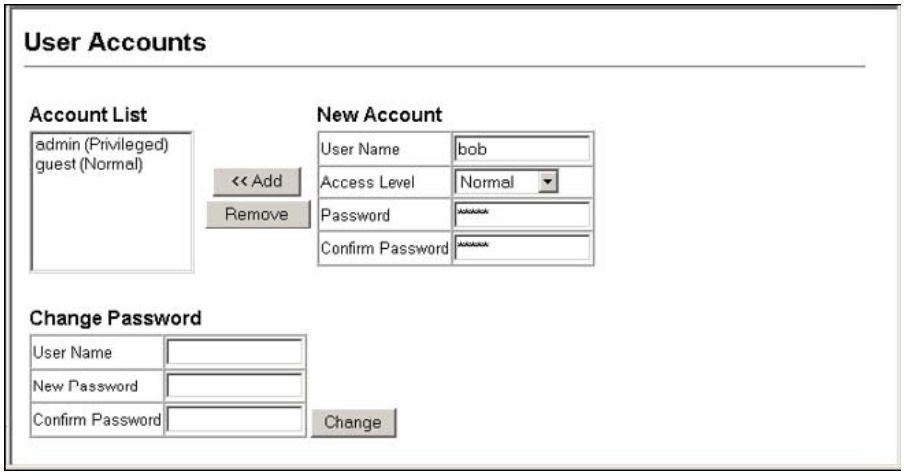
Add/Remove

ユーザアカウントのリストへの追加、又はリストからの削除を行います。

設定方法

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

す。既存ユーザアカウントのパスワードを変更する場合は、[Change Password] 欄にユーザ名 (User Name) 及び新たなパスワード (New Password) を入力し、再確認のためにパスワード (Confirm Password) を再度入力して [Change] をクリックします。

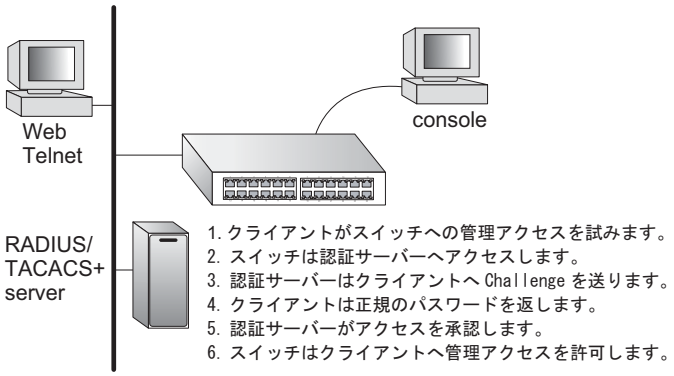


3.5.2 ローカル / リモート認証ログオン設定

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

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

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



機能解説

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

設定・表示項目

Authentication

認証方式を選択します。

- **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 Port Number

RADIUS サーバで使用される UDP ポート番号（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）

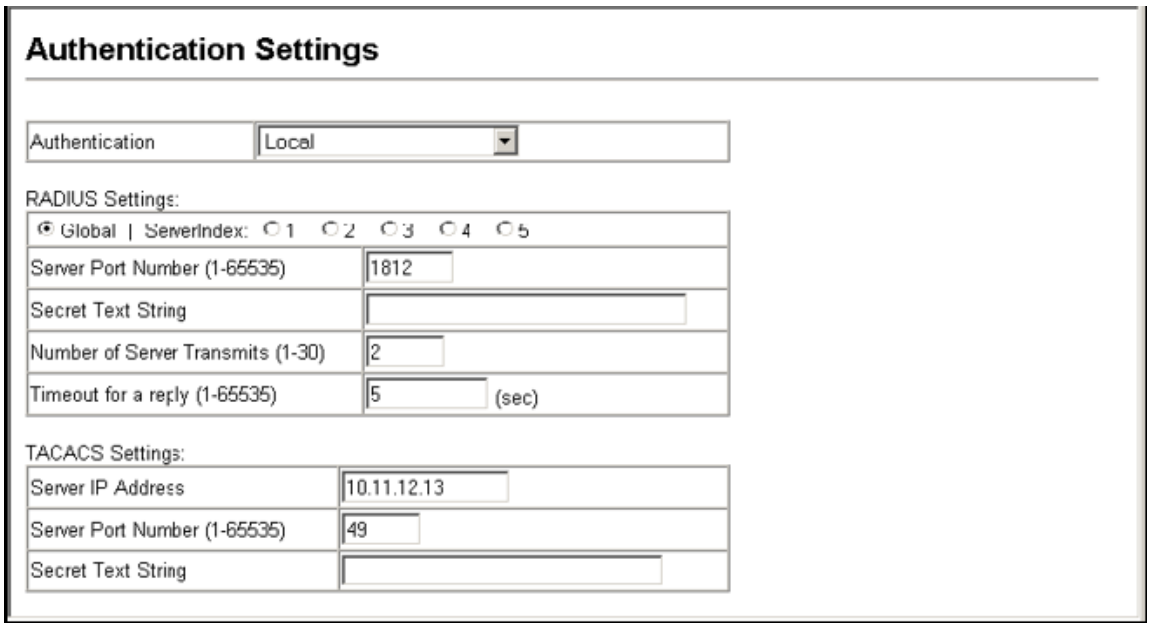
Secret Text String

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。



3.5.3 HTTPS 設定

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

機能解説

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

表 3-1

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

? 安全なサイトの証明を指定するためには、P59 「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

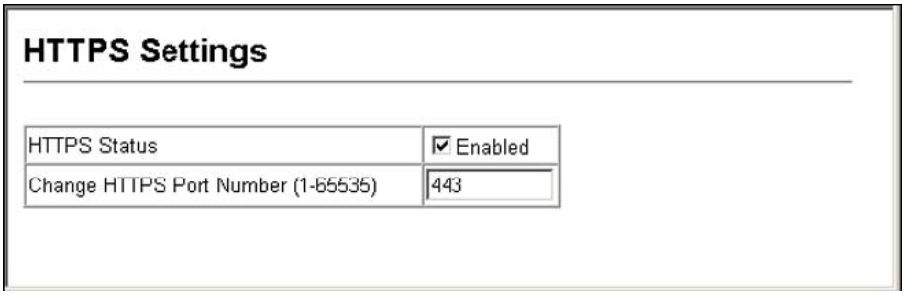
HTTPS サーバ機能を有効または無効に設定します（初期設定 : 有効 (Enabled)）

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。

表 3-1

```
Console#copy tftp https-certificate 3-21
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

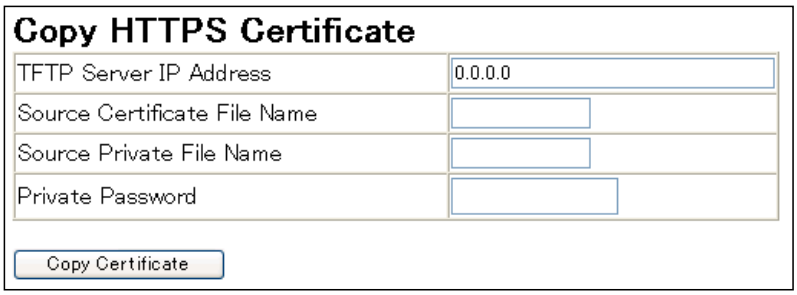
[注意] 証明書の変更を行った後に本機の再起動を行わないと、新しい証明書は有効になりません。再起動は CLI を使用し以下の手順で行います。

表 3-1

```
Console#reload
```

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。



3.5.4 Secure Shell 設定

Secure Shell (SSH) は、それ以前からあったバークレーリモートアクセスツールのセキュリティ面を確保した代替としてサーバ / クライアントアプリケーションを含んでいます。また、SSH は Telnet に代わる本機へのセキュアなリモート管理アクセスを提供します。

クライアントが SSH プロトコルによって本機と接続する場合、本機はアクセス認証のためにローカルのユーザ名およびパスワードと共にクライアントが使用する公開暗号キーを生成します。さらに、SSH では本機と SSH を利用する管理端末の間の通信をすべて暗号化し、ネットワーク上のデータの保護を行ないます。

[注意]　SSH 経由での管理アクセスを行なうためには、クライアントに SSH クライアントをインストールする必要があります。

[注意]　本機では SSH Version1.5 と 2.0 をサポートしています。

機能解説

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

公開暗号キー又はパスワード認証のどちらかを使用するに関わらず、本機上の認証キー（SSH ホストキー）を生成し、SSH サーバを有効にする必要があります。

SSH サーバを使用するには以下の手順で設定を行ないます。

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

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

```
10.1.0.54 1024 35
156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761171
```

(3) **クライアント公開キーの本機への取り込み** — P4-91「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。クライアントへはこれらのキーを使用し、認証が行なわれます。現在のファームウェアでは以下のような UNIX 標準フォーマットのファイルのみ受け入れることが可能です。

```
1024 35134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643    steve@192.168.1.19
```

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

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

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

以下のような手順で認証プロセスが行なわれます。

a. クライアントが公開キーを本機に送ります。

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

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

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

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

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

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

ホストキーペアの生成

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

設定・表示項目

Public-Key of Host-Key

ホストへのパブリックキー

- **RSA**: 最初のフィールドはホストキーのサイズ (1024) を表しています。2 番目のフィールドはエンコードされたパブリック指数 (65537)、最後の値はエンコードされた係数を表しています。
- **DSA**: 最初のフィールドはデジタル署名標準(DSS)に基づく SSHによって私用される暗号化方法を表示します。最後の値はエンコードされた係数を表します。

Host-Key Type

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

Save Host-Key from Memory to Flash

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

Generate

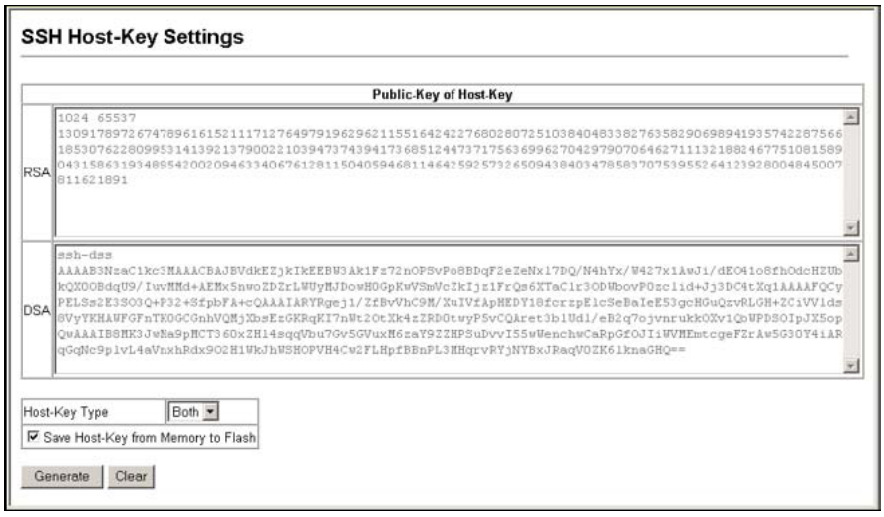
ホストキーペアを生成します。SSH サーバ設定ページで SSH サーバを有効にする前に、ホストキーペアを生成する必要があります。

Clear

RAM 及びフラッシュメモリの両方に保存されているホストキーを削除します。

設定方法

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

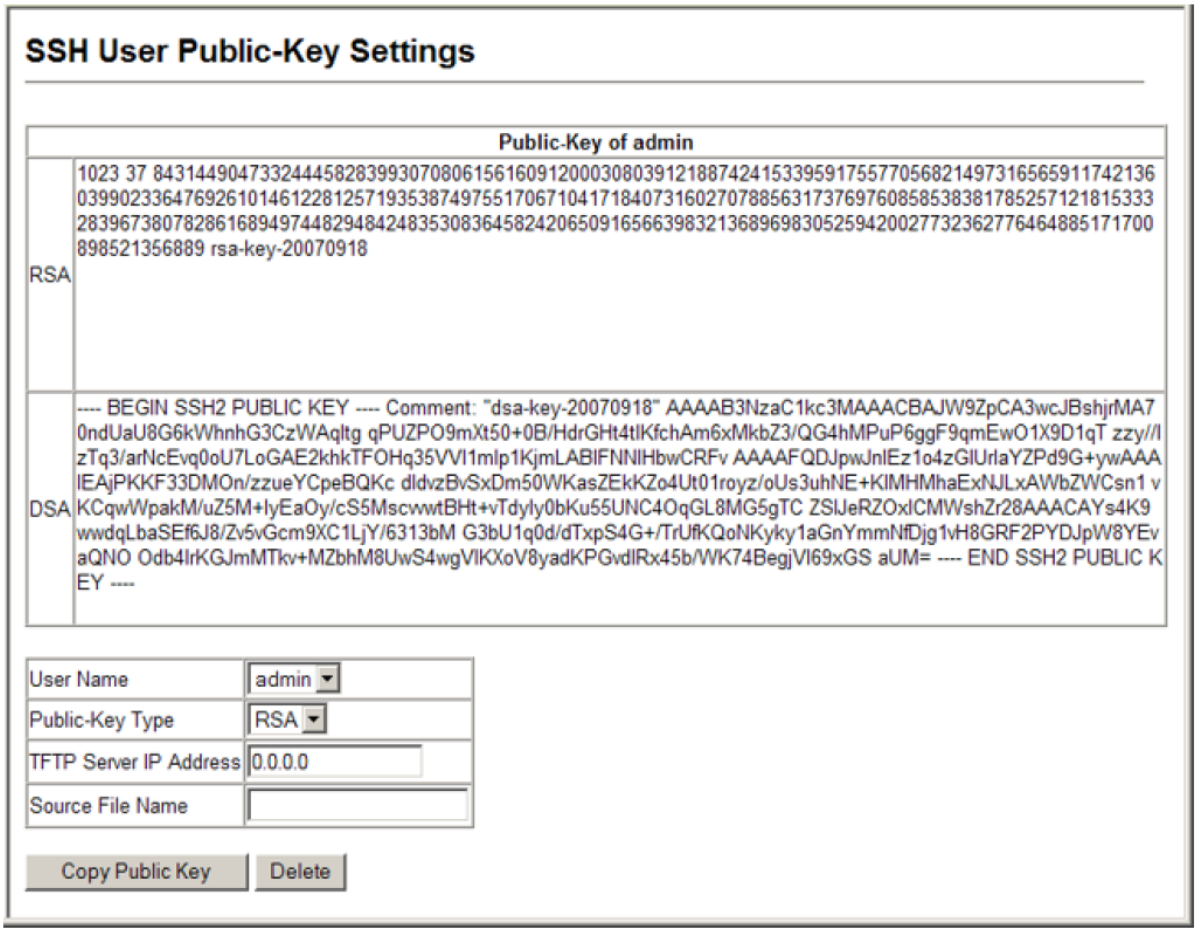


ユーザパブリックキーのインポート

設定・表示項目

設定方法

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



SSH サーバ設定

認証用の SSH サーバの設定

設定・表示項目

SSH Server Status

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

Version

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

SSH authentication timeout

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

SSH authentication Retries

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

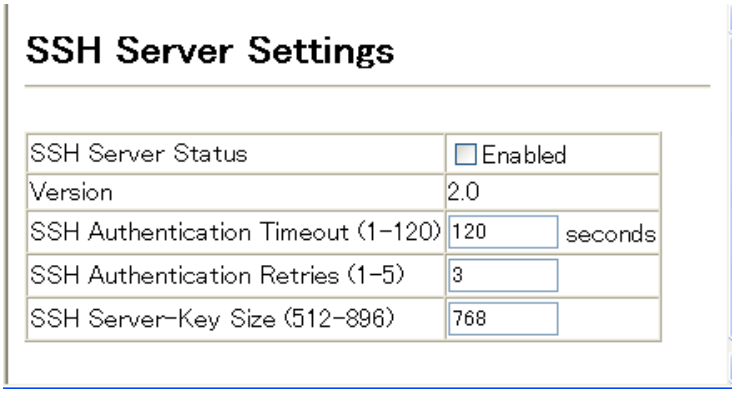
SSH Server-Key Size

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

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

設定方法

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



3.5.5 ポートセキュリティの設定

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

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

ポートセキュリティを使用する場合、ポートに許可する MAC アドレスの最大数を設定し、動的に < ソース MAC アドレス、VLAN> のペアをポートで受信したフレームから学習します。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、P84 「ポート設定」からポートの有効化を行なってください。

設定・表示項目

Port

ポート番号

Name

ポート説明

Action

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

Security Status

ポートセキュリティの有効 / 無効

初期設定：無効 (Disabled)

Max MAC Count

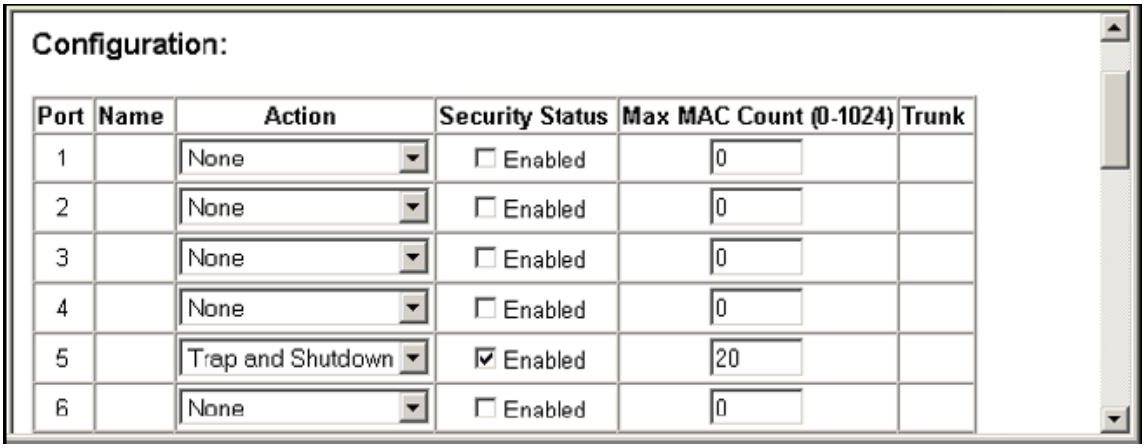
ポートが学習可能な MAC **アドレス数（設定範囲：**0-20**、**0 **は学習の無効）**

Trunk

ポートがトランクされている場合のトランク番号

設定方法

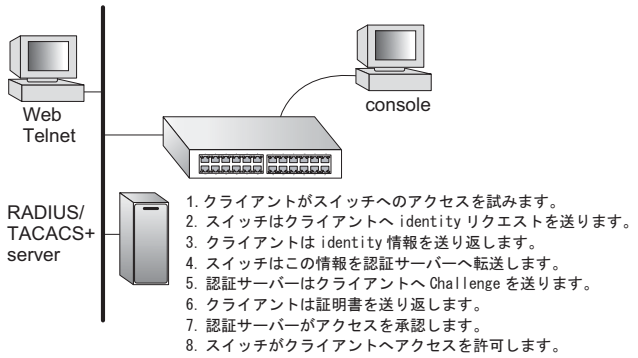
[Security] → [Port Security] **をクリックします。ポートのセキュリティを有効にするには、設定を行うポート番号の** Action **を選択し、**Security Status **チェックボックスをオンにし、最大** MAC **アドレス数を設定し、**[Apply] **をクリックします。**



3.5.6 802.1x ポート認証

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

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



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

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

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

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

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

クライアントは、パスワードや証明書などと共に、適切な方法により応答します。

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

IEEE802.1x 認証を使用するには本機に以下の設定を行います。

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

802.1x グローバルセッティングの表示

802.1X プロトコルはクライアントの認証を可能にします。

設定・表示項目

802.1X System Authentication Control

スイッチに対する 802.1X の設定

設定方法

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

802.1x グローバルセッティング

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

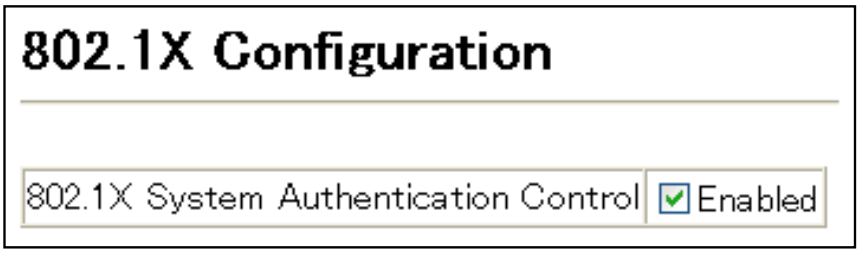
設定・表示項目

802.1X System Authentication Control

802.1X の設定（初期設定：無効）

設定方法

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



802.1X 認証ポート設定

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

設定・表示項目

Port

ポート番号

Status

ポートの認証の有効 / 無効

Operation Mode

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

Max Count

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

Mode

認証モードを以下のオプションの中から設定します。

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

Re-authen

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

Max-Req

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

Quiet Period

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

Re-authen Period

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

TX Period

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

Authorized

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

Supplicant

接続されたクライアントの MAC アドレス

Trunk

トランク設定がされている場合に表示

設定方法

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

802.1X Port Configuration

Port	Status	Operation Mode	Max Count (1-1024)	Mode	Re-authen	Max-Req	Quiet/ Period	Re-authen/ Period	Tx Period	Supplicant Timeout
1	Disabled	Single-Host	5	Force-Authorized	Enabled	2	60	3600	30	30
2	Disabled	Single-Host	5	Force-Authorized	Enabled	2	60	3600	30	30
3	Disabled	Single-Host	5	Force-Authorized	Enabled	2	60	3600	30	30
4	Disabled	Single-Host	5	Force-Authorized	Enabled	2	60	3600	30	30
5	Disabled	Single-Host	5	Force-Authorized	Enabled	2	60	3600	30	30

IEEE802.1x 統計情報の表示

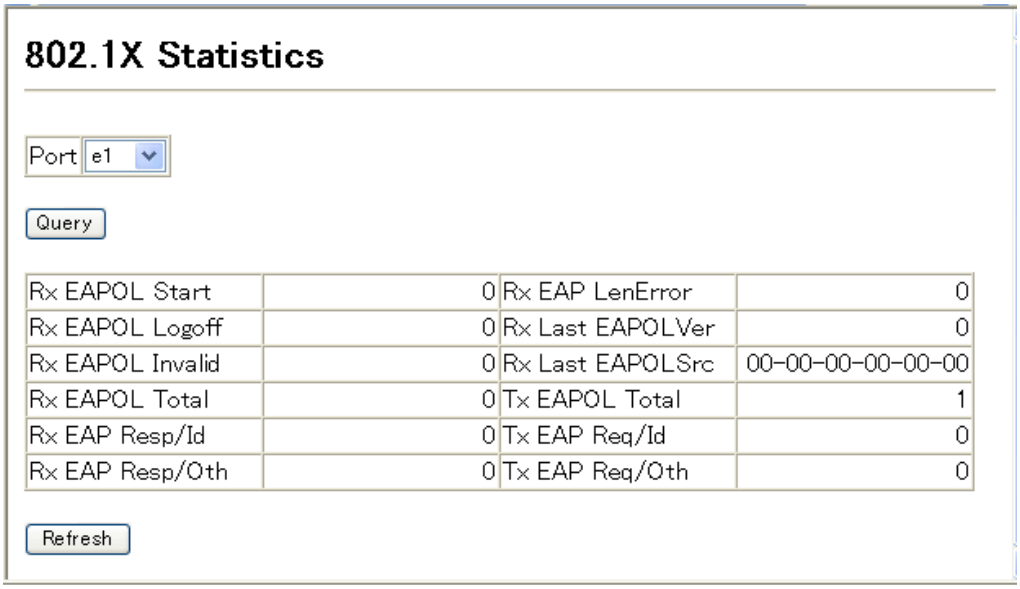
dot1x プロトコルの各ポートの統計情報を表示します。

機能解説

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

設定方法

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



3.5.7 管理アクセスの IP 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

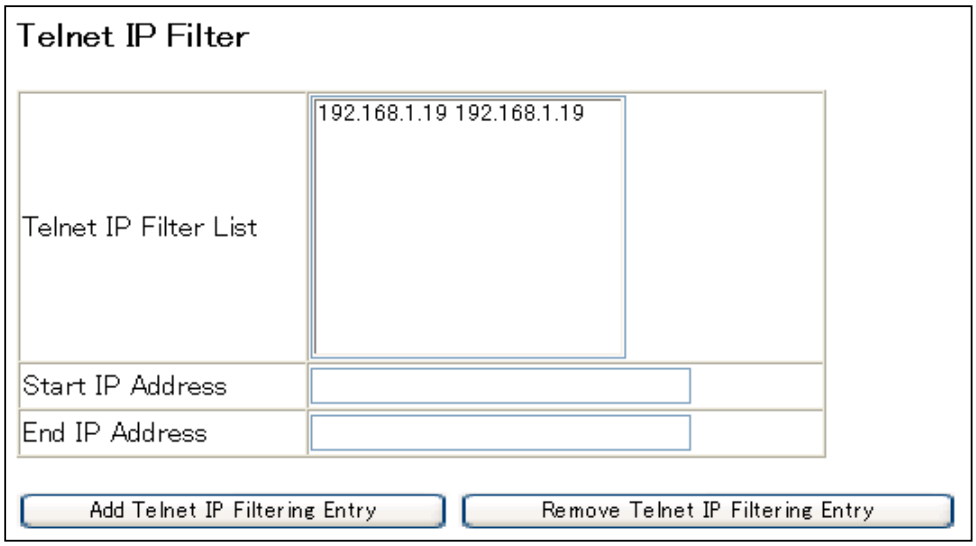
IP アドレスを範囲で指定している場合の最後の IP アドレス

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



3.6 ACL （Access Control Lists）

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

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

3.6.1 ACL の設定

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

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

機能解説

ACL は以下の制限があります。

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

有効な ACL は以下の順番で実行されます。

（1）出力ポートの出力 IP ACL のユーザに定義されたルール

（2）入力ポートの入力 IP ACL のユーザに定義されたルール

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

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

ACL 名およびタイプの設定

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

設定・表示項目

Name

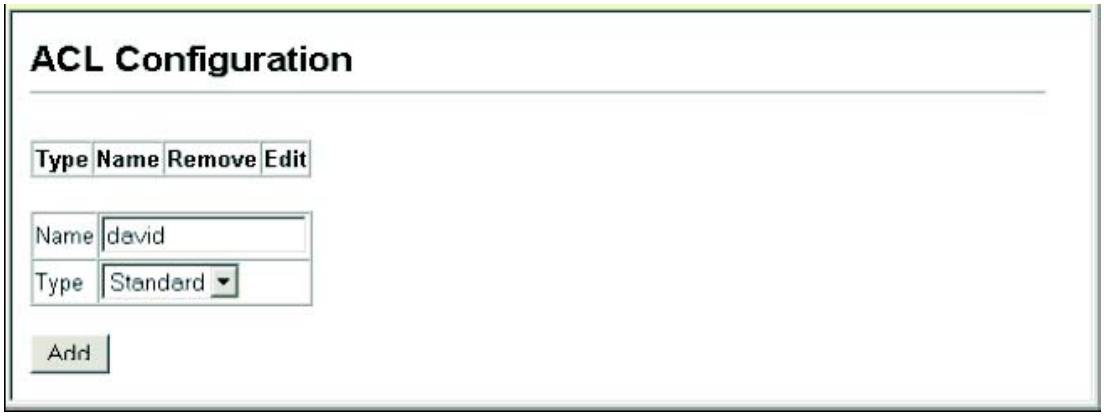
ACL 名（4 文字以上 15 文字以内）

Type

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

設定方法

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



Standard IP ACL の設定

設定・表示項目

Action

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

Address Type

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

（オプション：Any, Host, IP、初期設定：Any）

IP Address

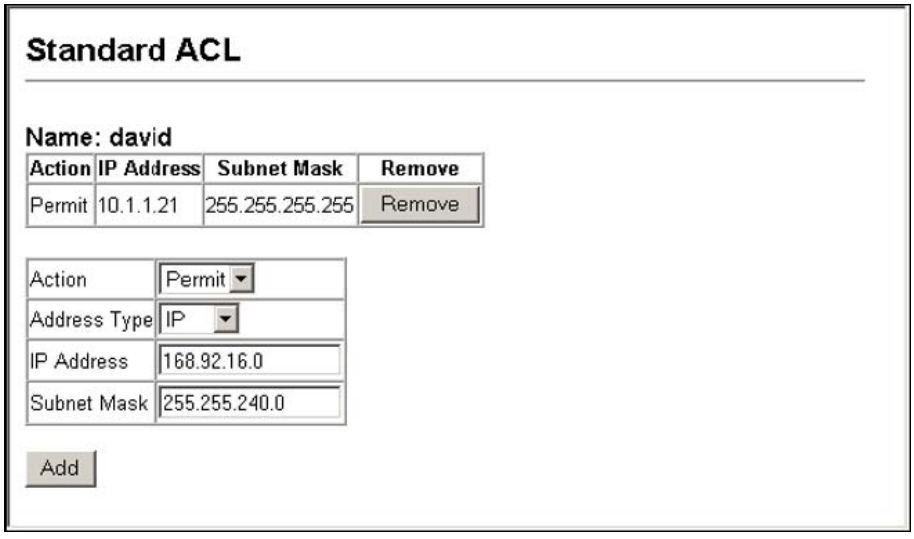
ソース IP アドレス

SubnetMask

サブネットマスク

設定方法

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



Extended IP ACL の設定

設定・表示項目

Action

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

Source/Destination Address Type

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

Source/Destination IP Address

ソース又はディスティネーション IP アドレス

Source/Destination Subnet Mask

ソース又はディスティネーション IP アドレスのサブネットマスク

Service Type

- **Precedence** — IP precedence レベル（範囲：0-7）
- **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 Bit Mask

一致するコードビットの値

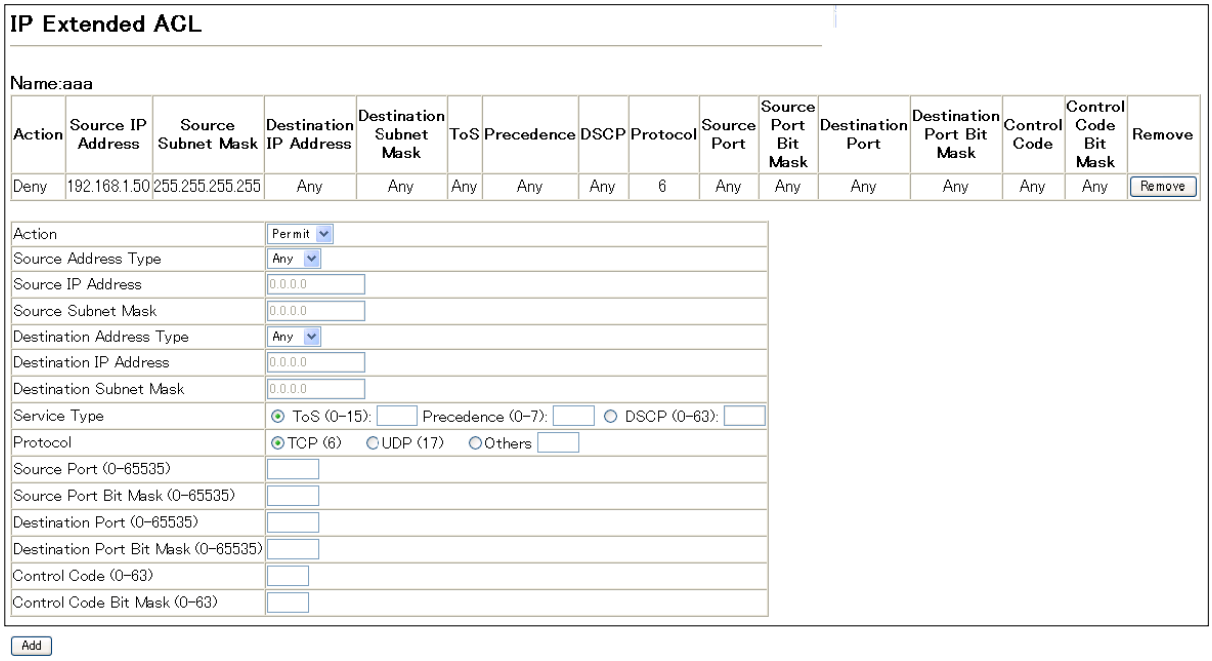
? コントロールビットマスクは、コントロールコードに使用される 10 進数の値です。10 進数の値を入力し、等価な 2 進数のビットが "1" の場合、一致するビットであり、"0" の場合、拒否するビットとなります。以下のビットが指定されます。

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

例えば、コード値及びコードマスクを利用し、パケットをつかむには以下のフラッグをセットします。
－有効な SYN flag — コントロールコード：2、コントロールビットマスク：2
－有効な SYN 及び ACK — コントロールコード：18、コントロールビットマスク：18
－有効な SYN 及び無効な ACK — コントロールコード：2、コントロールビットマスク：18

設定方法

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



MAC ACL の設定

設定・表示項目

Action

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

Source/Destination MAC

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

Source/Destination MAC Address

ソース又はディスティネーション MAC アドレス

Source/Destination MAC Bitmask

ソース又はディスティネーション MAC アドレスの 16 進数のマスク

VID

VLAN ID（範囲：1-4093）

VID Mask .

VLAN ビットマスク (範囲：1-4095)

Ethernet Type

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

Ethernet Type Mask

プロトコルビットマスク（範囲：600-fff hex）

Packet Format

本属性は次のパケット・タイプから選択できます。

- Any — **すべてのイーサネットパケットタイプ**
- Untagged-eth2 — **タグなしイーサネット** II **パケット**
- Untagged-802.3 — **タグなしイーサネット** IEEE802.3 **パケット**
- Tagged-eth2 — **タグ付イーサネット** II **パケット**
- Tagged-802.3 — **タグ付イーサネット** IEEE802.3 **パケット**

機能解説

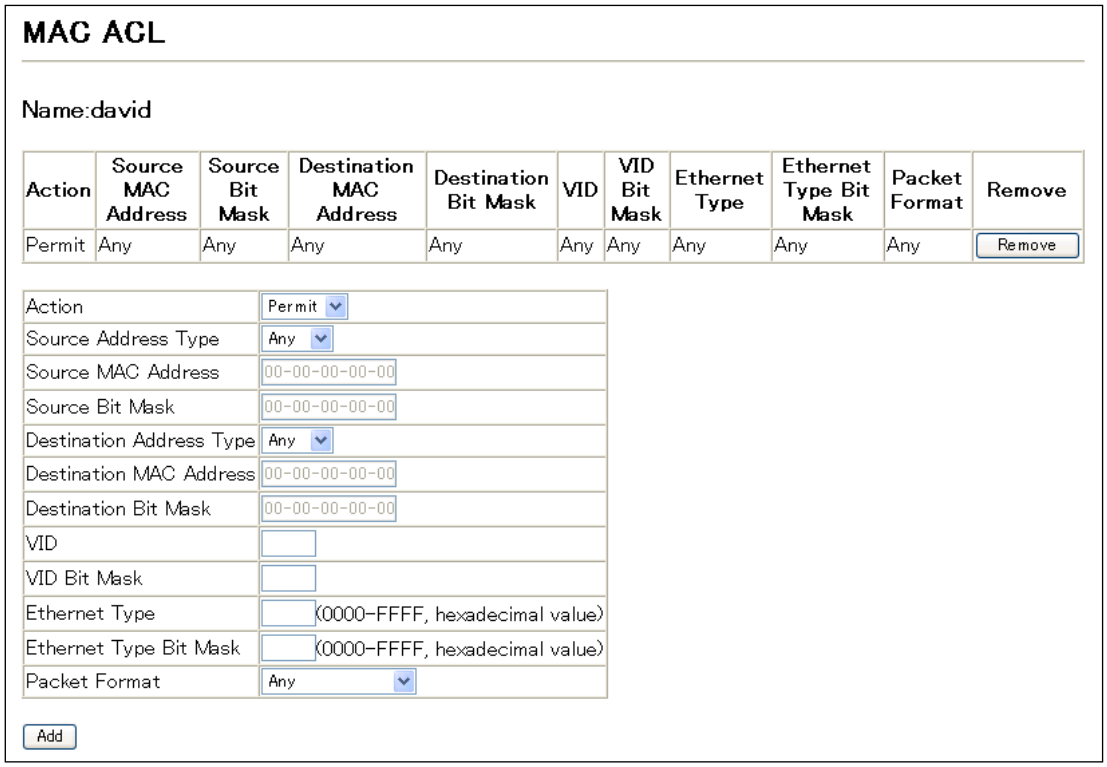
ACL **は以下の制限があります。**

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

設定方法

（permit/deny **の）動作を指定します。ソース及び** / **又はディスティネーションアドレスを指定し、アドレスタイプ** ((Any, Host, MAC) **を選択します。**"Host" **を選択した場合、特定のア**

ドレスを入力します。"MAC" を選択した場合、アドレス範囲を指定するためにベースアドレスとビットマスクを指定します。その他の必要項目を設定し、[Add] をクリックします。



3.6.2 ACL へのポートのバインド

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

機能解説

本機では ingress（入力）ACL をサポートします。

設定・表示項目

Port

ポート又は拡張モジュールスロット（範囲：1-12）

IP

ポートにバインドする IP ACL ルール

MAC

ポートにバインドする MAC ACL ルール

IN

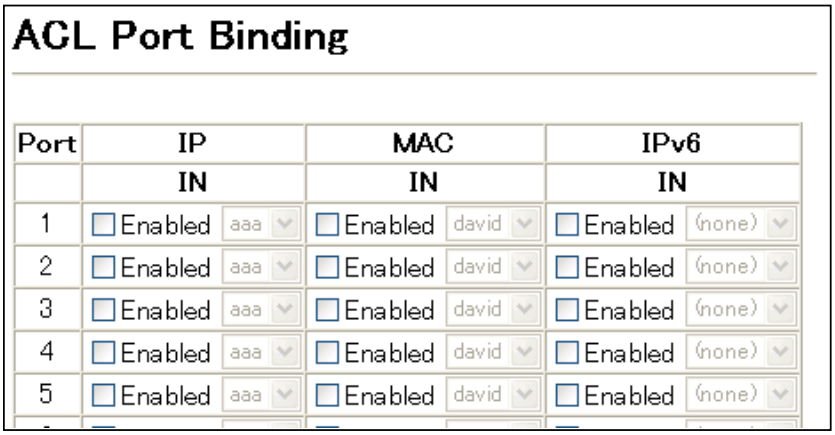
入力 (ingress) パケットに対する ACL

OUT

出力 (egress) パケットに対する ACL

設定方法

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



3.7 ポート設定

3.7.1 接続状況の表示

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

設定・表示項目

Name

インタフェースラベルの表示

Type

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

Admin Status

インタフェースの有効 / 無効の表示

Oper Status

リンクアップ / リンクダウンの表示

Speed/Duplex Status

通信速度及び通信方式の表示 (Auto, Fixed)

Flow Control Status

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

Autonegotiation

オートネゴシエーションの有効 / 無効の表示

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

メディアタイプ

Trunk Member

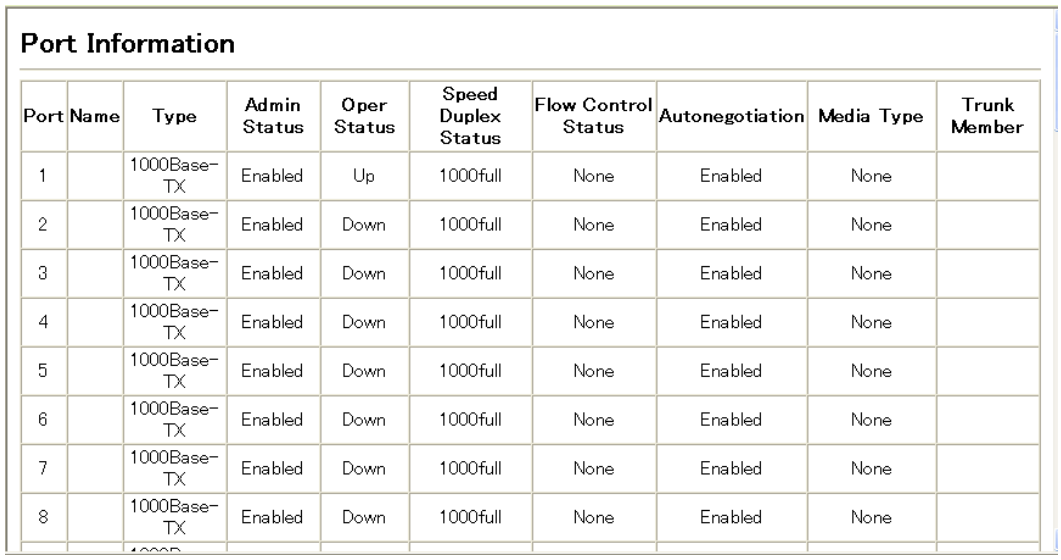
ポートのトランク状態の表示（Port Information **ページのみ**）

Creation

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

設定方法

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



Port Information

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

3.7.2 インタフェース接続の設定

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

設定・表示項目

Name

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

Admin

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

Speed/Duplex

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

Flow Control

フローコントロールを自動設定又は手動設定で行うことができます。

Autonegotiation(Port Capabilities)

オートネゴシエーションを有効又は無効にします。また、オートネゴシエーション時のポートの対応機能を通知する設定を行います。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 （コンボポートのみ）** — 1000 Mbps full-duplex で動作します。

Media Type

メディアタイプ（9-12 ポート）

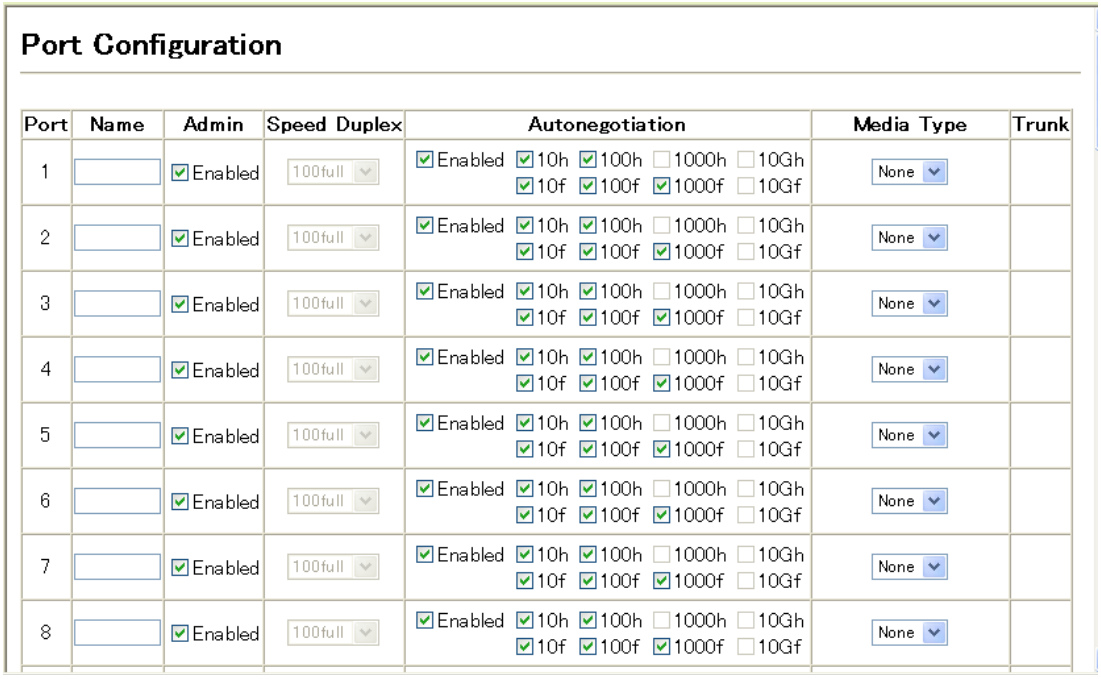
Trunk

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、P88 「トランクグループの設定」を参照して下さい。

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

設定方法

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



3.7.3 トランクグループの設定

ネットワーク接続におけるバンド幅の拡大によるボトルネックの解消や障害の回避のために複数のポートは束ねるトランク機能を利用することができます。最大 32 のトランクを同時に設定することができます。

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

機能解説

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

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

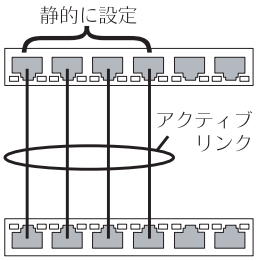
トランクの設定を行なう場合には以下の点に注意して下さい :

- ループを回避するため、スイッチ間のネットワークケーブルを接続する前にポートトランクの設定を行なって下さい。
- 1 トランク最大 8 ポート、最大 6 トランクを作成することができます。
- 両端のデバイスのポートをトランクポートとして設定する必要があります。
- 異なる機器同士で静的トランクを行なう場合には、Cisco EtherChannel と互換性がなければなりません。
- トランクの両端のポートは通信速度、通信方式、及びフロー制御の通信モード、VLAN 設定、及び CoS 設定等に関して同じ設定を行なう必要があります。
- トランクの全てのポートは VLAN の移動、追加及び削除を行なう際に 1 つのインタフェースとして設定する必要があります。
- STP、VLAN 及び IGMP の設定はトランク全体への設定のみが可能です。

静的トランクの設定

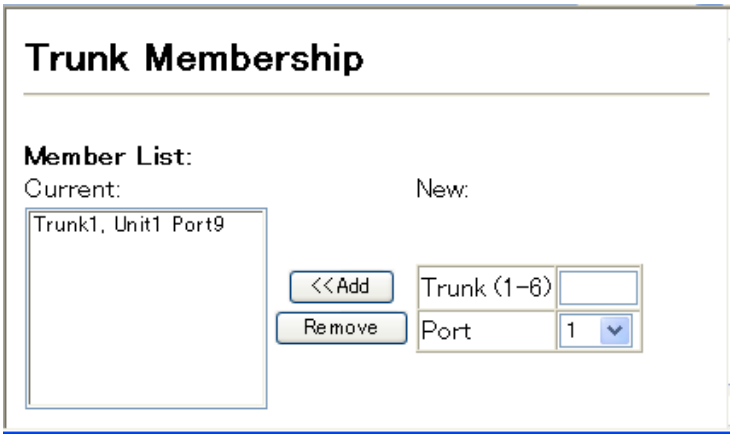
機能解説

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



設定方法

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



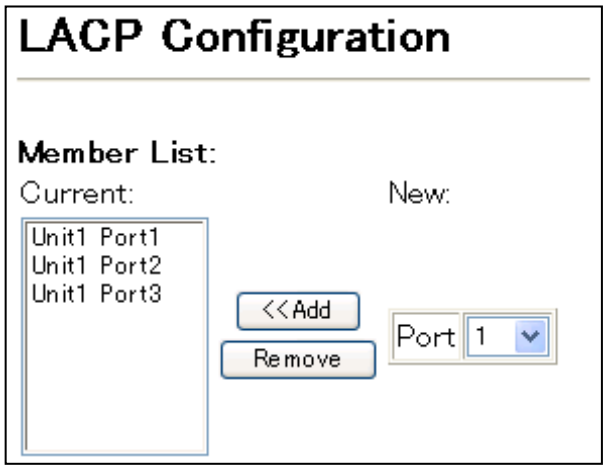
選択ポートで LACP を有効化

機能解説

- ネットワークのループを回避するため、ポート接続前に LACP を有効にし、LACP を無効にする前にポートの切断を行って下さい。
- 対向のスイッチのポートが LACP を有効に設定している場合、トランクは自動的にアクティブになります。
- LACP により対向のスイッチと構成されたトランクには、自動的に次の番号のトランク ID が割り当てられます。
- 8 つ以上のポートにより LACP トランクを有効にした場合、8 つのポート以外はスタンバイモードとなります。トランクしている 1 つのポートに障害が発生した場合には、スタンバイモードのポートの 1 つが自動的に障害ポートと置き換わります。
- LACP トランクの両端のポートは固定又はオートネゴシエーションにより full duplex に設定する必要があります。
- LACP により動的なトランクグループに設定されたトランク情報は、Member List 画面又は Trunk Membership 画面でも確認できます (P88)

設定方法

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



LACP パラメータ設定

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

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

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

設定・表示項目

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

Port

ポート番号（範囲：1-26/50**）**

System Priority

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

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

Admin Key

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

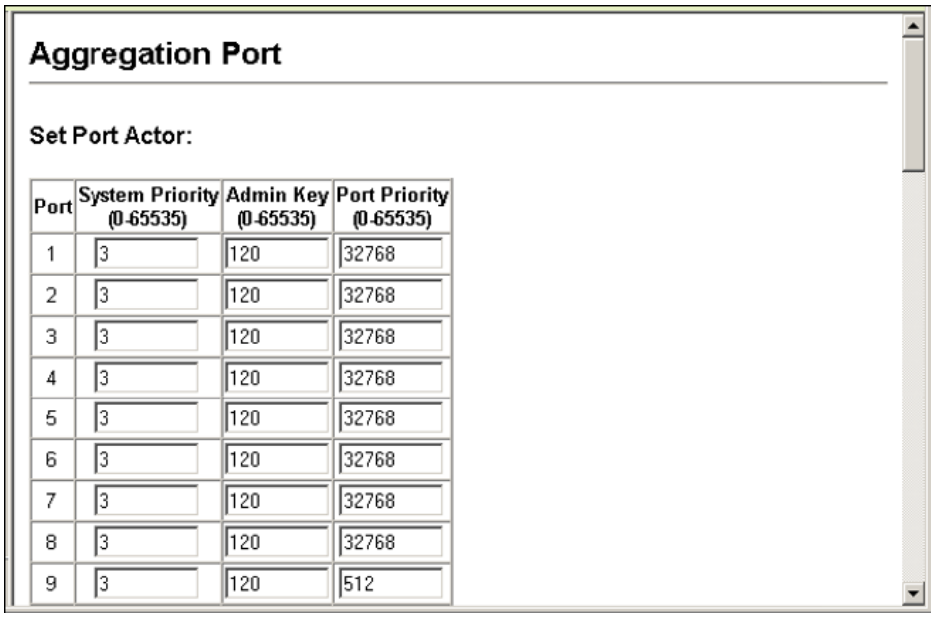
Port Priority

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

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

設定方法

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



LACP ポートカウンターの表示

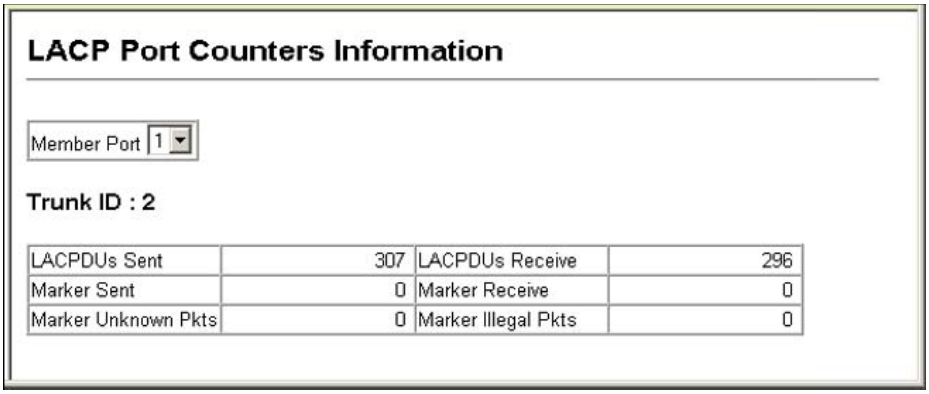
LACP プロトコルメッセージの統計情報の表示を行ないます。

カウンター情報

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

設定方法

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



ローカル側の LACP 設定及びステータスの表示

LACP のローカル側の設定及びステータスの表示を行なうことができます。

内部設定情報

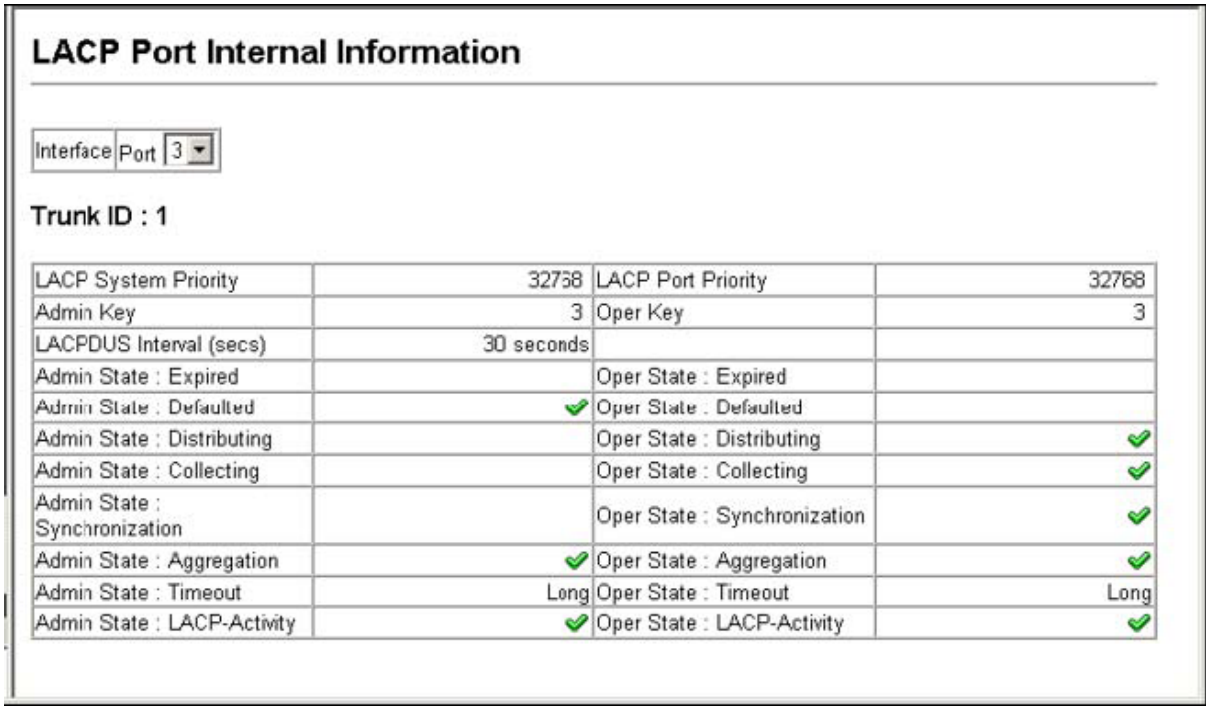
項目	解説
Oper Key	現在のアグリゲーションポートのキーの運用値
Admin Key	現在のアグリゲーションポートのキーの管理値
LACPDUs Internal	受信した LACPDU 情報を無効にするまでの秒数
LACP System Priority	本ポートチャンネルグループに割り当てられた LACP システムプライオリティ
LACP Port Priority	本ポートチャンネルグループに割り当てられた LACP ポートプライオリティ

内部設定情報

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	32738	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

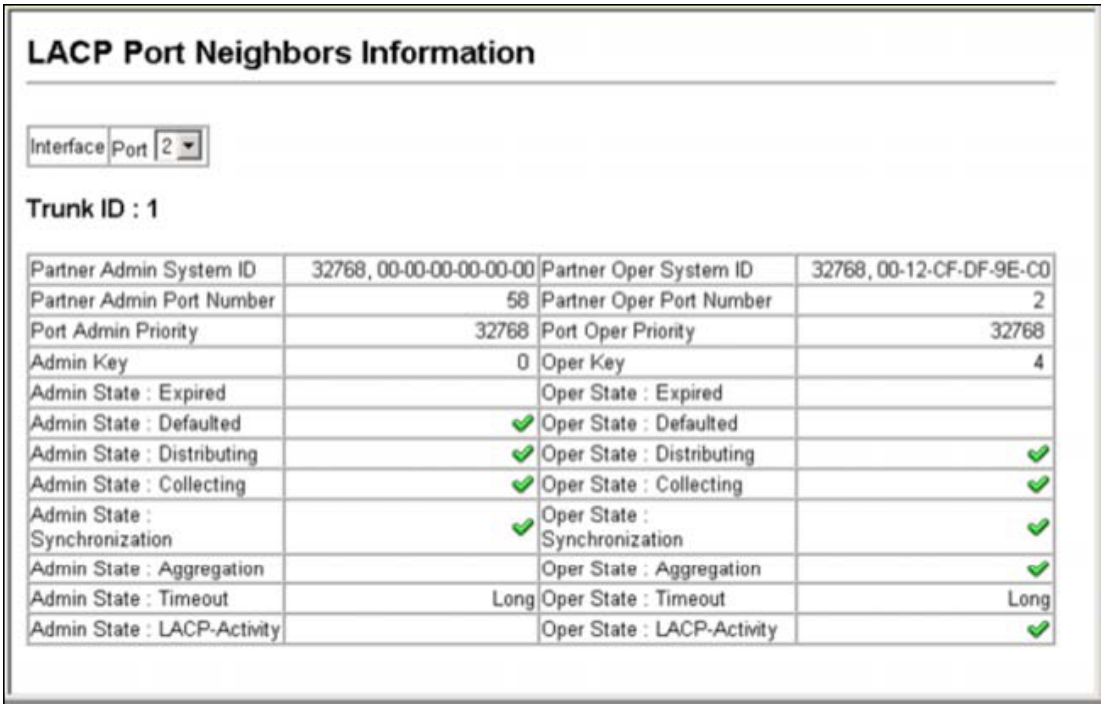
LACP のリモート側の設定及びステータスの表示を行なうことができます。

隣接設定情報

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

設定方法

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



3.7.4 ブロードキャストストームしきい値の設定

ブロードキャストストームはネットワーク上のデバイスが誤作動した場合や、アプリケーションプログラムの設計が正しくない場合、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。

設定・表示項目

Protect Status

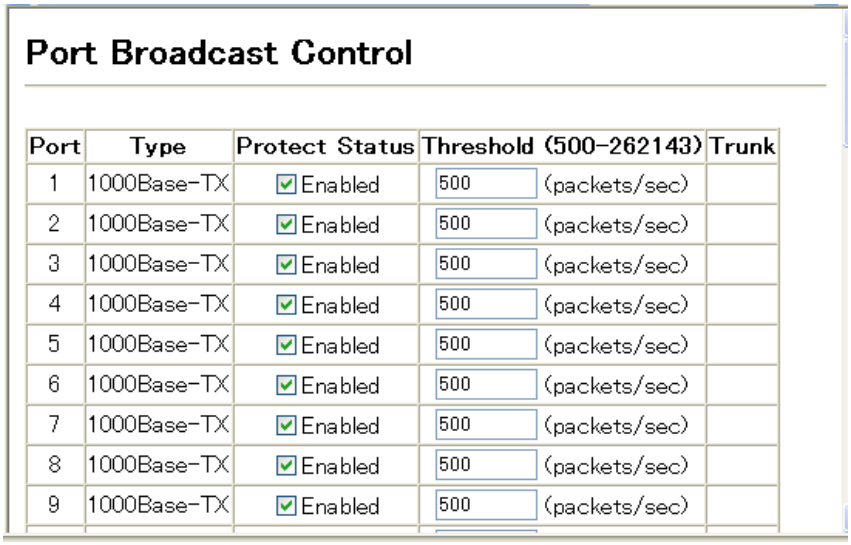
ブロードキャストストームコントロールの有効 / 無効（初期設定：有効）

Threshold

ポート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 :500-262143 パケット / 秒　初期設定：500 パケット / 秒）

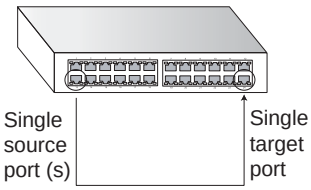
設定方法

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



3.7.5 ポートミラーリングの設定

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



機能解説

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

設定・表示項目

Mirror Sessions

現在のミラーセッションの一覧を表示します。

Source Port

通信がモニターされるソースポート

Type

モニターを行う通信の種類。

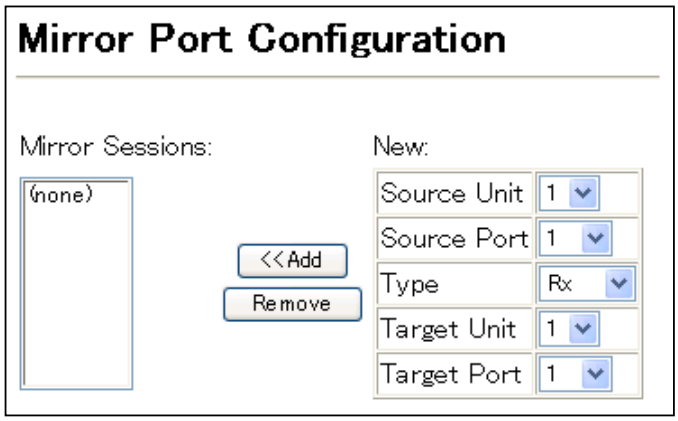
Rx（受信）、Tx（送信）、（初期設定：Rx）

Target Port

ソースポートの通信のミラーリングがされるターゲットポート

設定方法

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



3.7.6 帯域制御

帯域制御機能では各インタフェースの送信及び受信の最大速度を設定することができます。帯域制御は各ポート / 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。

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

Rate Limit

インタフェースの出力レートを設定します。

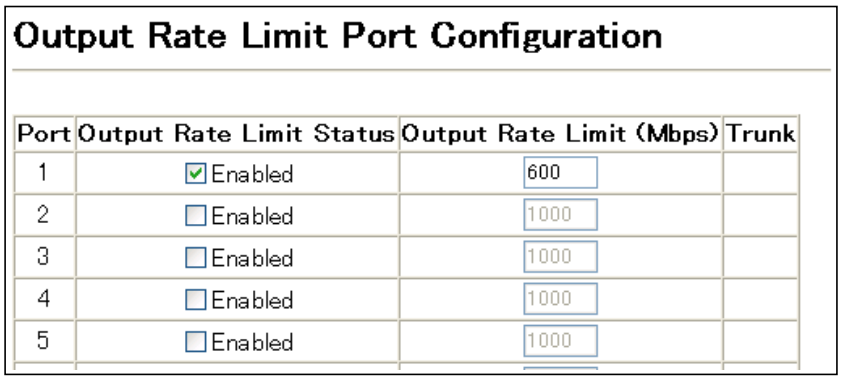
－初期ステータス：無効

－初期レート：1000Mbps

－範囲：1-1000Mbps

設定方法

[Port] → [Rate Limit] → [Input 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、rate limit（帯域制御）の値を設定し、[Apply] をクリックします。



3.7.7 ポート統計情報表示

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

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

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

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

統計値

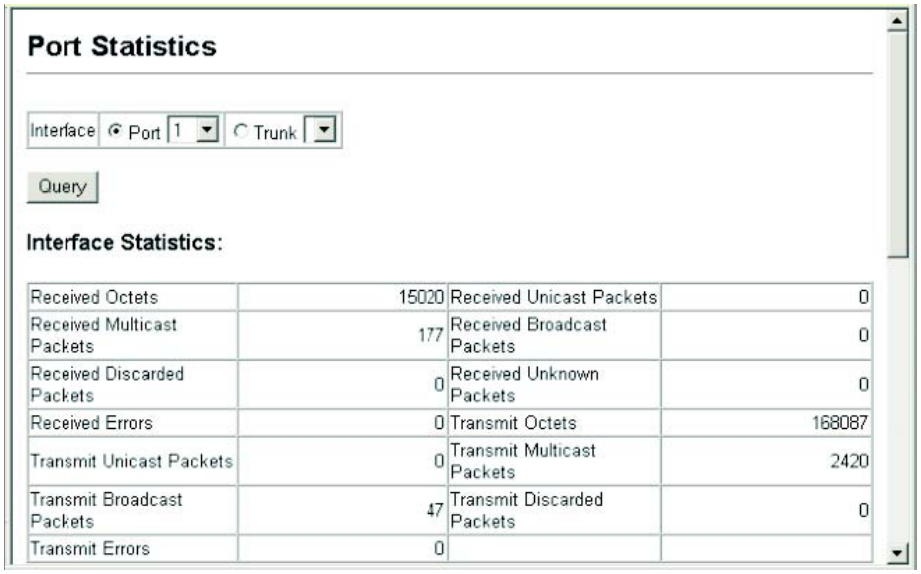
パラメータ	解説
Interface Statistics	
Received Octets	フレーム文字を含むインタフェースで受信されたオクテットの数
Received Unicast Packets	層位プロトコルで受信したサブネットワークユニキャストパケットの数
Received Multicast Packets	このサブレイヤから送信され、高層のレイヤで受信されたパケットで、このサブレイヤのマルチキャストアドレス宛てのパケットの数
Received Broadcast Packets	このサブレイヤから送信され、高層のレイヤで受信されたパケットで、このサブレイヤのブロードキャストアド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

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

設定方法

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

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



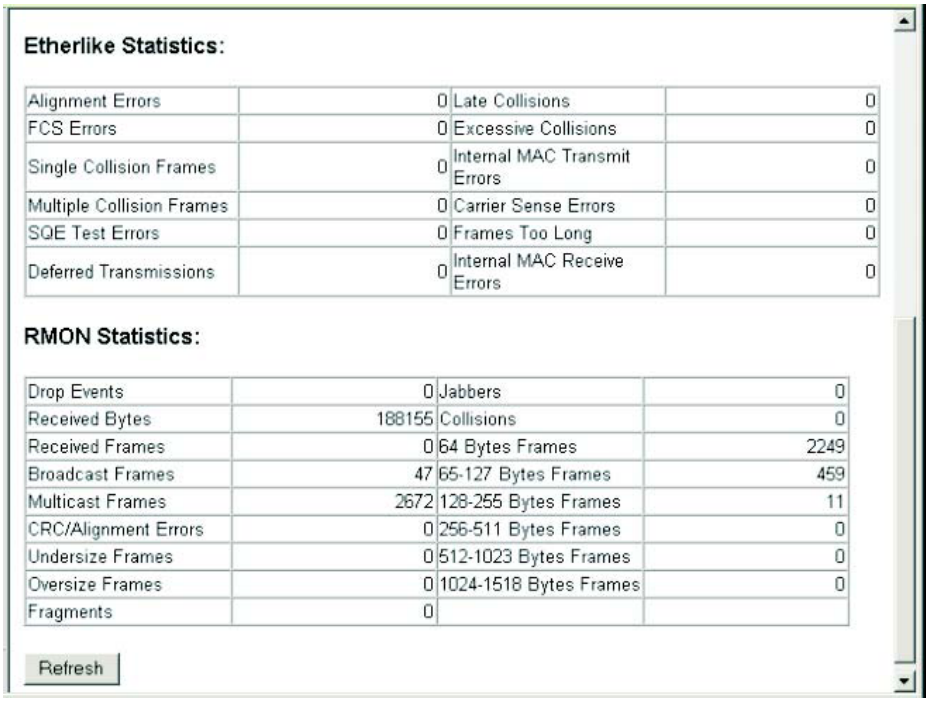
Port Statistics

Interface ◉ Port 1 ○ Trunk

Query

Interface Statistics:

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



Etherlike Statistics:

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

RMON Statistics:

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

Refresh

3.8 アドレステーブル

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

3.8.1 静的アドレステーブルの設定

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

設定・表示項目

Static Address Counts

手動設定した静的アドレス数

Current Static Address Table

静的アドレスの一覧

Interface

静的アドレスと関連したポート又はトランク

MAC Address

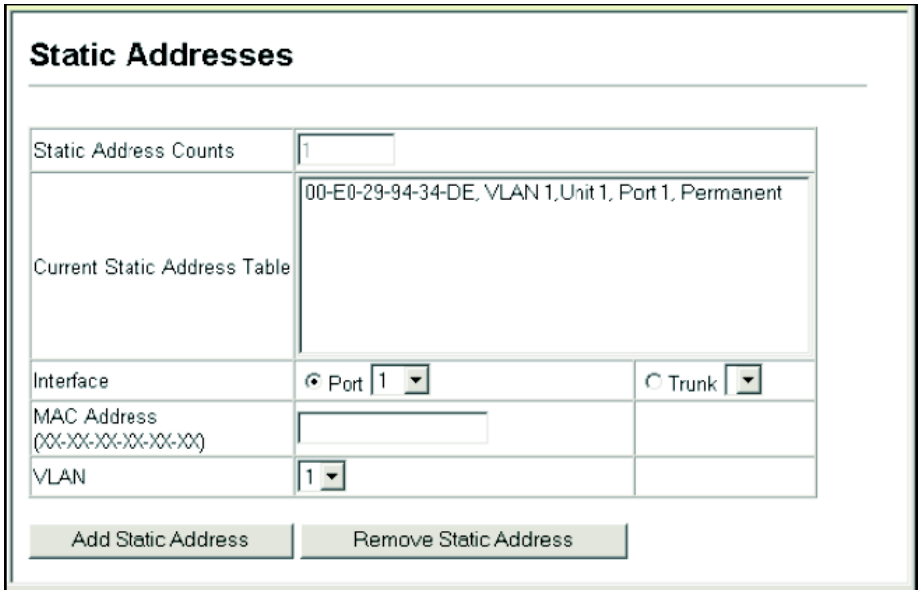
インタフェースの MAC アドレス

VLAN

VLAN ID(1-4094)

設定方法

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



3.8.2 アドレステーブルの表示

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

設定・表示項目

Interface

ポート又はトランク

MAC Address

インタフェースの MAC **アドレス**

VLAN

VLAN ID (1-4094)

Address Table Sort Key

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

Dynamic Address Counts

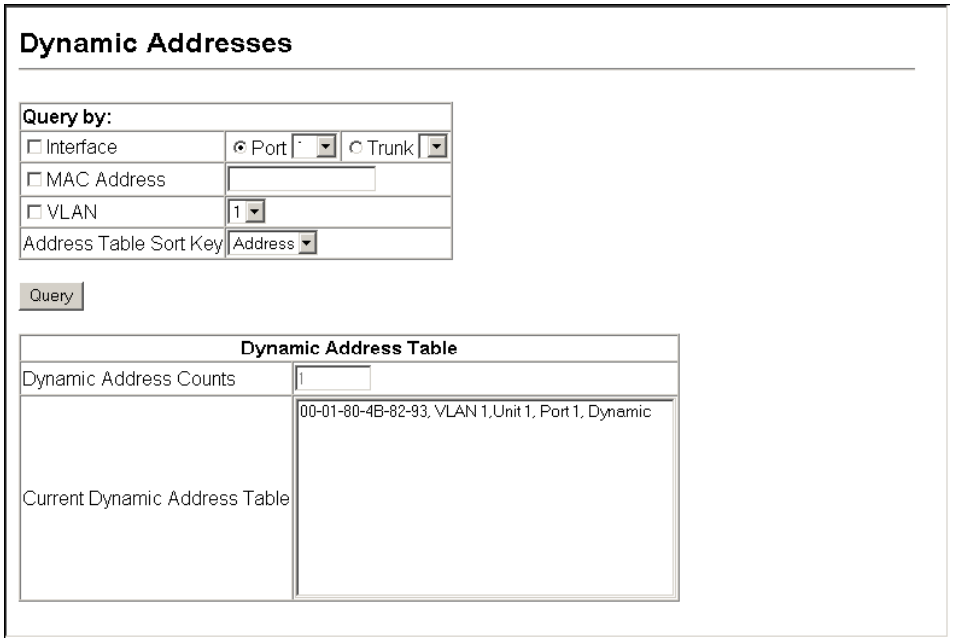
動的に学習する MAC **アドレス数**

Current Dynamic Address Table

動的に学習された MAC **アドレスのリスト**

設定方法

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



3.8.3 エージングタイムの変更

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

設定・表示項目

Aging Status

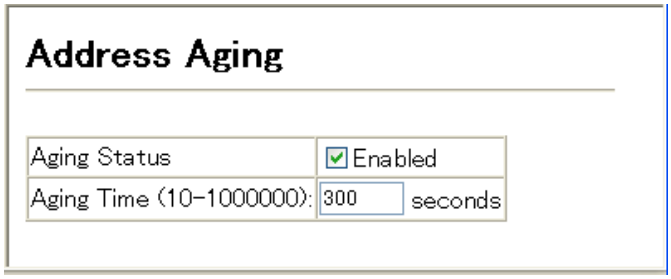
エージングタイムの機能の有効 / 無効

Aging Time

MAC **アドレスエージングタイム（範囲：**10-1000000 **秒、初期設定：**300 **秒）**

設定方法

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



3.9 スパニングツリーアルゴリズム

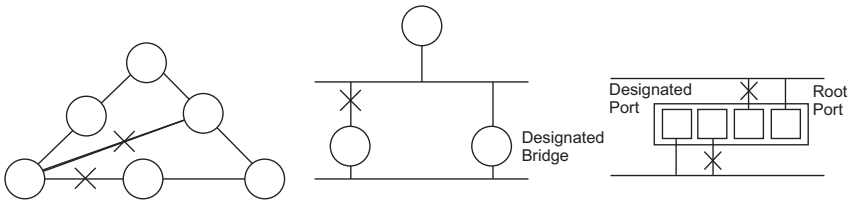
スパニングツリープロトコル STP はネットワークのループを防ぎ、また、スイッチ、ブリッジ及びルータ間のバックアップリンクを確保するために使用します。

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

本機は、以下の規格に準拠した STP に対応しています。

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

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



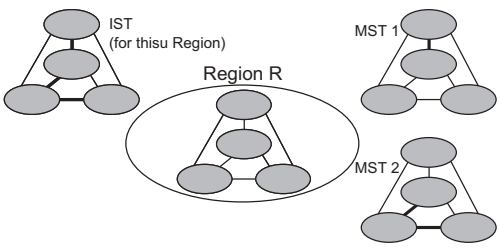
最小コストのスパニングツリーが決定した後、すべてのルートポートと指定ポートが有効となり、他のポートは無効となります。それによりパケットはルートポートから指定ポートにのみ送信され、ネットワークのループが回避されます。

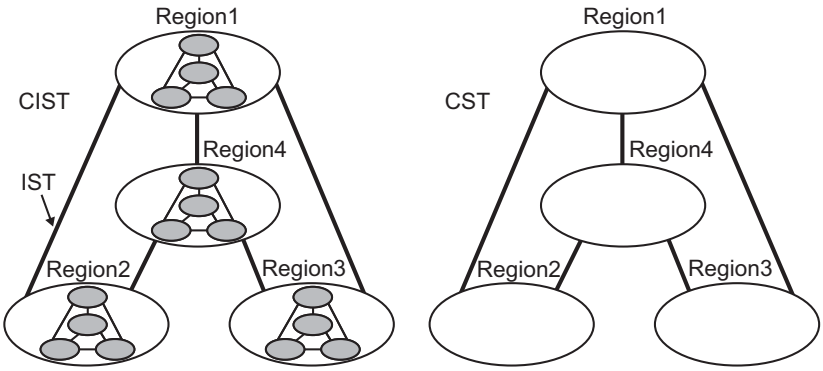
安定したネットワークトポロジーが確立された後、ルートブリッジから送信される Hello BPDU(Bridge Protocol Data Units) をすべてのブリッジが受信します。定められた間隔（最大値）以内にブリッジが Hello BPDU を確認できない場合、ルートブリッジへの接続を行っているリンクを切断します。そして、このブリッジはネットワークの再設定を行ない有効なネットワークトポロジーを回復するために、他のブリッジとネゴシエーションを開始します。

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

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

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




Region1
CIST
Region4
IST
Region2
Region3
Region1
CST
Region4
Region2
Region3

3.9.1 グローバル設定の表示

STP 情報ページから現在の STP の情報を確認することができます。

設定・表示項目

Spanning Tree State
STP が有効で STP ネットワークに参加しているかを表示します。

Bridge ID

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

Max Age

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

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

Hello Time

ルートデバイスが設定メッセージを送信する間隔（秒）が表示されます。

Forward Delay

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

Designated Root

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

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

Configuration Changes

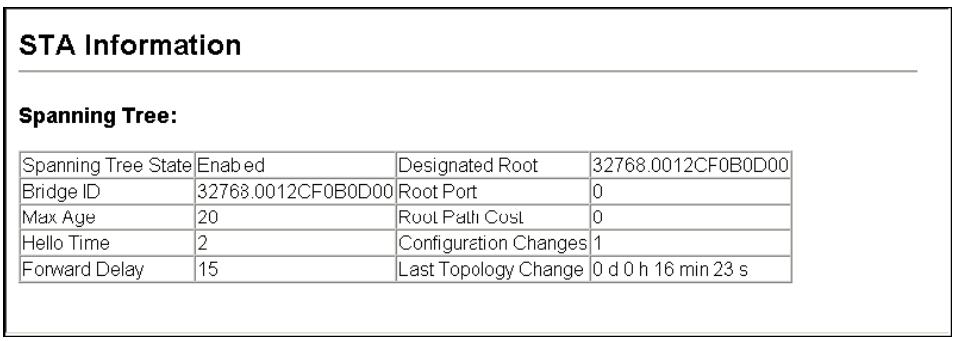
スパニングツリーが再設定された回数が表示されます。

Last Topology Change

最後にスパニングツリーが再設定されてから経過した時間が表示されます。

設定方法

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



3.9.2 グローバル設定

ここでの設定は本機全体に適用されます。

機能解説

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

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

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

- Multiple Spanning Tree Protocol

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

設定・表示項目

グローバル設定の基本設定

Spanning Tree State

スパニングツリーを有効又は無効にします。(**初期設定** : **有効**)

Spanning Tree Type

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

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

Priority

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

ルート機器設定

Hello Time

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

Maximum Age

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

Forward Delay

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

*RSTP **設定***

Path Cost Method

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

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

Transmission Limit

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

*MSTP **設定***

Max Instance Numbers

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

Region Revision*

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

Region Name*

MST インスタンス名（最大値：32 文字）

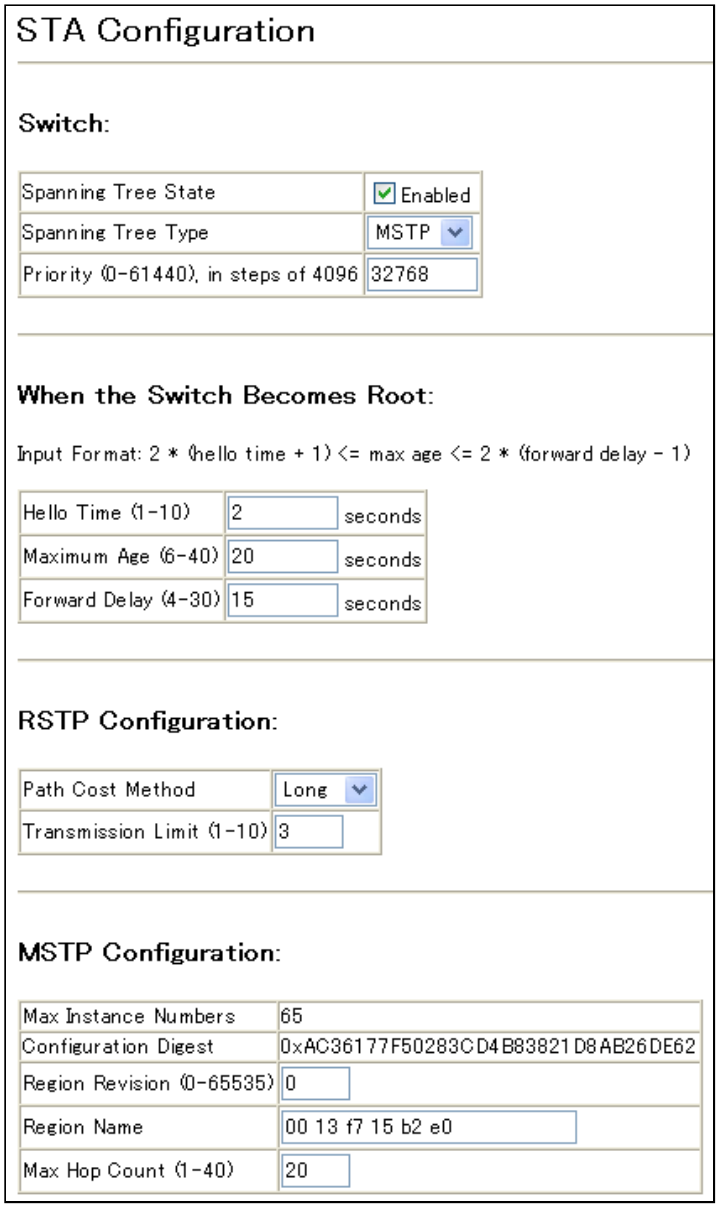
Maximum Hop Count

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

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

設定方法

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



3.9.3 インタフェース設定の表示

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

設定・表示項目

Spanning Tree

STA の有効 / 無効が表示されます。

STA Status

スパニングツリー内での各ポートの現在の状態を表示します :

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

ポート状態のルール :

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

Forward Transitions

ポートが転送状態 (Forwarding) に遷移した回数が表示されます。

Designated Cost

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

Designated Bridge

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

Designated Port

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

Oper Link Type

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

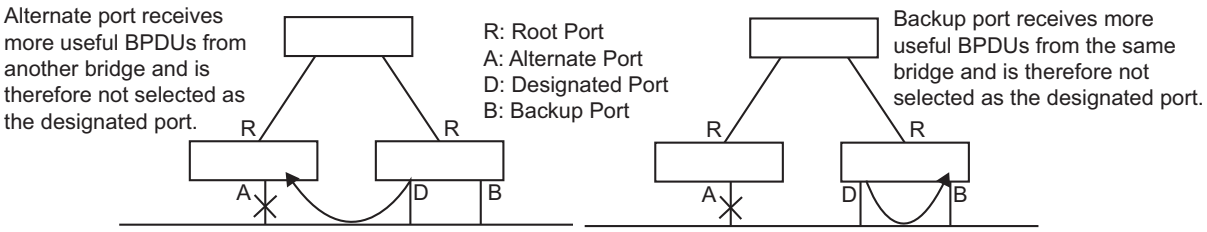
Oper Edge Port

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

Port Role

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

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



Trunk Member

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

設定方法

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

STA Port Information

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

3.9.4 インタフェース設定

ポートプライオリティ、パスコスト、リンクタイプ及びエッジポートを含む各インタフェースの RSTP 及び MSTP 属性を設定することができます。

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

設定・表示項目

以下の設定は変更することはできません。

STA Status

スパニングツリー内での各ポートの現在の状態を表示します :

(詳細は P111 「インタフェース設定の表示」を参照して下さい)

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

Trunk

トランクメンバーに設定されているかどうかを表示します。

(STA Port Configuration ページのみ)

以下の設定は変更することができます。

Spanning Tree

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

Priority

STP での各ポートのプライオリティを設定します。

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

Path Cost

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

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

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

Admin Link Type

インタフェースへ接続する接続方式（初期設定 :Auto）

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

Admin Edge Port (Fast Forwarding)

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

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

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

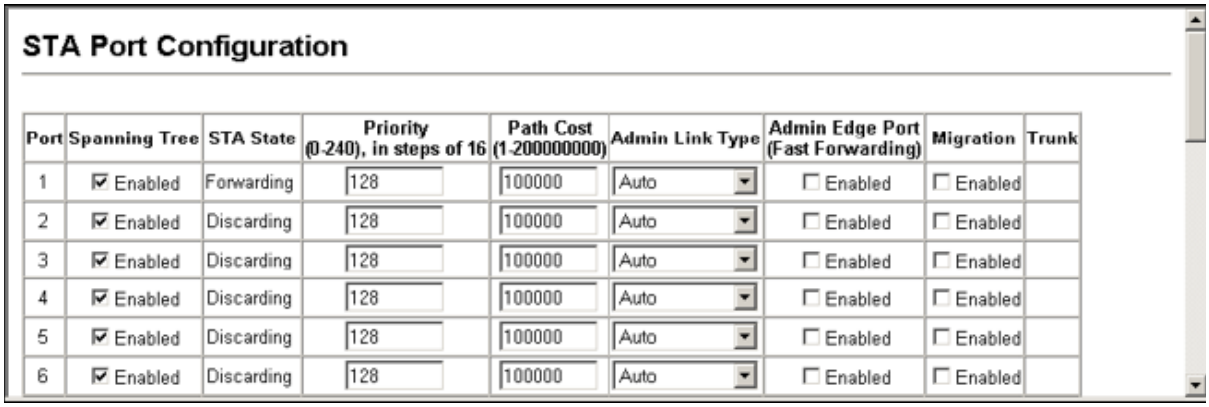
Migration

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

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

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	

3.9.5 MSTP 設定

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

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

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

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

MSTP を使用するには以下の手順で設定を行なってください。

（5）スパニングツリータイプを MSTP に設定します (P108 「グローバル設定」参照)

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

（7）MSTI を共有する VLAN を追加します。

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

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

設定・表示項目

MST Instance

スパニングツリーのインスタンス ID（初期設定：0）

Priority

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

VLANs in MST Instance

インスタンスに指定された VLAN

MST ID

設定のためのインスタンス ID（設定範囲：0-57、初期設定：0）

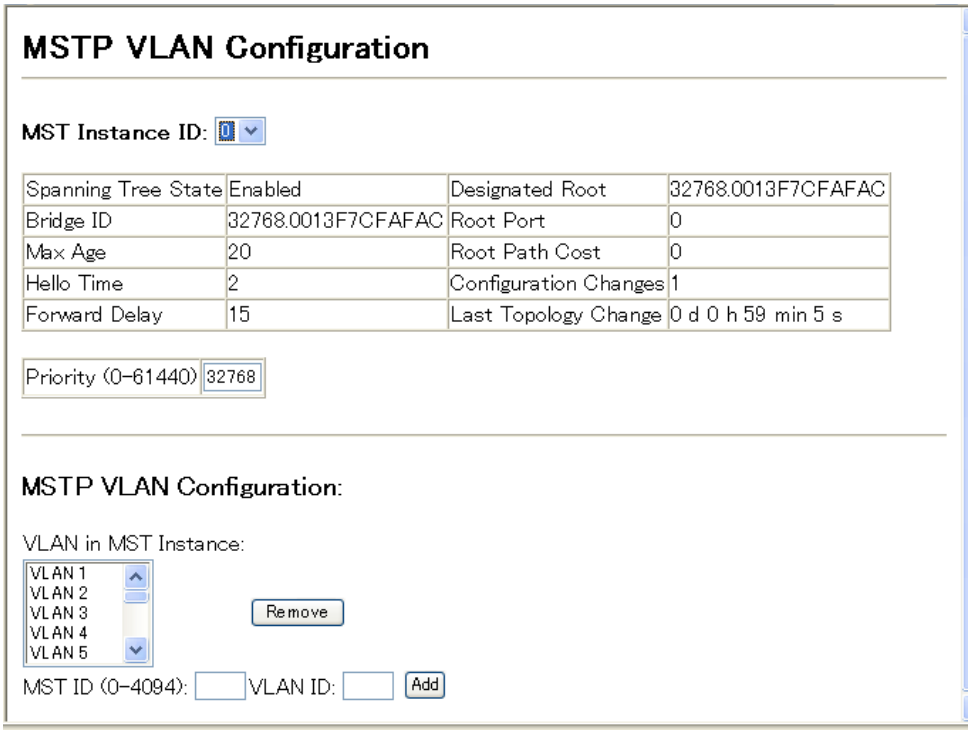
VLAN ID

MST インスタンスに指定する VLAN ID（設定範囲：1-4093）

他の項目は、P111 「インタフェース設定の表示」を参照して下さい。

設定方法

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



3.9.6 MSTP インタフェース設定の表示

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

設定・表示項目

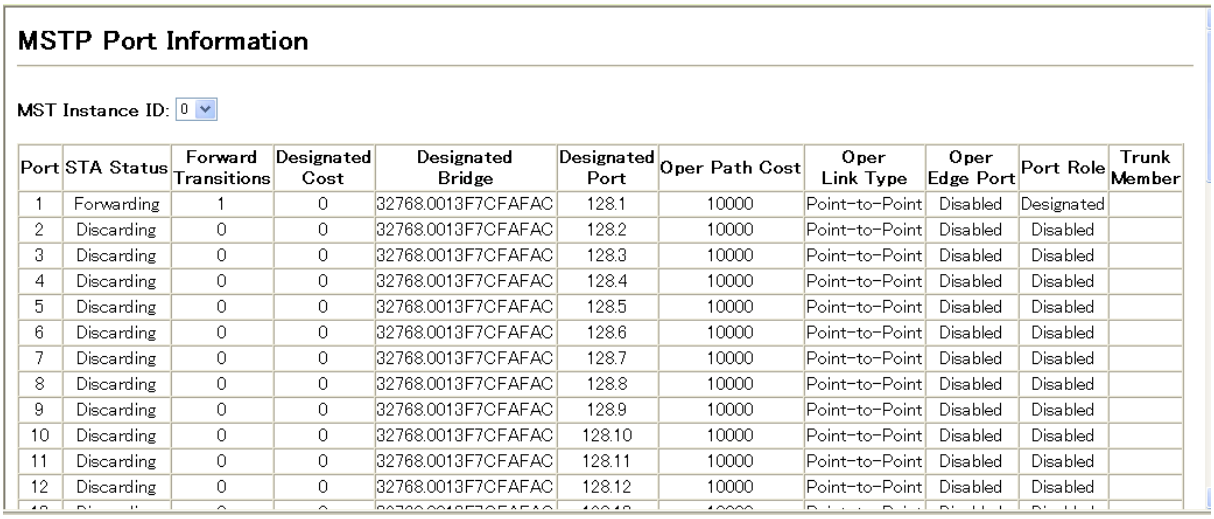
MST Instance ID

インスタンス ID（設定範囲：0-4094、初期設定：0）

[注意] 他の項目に関しては P111 「インタフェース設定の表示」を参照して下さい。

設定方法

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



MSTP Port Information

MST Instance ID: 0

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

3.9.7 MSTP インタフェースの設定

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

設定・表示項目

以下の項目は設定を変更できません。

STA Status

スパニングツリー内での各ポートの現在の状態を表示します :

（詳細は 3.9.3 項「インタフェース設定の表示」を参照して下さい）

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

Trunk Member

トランクメンバーに設定されているかどうかを表示します。

（STA Port Configuration ページのみ）

以下の項目は設定を変更できます。

MST Instance ID

設定のインスタンス ID（設定範囲：0-4094、初期設定：0）

Priority

STP での各ポートのプライオリティを設定します。

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

MST Path Cost

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

－設定範囲 :

Ethernet: 200,000-20,000,000
Fast Ethernet: 20,000-2,000,000
Gigabit Ethernet: 2,000-200,000

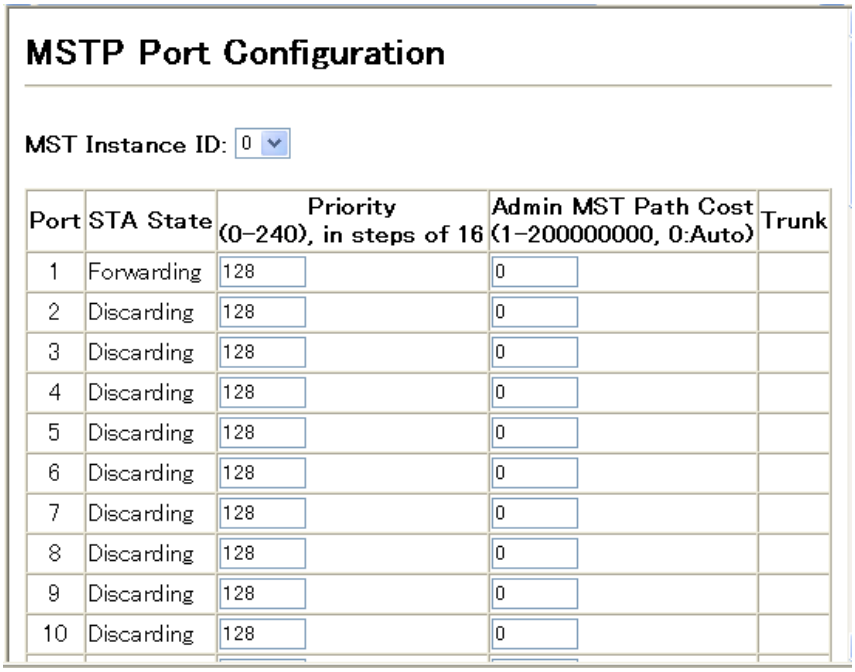
－初期設定 :

Ethernet — half duplex: 2,000,000、full duplex: 1,000,000、 trunk: 500,000
Fast Ethernet — half duplex: 200,000、full duplex: 100,000、 trunk: 50,000
Gigabit Ethernet — full duplex: 10,000、trunk: 5,000

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

設定方法

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



MSTP Port Configuration

MST Instance ID: 0

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

3.10 VLAN

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

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

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

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

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

本機では以下の VLAN 機能をサポートしています。

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

VLAN へポートの割り当て

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

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

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

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

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

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

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

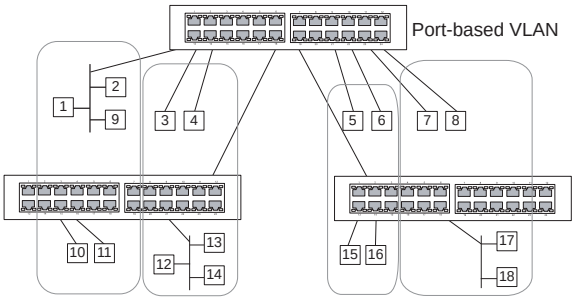
VLAN に割り当てられたユーザグループが、他の VLAN と分けられたブロードキャストドメインとなります。パケットは同じ VLAN 内の指定されたポート間でのみ送信されます。タグなし VLAN は手動でのユーザグループ又はサブネットの分割が行えます。また、GVRP を使用した IEEE802.3 タグ VLAN により、完全に自動化した VLAN 登録を行うことも可能となります。

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

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

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

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

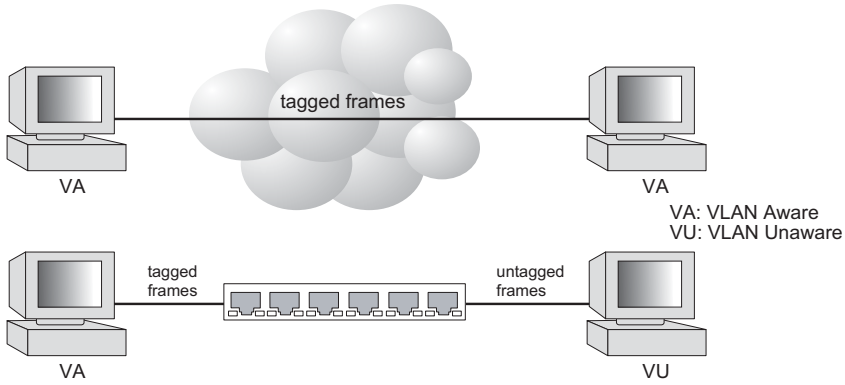


タグ付・タグなしフレームの送信

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

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

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

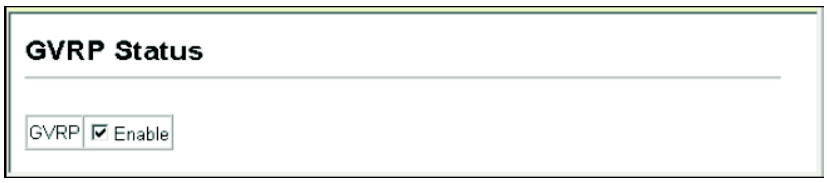

tagged frames
VA
VA
VA: VLAN Aware
VU: VLAN Unaware
tagged
frames
untagged
frames
VA
VU

3.10.1 GVRP の有効・無効（Global Setting）

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

設定方法

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



3.10.2 VLAN 基本情報の表示

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

設定・表示項目

VLAN Version Number

本機で使用している IEEE 802.1Q 標準の VLAN のバージョン

Maximum VLAN ID

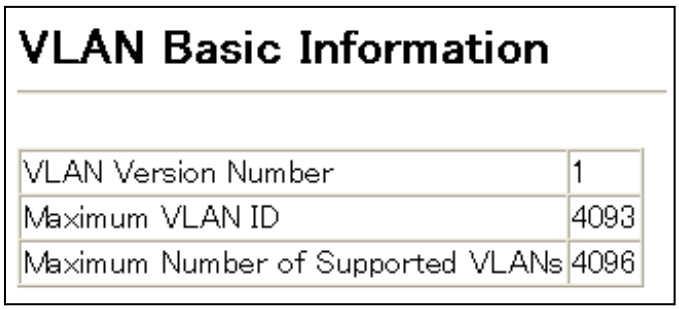
本機で認識可能な VLAN ID の最大値

Maximum Number of Supported VLANs

本機で設定することのできる最大 VLAN 数

設定方法

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



3.10.3 現在の VLAN 表示

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

設定・表示項目

VLAN ID

設定されている VLAN の ID (1-4094)

Up Time at Creation

VLAN が作成されてからの経過時間

Status

VLAN の設定方法 :

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

Egress Ports

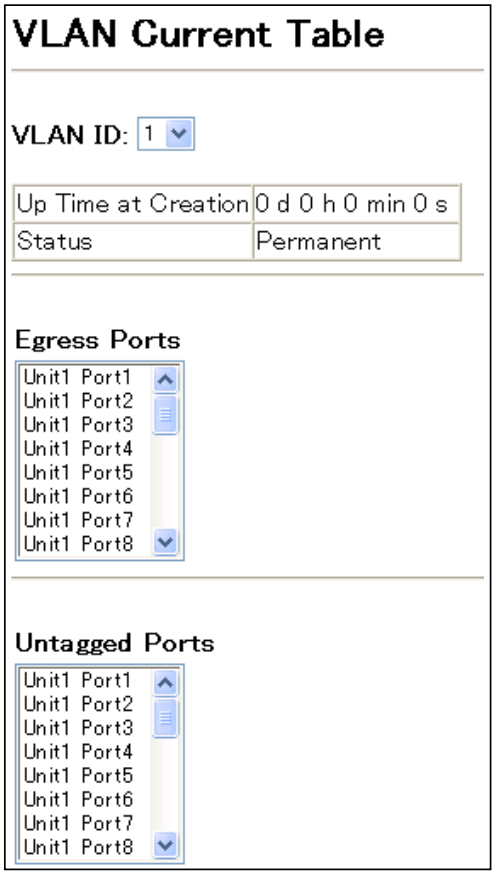
すべての VLAN ポートメンバー

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 Current Table
VLAN ID: 1
Up Time at Creation
0 d 0 h 0 min 0 s
Status
Permanent
Egress Ports
Unit1 Port1
Unit1 Port2
Unit1 Port3
Unit1 Port4
Unit1 Port5
Unit1 Port6
Unit1 Port7
Unit1 Port8
Untagged Ports
Unit1 Port1
Unit1 Port2
Unit1 Port3
Unit1 Port4
Unit1 Port5
Unit1 Port6
Unit1 Port7
Unit1 Port8

3.10.4 VLAN の作成

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

設定・表示項目

Current

このシステムを作成する全ての現在の VLAN グループを表示します。最大 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（1 から 4094）

VLAN Name

VLAN 名 (1 から 32 文字)

Status (Web)

この VLAN を有効にします。

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

Status (CLI)

この VLAN を有効にします。

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

Add

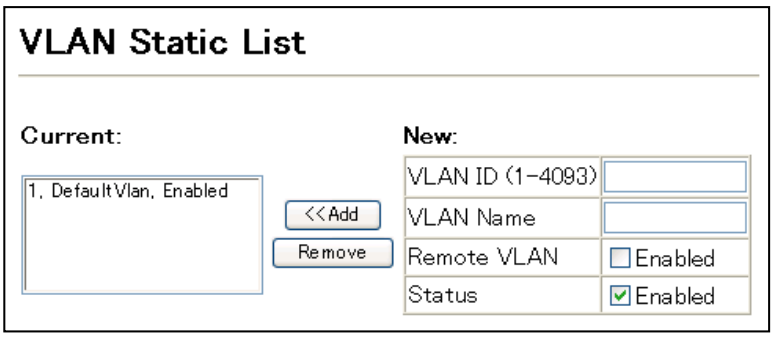
リストに新しい VLAN グループを追加します。

Remove

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

設定方法

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



3.10.5 VLAN への静的メンバーの追加（VLAN Index）

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

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

[注意] P129「VLAN への静的メンバーの追加（Port Index）」でも、ポートインデックスを元に VLAN グループの設定を行なうことができますが、タグ付としてしかポートの追加はできません。

[注意] VLAN 1 は本機のすべてのポートが参加するデフォルトタグなし VLAN です。P130「インタフェースの VLAN 動作の設定」にあるデフォルトポート VLAN ID を変更することができます。

設定・表示項目

VLAN

設定された VLAN ID（1 から 4094）

Name

VLAN 名（1 から 32 文字）

Status

この VLAN が有効か無効かを表示します。

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

Port

ポート番号

Membership Type

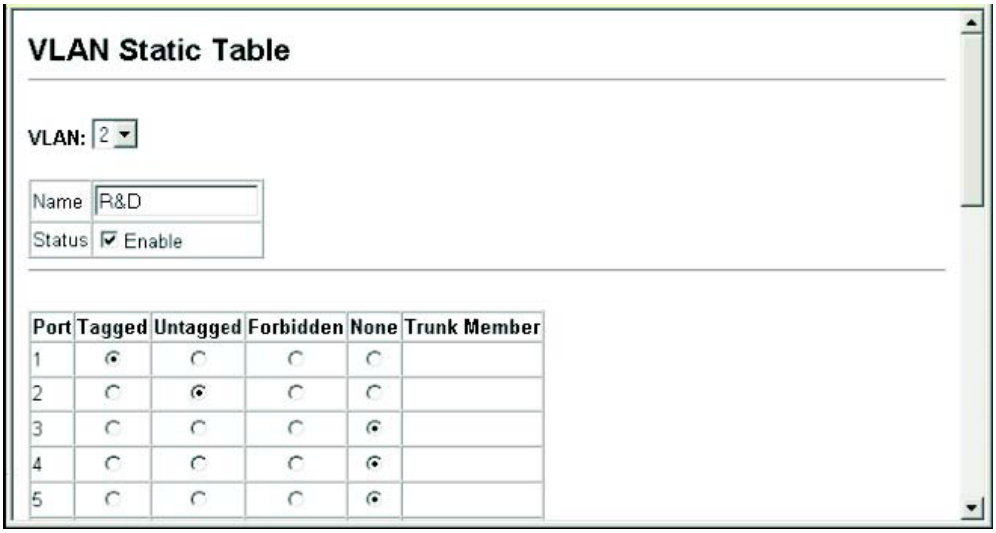
ラジオボタンをマークすることにより、各インタフェースへの VLAN メンバーシップを選択します。

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

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

設定方法

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



3.10.6 VLAN への静的メンバーの追加（Port Index）

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

設定・表示項目

Interface

ポート又はトランク番号

Member

選択されたインタフェースがタグ付メンバーとして登録されている VLAN

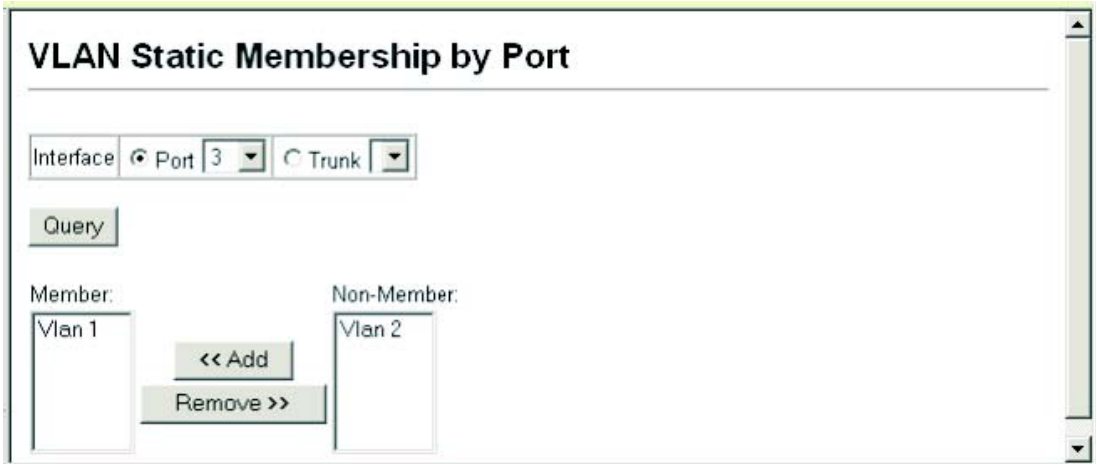
Non-Member

選択されたインタフェースがタグ付メンバーとして登録されていない VLAN

設定方法

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

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



3.10.7 インタフェースの VLAN 動作の設定

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

機能解説

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

設定・表示項目

PVID

タグなしフレームを受信した際に付ける VLAN ID（初期設定 : 1）

－インタフェースが VLAN 1 のメンバーでない場合に、この VLAN へ PVID ”1” を割り当てた場合、インタフェースは自動的にタグなしメンバーとして VLAN 1 に参加します。その他の VLAN に関しては、まず「Static table」（127 ページの「VLAN への静的メンバーの追加（VLAN Index）」を参照）にて、各 VLAN に所属しているポートごとに Tag 付き、Tag なしの設定を行う必要があります。

Acceptable Frame Type(受け入れ可能なフレームの種類)

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

Ingress Filtering

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

－イングレスフィルタリングはタグ付フレームでのみ機能します。

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

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

Mode

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

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

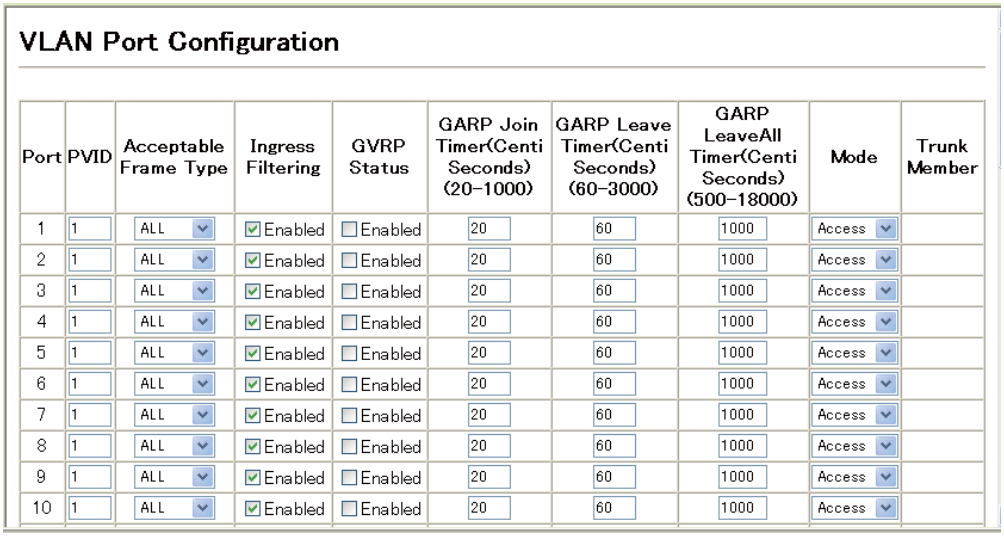
－ Hybrid — ハイブリッド VLAN インタフェースを指定します。ポートはタグ付又はタグなしフレームを送受信します。

Trunk Member

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

設定方法

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



VLAN Port Configuration

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer(Centi Seconds) (20-1000)	GARP Leave Timer(Centi Seconds) (60-3000)	GARP LeaveAll Timer(Centi Seconds) (500-18000)	Mode	Trunk Member
1	1	ALL	Enabled	Enabled	20	60	1000	Access	
2	1	ALL	Enabled	Enabled	20	60	1000	Access	
3	1	ALL	Enabled	Enabled	20	60	1000	Access	
4	1	ALL	Enabled	Enabled	20	60	1000	Access	
5	1	ALL	Enabled	Enabled	20	60	1000	Access	
6	1	ALL	Enabled	Enabled	20	60	1000	Access	
7	1	ALL	Enabled	Enabled	20	60	1000	Access	
8	1	ALL	Enabled	Enabled	20	60	1000	Access	
9	1	ALL	Enabled	Enabled	20	60	1000	Access	
10	1	ALL	Enabled	Enabled	20	60	1000	Access	

3.10.8 802.1Q トンネリングの設定

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

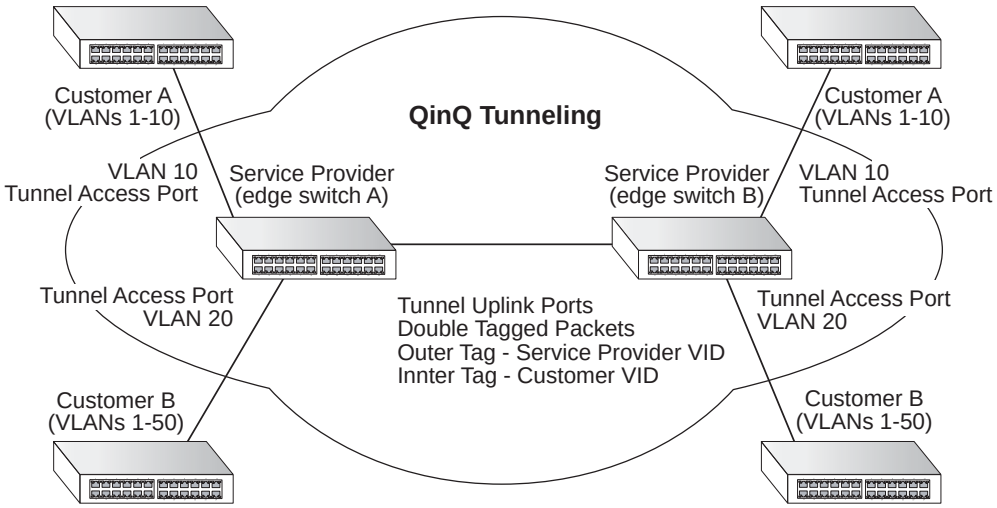
多くの場合、サービスプロバイダのカスタマーには、VLAN ID と、サポートの対象となる VLAN 数についての特定の要件があります。
同じサービスプロバイダネットワーク内の様々なカスタマーが必要とする VLAN の範囲は重複する場合があり、インフラストラクチャを介したカスタマーのトラフィックが混在する場合もあります。各カスタマーに、固有の範囲の VLAN ID を割り当てると、カスタマーの設定を制限することになり、IEEE802.1Q 仕様の 4096 という VLAN の制限を容易に超える可能性があります。

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

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

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

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


Customer A
(VLANs 1-10)
QinQ Tunneling
Customer A
(VLANs 1-10)
VLAN 10
Tunnel Access Port
Service Provider
(edge switch A)
Service Provider
(edge switch B)
VLAN 10
Tunnel Access Port
Tunnel Access Port
VLAN 20
Tunnel Uplink Ports
Double Tagged Packets
Outer Tag - Service Provider VID
Innter Tag - Customer VID
Tunnel Access Port
VLAN 20
Customer B
(VLANs 1-50)
Customer B
(VLANs 1-50)

QinQ トンネリングの有効

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

設定・表示項目

Tunnel Status

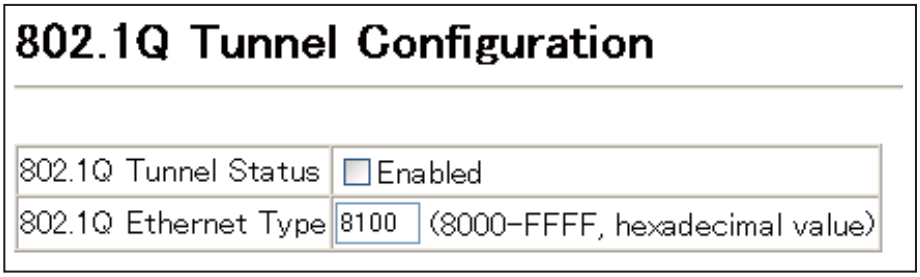
スイッチを QinQ モードに設定します。

802.1Q Ethernet Type

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

設定方法

（1）[VLAN → [Tunnel] をクリックします。
（2）「Step」リストから「Configure Global」を選択します。
（3）トンネルステータスを有効にし、TPID を指定します。
（4）＜ Apply ＞をクリックします。



インタフェースを QinQ トンネリングへ追加

前のセクションに従い、QinQ トンネルの準備を行ってください。

機能解説

- VLAN ポート設定または VLAN トランク設定画面を使用し、エッジスイッチのアクセスポートを 802.1Q トンネルモードに設定してください。
- トンネルポートの設定を行う前に 802.1Q トンネル設定画面を使用し、スイッチを QinQ モードに設定してください。（P134 「QinQ トンネリングの有効」を参照）

設定・表示項目

Interaface

ポートまたはトランクのリストを表示

Port

ポート識別子（範囲：1-10）

Trunk

トランク識別子（範囲：1-5）

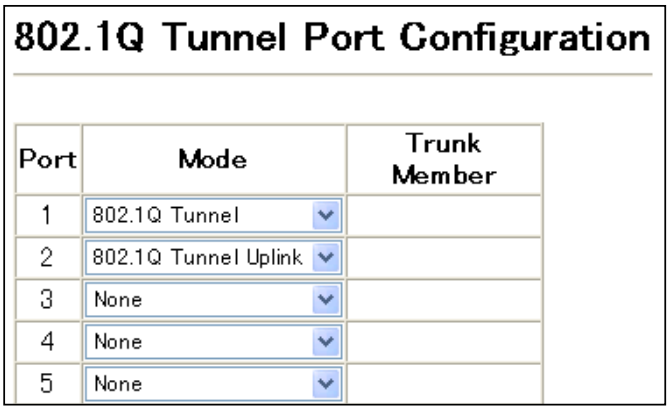
Mode

ポートの VLAN モードを設定します（初期設定 : 無効）

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

設定方法

（1）[VLAN → [Tunnel] をクリックします。
（2）「Step」リストから「Configure Interface」を選択します。
（3）トンネルアクセスポートにモードを設定します。
（4）＜ Apply ＞をクリックします。



3.10.9 プライベート VLAN の設定

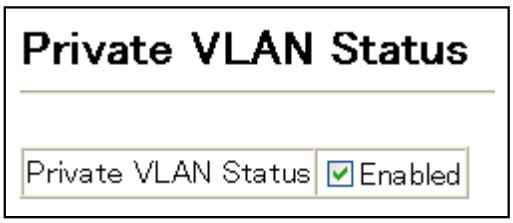
プライベート VLAN は、ポートベースのセキュリティと VLAN 内のポート間の独立を確保ことができます。ダウンリンクポートはアップリンクポートとのみデータの転送を行なうことができます（プライベート VLAN と通常の VLAN は同一機器内に両方の設定を行うことが可能です）

プライベート VLAN の有効化

プライベート VLAN ステータスページでプライベート VLAN 機能の有効 / 無効の設定を行なうことができます。

設定方法

[VLAN] → [Private VLAN] → [Status] をクリックします。スクロールダウンリストから Enable/Disable を選択し、[Apply] をクリックします。

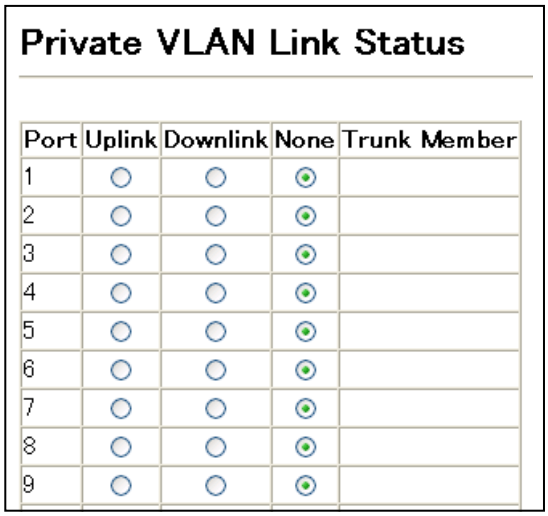


アップリンク・ダウンリンクポートの設定

プライベート VLAN リンクステータスページでは各ポートをダウンリンク又はアップリンクポートに設定できます。ダウンリンクポートに指定したポートはアップリンクポート以外との通信はできなくなります。アップリンクポートに指定したポートはダウンリンクポートを含む本機のすべてのポートと通信が可能です。

設定方法

[VLAN] → [Private VLAN] → [Link Status] をクリックします。プライベート VLAN のアップリンク又はダウンリンクとするポートをチェックし、[Apply] をクリックします。



3.10.10 プロトコル VLAN

複数のプロトコルのトラフィックが、異なった VLAN を通過することを可能にします。

ポートでパケットが受け取られる際、そのパケットのプロトコルタイプにより VLAN メンバーシップを決定します。

プロトコル VLAN グループ設定

設定・表示項目

Protocol Group ID

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

Frame Type

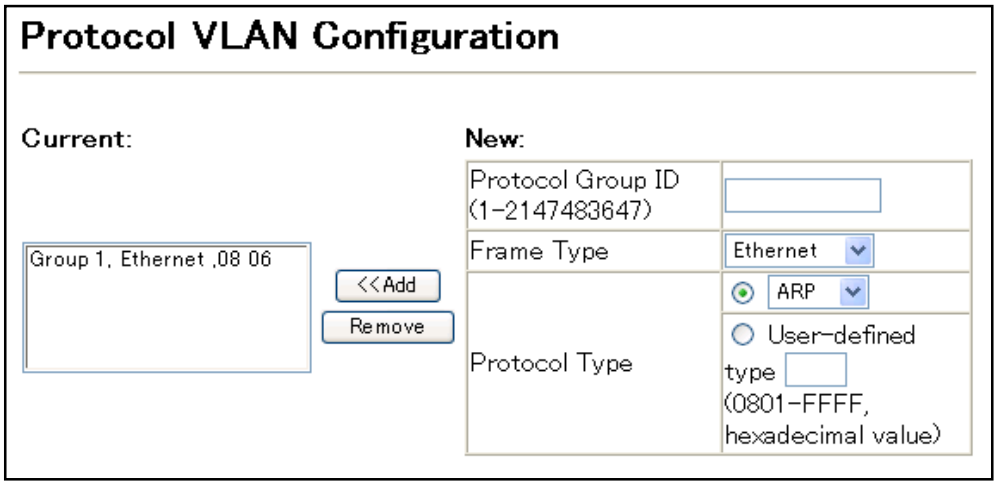
Ethernet, RFC 1042, **または** LLC **のいずれかを選択してください。**

Protocol Type

LLC **は** IPX Raw**、その他フレームタイプは** IP, ARP **または** RARP **です。**

設定方法

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



プロトコル VLAN インタフェース設定

ポートごとのプロトコル VLAN 設定を行います。

設定・表示項目

Interface

ポートまたはトランクを指定

Protocol Group ID

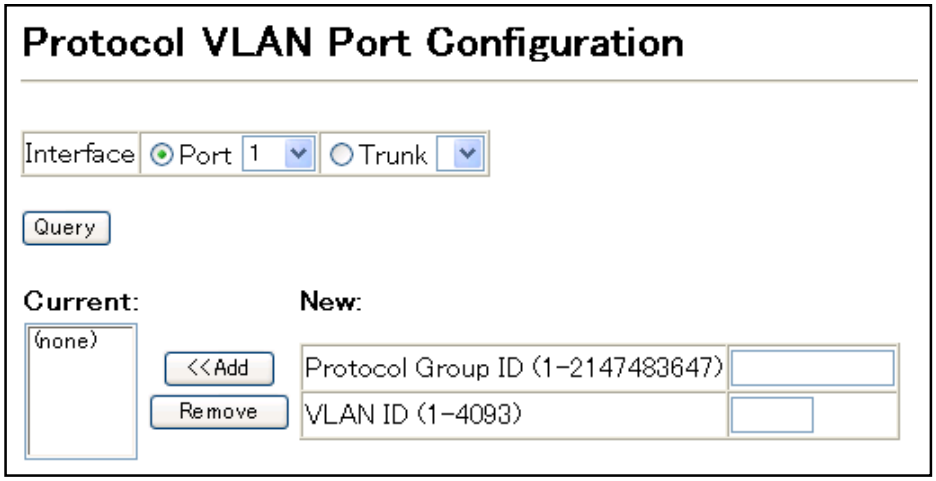
プロトコル VLAN グループに割り当てられたプロトコルグループ ID（範囲：1-2147483647）

VLAN ID

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

設定方法

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



3.10.11 LLDP

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

3.10.12 LLDP タイム属性の設定

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

設定・表示項目

LLDP

LLDP をスイッチグローバルで有効 / 無効にします。（初期設定：有効）

Transmission Interval

LLDP の情報伝達のため周期的に送信する間隔を設定します

（範囲：5 － 32768 秒初期設定：30 秒）

この値は下の数式に従って計算します。

（Transmission Interval × Hold Time Multiplier）≦ 65536
Transmission Interval >= （4 × Delay Interval）

Hold Time Multiplier

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

TTL は、タイムリーな方法でアップデートが送信されない場合、送信した LLDP エージェントに関係のあるすべての情報をどのくらいの期間維持するかを受信した LLDP エージェントに伝達します。TTL は秒で表され、下の数式で計算します。
Transmission Interval × Hold Time Multiplier ≦ 65536
つまり上の式からデフォルトの TTL は下のようになります。
4 × 30 ＝ 120

Delay Interval

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

この値は下の数式に従って計算します。
(4 ×Delay Interval) ≦ Transmission Interval

Reinitialization Delay

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

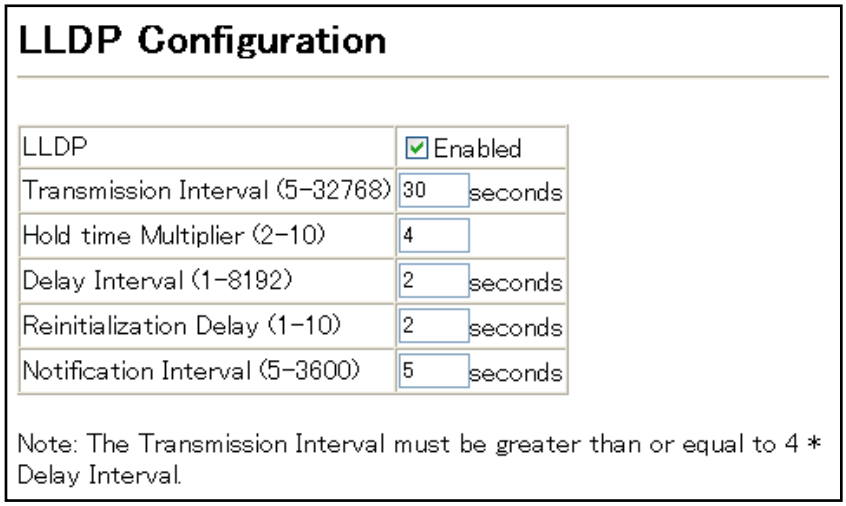
Notification Interval

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

（範囲：5 － 3600 秒　初期設定：5 秒）

設定方法

(1) [Administration] → [LLDP] をクリックします。
(2)「Step」リストから「Configure Global」を選択します。
(3) LLDP を有効にし、各パラメータを編集します。
(4) ＜ Apply ＞をクリックします。



3.10.13 LLDP インタフェースの設定

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

設定・表示項目

Admin Status

LLDP メッセージの送信・受信のモードを有効にします

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

SNMP Notification

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

（初期設定：有効）

Basic Optional TLVs

アドバタイズするメッセージの TLV フィールドの情報について設定します。

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

802.1 Organizationally Specific TLVs

アドバタイズドメッセージの TLV フィールドに含まれる 802.1 情報を設定。

- **Protocol Identity**— このインタフェースを通してアクセス可能なプロトコル（P138「プロトコル VLAN」参照）
- **VLAN ID** — ポートのデフォルト VLAN 識別子（PVID）は VLAN がタグ無しであるか、関連付けられたプライオリティタグ付きフレームであるかを示します (P130 参照)
- **VLAN Name**— このインタフェースがアサインされる全ての VLAN の名前 (P127、P138「プロトコル VLAN」参照）
- **Port And Protocol VLAN ID**— このインタフェースに設定されたポートベースとプロトコルベース VLAN(P126 「VLAN の作成」、P138 「プロトコル VLAN」参照）

802.3 Organizationally Specific TLVs

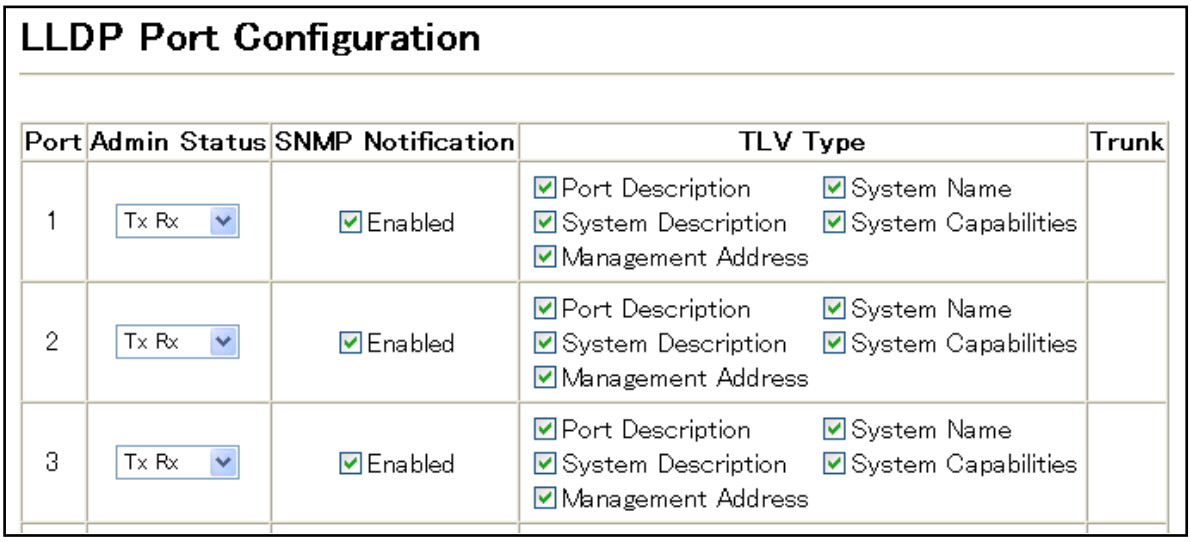
アドバタイズドメッセージの TLV フィールドに含まれる IEEE802.3 情報

- **Link Aggregation**— リンクアグリゲーション機能、リンクのアグリゲーションステータス、このインタフェースが現在リンクアグリゲーションメンバーである場合は IEEE802.3 アグリゲーションポート識別子
- **Max Frame Size** — 最大フレームサイズ（P26 「ジャンボフレームの設定」を参照）

ーMAC/PHY Configuration/Status — オートネゴシエーションサポート/性能の情報を含む、MAC/PHY 設定とステータスと、操作可能な Multistation Access Unit（MAU）タイプ

設定方法

（1）[Administration] → [LLDP] をクリックします。
（2）「Step」リストから「Configure Interface」を選択します。
（3）LLDP 送信 / 受信モードを設定し、SNMP トラップメッセージを送信するか否かを指定します。LLDP メッセージでアドバタイズする情報を選択します。
（4）＜ Apply ＞をクリックします。



3.10.14 LLDP ローカルデバイス情報の表示

Administration > LLDP (Show Local Device Information) を使用し、MAC アドレス、シャーシ ID、管理 IP アドレス、ポート等、本機の情報を表示します。

設定・表示項目

グローバル設定

Chassis Type

送信 LLDP エージェントと関連付けられる IEEE802 LAN エンティティを含むシャーシを識別します。シャーシを識別し、コンポーネントのタイプを示すために使用されるシャーシ ID サブタイプが、シャーシ ID フィールドに参照されるためにはいくつかの方法があります。

シャーシ ID サブタイプ

ID Basis	Reference
Chassis component	entPhysClass が "chassis(3)" の値を持つ時は EntPhysicalAlias（IETF RFC 2737）
Interface alias	IfAlias （IETF RFC 2863）
Port component	entPhysicalClass が "port(10)" または "backplane(4)" の値を持つ時は EntPhysicalAlias （IETF RFC 2737）
MAC address	MAC アドレス（IEEE Std 802-2001）
Network address	ネットワークアドレス
Interface name	ifName （IETF RFC 2863）
Locally assigned	ローカルに割り当てられる

Chassis ID

このシステムの特定のシャーシの指定された識別子を示す、8 進数ストリング .

System Name

システムの管理上に割り当てられた名前を示すストリング （P20 「システム情報の表示」を参照）

System Description

ネットワークエンティティの記述。このフィールドは "show system" コマンドでも表示されます。

System Capabilities Supported

システムのプライマリファンクションを定義するケイパビリティ

システム性能

ID Basis	Reference
Other	ー
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 および IETF RFC 2670
End Station Only	IETF RFC 2011

System Capabilities Enabled

現在有効になっているシステムのプライマリファンクション。前のテーブルを参照してください。

Management Address

ローカルシステムに関連付けられる管理アドレス。

インタフェース設定

下のリストされた属性はポートとトランクインタフェースタイプ両方に適用可能です。

トランクがリストされた時、説明はトランクの最初のポートに適用されます。

Port/Trunk Description

ポートまたはトランクの説明。RFC 2863 **が実装されている場合、**ifDescr **オブジェクトがこのフィールドに使用されます。**

Port/Trunk ID

ポートまたはトランクの識別子

設定方法

LLDP **のローカルデバイス情報を表示（**General**）**

（1**）**[Administration] → [LLDP] **をクリックします。**

（2**）「**Step**」リストから「**Show Local Device Information**」を選択します。**

（3**）**"General"、"Port"、"Trunk" **からいずれかを選択します。**

LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-17-2E-0F-E2-A0
System Name	
System Description	10/100/1000 L3 SWITCH
System Capabilities Supported	Bridge, Router
System Capabilities Enabled	Bridge, Router
Management Address	192.168.1.2 (IPv4)

Port	Port Desc	Port ID	Trunk
1	Ethernet Port on unit 1, port 1	00-17-2E-0F-E2-A1	
2	Ethernet Port on unit 1, port 2	00-17-2E-0F-E2-A2	
3	Ethernet Port on unit 1, port 3	00-17-2E-0F-E2-A3	
4	Ethernet Port on unit 1, port 4	00-17-2E-0F-E2-A4	
5	Ethernet Port on unit 1, port 5	00-17-2E-0F-E2-A5	

LLDP のローカルデバイス情報を表示（Port）

LLDP Port Remote Device Information

Local Port	Chassis ID	Port ID	Port Name	System Name
1	00-01-02-03-04-05	00-01-02-03-04-06	Ethernet Port on unit 1, port 1	

3.10.15 LLDP リモートポート情報の表示

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

設定・表示項目

ポート

Local Port

リモート LLDP 対応の装置が取り付けられているローカルポート

attached.

Chassis ID

このシステムの特定のシャーシの指定された識別子を示す、8 進数ストリング

Port ID

ポート識別子

System Name

システムの管理上に割り当てられた名前を示すストリング

ポート詳細

Local Port

リモート LLDP 対応の装置が取り付けられているローカルポート

Chassis Type

送信 LLDP エージェントと関連付けられる IEEE802 LAN エンティティを含むシャーシを識別します。シャーシを識別し、コンポーネントのタイプを示すために使用されるシャーシ ID サブタイプが、シャーシ ID フィールドに参照されるためにはいくつかの方法があります。(P144 「シャーシ ID サブタイプ」を参照)

Chassis ID

このシステムの特定のシャーシの指定された識別子を示す、8 進数ストリング。

System Name

システムの管理上に割り当てられた名前を示すストリング。

System Description

ネットワークエンティティの記述。

Port Type

ポート ID フィールドでリストされる識別子を基礎に示します。

ポート ID **サブタイプ**

ID Basis	Reference
Interface alias	IfAlias （IETF RFC 2863）
Chassis component	entPhysClass **が** 'chassis(3)' **の値を持つ時に** EntPhysicalAlias (IETF RFC 2737)
Port alias	entPhysicalClass **が** 'port(10)' **または** 'backplane(4)' **を持つ時は** EntPhysicalAlias(IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	**ネットワークアドレス**
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	**エージェントサーキット** (IETF RFC 3046)
Locally assigned	**ローカルに割り当てられる**

Port Description

ポートの説明。RFC 2863 **が実装されている場合、**ifDescr **オブジェクトがこのフィールドに使用されます。**

Port ID

ポート識別子。

System Capabilities Supported

システムのプライマリファンクションを定義するケイパビリティ (P144 **「システム性能」を参照**)

System Capabilities Enabled

現在有効になっているシステムのプライマリファンクション。(P144 **「システム性能」を参照**)

Management Address List

このデバイスの管理アドレス。一般的には、レイヤ 3 **デバイスに結び付けられる多くの異なるアドレスが存在するため、個々の** LLDP PDU **は** 1 **つ以上の管理アドレス** TLV **を含みます。**
マネージメントアドレスが利用可能でない場合、アドレスは CPU **またはポートのためにこのアドバタイズメントを送信します。**

ポート詳細（802.1 拡張情報）

Remote Port VID

ポートのデフォルト VLAN **識別子（**PVID**）は** VLAN **がタグ無しまたはプライオリティタグフレームが割り当てられているかを示します。**

Remote Port-Protocol VLAN List

このインタフェースに設定されているポートベースおよびプロトコルベース VLAN**。**

Remote VLAN Name List

ポートに関連付けられる VLAN **名。**

Remote Protocol Identity List

ポートを通過してアクセス可能な特定のプロトコルの情報。

ポート詳細（802.3 拡張情報）

Remote Port Auto-Neg Supported

所定のポート（リモートシステムに関連付けられた）がオートネゴシエーションをサポートするか否かを示します。

Remote Port Auto-Neg Adv-Capability

リモートシステムのポートに関連付けられた IfMauAutoNegCapAdvertisedBits **オブジェクトの値（ビットマップ）（**IETF RFC 3636 **で定義）**

リモートポートオートネゴシエーションアドバタイズドキャパビリティ

Bit	Reference
0	**その他または未知**
1	10BASE-T half duplex mode
2	10BASE-T full duplex mode
3	100BASE-T4
4	100BASE-TX half duplex mode
5	100BASE-TX full duplex mode
6	100BASE-T2 half duplex mode
7	100BASE-T2 full duplex mode
8	PAUSE for full-duplex links
9	Asymmetric PAUSE for full-duplex links
10	Symmetric PAUSE for full-duplex links
11	Asymmetric and Symmetric PAUSE for full-duplex links
12	1000BASE-X, -LX, -SX, -CX half duplex mode
13	1000BASE-X, -LX, -SX, -CX full duplex mode
14	1000BASE-T half duplex mode
15	1000BASE-T full duplex mode

Remote Port Auto-Neg Status

リモートシステムに関連付けられたポートでオートネゴシエーションが有効か否かを表示。

Remote Port MAU Type

送信デバイスの稼動している MAU **タイプを示す整数値。このオブジェクトは** IETF RFC 3636 **にリストされた** dot3MauType **に対応するリストポジションから得られる整数値を含み、それぞれの** dot3MauType OID **の最後の数と等しいです。**

ポート詳細（802.3 拡張パワー情報）

Remote Power Class

リモートシステムに関連付けられる所定のポートのポートクラス (PSE - Power Sourcing Equipment **または** PD - Powered Device)

Remote Power MDI Status

リモートシステムに関連付けられる所定のポートで MDI **パワーが有効か否かを表示**

Remote Power Pairs

"Signal" **は信号ペアのみ使用されていることを意味します。**"Spare" **は予備のペアのみしようされていることを意味します。**

Remote Power MDI Supported

リモートシステムに関連付けられた所定のポートに、MDI パワーがサポートされているか否かを表示します。

Remote Power Pair Controlable

ペアセレクションがリモートシステムに関連付けられた所定のポートの sourcing power でコントロール可能か否かを示します。

Remote Power Classification

LAN ネットワーク上の異なるパワーターミナルを電力消費量に従いタグを使用することで分類します。IP 電話のようなデバイス、WLAN アクセスポイント、その他はそれらの必要電力条件によって分類されます。

ポート詳細（802.3 拡張トランク情報）

Remote Link Aggregation Capable

リモートポートがリンクアグリゲーション状態にあるか否か、またはリンクアグリゲーションをサポートしているかいないかを表示。

Remote Link Aggregation Enable

リンクの現在のアグリゲーション状態。

Remote Link Aggregation Port ID

リモートシステムに関連付けられたポートコンポーネントの ifIndex の ifNumber から得られた IEEE 802.3 aggregated port identifier、aAggPortID (IEEE 802.3-2002, 30.7.2.1.1) を含みます。リモートポートがリンクアグリゲーション状態に無いかサポートしていない場合、この値は 0 になります。

設定方法

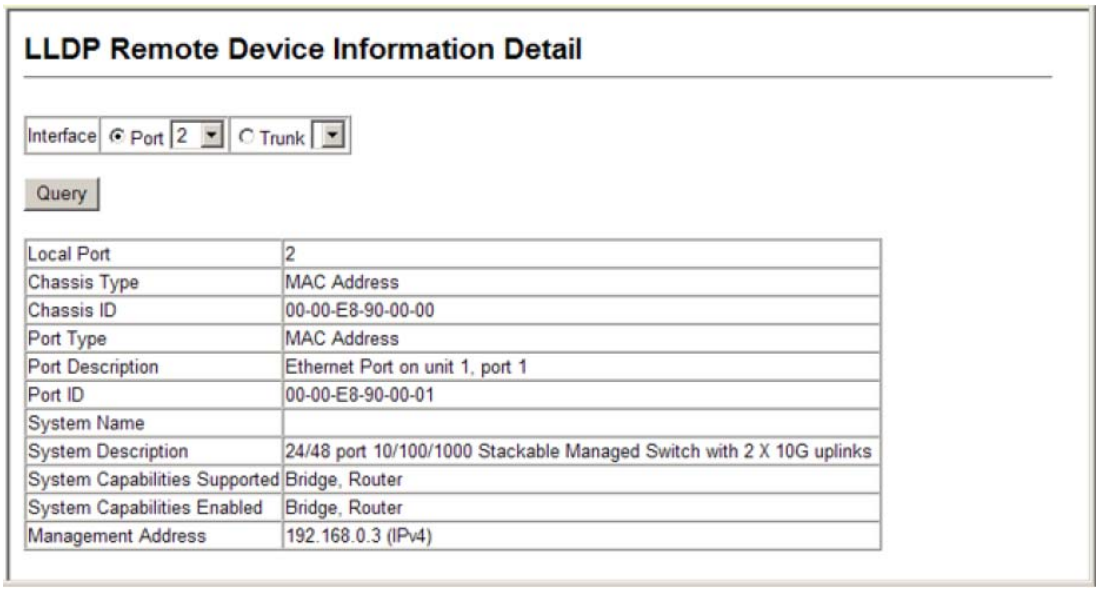
LLDP のリモートデバイス情報を表示（Port）

（1）[Administration] → [LLDP] をクリックします。

（2）「Step」リストから「Remote Device Information」を選択します。

（3）“Port“、"Port Details"、"Trunk"、"Trunk Details" からいずれかを選択します。

（4）＜ Apply ＞をクリックします。



3.10.16 デバイス統計値の表示

LAdministration > LLDP (Show Device Statistics) ページを使用し、このスイッチに接続されている LLDP が有効なすべてのデバイスの統計を表示します。

設定・表示項目

リモートデバイスの概要統計値

Neighbor Entries List Last Updated

LLDP 隣接エントリリストが最後に更新された時。

New Neighbor Entries Count

リモート TTL の期限が切れていない LLDP 隣接の数。

Neighbor Entries Deleted Count

なんらかの理由で、LLDP リモートシステム MIB から取り除かれた LLDP 隣接の数。

Neighbor Entries Dropped Count

リソース不足のために、スイッチ上のリモートデータベースが LLDP DU をドロップした時間数

Neighbor Entries Age-out Count

TTL タイマーの期限切れが原因で、近隣の情報が LLDP リモートシステム MIB から削除された時間数。

ポート / トランク

Frames Discarded

特定の TLV に定義された指定の使用ルールに加え、通常の承認規則に準じずに破棄されたフレーム数。

Frames Invalid

全ての LLDPDU の 1 つまたはそれ以上で探知可能なエラーの数。

Frames Received

受信された LLDP PDU。

Frames Sent

送信された LLDP PDU。

TLVs Unrecognized

受信された LLDP ローカルエージェントによって認識されない全ての TLV の数。

TLVs Discarded

受信され、メモリ不足、アウトオブシーケンスまたはその他の理由で破棄された全ての LLDPDU の数

Neighbor Ageouts

TTL タイマの期限切れが理由で、近隣情報が LLDP リモートシステム MIB から削除された時間。

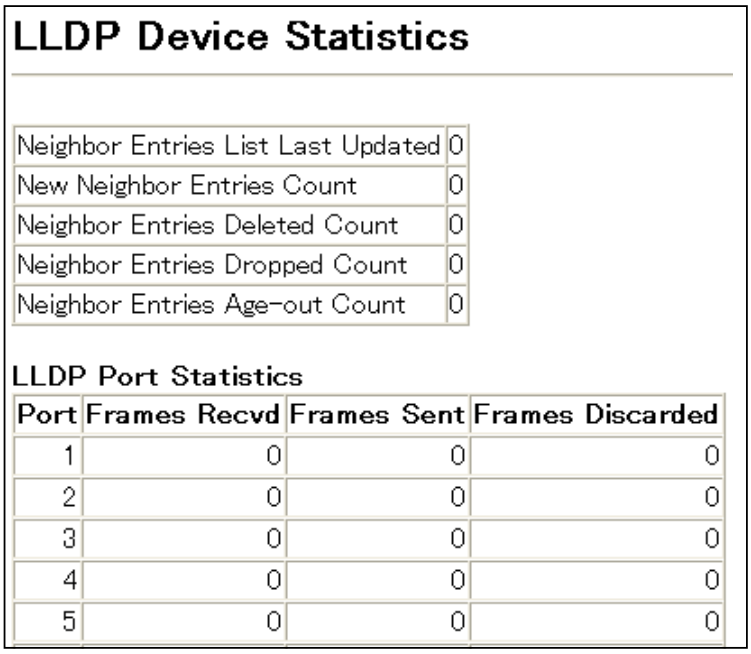
設定方法

LLDP デバイス統計値の表示（General）

（1）[Administration] → [LLDP] をクリックします。

（2）「Step」リストから「Show Device Statistics」を選択します。

（3）“General“、“Port“、“Trunk” からいずれかを選択します。



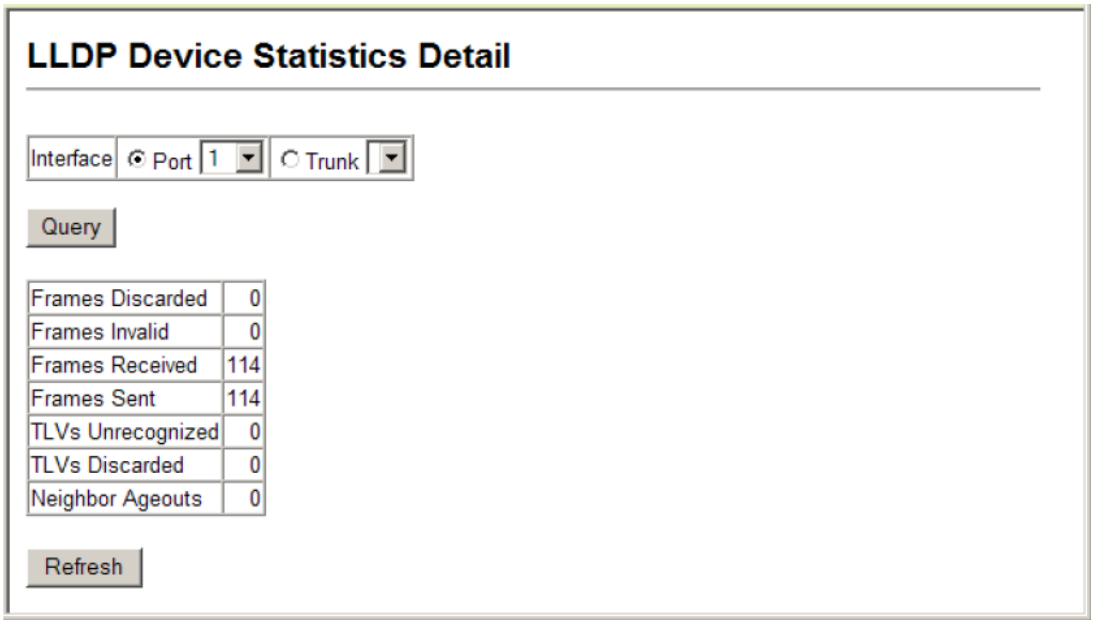
LLDP Device Statistics

Neighbor Entries List Last Updated	0
New Neighbor Entries Count	0
Neighbor Entries Deleted Count	0
Neighbor Entries Dropped Count	0
Neighbor Entries Age-out Count	0

LLDP Port Statistics

Port	Frames Recvd	Frames Sent	Frames Discarded
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0

LLDP デバイス統計値の表示（Port）



LLDP Device Statistics Detail

Interface ◉ Port 1 ○ Trunk

Query

Frames Discarded	0
Frames Invalid	0
Frames Received	114
Frames Sent	114
TLVs Unrecognized	0
TLVs Discarded	0
Neighbor Ageouts	0

Refresh

3.11 Class of Service（CoS）

Class of Service(CoS) は、ネットワークの混雑状態のために通信がバッファされる場合に、優先するデータパケットを指定することができます。本機では各ポートで 4 段階のキューの CoS をサポートしています。高いプライオリティのキューを持ったデータパケットを、より低いプライオリティのキューを持ったデータパケットよりも先に転送します。各インタフェースにデフォルトプライオリティを設定することができ、又本機のプライオリティキューに対し、フレームプライオリティタグのマッピングを行うことができます。

3.11.1 レイヤ 2 キュー設定

インタフェースへのデフォルトプライオリティの設定

各インタフェースのデフォルトポートプライオリティを指定することが出来ます。スイッチへ入る全てのタグなしパケットは指定されたデフォルトポートプライオリティによりタグが付けられ、出力ポートでの適切なプライオリティキューが設定されます。

機能解説

- 本機は各ポートで 4 つのプライオリティキューを提供します。head-of-queue blockage を防止するために重み付けラウンドロビン (WRR) を使用します。
- デフォルトプライオリティは、"accept all frame type" に設定されたポートで受信したタグなしフレームの場合に適用されます。このプライオリティは IEEE 802.1Q VLAN タグ付フレームに対応していません。受信フレームが IEEE 802.1Q VLAN タグ付フレームの場合、IEEE 802.1Q VLAN User Priority ビットが使用されます。
- 出力ポートが関連 VLAN のタグなしメンバーの場合、これらのフレームは送信前に全ての VLAN タグを外します。

設定・表示項目

Default Priority

各インタフェースの受信されたタグなしフレームに割り当てられるプライオリティ

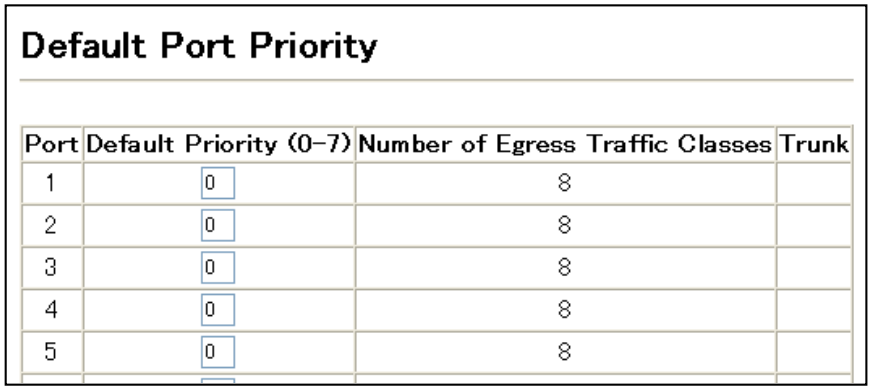
（範囲 :0 - 7、初期設定 :0）

Number of Egress Traffic Classes

各ポートに割り当てられたキューバッファの値

設定方法

[Priority] → [Default Port Priority] 又は [Default Trunk Priority] をクリックします。インタフェースのデフォルトプライオリティを変更し、[Apply] をクリックします。



Egress キューへの CoS 値のマッピング

本機は各ポートの 8 つのプライオリティキューを使用することによる CoS プライオリティタグ付通信の処理を、重み付けラウンドロビン (Weighted Round Robin/WRR) に基づいたサービススケジュールにより行います。
最大 8 つに分けられた通信プライオリティは IEEE802.1p で定められます。デフォルトプライオリティレベルは次の表に記載されている IEEE802.1p の勧告に基づいて割り当てられています。

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

様々なネットワークアプリケーションの IEEE 802.1p 標準で推奨されたプライオリティレベルが以下の表に記載されています。しかし、アプリケーションの通信に対して、自由にアウトプットキューのプライオリティレベルを設定することが可能です。

プライオリティレベル	トラフィックタイプ
1	Background
2	(Spare)
0（初期設定）	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

設定・表示項目

Priority

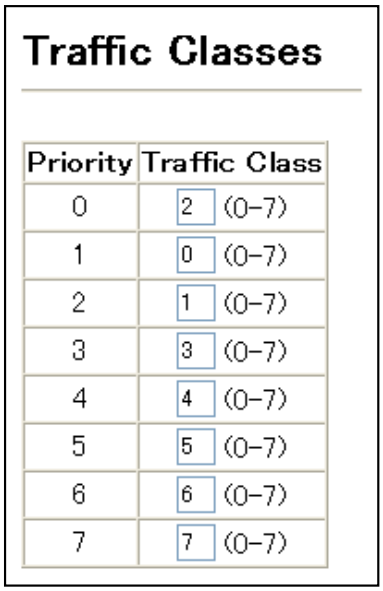
CoS 値（範囲 :0 から 7、7 が最高プライオリティ）

Traffic Class

アウトプットキューバッファ (範囲 :0 から 3、3 が最高 CoS プライオリティキュー)

設定方法

[Priority] → [Traffic Classes] をクリックします。各インタフェースのアウトプットキューへプライオリティ (Traffic Class) を割り当て、[Apply] をクリックします。



キューモードの選択

本機では、すべての高プライオリティキューが低プライオリティキューに優先される strict ルール、又は各キューの重み付けを行う Weighted Round-Robin (WRR) を用いてキューイングを行います。WRR では、あらかじめ設定した重みに応じて各キューの転送時間の割合を決定します。それにより、Strict ルールにより生じる HOL Blocking を防ぐことができます（初期設定では WRR に設定されています）

設定・表示項目

WRR

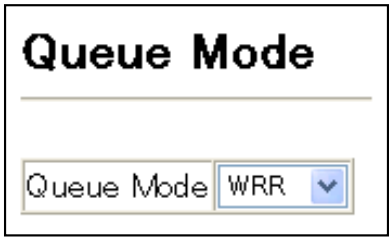
Weighted Round-Robin ではイングレスポートの帯域を それぞれの 0-3 のキューに対して 1, 2, 4, , 8 のスケジューリングウェイトを設定し共有します。

Strict

イングレスキューを順次処理します。すべての高プライオリティキューのトラフィックが低プライオリティキューのトラフィックより優先的に処理されます

設定方法

[Priority] → [Queue Mode] をクリックします。Strict 又は WRR を選択し、[Apply] をクリックします。



トラフッククラスのサービスウェイト設定

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。P155 「Egress キューへの CoS 値のマッピング」に記載されているように、トラフィッククラスは各ポートに供給された 8 つの Egress キューのうちの一つにマッピングされます。これらのキューと対応しているトラフィックプライオリティのそれぞれへのウェイトを割り当てることができます。このウェイトは、各キューがサービスに登録され、それにより、特定のプライオリティ値に応じたソフトウェア・アプリケーション毎のレスポンス時間に影響する頻度が設定されます。

設定・表示項目

WRR Setting Table

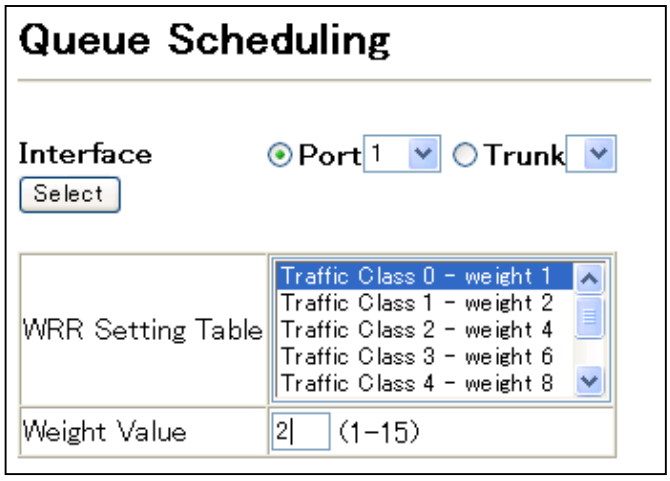
各トラフィッククラス（キュー）のウェイトの値を表します。

Weight Value

選択されたトラフィッククラスの新しいウェイトを設定します。(範囲 :1-15)

設定方法

[Priority] → [Queue Scheduling] をクリックします。インタフェースを選択し、トラフィッククラスを選択します。ウェイト値を入力後、[Apply] をクリックします。



3.11.2 レイヤ 3/4 プライオリティの設定

CoS 値へのレイヤ 3/4 プライオリティのマッピング

本機はアプリケーションの要求を満たすため、レイヤ 3/4 プライオリティをサポートしています。通信プライオリティは Type of Service (ToS) オクテットのプライオリティビットや TCP ポート番号を使用しフレームの IP ヘッダで指定します。プライオリティビットを使用する場合、ToS オクテットは Differentiated Services Code Point(DSCP) サービスの 6 ビットを使用します。これらのサービスが有効な時、プライオリティは CoS 値へマッピングされ、該当する出力キューへ送られます。

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

- プライオリティマッピングの優先順位は IP ポートプライオリティ、IP Precedence または DSCP プライオリティ、デフォルトポートプライオリティの順番となります。
- IP Precedence と DSCP プライオリティを両方共有効にすることはできません。どちらか一方を有効にすると、もう一方は自動的に無効になります。

IP Precedence/DSCP プライオリティの選択

IP Precedence または DSCP プライオリティのどちらかを有効にすることができます。

設定・表示項目

Disabled

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。DSCP Priority Status メニューから Enabled にチェックを入れます。その後［Apply］をクリックします。

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

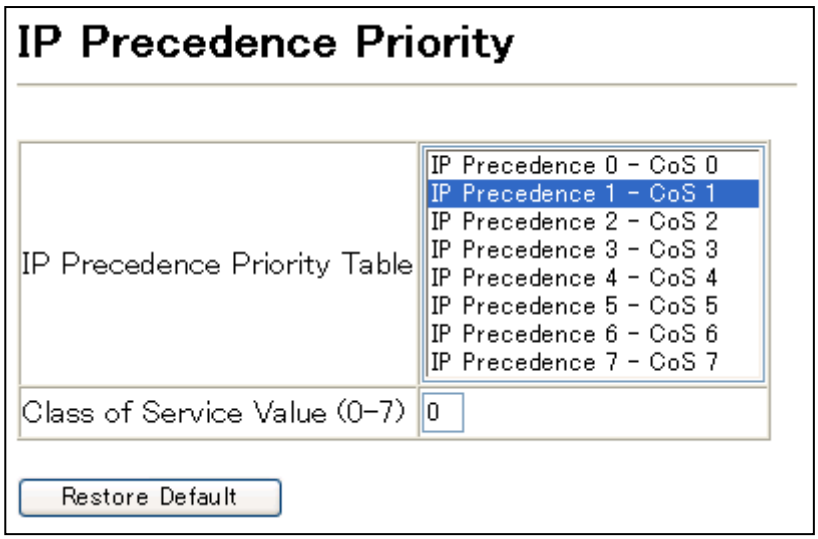
CoS 値と各 IP Precedence 値 の相関マップを表示します。

Class of Service Value

選択された IP Precedence 値へ CoS 値をマッピングします。"0" が低いプライオリティ、"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 値を入力し［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。指定されていない全ての DSCP 値は CoS 値 0 にマッピングされます：

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

設定・表示項目

DSCP Priority Table

CoS 値と各 DSCP プライオリティの相関マップを表示します。

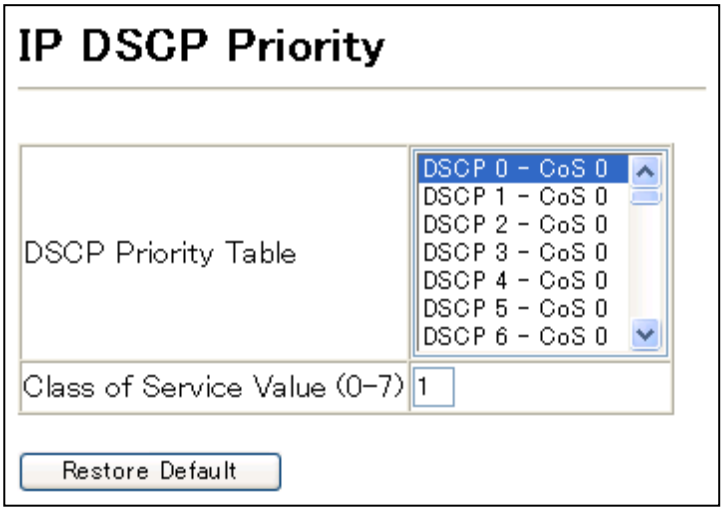
Class of Service Value

選択された DSCP プライオリティ値へ CoS 値をマッピングします。"0" が低いプライオリティ、"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 Priority 値を選択し、Class of Service Value 値を入力し［Apply］をクリックします。



IP ポートプライオリティのマッピング

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

設定・表示項目

IP Port Priority Status

IP ポートプライオリティの有効 / 無効

IP Port Priority Table

CoS 値と各 IP ポート番号との相関マップを表示します

IP Port Number (TCP/UDP)

IP ポート番号を設定します。

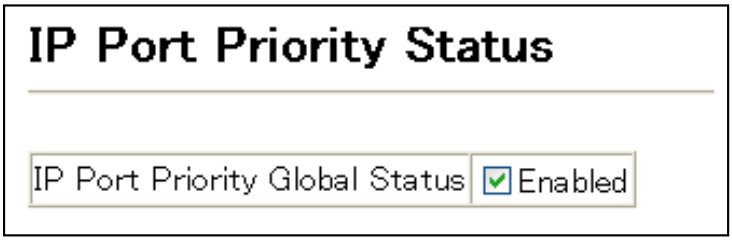
Class of Service Value

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

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

設定方法

[Priority] → [IP Port Status] をクリックします。



3.12 Quality of Service

3.12.1 Quality of Service の設定

ここで記載されているコマンドは QoS(Quality of Service) 機能の基準とサービスポリシーを構成するために使用されます。DiffServ(Differentiated Services) 機能は、ネットワーク上を流れるフレームの 1 つの単位を特定のトラフィックの要件に合致させるため、ネットワークリソースを優先する管理機能を提供します。それぞれのパケットはアクセスリスト、IP Precedence、DSCP、VLAN リストをベースにしたネットワークの中のエントリによって分類されます。アクセスリストを使用することにより、それぞれのパケットが含んでいるレイヤ 2 ～ 4 の情報を元にトラフィックの選別を許可します。設定されたネットワークポリシーをベースにして、異なる種類のトラフィックに対し、異なる種類の転送のためにマークを付けることができます。

インターネットにアクセスするすべてのスイッチとルーターは、同じクラスのパケットには同じ方向への転送を行うためにクラス情報を使用します。クラス情報は、経路の終端のホスト、スイッチ、ルーターのいずれかから割り当てられます。そして、優先度は一般的なポリシー、もしくはパケット詳細調査によって割り当てられます。しかし、パケットの詳細調査はコアスイッチとルーターに負荷がかかり過ぎないようにするため、ネットワークのエッジ側に近いところで行われる必要があります。

経路に属するスイッチとルーターは、異なるクラスにリソースの割り当ての優先順位をつけるため、クラス情報を使用することができます。個々のデバイスが DiffServ 機能に基づいてトラフィックを扱う方法は、Per-Hop Behavior と呼ばれます。経路に属するすべてのデバイスは、エンド・トゥ・エンドの QoS ソリューションを構成するために矛盾のない方法で設定されます。

[注意] クラスマップごとに最大 16 個のルールを設定することができます。ポリシーマップには複数のクラスを設定することもできます。

[注意] ポリシーマップを作成する前にクラスマップを作成してください。作成しない場合、ポリシールールの設定画面からクラスマップを選択することはできません。

QoS パラメータの設定

特定のカテゴリや入力トラフィックのためのサービスポリシーを作成するには、下のステップを実施してください。

(1) Class Map を使用して、トラフィックの特定のカテゴリにクラスの名前を設定します。

(2) アクセスリスト、DSCP、IP Precedence の値、VLAN に基づいてトラフィックの種類を指定するために、それぞれのクラスのルールを編集します。

(3) Policy Map を使用して、入力トラフィックを取り扱う特定の方法のポリシーの名前を設定します。

(4) ポリシーマップに 1 つ、もしくはそれ以上のクラスを追加します。トラフィックに合致するクラスに QoS の値を割り当てるため、setting 画面でそれぞれのクラスにルールを割り当てます。ポリシールールはフローレートとバーストレートの平均の監視、特定のレートを超えたトラフィックの破棄、特定のレートを超えたトラフィックの DSCP サービスレベルを減らすよう構成できます。

(5) Service Policy を使用して、特定のインターフェースにポリシーマップを割り当てます。

クラスマップの設定

- クラスマップは以下の手順で設定します。
  - Class Map ページを開き、[Add Class] をクリックします。
  - Class Configuration ページが開きます。“Class Name” フィールドへ入力し、[Add] をクリックします。
  - Match Class Settings ページが開きます。アクセスリスト、DSCP または IP Precedence 値に基づき、このクラスのトラフィックタイプを指定し、選択したトラフィック基準の隣の [Add] ボタンをクリックします。
    入力トラフィックをクラスマップに割り当てる際、最大 16 項目を指定することが可能です。
- クラスマップはポリシーマップ（P165）と共にサービスポリシー（P168）を作成する為に使用されます。
  1 つ以上のクラスマップをポリシーマップへ割り当てることが可能です。

設定・表示項目

Class Map

Modify Name and Description

クラスマップの名前と簡単な説明を設定（範囲：name-1-16 文字、Description-1-64 文字）

Edit Rules

Match Class Settings ページを開きます。

Add Class

Class Configurationn ページを開きます。

Remove Class

選択したクラスを削除します。

Class Configuration

Class Name

クラスマップ名（範囲：1-16 文字、）

Type

タイプを指定します。

Description

クラスマップの簡単な説明（範囲：1-64 文字）

Add

指定したクラスを追加します。

Back

前のページに戻ります。

Match Class Settings

Class Name

クラスマップ名（範囲：1-16 文字）

ACL List

ACL リスト名（範囲：1-16 文字）

IP DSCP

IP DSCP **値（範囲：**0-63 **文字）**

IP Precedence

IP Precedence **値（範囲：**0-7 **文字）**

VLAN

VLAN（**範囲：**1-4094）

Add

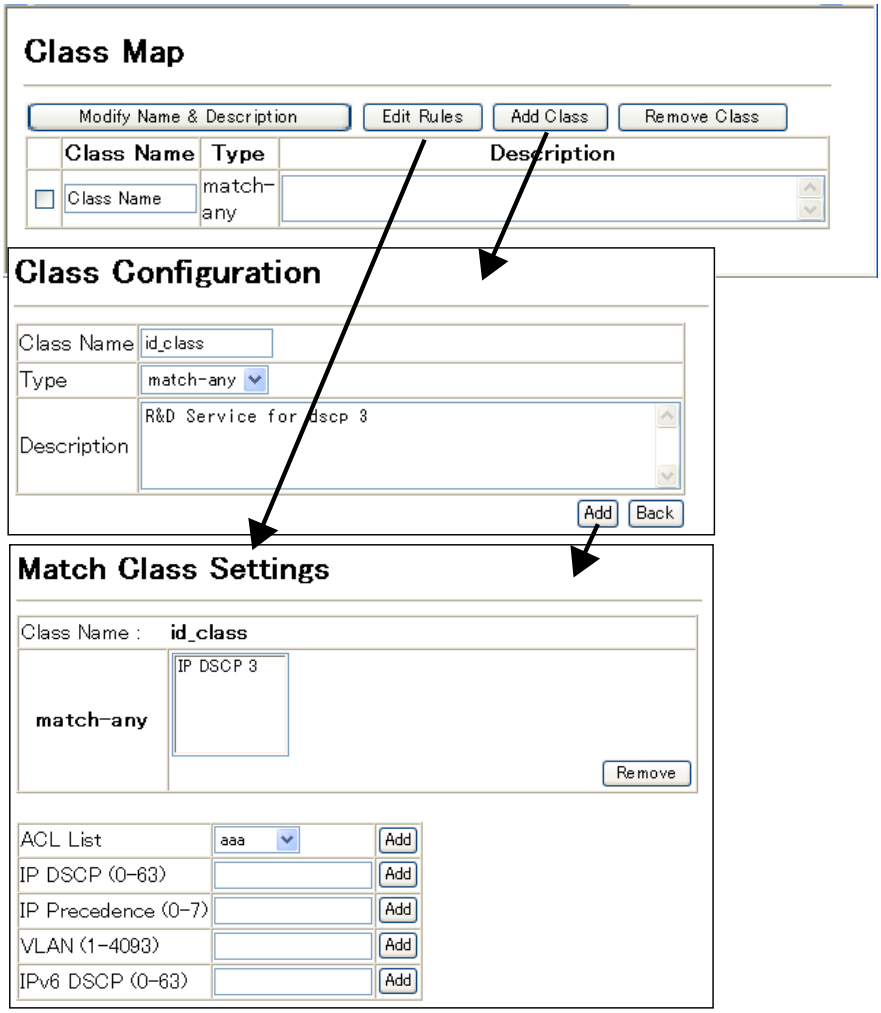
クラスマップに追加します。１つのクラスにつき、最大 16 **個まで登録できます。**

Remove

選択した基準をクラスから削除します。

設定方法

[QoS] → [DiffServ] → [Class Map] **をクリックします。**[Add Class] **をクリックし、新しいクラスを作成するか、**[Edit Rules] **をクリックし、既存のクラスのルールを編集します。**



QoS ポリシーの作成

この機能は複数のインターフェースに結び付けられたポリシーマップを作成します。
ポリシーマップの設定手順

（1）クラスマップを作成します（P163 「クラスマップの設定」参照）

（2）Policy Map ページを開き、「Add Policy」をクリックします。

（3）「Policy Configuration」ページで「Policy Name」を入力し「Add」をクリックしてください。

（4）「Policy Rule Settings」ページが開きます。スクロールダウンリスト（Class Name の下）からクラス名を選択します。受信した IP パケットの QoS の設定（Action 欄）、最大スループットとバーストレートの設定（Meter 欄）、ポリシーに反するパケットの取り扱い設定（Exceed 欄）で、このクラスの条件に合致したトラフィックのポリシーを構成します。最後に Add をクリックして新しいポリシーを登録します。

- ポリシーマップには複数のクラス設定が含まれています。インターフェースへのポリシーの設定は Service Policy Settings 画面で行います（P154 参照）。それぞれのアクセスリスト（MAC ACL、Standard ACL、Extend ACL）に最大 64 個のポリシーを構成することができます。また、ポリシーマップに適用できるクラスの最大数は 16 個です。
- ポリシングはトークンバケットを基にしています。バケットの深さ（バケットがオーバーフローする前の最大バーストレート）は Burst 欄で指定します。またバケットから移動するトークンの平均レートは Rate 欄で指定します。
- パケットのクラス分け、サービスタグ、帯域幅のポリシーを定義してポリシーマップを作成した後、設定を反映させるため Service Policy 画面で特定のインターフェースにポリシーマップを割り当ててください。

設定・表示項目

Policy Map

Modify Name and Description

ポリシーマップの名前と簡単な説明を設定（範囲：name-1-16 文字、Description-1-64 文字）

Edit Classes

選択したクラスの Policy Rule Settings 画面を開きます。この画面で入力トラフィックへの条件を設定します。

Add Policy

Policy Configuration 画面を開きます。この画面でポリシーの名前と概要を入力し、Add をクリックして Policy Rule Settings 画面を開きます。ここで入力されるトラフィックへの条件を設定します。

Remove Policy

選択したポリシーを削除します。

Policy Configurataion

Policy Name

ポリシー名（範囲：1-16 **文字、）**

Description

ポリシーマップの簡単な説明（範囲：1-64 **文字）**

Add

指定したポリシーを追加します。

Back

ポリシーを追加せず前のページに戻る。

Policy Rule Settings

- Class Settings -

Class Name

クラスマップ名

Action

条件に合致するパケットに適用する CoS、DSCP、IP Precedence **の値。**

Meter

最大スループットとバーストレート

- Rate(kbps) - 1 **秒あたりの転送レート**
- Burst(byte) - **バーストレート**

Exceed Action

特定のレートを超えたトラフィックの破棄、または DSCP **サービスレベルを減らすかを指定します。**

Remove Class

クラスを削除します。

- Policy Options -

Class Name

クラスマップ名

Action

条件に合致するパケットに CoS、IP DSCP **を設定。**

（範囲：CoS-0-7、DSCP-0-63）

Meter

最大スループット / バーストレート

- Rate(kbps) - 1 **秒あたりの転送レート（範囲：**1-100000kbps **または最大ポート速度）**
- Burst(byte) - **バーストレート（範囲：**64-1522）

Exceed

指定したレート / バースト値を超えたトラフィックの処理

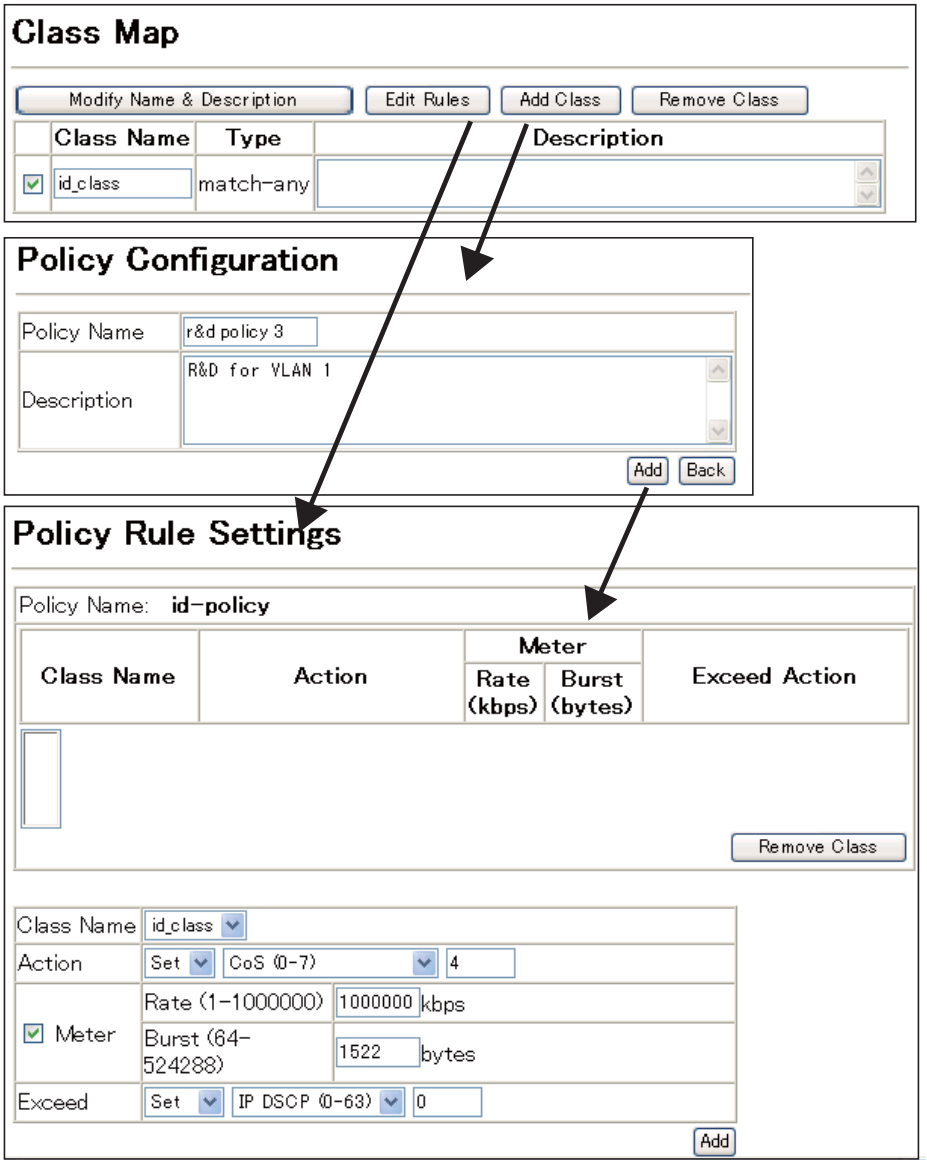
- Drop - **条件に一致しないトラフィックを破棄する**

Add

ポリシーマップに設定した条件を追加。

設定方法

[QoS] → [DiffServ] → [Policy Map] をクリックます。



イングレスキューへのポリシーマップ適用

ポリシーマップをインタフェースの入力キューへ適用します。

設定方法

- 始めにクラスマップの定義を行ってください。その後、ポリシーマップの定義を行い、最後にサービスポリシーをインタフェースへ適用します。
- 一つのインタフェースに一つのポリシーをバインド可能です。
- 現在のファームウェアは、ポリシーマップの出力キューへの適用をサポートしていません。

設定・表示項目

Port

ポートを指定。

Ingress

入力トラフィックへルールを適用します。

Enabled

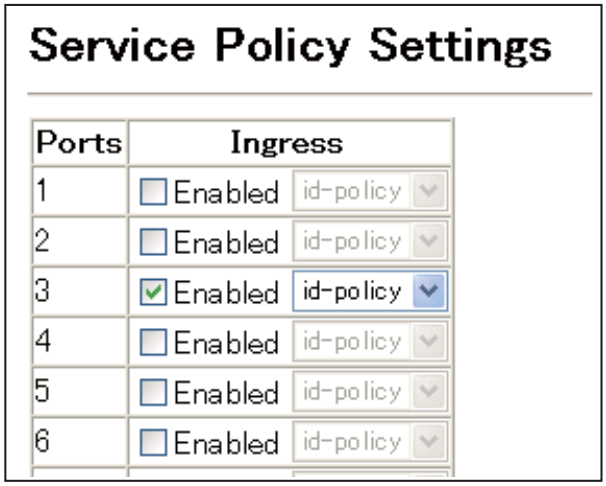
指定したポートでポリシーマップを有効にします。

Policy Map

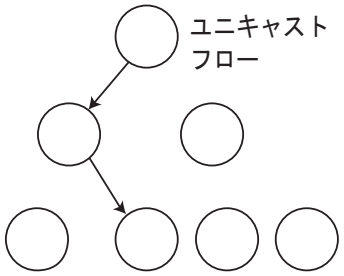
スクロールダウンボックスからポリシーマップを選択。

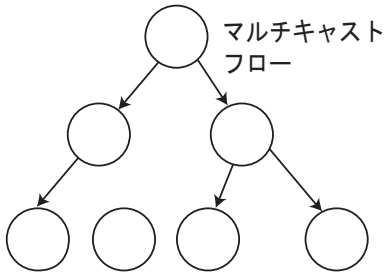
設定方法

[QoS] → [DiffServ] → [Service Policy Settings] をクリックします。



3.13 マルチキャストフィルタリング





マルチキャストはビデオカンファレンスやストリーミングなどのリアルタイムアプリケーションの動作をサポートします。マルチキャストサーバは各クライアントに対し異なるコネクションを確立することができません。ネットワークにブロードキャストを行うサービスとなり、マルチキャストを必要とするホストは接続されているマルチキャストサーバ / ルータと共に登録されます。また、この方法はマルチキャストサーバによりネットワークのオーバヘッドを削減します。ブロードキャストトラフィックは各マルチキャストスイッチ / ルータによって本サービスに加入しているホストにのみ転送されるよう処理されます。

本機では接続されるホストがマルチキャストサービスを必要とするか IGMP (Internet Group Management Protocol) のクエリを使用します。サービスに参加を要求しているホストを含むポートを特定し、そのポートにのみデータを送ります。また、マルチキャストサービスを受信しつづけるためにサービスリクエストを隣接するマルチキャストスイッチ / ルータに広めます。この機能をマルチキャストフィルタリングと呼びます。

IP マルチキャストフィルタリングの目的は、スイッチのネットワークパフォーマンスを最適化し、マルチキャストパケットをマルチキャストグループホスト又はマルチキャストルータ / スイッチに接続されたポートのみに転送し、サブネット内の全てのポートにフラッディングするのを防ぎます。

3.13.1 レイヤ 2 IGMP（Snooping and Query）

IGMP Snooping and Query －マルチキャストルーティングがネットワーク上の他の機器でサポートされていない場合、IGMP Snooping 及び Query を利用し、マルチキャストクライアントとサーバ間での IGMP サービスリクエストの通過を監視し、動的にマルチキャストトラフィックを転送するポートの設定を行なうことができます。

静的 IGMP ルータインタフェース－ IGMP Snooping が IGMP クエリアを検索できない場合、手動で IGMP クエリア（マルチキャストルータ / スイッチ）に接続された本機のインタフェースの指定を行なうことができます。その後、指定したインタフェースは接続されたルータ / スイッチのすべてのマルチキャストグループに参加し、マルチキャストトラフィックは本機内の適切なインタフェースに転送されます。

静的 IGMP ホストインタフェース－確実にコントロールする必要のあるマルチキャストアプリケーションに対しては、特定のポートに対して手動でマルチキャストサービスを指定することができます。（P176 参照）

IGMP Snooping Query パラメータの設定

マルチキャストトラフィックの転送設定を行います。

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

機能解説

- IGMP Snooping — 本機は、IGMP クエリの snoop を受け、リポートパケットを IP マルチキャストルータ / スイッチ間で転送し、IP マルチキャストホストグループを IP マルチキャストグループメンバーに設定します。IGMP パケットの通過を監視し、グループ登録情報を検知し、それに従ってマルチキャストフィルタの設定を行います。
- IGMP Query — ルータ又はマルチキャスト対応スイッチは、定期的にホストに対しマルチキャストトラフィックが必要かどうかを質問します。もしその LAN 上に 2 つ以上の IP

マルチキャストルータ / スイッチが存在した場合、1 つのデバイスが " クエリア " となります。その後、マルチキャストサービスを受け続けるために接続されたマルチキャストスイッチ / ルータに対しサービスリクエストを広げます。

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

設定・表示項目

IGMP Status

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

（初期設定 : 有効 (Enabled)）

Act as IGMP Querier

有効にした場合、本機はクエリアとして機能し、ホストに対しマルチキャストトラフィックが必要かを聞きます。

（初期設定 : 有効 (Enabled)）

IGMP Query Count

応答を受けて、レポートの要求を開始するまで送信するクエリの最大数を入力します。

（2-10、初期設定 :2）

IGMP Query Interval

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

IGMP Report Delay

IP マルチキャストアドレスのレポートをポートで受信してから、IGMP クエリがそのポートから送信され、リストからエントリーが削除されるまでの時間（秒）を設定します（5-25、初期設定 : 10）

IGMP Query Timeout

前のクエリアが停止した後、クエリパケットを受信していたルータポートが無効と判断されるまでの時間（秒）を設定します（300-500、初期設定 :300）

IGMP Version

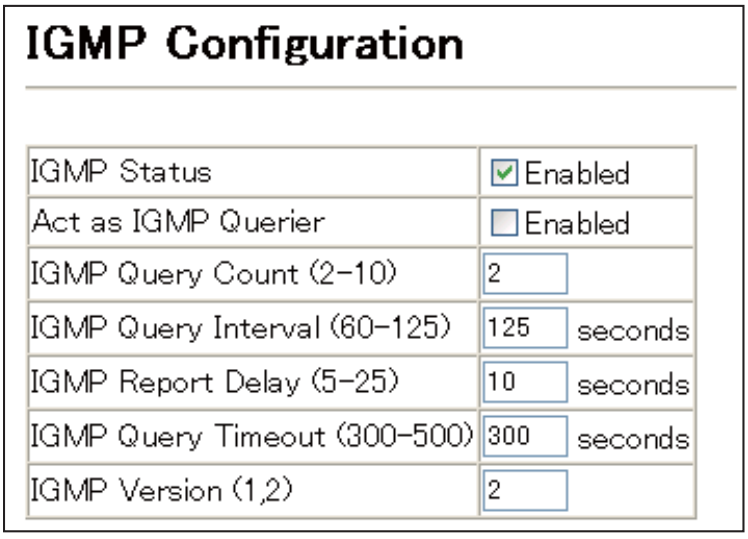
ネットワーク上の他のデバイスと互換性のある IGMP バージョンの設定を行います
（1-2、初期設定 :2）

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

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

設定方法

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



IGMP Immediate Leave（即時脱退機能）の有効

IGMP スヌーピング immediate-leave（即時脱退機能）の有効 / 無効を設定します。
immediate-leave を有効にすることによって、複数のマルチキャスト グループを同時に使用する環境でも、スイッチド ネットワーク上のすべてのホストに対して最適な帯域幅管理を行うことができます。

機能解説

- 即時脱退機能（Immediate leave）を使用しない場合、マルチキャストルータ（またはクエリア）は IGMPv2/v3 group leave メッセージを受信した時、group-specific クエリメッセージを送信します。
  ホストが指定されたタイムアウト時間内にクエリを返さない限り、ルータ / クエリアはこのグループのためのトラフィックの転送を停止します。
  タイムアウトピリオドは " IGMP Query Report Delay"（ "P169 「IGMP Snooping Query パラメータの設定」" を参照）で決定されます。

- 即時脱退機能（Immediate leave）は IGMP スヌーピングが有効の場合のみ動作し、IGMPv2 または IGMP v 3 スヌーピングが使用されます。

- スイッチがマルチキャストルータが接続されていることを学習している場合、即時脱退機能（Immediate leave）はポートに適用されません。

- 即時脱退機能（Immediate leave）はネットワークで、IGMP ホストの追加・離脱リクエストにより頻繁に発生する帯域幅使用を改善できます。

設定・表示項目

VLAN ID

VLAN ID（1-4094）

Immediate Leave

選択した VLAN で、IGMP immediate leave を有効 / 無効（初期設定：無効）

設定方法

[IGMP Snooping] → [IGMP Immediate Leave] をクリックします。

マルチキャストルータに接続されたインタフェースの表示

マルチキャストルータは、IGMP からの情報に加え、インターネットでの IP マルチキャスティングを行うため DVMRP、PIM 等のマルチキャスト・ルーティング・プロトコルを使用します。ルータは、本機により動的に設定されるか、静的にインタフェースの追加を行うことができます。
Multicast Router Port Information ページでは、各 VLAN ID で隣接するマルチキャストルータ / スイッチの接続されたポートを表示します。

設定・表示項目

VLAN ID

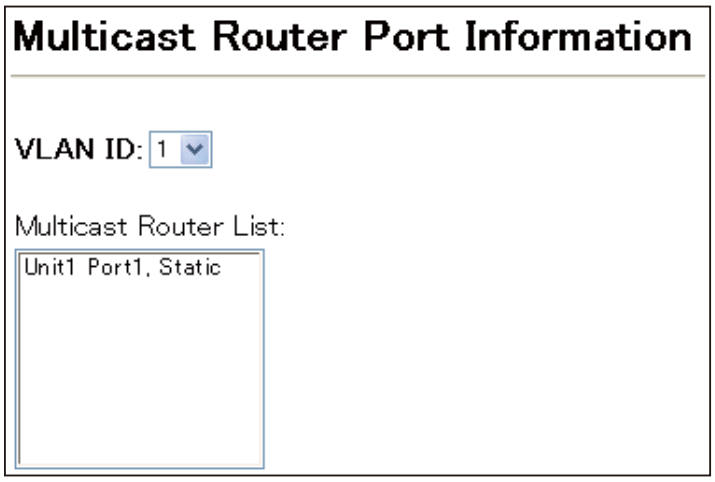
リストを表示させる VLAN ID（1-4094）

Multicast Router List

動的及び静的に設定されたマルチキャストルータの設定情報

設定方法

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



マルチキャストルータに接続するインタフェースの設定

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

設定・表示項目

Interface

ポート (Port) 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

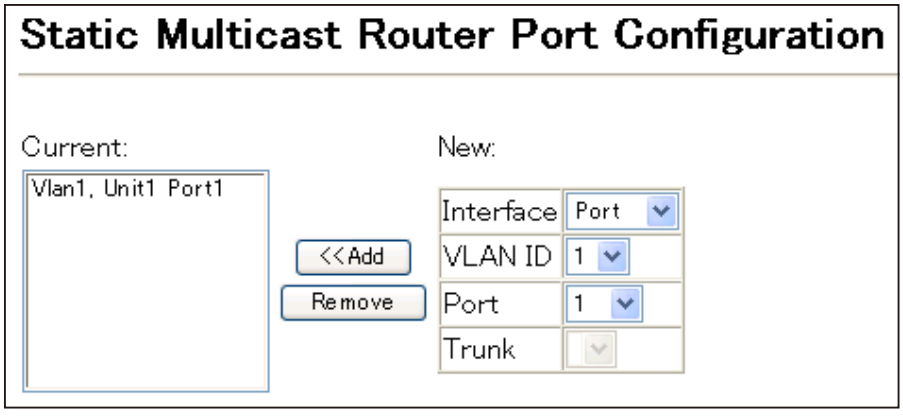
マルチキャストルータ / スイッチから送られるマルチキャストトラフィックを受信し、転送する VLAN を選択します。

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アサイン

マルチキャストフィルタリングは、P169 「IGMP Snooping Query パラメータの設定」の通り、IGMP snooping と IGMP クエリメッセージを使用し、動的に設定することができます。一部のアプリケーションではさらに細かい設定が必要なため、静的にマルチキャストサービスの設定を行う必要があります。同じ VLAN に参加するホストの接続されたすべてのポートを加え、その後 VLAN グループにマルチキャストサービスの設定を行います。

機能解説

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

設定・表示項目

Interface

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

VLAN ID

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

Multicast IP

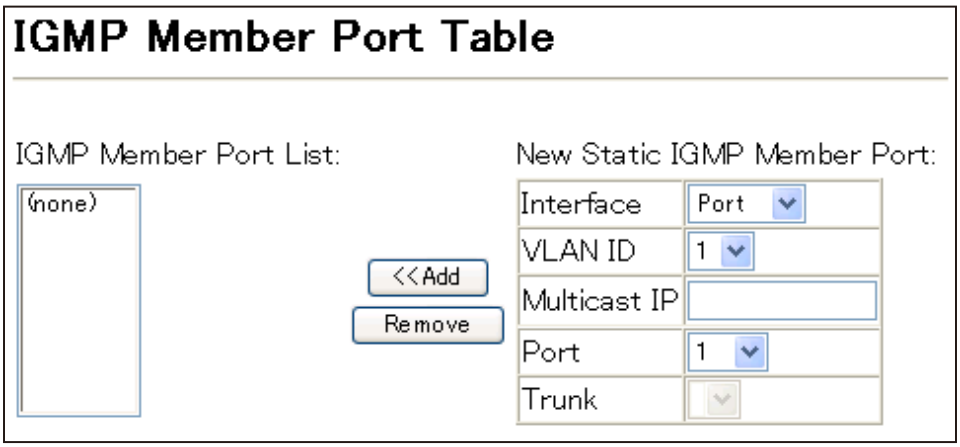
マルチキャストサービスを行う IP アドレスを入力します。

Port 又は Trunk

マルチキャストルータに接続されたインタフェースの番号を指定します。

設定方法

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



3.14 DNS（Domain Name Service）

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

3.14.1 DNS サービスの一般設定

機能解説

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

設定・表示項目

Domain Lookup Status

DNS ホスト名・アドレス変換を有効にします

Default Domain Name

不完全なホスト名に付加するデフォルトドメイン名を指定します

Domain Name List

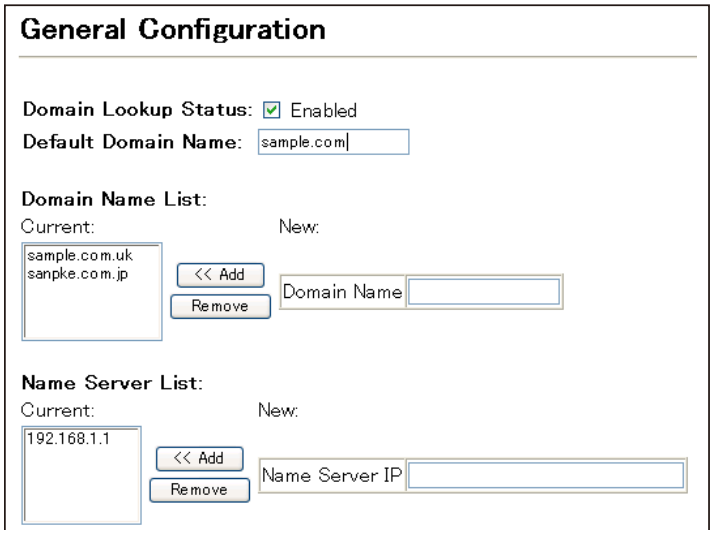
不完全なホスト名に追加するドメイン名のリストを設定します。

Name Server List

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

設定方法

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



3.14.2 静的 DNS ホストのアドレスエントリ

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

機能解説

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

設定・表示項目

Host Name

ホスト名（設定範囲：1-64 文字）

IP Address

IP アドレス（設定範囲：1-8 アドレス）

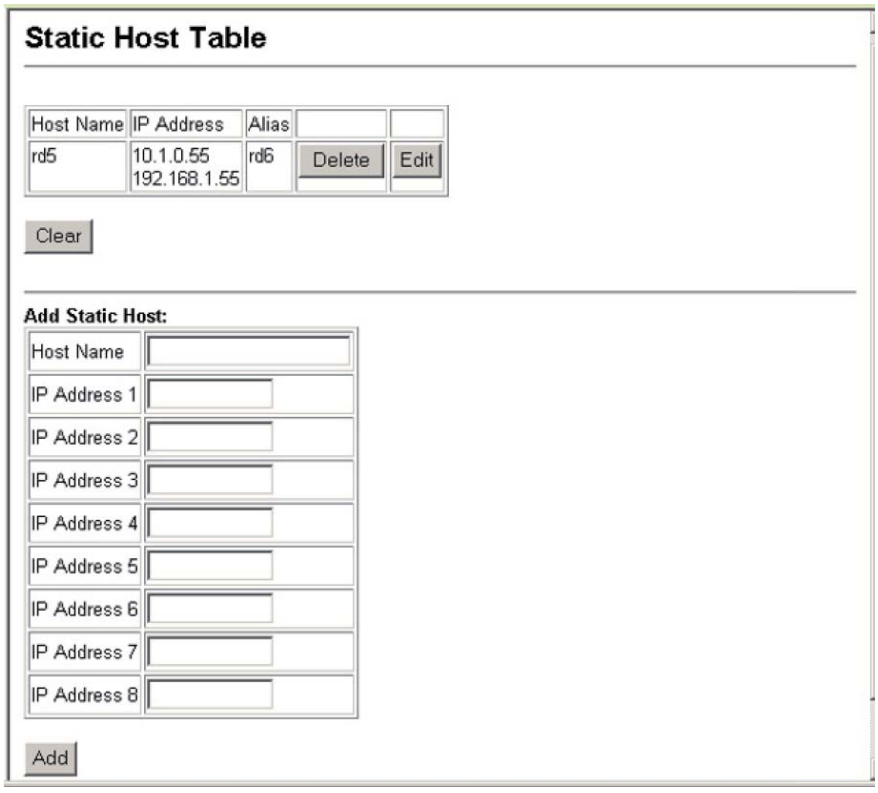
Alias

IP アドレス（設定範囲：1-8 アドレス）

以前に設定されたエントリと同じアドレスにマップされるホスト名を表示

設定方法

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



3.14.3 DNS キャッシュの表示

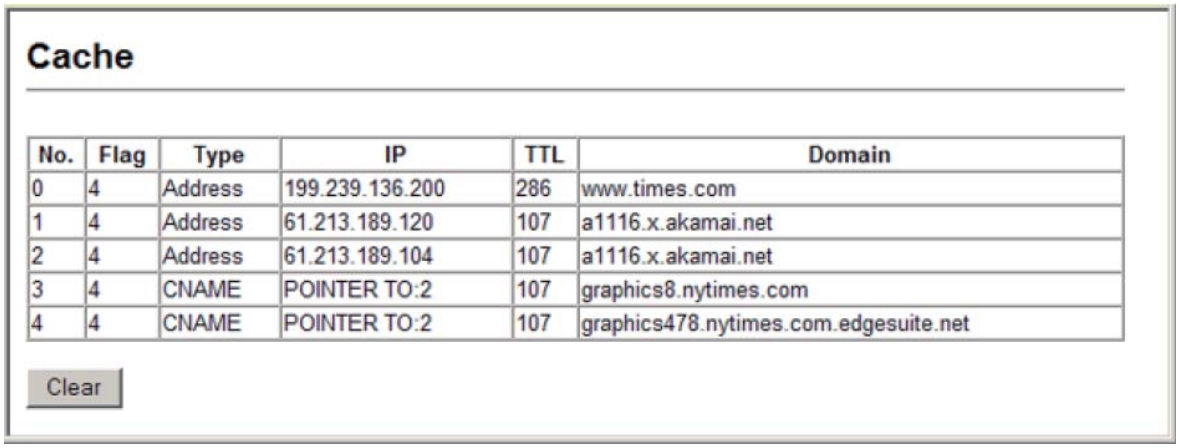
DNS キャッシュの内容を表示します。

設定・表示項目

No
各リソースレコードのエントリ番号
Flag
キャッシュエントリのフラグは常に "4"
Type
標準的又はプライマリ名が指定された「CNAME」、既存のエントリと同じ IP アドレスをマッピングされている多数のドメイン名が指定された「ALIAS」
IP
レコードに関連した IP アドレス
TTL
ネームサーバにより報告された生存可能時間
Domain
レコードに関連するドメイン名

設定方法

[DNS] → [Cache] をクリックします。



3.15 DHCP サーバ

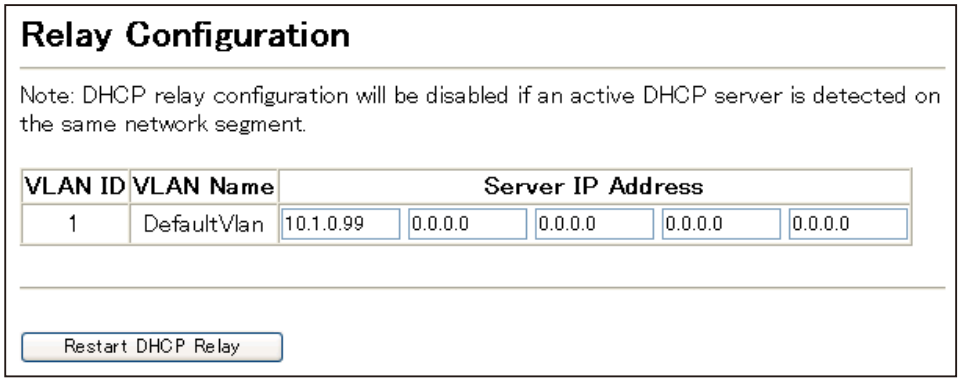
3.15.1 DHCP リレーサービスの設定

設定・表示項目

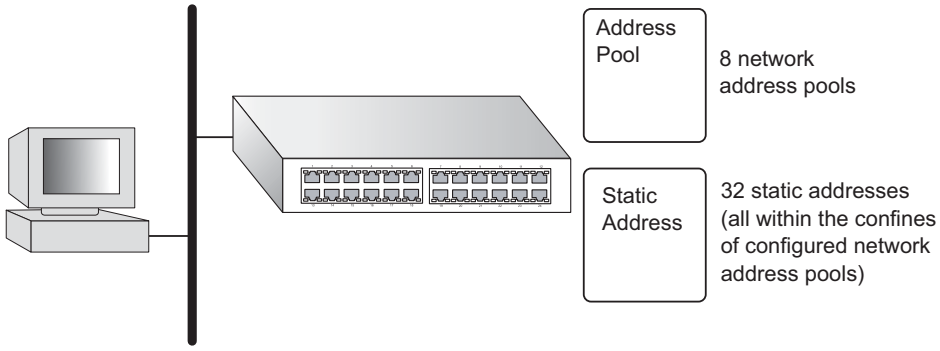
VLAN ID
設定を行う VLAN の ID
VLAN Name
VLAN 名
Service IP Address
優先の順にスイッチの DHCP リレーエージェントによって使われる DHCP サーバーのアドレス。

設定方法

[DHCP] → [Relay Configuration] をクリックします。



3.15.2 DHCP サーバの設定



サーバーの有効化、除外アドレスの設定

設定・表示項目

DHCP Server

スイッチで DHCP **サーバを有効 / 無効化（初期設定：無効）**

Excluded Addresses

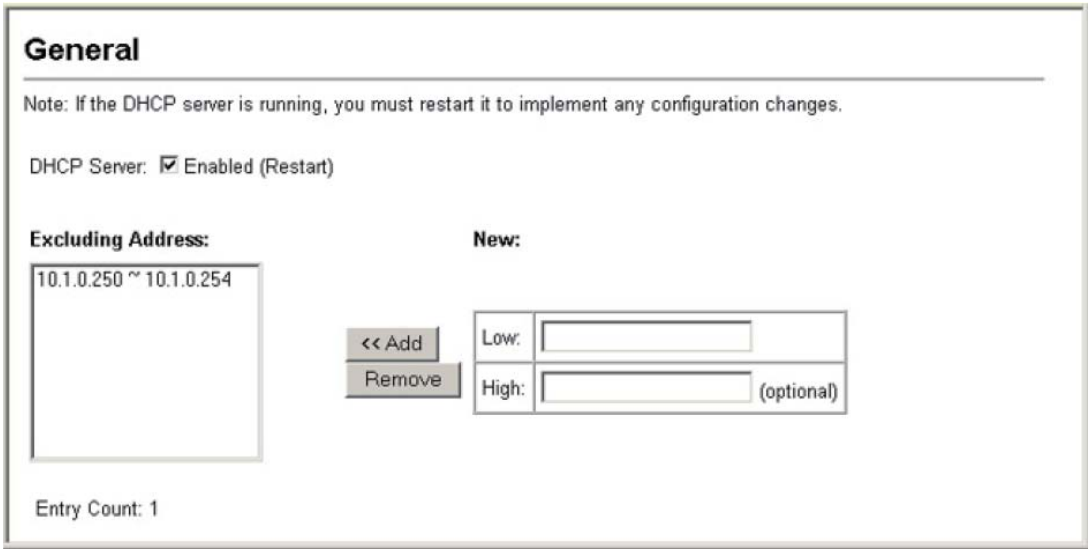
DHCP **サーバーが** DHCP **クライアントに割り当てるべきでない** IP **アドレスを指定します。一つのアドレスあるいはアドレス範囲を指定できます。**

New (Excluded Addresses)

除外するアドレスを新規にエントリします。

設定方法

[DHCP] → [Server] → [General] **をクリックします。**



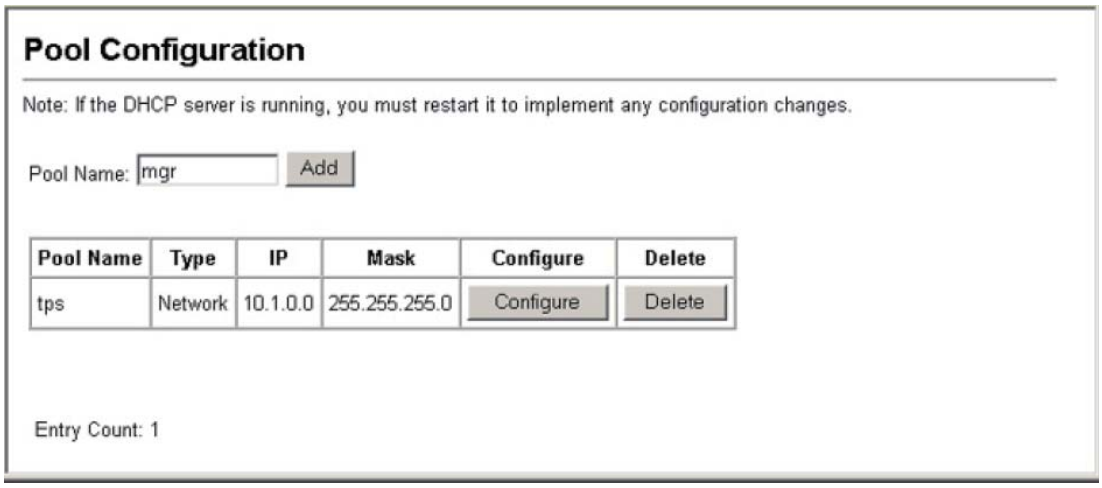
3.15.3 アドレスプールの設定

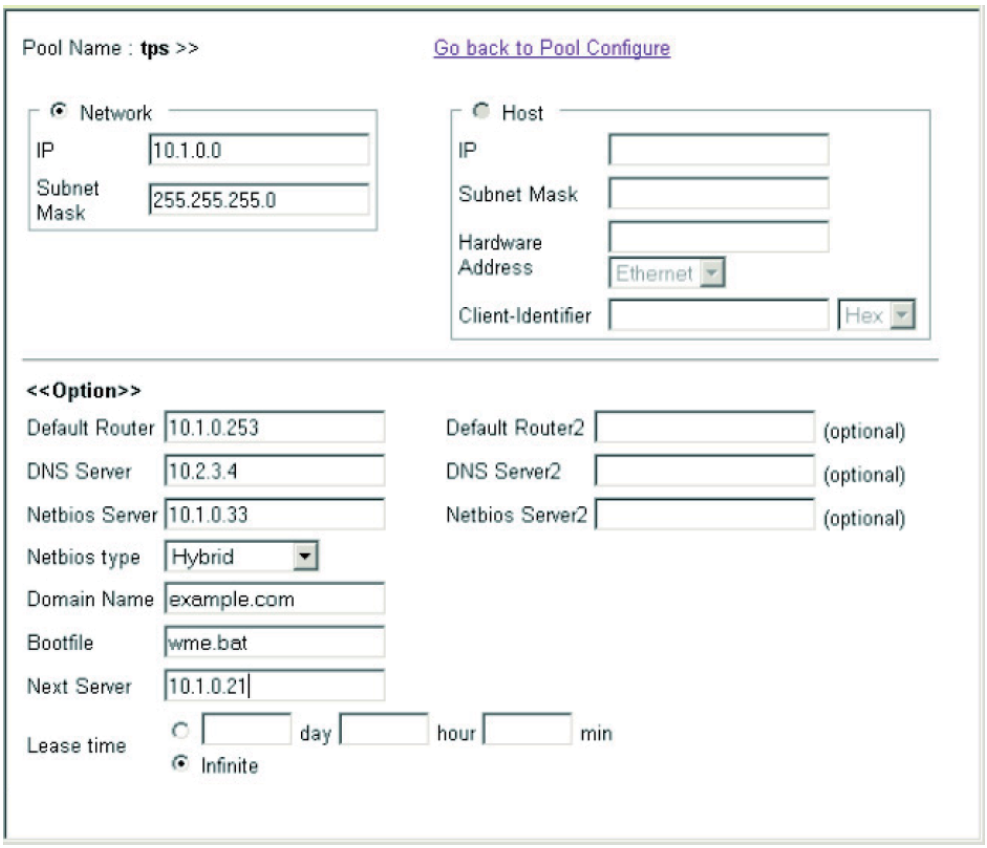
設定・表示項目

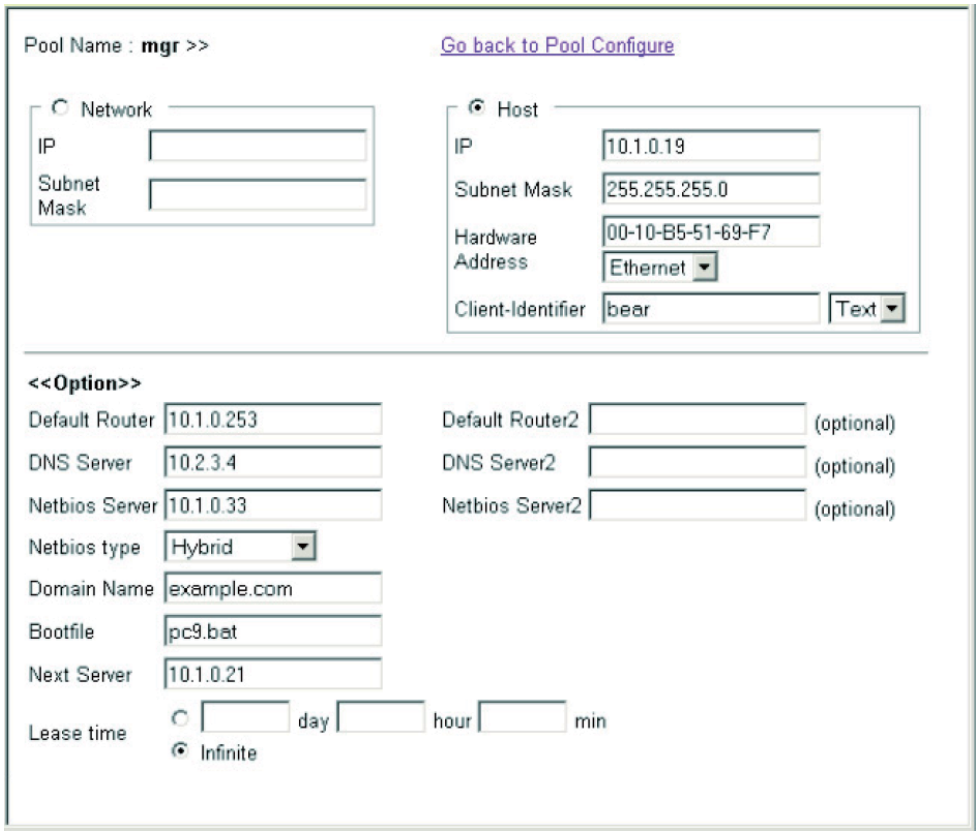
Pool Name
プール名（範囲：1-8 **文字）**
IP
DHCP **アドレスプールの** IP **アドレス**
Subnet Mask
アドレスプールのサブネットマスク。

設定方法

[DHCP] → [Server] → [Pool Configuration] **をクリックします。**




Pool Name : tps >>
Go back to Pool Configure
Network
IP 10.1.0.0
Subnet Mask 255.255.255.0
Host
IP
Subnet Mask
Hardware Address
Ethernet
Client-Identifier
Hex
<<Option>>
Default Router 10.1.0.253
Default Router2 (optional)
DNS Server 10.2.3.4
DNS Server2 (optional)
Netbios Server 10.1.0.33
Netbios Server2 (optional)
Netbios type Hybrid
Domain Name example.com
Bootfile wme.bat
Next Server 10.1.0.21
Lease time day hour min
Infinite


Pool Name : mgr >>
Go back to Pool Configure
Network
IP
Subnet Mask
Host
IP 10.1.0.19
Subnet Mask 255.255.255.0
Hardware Address 00-10-B5-51-69-F7
Ethernet
Client-Identifier bear
Text
<<Option>>
Default Router 10.1.0.253
Default Router2 (optional)
DNS Server 10.2.3.4
DNS Server2 (optional)
Netbios Server 10.1.0.33
Netbios Server2 (optional)
Netbios type Hybrid
Domain Name example.com
Bootfile pc9.bat
Next Server 10.1.0.21
Lease time day hour min
Infinite

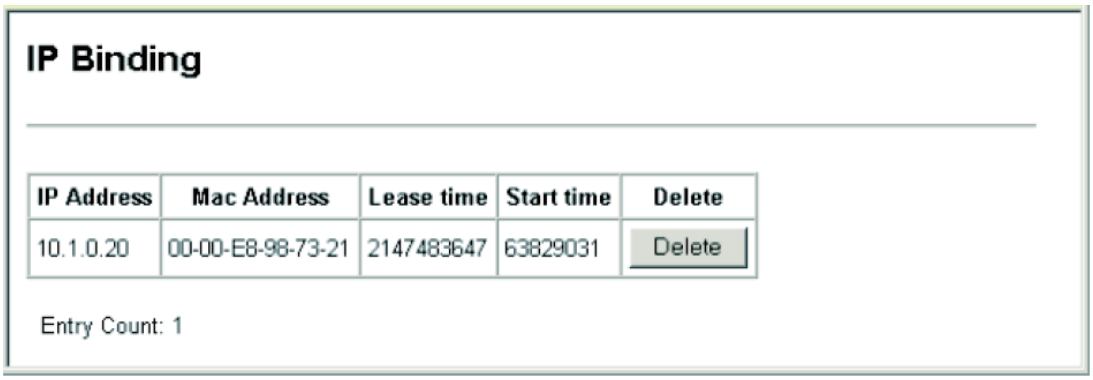
3.15.4 アドレスバインディングの表示

設定・表示項目

IP Address
ホストにアサインされた IP **アドレス**
MAC Address
ホストの MAC **アドレス**
Lease time
ホストによって使用される継続時間
Start time
スイッチにアサインされた時間
Delete
指定したバインディングを削除します。
Entry Count
スイッチによってアドレスが割り当てられたホストの数

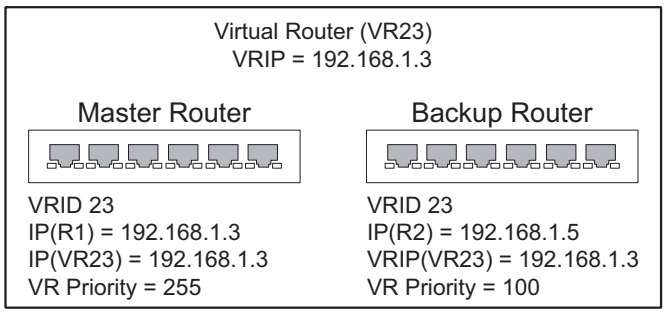
設定方法

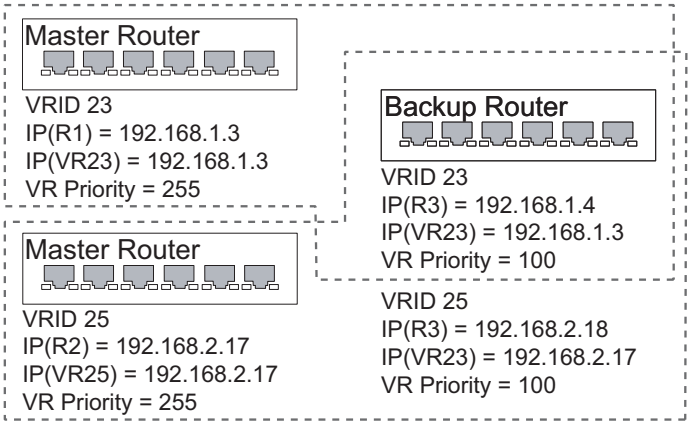
[DHCP] → [Server] → [IP Binding] **をクリックします。**

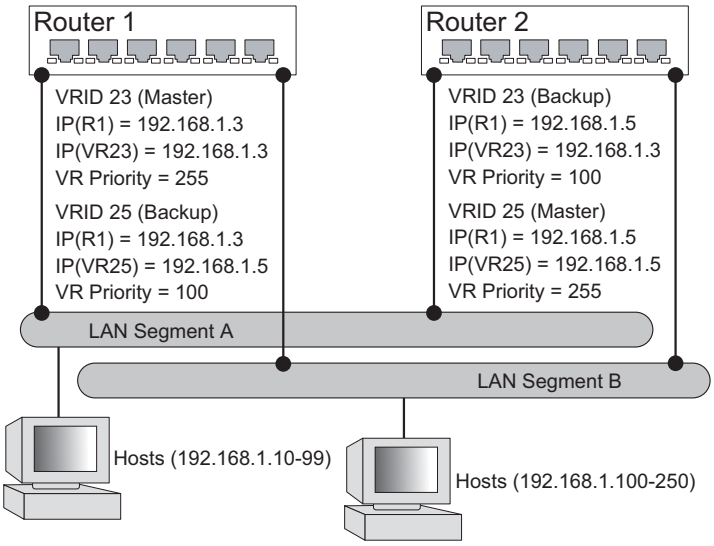


3.16 ルータ冗長

ルータ冗長性プロトコルは、プライマリ ルータおよび複数のバックアップ ルータをサポートするために、仮想 IP アドレスを使用します。マスター ルータに障害が発生した時にワークロードを引き継ぐように、バックアップ ルータを構成することができます。また、トラフィック ロードを共有するように構成することもできます。ルータ冗長性の主な目的は、プライマリ ゲートウェイの障害発生時に、固定ゲートウェイで構成されたホスト デバイスがネットワーク コネクティビティを保持できるようにすることです。







3.16.1 VRRP

VRRP を構成するには、グループ内でマスター仮想ルータとして機能する 1 つのルータ上のインタフェースを選択します。この物理インタフェースは、ルータ グループの仮想アドレスとして使用されます。ここで、バックアップ ルータに同じ仮想アドレスとプライオリティを設定し、認証ストリングを構成します。また、オンラインになった時にマスタールータとして処理を引き継ぐことを可能にするプリエンプト機能を、ルータで有効にすることもできます。

VRRP グループの設定

設定・表示項目

VLAN ID

設定を行う VLAN の ID (範囲：1-4094　初期設定：1)

VRID

VRRP グループ識別子 (範囲：1-255)

State

VRRP ルータロール . (値：Master、Backup)

Virtual Address

このグループの仮想 IP アドレス

Interval

通知間隔の指定

Preemption

現在マスターとして動作しているルータよりも高いプライオリティを持つルータが VRRP グループに参加した時、このルータがマスター仮想ルータとして処理を引き継ぐように構成します。

Priority

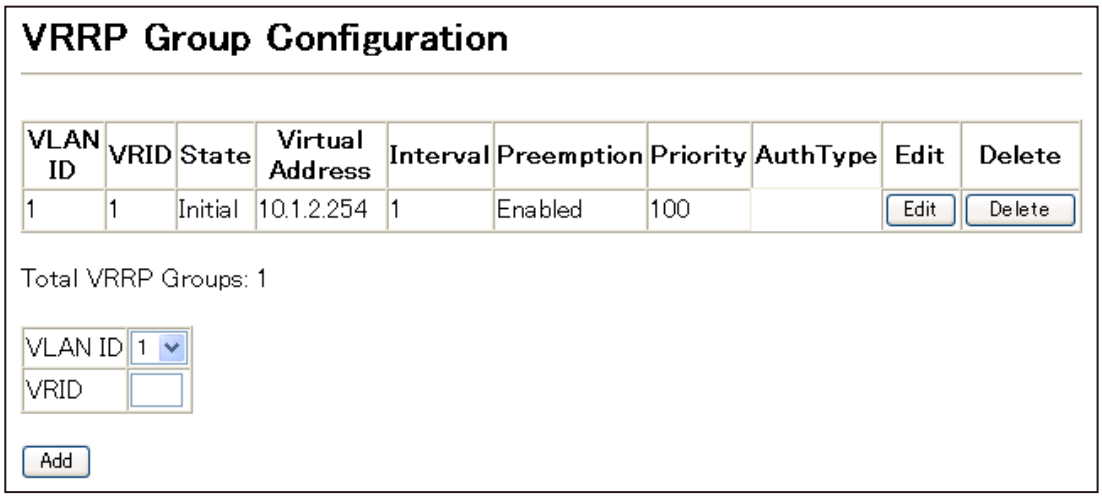
VRRP グループ内でのこのルータのプライオリティを設定します。

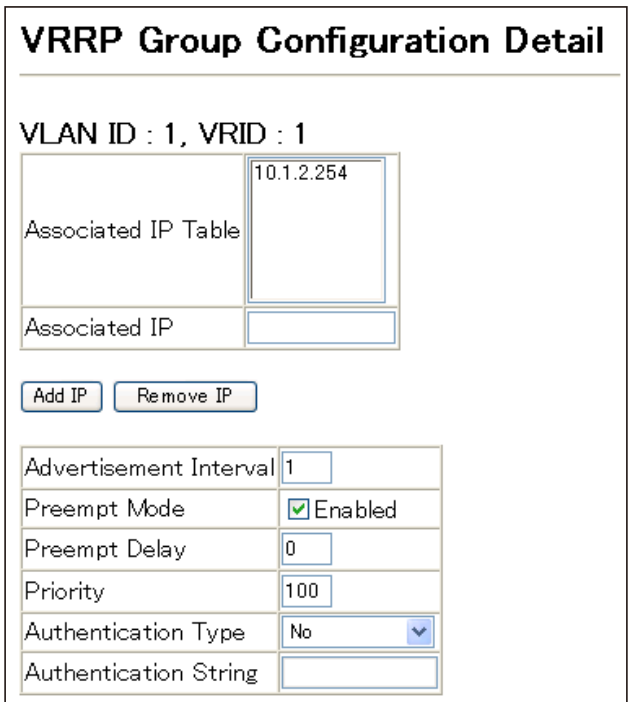
AuthType

認証モード

設定方法

[IP] → [VRRP] → [Group Configuration] をクリックします。





VRRP グローバル統計の表示

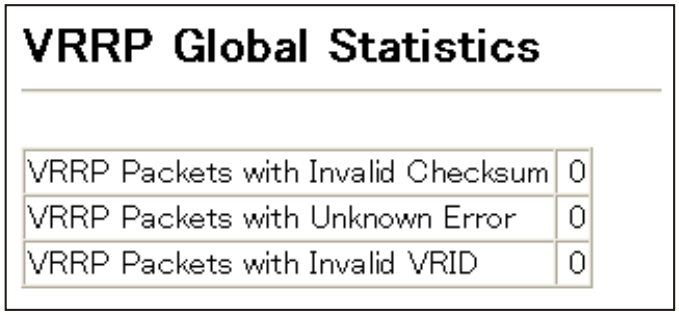
設定・表示項目

VRRP Packets with Invalid Checksum
無効な VRRP **チェックサム値で受信診された** VRRP **パケットの合計数**
VRRP Packets with Unknown Error
サポート外のバージョンで受信された VRRP **パケットの合計数**
VRRP Packets with Invalid VRID

無効は VRID **で受信された** VRRP **パケットの合計数**
The total number of VRRP
packets received with an invalid VRID for this virtual router.

設定方法

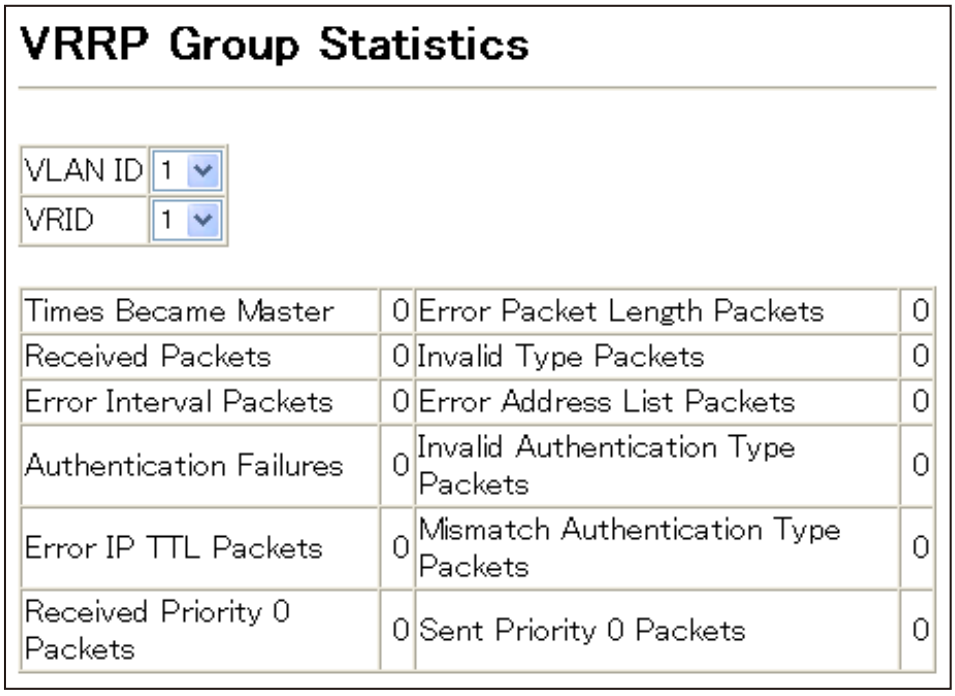
[IP] → [VRRP] → [Global Statistics] **をクリックします。**



VRRP グループ統計の表示

設定方法

[IP] → [VRRP] → [Group Statistics] **をクリックします。**



3.17 IP ルーティング

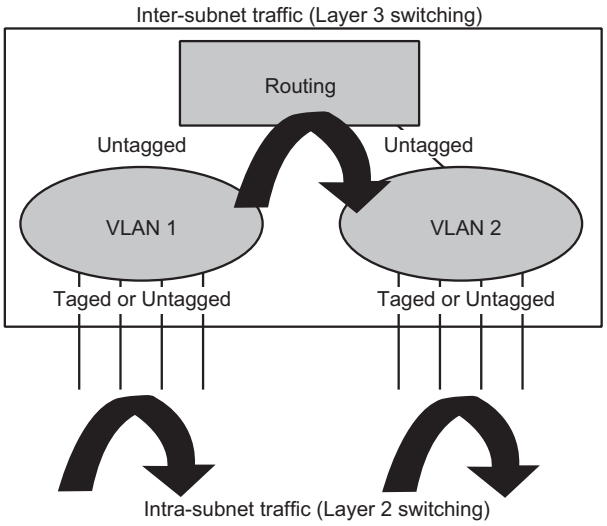
概要

本機は IP ルーティング機能をサポートしており、ルーティングパスの管理は、静的な経路の設定（P205）、または RIP（P207）、OSPF（P217）の動的な設定により可能になります。IP ルーティング機能を有効に設定していると、本機はワイヤスピードを実現するルータ同様に動作するため、異なる IP インタフェースを介した VLAN 間通信や、外部 IP ネットワークへのトラフィックのルーティングを行います。しかし、本機の初期設定ではルーティング機能は設定されていません。ルーティング機能を使用するには、既存のルータ製品のように、最初にこれらの設定を行う必要があります。

初期設定

工場出荷時の設定では、ポートはすべて単一の VLAN に所属し、レイヤ 2 機能のみを使用するようになっています。そのため、まず、各ユーザグループまたはトラフィックのアプリケーション別に VLAN を作成し、同じグループに所属するすべてのポートを各 VLAN に割り当て、それから各 VLAN に IP インタフェースを設定する必要があります。ネットワークを複数の異なる VLAN に分けることによって、レイヤ 2 レベルで分割されているサブネットワークで分けることができます。同一サブネット内でやり取りされるトラフィックは、レイヤ 2 のスイッチング機能を使用して通信されます。そして、必要な場合には、レイヤ 3 のスイッチング機能を使用して VLAN 間通信ができることになります。

各 VLAN はレイヤ 3 での仮想的なインタフェースに相当します。この仮想インタフェースに対してネットワークアドレスを設定しさえすれば、トラフィックは、異なるサブネット間でレイヤ 3 レベルでルーティングされるようになります。



3.17.1 IP スイッチング

IP スイッチング（パケットのフォワーディング）は、従来のルーティング同様、レイヤ 2 およびレイヤ 3 の両方で、パケットをフォワーディングするのに必要な処理の全体のことを示しています。

IP スイッチングには、例えば次の機能が含まれます。

- レイヤ 2 のフォワーディング（スイッチング）。レイヤ 2 のディスティネーション MAC アドレスに基づく。
- レイヤ 3 のフォワーディング（ルーティング）。
  - レイヤ 3 のディスティネーションアドレスに基づく。

- 各ホップでディスティネーション / ソース MAC アドレスを置き換える。
- ホップカウントを 1 つ増やす。
- 生存時間を 1 つ減らす。
- レイヤ 3 チェックサムの検証と再計算を行う。

ディスティネーションノードがソースと同じサブネットに所属する場合、パケットは、ルータを経由せず直接送信されます。ただし、パケットの MAC アドレスがスイッチで認識されていない場合、ディスティネーション IP アドレスを含む ARP（Address Resolution Protocol）パケットがブロードキャストされ、ディスティネーションノードからディスティネーション MAC アドレスを取得します。そして、パケットは直接ディスティネーション MAC アドレスで送信されます。

ディスティネーションノードが本機とは別のサブネットに所属する場合、パケットはディスティネーションノードに直接ルーティングされます。ただし、パケットが本機が所属していないサブネットのものである場合、（ルータ自体の MAC アドレスをディスティネーション MAC アドレスとして、またディスティネーションノードのディスティネーション IP アドレスを使用して）パケットはルータに送信されます。ルータは正当なパスを経由してディスティネーションノード宛てにパケットをフォワーディングします。ルータは、必要に応じて ARP プロトコルを使用し、隣接ルータのディスティネーションノードの MAC アドレスを取得することもできます。

[注意] IP スイッチングを実現するためには、本機が他のネットワークノードから IP ルータとして認識される必要があります。このためには、本機にデフォルトゲートウェイを設定するか ICMP プロセスで他のルータからリダイレクトさせることが必要です。

MAC アドレスを含む IP パケットを本機が受信すると、パケットはレイヤ 3 でのルーティングプロセスに移行します。ディスティネーション IP アドレスはレイヤ 3 のアドレステーブルでチェックされます。このアドレスがアドレステーブルに登録されていない場合、本機は ARP パケットをディスティネーション VLAN のすべてのポートに向けてブロードキャストし、ディスティネーション MAC アドレスの取得を試みます。MAC アドレスを取得できると、パケットの再構築が行われ、ディスティネーションへ送信されます。パケットの再構築プロセスでは IP ヘッダの TTL（Time-To-Live）フィールドの削減、IP ヘッダのチェックサムの再計算、およびディスティネーション MAC アドレスの（ディスティネーションノードの MAC アドレスか、隣接ルータの MAC アドレスへの）置き換えがあります。

同じノード宛の別のパケットを受信した場合、レイヤ 3 のアドレステーブルから直接 MAC アドレスを取得できるため、パケットはすぐに再構築されてディスティネーションポートに送信されます。レイヤ 3 のアドレステーブルにディスティネーションアドレスがすでに登録されている場合、IP スイッチングはワイヤスピードで処理することができます。

本機が、フレームのルーティングが必要と判断した場合、送信経路の計算はセットアップ内でのみ行われます。1 度経路が決定されると、その時点で処理中のすべてのパケットは選択されたパスへスイッチング（フォワーディング）されるだけになります。この方法は、1 度パスの計算が完了したらトラフィックはルーティングエンジンを迂回することができるようになるため、遅延を抑え、高いスループットが得られることが利点です。

ルーティングパスの管理

ルーティングパスの管理では、パケットのフォワーディングに必要な、すべてのルーティング情報の決定とアップデートを行います。これには、以下が含まれます。

- ルーティングプロトコルの処理。
- ルーティングテーブルのアップデート。
- レイヤ 3 のスイッチングデータベースのアップデート。

ルーティングプロトコル

本機は、静的なルーティングと動的なルーティングの両方をサポートしています。

- 静的なルーティングには、手作業により、あるいは本機以外のアプリケーションで接続が設定されることにより、本機内にルーティング情報が保存される必要があります。
- 動的ルーティングにはルーティングプロトコルが必要で、これによりルーティング情報の交換、ルーティングテーブルの計算、およびネットワーク情報の読み込みやステータスの変化への対応を行います。

IP インタフェースの基本的な設定

異なる IP サブネットと通信するためには、本セクションに示したように IP ルーティングを有効にする必要があります。さらに、本機に直接接続する各 IP サブネットの VLAN を定義します。P126 「VLAN の作成」に従い、まず VLAN を作成し、それから各サブネットの設定を行わなくてはならないことに注意が必要です。また、インバンドで本機を管理する場合は、最低 1 つの VLAN に IP サブネットアドレスを定義しなくてはなりません。

設定・表示項目

IP Routing Status

本機を、レイヤ 2 スイッチまたはマルチレイヤルーティングスイッチのどちらで動作するかを設定します。（選択肢：無効（レイヤ 2 のスイッチングのみに限定）、有効（状況に応じてマルチレイヤ（レイヤ 2 およびレイヤ 3）で動作））

－このコマンドは、静的 / 動的両方のユニキャストルーティングに影響します。

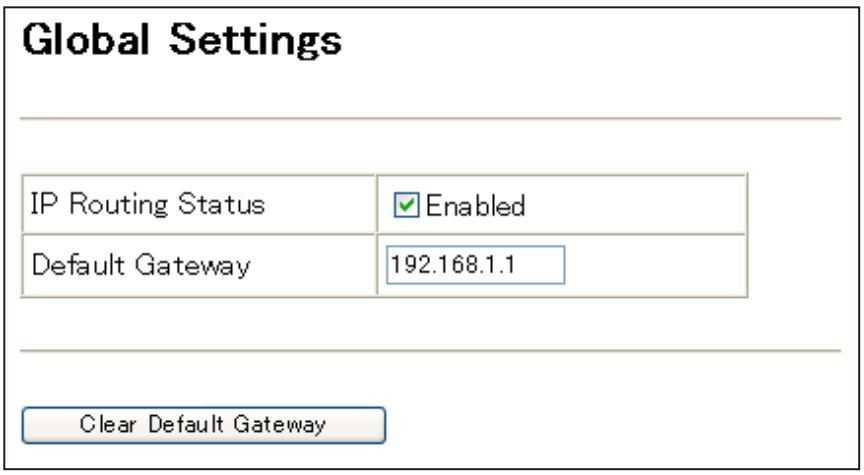
－IP ルーティングを有効にすると、すべての IP パケットは静的にまたは RIP により動的にルーティングされ、非 IP プロトコル（NetBuei、NetWare、AppleTalk など）のパケットは MAC アドレスでスイッチングされます。IP ルーティングを無効にすると、すべてのパケットは、MAC アドレスのみでフィルタリングとフォワーディングされてスイッチングされます。

Default Gateway

例えば、ルーティングテーブルのエントリに存在しないパケットなど、すべての不明なサブネット宛てのパケットを渡すルーティングデバイスを設定します。（有効な IP アドレスの形式は、ピリオドで区切られた 0 ～ 255 の 4 つの数字から構成されています）

設定方法

[IP] → [General] → [Global Settings] をクリックします。IP Routing Status の Enabled にチェックを入れない場合、レイヤ 2 での動作に限定します。Enabled にチェックを入れると、マルチレイヤでのスイッチングを行います。不明なサブネット宛てのパケットをフォワーディングするデフォルトゲートウェイ（Default Gateway）を設定します。[Apply] をクリックします。


Global Settings
IP Routing Status
Enabled
Default Gateway
192.168.1.1
Clear Default Gateway

IP ルーティングインタフェースの設定

本機に接続している IP サブネットは、各 VLAN の IP アドレスを手作業により設定する方法か、または RIP による動的なプロトコルを使用してネットワークの他のルータとプロトコルメッセージをやり取りすることにより、他のインタフェースへの経路を特定する方法のいずれかで設定できます。

機能解説

- 本機にエンドノードのデバイスが直接接続している場合（または共有メディアを介してエンドノードが接続している場合）、これには特定のサブネットが割り当てられるため、ルーティングをサポートするよう各 VLAN に対してルーティングインタフェースを作成する必要があります。ルーティングインタフェースは IP アドレスとサブネットマスクから構成されます。このインタフェースのアドレスは、ルーティングインタフェースが接続するネットワーク番号とそのネットワークに所属するルータのホスト番号の両方を定義するものです。つまり、ルーティングインタフェースのアドレスは、インタフェースに接続するセグメントのネットワーク番号およびサブネット番号であり、これによりルータと IP パケットの送受信ができるようになります。

- 本機のネットワークインタフェースを設定する前に、まず各ユーザグループに対して、または各ネットワークアプリケーションとそれに関与するユーザに対して、それぞれに VLAN を作成しなくてはなりません。

設定・表示項目

VLAN

設定する VLAN の ID（1-4094）

IP Address Mode

このインタフェースの IP アドレスを静的に設定するか、またはネットワークアドレスサーバから取得するのかを設定します。（選択肢：Static、DHCP（Dynamic Host Configuration Protocol）、BOOTP（Boot Protocol）。初期設定：Static）

- IP Address Mode で Static を選択すると、IP アドレスがその VLAN でプライマリかセカンダリかの設定も必要になります。1 つのインタフェースにはプライマリ IP アドレスを 1 つのみ、セカンダリ IP アドレスは複数設定できます。つまり、このインタフェース経由で複数の IP サブネットがアクセスできるようにするには、セカンダリアドレスを設定する必要があります。
- DHCP または BOOTP を選択すると、アドレスサーバからの応答を受信して初めて、IP スイッチング機能が動作するようになります。IP アドレスを要求するリクエストは本機から周期的にブロードキャストされます。（DHCP/BOOTP に、IP アドレスとサブネットマスクが含まれます）

IP Address

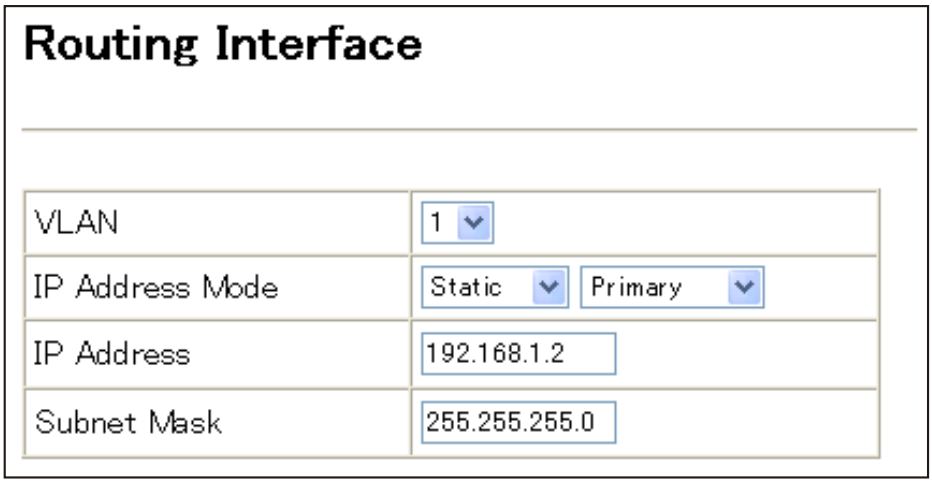
VLAN インタフェースの IP アドレス。（有効な IP アドレスの形式は、ピリオドで区切られた 0 ～ 255 の 4 つの数字から構成されています）

Subnet Mask

サブネットマスクは、特定のサブネットにルーティングするために使用するホストアドレスのビットを識別します。

設定方法

[IP] → [General] → [Routing Interface] をクリックします。他のサブネットへのルーティングをサポートする各 VLAN に対し、1 つの IP インタフェースを設定します。まずプライマリの IP アドレスを設定し、[Set IP Configuration] をクリックします。複数のセカンダリ IP アドレスを設定する場合は、1 度に 1 つずつ入力します。そして、各アドレスの入力後に [Set IP Configuration] ボタンをクリックします。



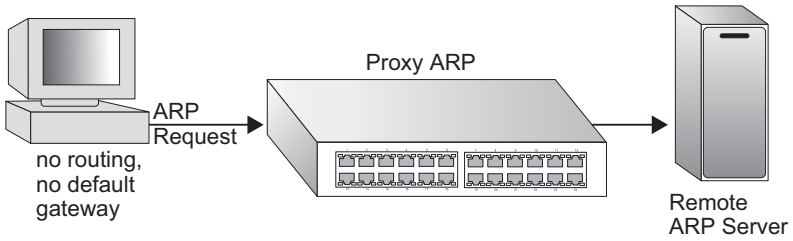
3.17.2 ARP

IP ルーティング機能が有効に設定されている場合（P17-5）、経路の決定のためにルーティングテーブルが使用され、ARP（Address Resolution Protocol）を使用してホップから次のホップへトラフィックをフォワーディングします。ARP は IP アドレスを物理レイヤのアドレス（MAC アドレス）にマッピングするプロトコルです。IP のフレームがルーティングインタフェース（または標準に準拠したルータ）で受信されると、ARP のキャッシュから、ディスティネーション IP アドレスにあたる MAC アドレスをまず検索します。IP アドレスが見つかった場合、本機はフレームヘッダの適切なフィールドに MAC アドレスを書き込み、ネクストホップへ向けてフレームをフォワーディングします。このように、宛先に向けて各ルーティングデバイスでディスティネーション IP アドレスとネクストホップの MAC アドレスのマッピングを行いながら、最終のディスティネーションにパケットが配送されるまで IP パケットはパスに従って渡されます。

ARP のキャッシュに IP アドレスエントリがない場合、本機は ARP リクエストパケットを同一ネットワーク上のすべてのデバイスに向けてブロードキャストします。ARP リクエストは次の例に示すようなフィールドを含みます。

ディスティネーション IP アドレス	10.1.0.19
ディスティネーション MAC アドレス	?
ソース IP アドレス	10.1.0.253
ソース MAC アドレス	00-00-ab-cd-00-00

デバイスがリクエストを受信した際、デバイス自身のアドレスとメッセージのディスティネーション IP アドレスとが一致していない場合、このパケットは破棄されます。しかし、一致した場合は、自身のハードウェアアドレスをディスティネーション MAC アドレスフィールドに書き込み、ソースのハードウェアアドレス宛てにメッセージを返信します。ソースデバイスがこのリプライを受信すると、ディスティネーション IP アドレスとこれに対応する MAC アドレスをキャッシュに書き込み、ネクストホップに IP パケットをフォワーディングします。このエントリがタイムアウトを迎えない限り、このディスティネーションについては、本機は新たに ARP リクエストをブロードキャストすることなく、ネクストホップに直接トラフィックをフォワーディングできます。



プロキシ ARP

接続しているサブネットに所属するノードがルーティングの設定またはデフォルトゲートウェイの設定がされていない場合、プロキシ ARP でリモートのサブネットへ ARP リクエストをフォワーディングできます。本機でプロキシ ARP が有効に設定されており、リモートネットワークの ARP リクエストを受信すると、本機はリモートネットワークへの最良の経路情報を所持しているか検討し、リクエストを送信してきたノードへ自身の MAC アドレスを返信することにより ARP リクエストに応答します。ノードは本機へデータを送信しますが、言い換えると本機自身のルーティングテーブルを使用してパケットをリモートディスティネーションにフォワーディングすることになります。

ARP の基本的な設定

ARP の General 設定メニューを使用し、ARP キャッシュエントリのタイムアウト設定や、特定の VLAN インタフェースのプロキシ ARP を有効に設定します。

機能解説

- エージングタイムは動的なエントリがキャッシュに保持される時間的な長さを決定します。タイムアウトが短すぎる場合、本機はテーブルから削除されたばかりのアドレスを求めて何度も ARP リクエストを送信することになるので、リソースを消耗する可能性があります。
- プロキシ ARP を使用するエンドステーションは、ネットワーク全体を単一のネットワークとして認識している必要があります。したがって、各ノードは本機または本機と同等のネットワークデバイスが使用しているサブネットマスクよりも小さなサブネットマスクを使用していなくてはなりません。
- プロキシ ARP の使用が多いと本機のパフォーマンスが低下します。多用により ARP トラフィックが増え、ARP アドレステーブルの増大にともなって検索に時間がかかるようになるからです。

設定・表示項目

Timeout

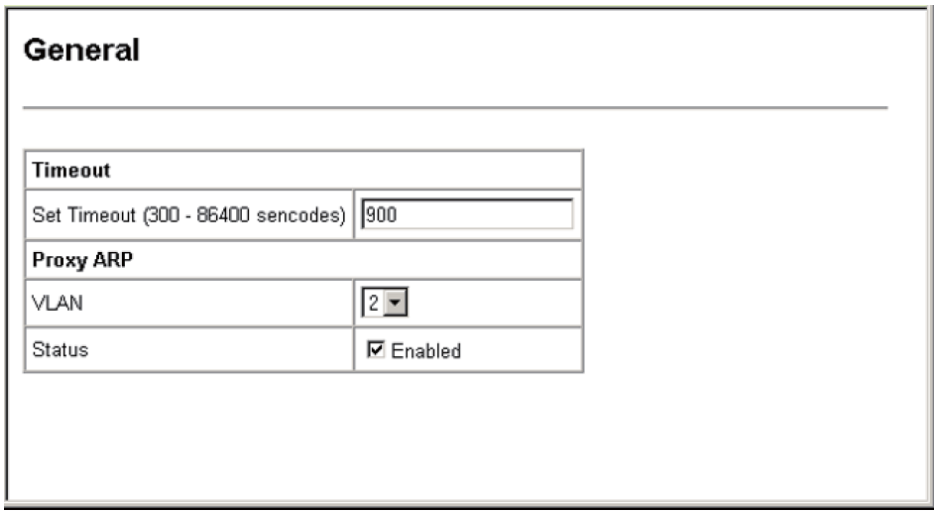
ARP キャッシュに保存される動的なエントリのエージングタイムを設定します。（範囲：300-86400 秒。初期設定：1200 秒）

Proxy ARP

選択した VLAN インタフェースのプロキシ ARP について、有効または無効を設定します。

設定方法

[IP] → [ARP] → [General] をクリックします。ARP キャッシュのタイムアウト値を適切に設定し、ルーティング機能やデフォルトゲートウェイを持たないサブネットワークのプロキシ ARP を有効に設定します。[Apply] をクリックします。



静的な ARP アドレスの設定

ARP リクエストに応答しないデバイスは、IP アドレスと MAC アドレスとのマッピングができないため、パケットは破棄されます。このような場合、手作業で、ARP キャッシュに IP アドレスとこれに対応する MAC アドレスとのマッピング情報を設定することができます。

機能解説

- ARP キャッシュには最大 128 エントリを静的に設定できます。
- 静的なエントリは、一定の時間を経過したとき自動的に消去されたり、電源をリセットした場合でも消去されません。静的なエントリは設定インタフェースからのみ消去できます。

設定・表示項目

IP Address

MAC アドレスとのマッピングを行う IP アドレス。(有効な IP アドレスの形式は、ピリオドで区切られた 0 ～ 255 の 4 つの数字から構成されています)

MAC Address

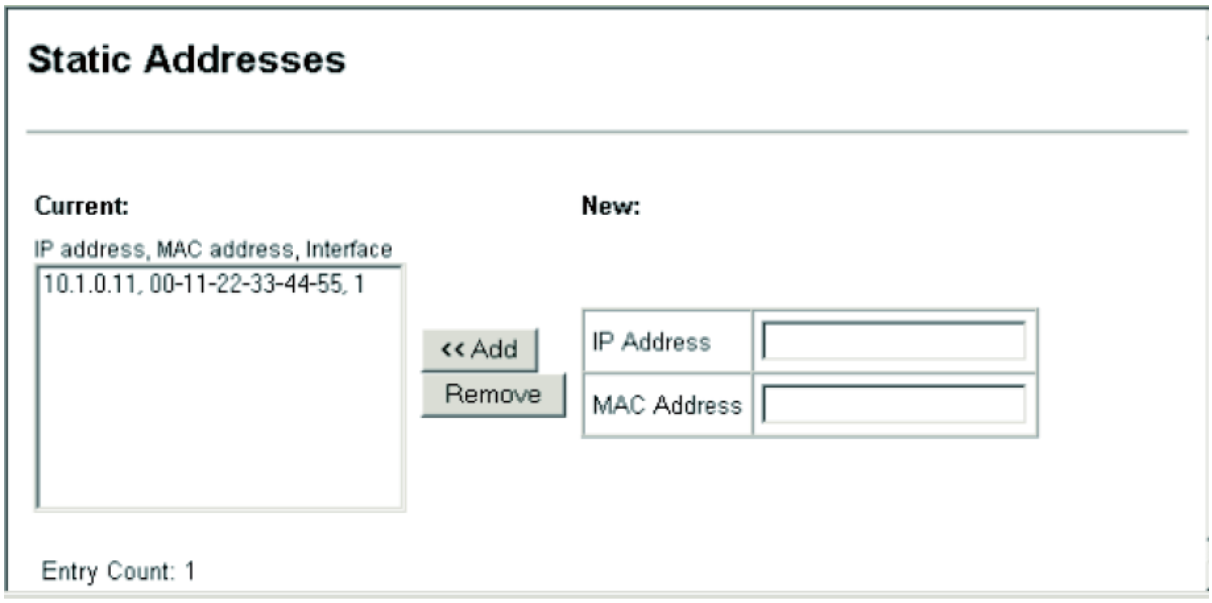
IP アドレスに対応する、静的にマッピングする MAC アドレス。(有効な MAC アドレスは 16 進数で、形式は xx-xx-xx-xx-xx-xx です)

Entry Count

ARP キャッシュに保存されている静的なエントリの数。

設定方法

[IP] → [ARP] → [Static Addresses] をクリックします。IP アドレスとこれに対応する MAC アドレスを入力します。[Apply] をクリックします。



動的に学習された ARP エントリの表示

IP アドレスと、これに対応する MAC アドレスがマッピングされた各エントリが、ARP キャッシュに保存されています。エントリのほとんどはブロードキャストメッセージからの応答により動的に学習されたものです。ARP キャッシュに保存されているすべての動的エントリを表示したり、特定の動的エントリを静的なエントリに変更したり、キャッシュからすべての動的なエントリを削除したりできます。

設定・表示項目

IP Address

キャッシュに保存されている動的エントリの IP アドレス。

MAC Address

IP アドレスにマッピングされている MAC アドレス。

Interface

アドレスエントリに関連付けられている VLAN インタフェース。

Dynamic to Static*

選択した動的エントリを静的エントリに変更します。

Clear All *

ARP キャッシュからすべての動的エントリを削除します。

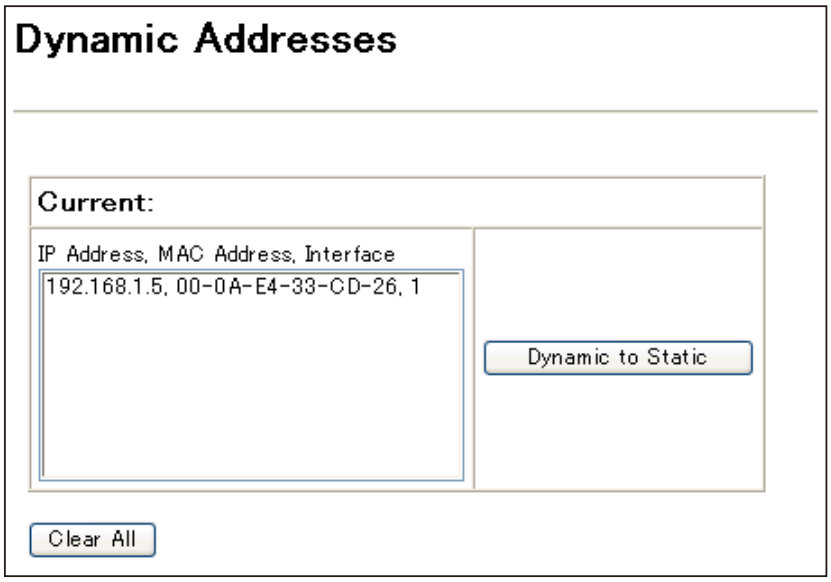
Entry Count

ARP キャッシュに保存されている動的エントリの数。

* これらのボタンをクリックすると、設定はすぐに反映されます。実行を確認するためのプロンプトメッセージは表示されません。

設定方法

[IP] → [ARP] → [Dynamic Addresses] をクリックします。キャッシュに保存されている動的エントリを静的エントリに変更するためのボタンや、すべての動的エントリを削除するためのボタンを使用できます。



ローカルな ARP エントリの表示

ARP キャッシュはローカルインタフェース（サブネット、ホスト、ブロードキャストアドレス）のエントリも保存しています。

設定・表示項目

IP Address

キャッシュに保存されている動的エントリの IP アドレス。

MAC Address

IP アドレスにマッピングされている MAC アドレス。

Interface

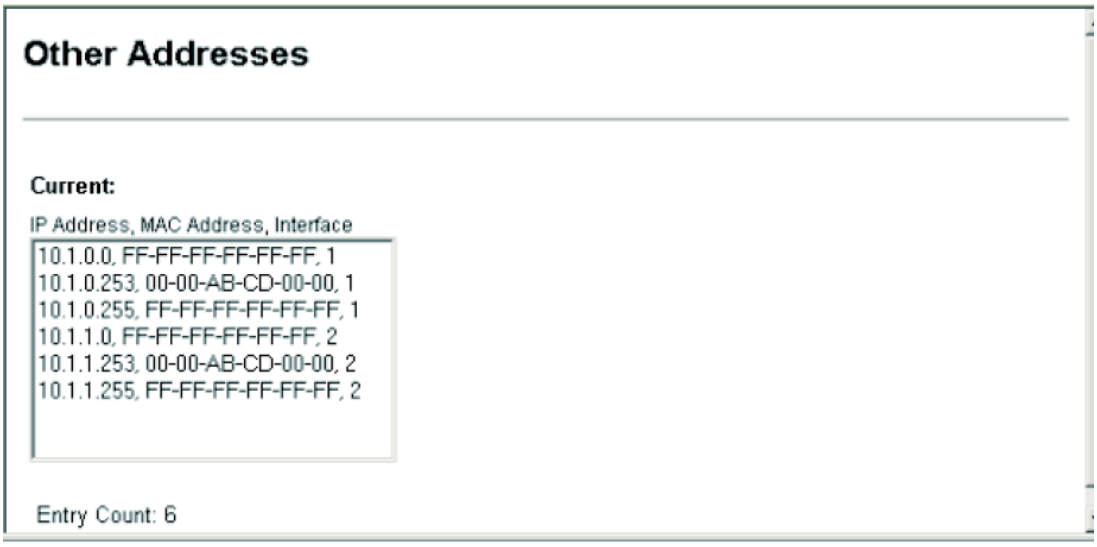
アドレスエントリに関連付けられている VLAN インタフェース。

Entry Count

ARP キャッシュに保存されているローカルエントリの数。

設定方法

[IP] → [ARP] → [Other Addresses] をクリックします。



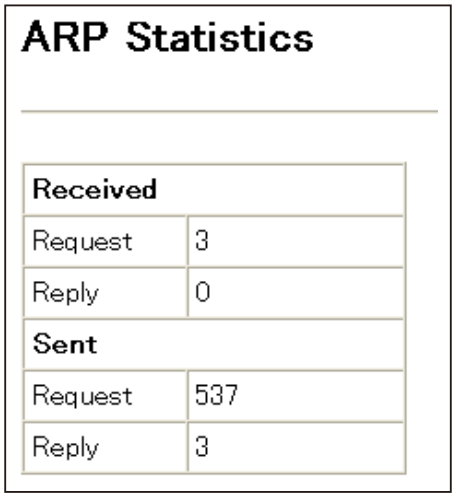
ARP の統計情報

本機のすべてのインタフェースを通過する ARP メッセージに関する統計情報を表示できます。

Received Request	本機が受信した ARP リクエストパケット数
Received Reply	本機が受信した ARP リプライパケット数
Sent Request	本機が送信した ARP リクエストパケット数
Sent Reply	本機が送信した ARP リプライパケット数

設定方法

[IP] → [ARP] → [Statistics] をクリックします。



3.17.3 IP プロトコルの統計情報の表示

IP の統計情報

IP（Internet Protocol）はソースからディスティネーションまで、データの固まり（パケット、フレームなどと呼ばれます）を送り届けるメカニズムを提供します。ここで、ネットワークデバイス（ホスト）は、固定長のアドレスで識別されます。IP はまた、必要に応じて長いパケットの分割と再構築の機能を提供し、「小さなパケット」で構成されるネットワークでデータがやり取りされるようにします。

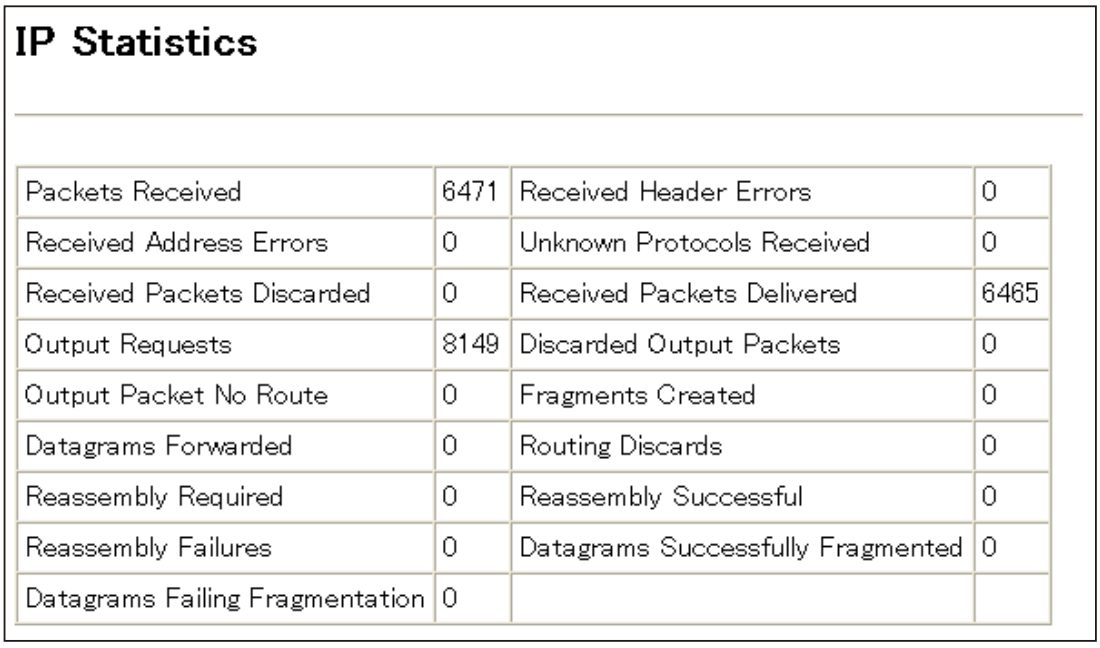
本機のすべてのインタフェースを通過する ARP メッセージに関する統計情報を表示できます。

項目	内容
Packets Received	インタフェースで受信した着信データグラムの総数（エラーを含む）
Received Address Errors	IP パケットヘッダのディスティネーションフィールドに含まれている IP アドレスがエンティティに有効でないアドレスであったため、破棄された着信データグラムの数
Received Packets Discarded	通信処理継続のためには問題がなかったが、（バッファ容量の問題等で）破棄された着信データグラムの数
Output Requests	送信リクエストに対して IP ネットワークに送信した、ローカルの IP ユーザプロトコル（ICMP を含む）のデータグラムの総数
Output Packet No Route	ディスティネーションへの送信経路を検出できなかったために、破棄されたデータグラムの数。ここには、デフォルトゲートウェイがすべてダウンしていたためホストが配送できなかったデータグラムの数も含まれることに注意してください。
Datagrams Forwarded	エンティティが最終の IP ディスティネーションでなく、最終のディスティネーションにフォワーディングするために経路を検出した着信データグラムの数
Reassembly Required	このエンティティで再構築が必要だった IP フラグメントの受信数

Reassembly Failures	タイムアウト、エラーなど様々な理由により、IP パケットの再構築に失敗したと検出された数
Datagrams Failing Fragmentation	「分割しない」フラグが設定されていたなどの理由により）このエンティティで分割すべきであったができず、破棄されたデータグラムの数
Received Header Errors	チェックサムエラー、バージョン番号の不一致、その他のフォーマットエラー、生存時間の超過、IP オプション処理でのエラー検出など、IP ヘッダのエラーのために破棄された着信データグラムの数
Unknown Protocols Received	不明またはサポートしていないプロトコルのデータのため、受信には成功したが破棄された、ローカルなアドレスを持つデータグラムの数
Received Packets Delivered	IP ユーザプロトコル（ICMP を含む）まで正しく配送された、着信データグラムの総数
Discarded Output Packets	ディスティネーションへの送信のためには問題がなかったが、（バッファ容量の問題等で）破棄された発信データグラムの数
Fragments Created	このエンティティで分割を行った結果生成された、データグラムフラグメントの数
Routing Discards	有効なエントリであったにもかかわらず、破棄されてしまったルーティングエントリの数。エントリがこのように破棄される理由の 1 つに、他のルーティングエントリのためにバッファ容量を空ける必要があったことが考えられる。
Reassembly Successful	再構築に成功したデータグラムの数
Datagrams Successfully Fragmented	このエンティティで分割に成功した IP データグラムの数

設定方法

[IP] → [Statistics] → [IP] をクリックします。



IP Statistics

Packets Received	6471	Received Header Errors	0
Received Address Errors	0	Unknown Protocols Received	0
Received Packets Discarded	0	Received Packets Delivered	6465
Output Requests	8149	Discarded Output Packets	0
Output Packet No Route	0	Fragments Created	0
Datagrams Forwarded	0	Routing Discards	0
Reassembly Required	0	Reassembly Successful	0
Reassembly Failures	0	Datagrams Successfully Fragmented	0
Datagrams Failing Fragmentation	0		

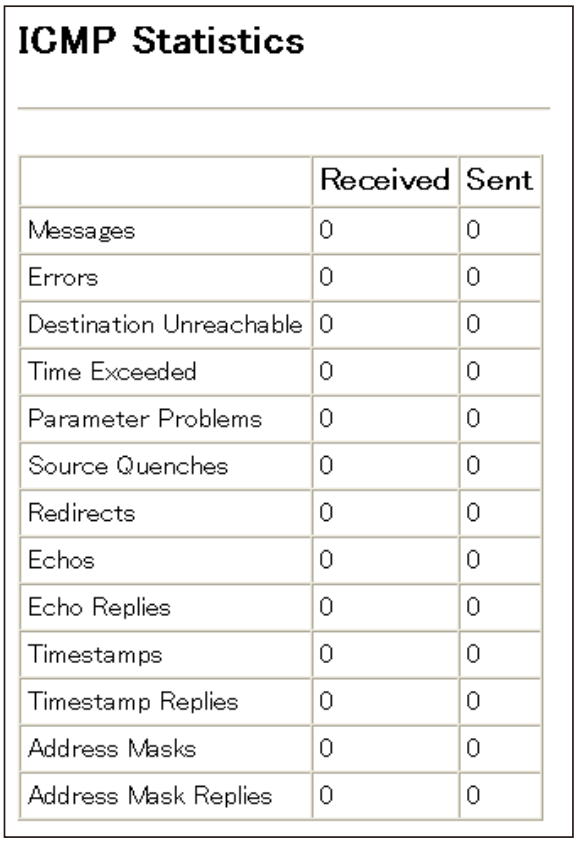
ICMP の統計情報

ICMP（Internet Control Message Protocol）はネットワークレイヤのプロトコルで、IP パケットの処理中に発生したエラーをレポートする情報パケットを送信します。そのため、ICMP は IP の全体的な部分をカバーしています。ICMP メッセージは様々な状況をレポートするのに使用されます。例えば、データグラムがディスティネーションに到達しない場合、データグラムをフォワーディングできるだけのバッファ容量がゲートウェイで不足している場合、またゲートウェイがホストにトラフィックをより短い経路で送信するよう指示する場合などです。ICMP はまた、特定のディスティネーションに関する、より最適な経路（ネクストホップのルータ）についての情報をフィードバックする際にも、ルータにより使用されます。

項目	内容
Messages	このエンティティが送受信した ICMP メッセージの総数
Errors	このエンティティが送受信した ICMP メッセージのうち、ICMP に関するエラー（ICMP チェックサムエラー、パケット長のエラーなど）が検出された ICMP メッセージの数
Destination Unreachable	送受信した ICMP Destination Unreachable メッセージの数
Time Exceeded	送受信した ICMP Time Exceeded メッセージの数
Parameter Problems	送受信した ICMP Parameter Problem メッセージの数
Source Quenches	送受信した ICMP Source Quench メッセージの数
Redirects	送受信した ICMP Redirect メッセージの数
Echos	送受信した ICMP Echo（リクエスト）メッセージの数
Echo Replies	送受信した ICMP Echo Reply メッセージの数
Timestamps	送受信した ICMP Timestamp（リクエスト）メッセージの数
Timestamp Replies	送受信した ICMP Timestamp Reply メッセージの数
Address Masks	送受信した ICMP Address Mask Request メッセージの数
Address Mask Replies	送受信した ICMP Address Mask Reply メッセージの数

設定方法

[IP] → [Statistics] → [ICMP] をクリックします



ICMP Statistics

	Received	Sent
Messages	0	0
Errors	0	0
Destination Unreachable	0	0
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenches	0	0
Redirects	0	0
Echos	0	0
Echo Replies	0	0
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0

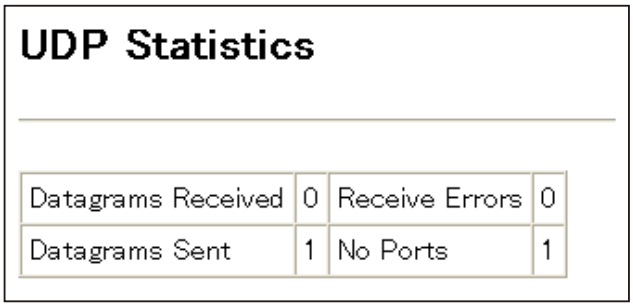
UDP の統計情報

UDP（User Datagram Protocol）は、パケット交換によるデータグラムの通信モードを提供します。UDP は、下位の転送メカニズムに IP を使用し、IP に類似するサービスを提供します。UDP パケットは、目的地への到達前に破棄される可能性のあるコネクションレス型のデータグラムで、IP パケットのように配送されます。UDP は TCP が複雑過ぎて時間がかかったり、単に TCP が必要でない場合に有効です。

項目	内容
Datagrams Received	UDP ユーザに配送した UDP データグラムの総数
Datagrams Sent	このエンティティから送信した UDP データグラムの総数
Receive Errors	ディスティネーションポートにアプリケーションがないという理由以外で配送されず受信した、UDP データグラムの数
No Ports	ディスティネーションポートでアプリケーションがないという理由で受信した、UDP データグラムの総数

設定方法

[IP] → [Statistics] → [UDP] をクリックします。



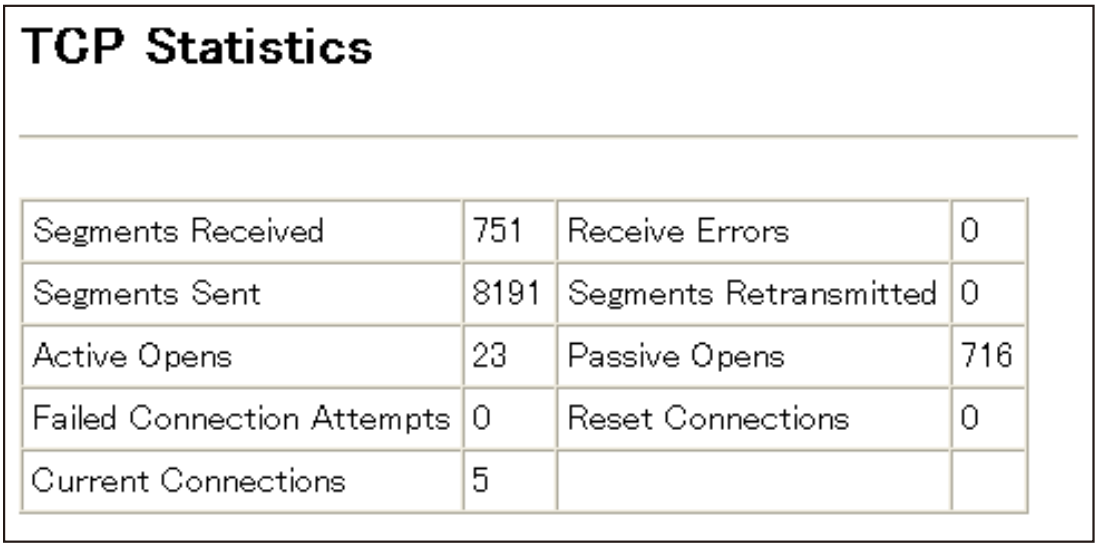
TCP の統計情報

TCP（Transmission Control Protocol）は、パケット通信網で信頼性の高いホスト - ホスト間の通信を提供します。TCP は IP と一緒に使用され、多様なインターネットプロトコルをサポートします。

項目	内容
Segments Received	ラーを含む、受信したセグメントの総数。現在確立している接続で受信したセグメント数もこの数に含まれます。
Segments Sent	送信したセグメントの総数。現在確立している接続で送信したセグメント数は含まれますが、再送のみのセグメント数は含まれません。
Active Opens	CLOSED ステートから SYN-SENT ステートに直接遷移した TCP コネクションの回数
Failed Connection Attempts	SYN-SENT ステートまたは SYN-RCVD ステートから CLOSED ステートに直接遷移した TCP コネクションの回数と、SYN-RCVD ステートから LISTEN ステートに直接遷移した TCP コネクションの回数を合算した数
Current Connections	現在のステートが ESTABLISHED または CLOSE-WAIT ステートの TCP コネクションの数
Receive Errors	TCP チェックサムエラーなど、エラーで受信したセグメントの総数
Segments Retransmitted	再送されたセグメントの総数。すでに 1 回以上送信された部分を含む TCP セグメントの数のことです。
Passive Opens	LISTEN ステートから SYN-RCVD ステートに直接遷移した TCP コネクションの回数
Reset Connections	STABLISHED ステートまたは CLOSE-WAIT ステートから CLOSED ステートに直接遷移した TCP コネクションの回数

設定方法

[IP] → [Statistics] → [TCP] をクリックします。



TCP Statistics

Segments Received	751	Receive Errors	0
Segments Sent	8191	Segments Retransmitted	0
Active Opens	23	Passive Opens	716
Failed Connection Attempts	0	Reset Connections	0
Current Connections	5		

3.17.4 静的な経路の設定

本機は動的なルーティングプロトコル（RIP、OSPF）を使用して、他のネットワークセグメントへ動的に経路を設定することができます。また、ルーティングテーブルに、手作業により経路を静的に入力することもできます。静的な経路は、動的なルーティングをサポートしていないネットワークセグメントへアクセスする場合や、特定のサブネットへの経路を限定したい場合など、動的なルーティングを使いたくない際に必要です。静的な経路はネットワークトポロジの変化にともなって自動的に変更されることはないため、ネットワークでのアクセスビリティを確保するために、静的な経路の設定は最小限にとどめる方が良いでしょう。

設定・表示項目

Interface

IP インタフェースの識別番号。

IP Address

ディスティネーションネットワーク、サブネットワーク、またはホストの IP アドレス。

Netmask

IP サブネットに関連付けられているネットマスク。このマスクは、特定のサブネットにルーティングされる際に使用されるホストアドレスのビットを識別します。

Gateway

ルーティングに使用されるゲートウェイの IP アドレス。

Metric

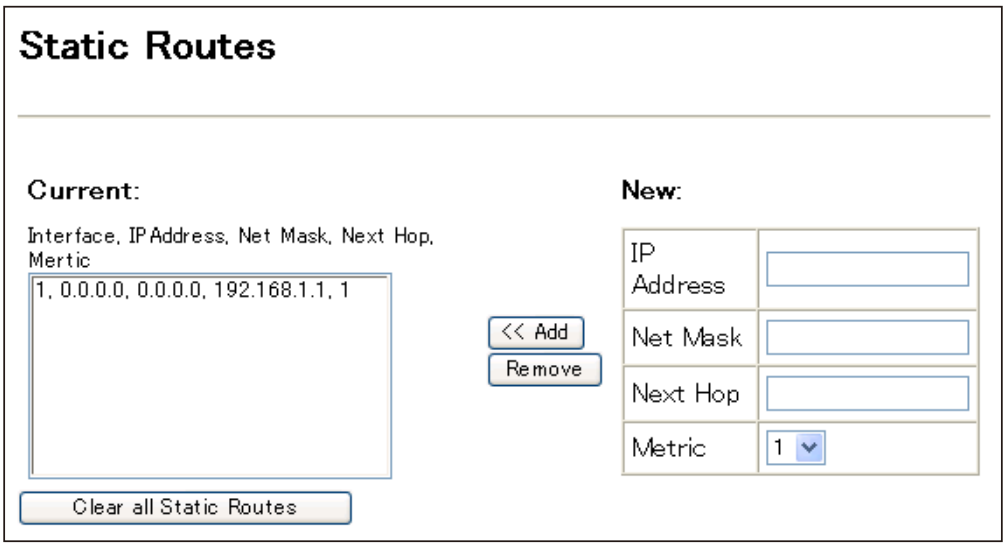
このインタフェースのコスト。このコストは RIP などの動的なルーティングプロトコルによって経路が読み込まれた場合のみに使用されます。（範囲：1-5、初期設定：1）

Entry Count

テーブルエントリの数。

設定方法

[IP] → [Routing] → [Static Routes] をクリックします。



ルーティングテーブルの表示

ローカルネットワークインタフェース、静的な経路、または動的に学習された経路を介してアクセス可能なすべての経路を表示できます。これらの経路情報が重複する場合、経路選択される際の優先順位はローカル、静的、動的の順になります。また、ローカルインタフェースの経路については、たとえルーティングテーブルに表示されていても、少なくとも 1 つのアクティブなリンクがこのインタフェースに接続しない限り有効とならないことに注意が必要です。

設定・表示項目

Interface

IP インタフェースのインデックス番号。

ディスティネーションネットワーク、サブネットワーク、またはホストの IP アドレス。IP アドレス 0.0.0.0 は本機のデフォルトゲートウェイを示すことに注意してください。

Netmask

IP サブネットに関連付けられているネットマスク。このマスクは、特定のサブネットにルーティングされる際に使用されるホストアドレスのビットを識別します。

Next Hop

経路のネクストホップ（ゲートウェイ）の IP アドレス。

Protocol

経路情報を生成した方法 / プロトコル名。（表示項目：local、static、RIP）

Metric

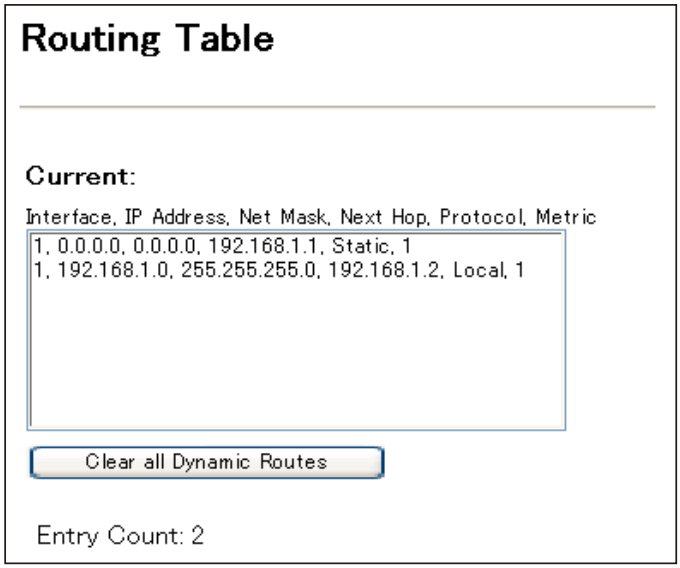
インタフェースのコスト。

Entry Count

テーブルエントリの数。

設定方法

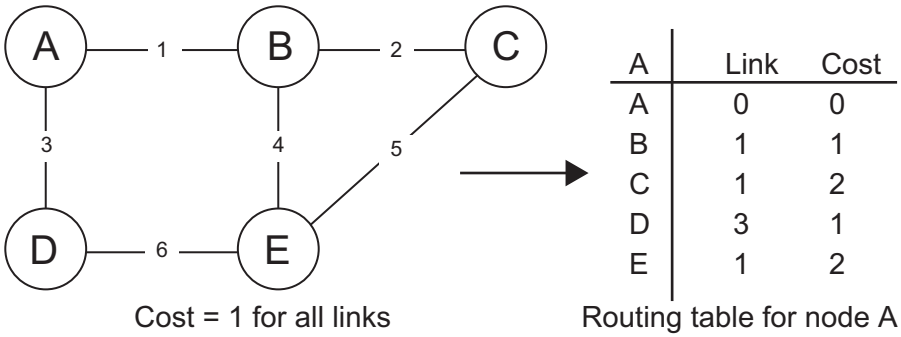
[IP] → [Routing] → [Routing Table] をクリックします。



3.18 ユニキャストルーティング

3.18.1 RIP の設定

RIP（Routing Information Protocol）は最も広く使用されているルーティングプロトコルです。RIP はルーティングに距離ベクトル型の手法を採用しています。経路は、より小さな距離ベクトル（ホップ数。通信時のコストの大まかな見積もりのために使用される）を選択することにより決定されます。各ルータは 30 秒ごとに、自身のルーティングテーブルの更新情報を含め、広告をブロードキャストします。これにより、同一ネットワーク上のすべてのルータは、正しいサブネットに導くネクストホップのリンクについて、一貫性のあるテーブルを所有することができます。



機能解説

- レイヤ 2 スイッチがループを回避するために STP（Spanning Tree）アルゴリズムを採用するように、ルータもデータトラフィックのエンドレスな再送を発生させるループを回避する手法を使用しています。RIP は次の 3 つの方法を使用してループの発生を回避します。
  静的なエントリは、一定の時間を経過したとき自動的に消去されたり、電源をリセットした場合でも消去されません。静的なエントリは設定インタフェースからのみ消去できます。

  －スプリットホライズン
  その経路情報を送信してきたインタフェースポートには経路情報を広告しません。

－ポイズンリバース
その経路情報を送信してきたインタフェースポートに経路情報を広告するが、距離ベクトル型のメトリックは無限大に設定します。（これにより収束時間を短縮できます）
－トリガアップデート
経路が変化した際はいつでも、短い遅延時間を経てアップデートメッセージを広告しますが、周期的なサイクルで待つことはありません。

- RIP v2 は RIP からアップグレードされたもので、RIP と互換性があります。RIP v2 には平文認証、複数の独立する RIP ドメイン、可変長のサブネットマスク、および経路情報の広告にマルチキャストの転送方法を採用、という追加されたより使いやすい機能があります。（RFC1723）
- RIP には考慮すべき重要な問題がいくつかあります。まず、RIP v1 にはサブネットの概念がありません。RIP v1/v2 はリンクやルータに障害が発生したあと新たな経路情報が収束するまでに長い時間が必要なため、この間にルーティングループが発生する可能性があります。それから、ホップ数の制限がわずか 15 のために大規模ネットワークでは使用できません。また、RIP v1 は経路情報をブロードキャストするため、大切なネットワーク帯域を浪費します。さらに、ネットワーク変数をほとんど考慮しないため最良の経路を決定できません。

RIP の設定

RIP はルータが経路情報を交換する方法を定義するのに使用されます。本機で RIP を有効に設定すると、本機と同じネットワークに所属するすべてのデバイスに向けて RIP メッセージを（初期設定で）30 秒ごとに送信し、他のルータから RIP メッセージを受信すると本機自身のルーティングテーブルを更新します。RIP を使用して他のルータと正しく通信するためには、本機全体で使用する RIP のバージョンや（Global RIP Version）、インタフェースで使用する RIP の送受信のバージョン（Receive or Send Version）を設定する必要があります。

機能解説

- Global RIP Version を設定する場合、Receive or Send Version（P17-35）で設定されていない VLAN インタフェースに次の値を設定します。
  － RIPv1：未設定のインタフェースに対し、送信には RIP v1 互換プロトコルメッセージを使用し、受信には RIP v1 または RIP v2 プロトコルメッセージを使用するよう設定します。
  － RIPv2：未設定のインタフェースに対し、送受信両方のプロトコルメッセージに RIP v2 を使用するよう設定します。
- アップデートタイマーはすべての基本的な RIP プロセスを制御するのに使用される、重要なタイマーです。
  －アップデートタイマーの間隔を短くしすぎると、ルータがアップデートの処理に膨大な時間を費やすことになります。一方、長くしすぎるとネットワーク構成の変更を検出しにくいルーティングプロトコルになってしまいます。
  －アップデートタイマーは、同一ネットワークのすべてのルータに同じ値を設定しなくてはなりません。

設定・表示項目

Global

RIP Routing Process

本機の IP インタフェースで RIP によるルーティングを使用する（Enabled）かしない（Disabled）かを設定します。（初期設定：Disabled）

Global RIP Version

本機でグローバルに使用する RIP のバージョンを設定します。（初期設定：RIPv1）

Timer

Update

アップデート情報の送信間隔を設定します。この値を 6 倍した値がタイムアウト時間として、4 倍した値がガベージコレクション時間として設定されます。（範囲：15-60 秒、初期設定：30 秒）

Timeout

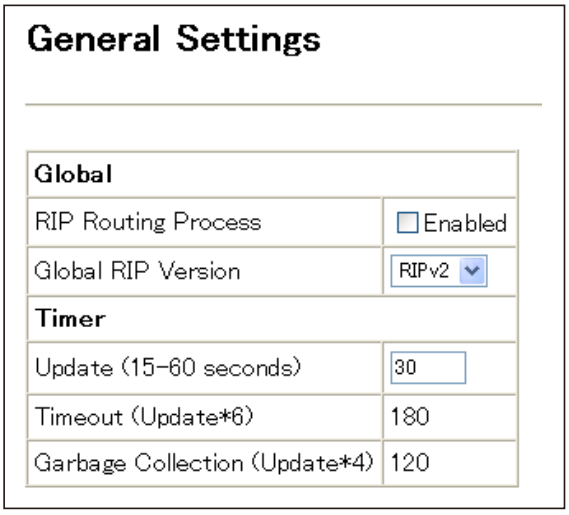
経路の障害を通知するアップデートメッセージが送信されなくなってからの経過時間を設定します。経路が（メトリックが無限大などの理由により）アクセスできないと判断され、到達不可能と広告されます。ただし、パケットはこの経路にフォワーディングされ続けます。（初期設定：180 秒）

Garbage Collection

タイムアウト時間の経過後、ルーティングテーブルからエントリを削除するまでのガベージコレクション時間を設定します。ガベージコレクション時間の設定により、隣接ルータが経路情報を削除する前に無効な経路を認識するのに役立ちます。（初期設定：120 秒）

設定方法

[Routing Protocol] → [RIP] → [General Settings] をクリックします。RIP の有効または無効を設定し、未設定のインタフェースに対して RIPv1 または RIPv2 を設定し、基本のアップデートタイマー（Update）を設定します。[Apply] をクリックします。



RIP をサポートさせるネットワークインタフェースの指定

RIP のルーティングプロセスに組み込むネットワークインタフェースを指定します。

機能解説

- このコマンドで設定したインタフェースにのみ RIP のアップデート情報が送信されます。
- サブネットアドレスは、設定したアドレスの最初のフィールドに基付き、クラス A、B、C のいずれかに解釈されます。つまり、サブネットアドレス nnn.xxx.xxx.xxx を入力した場合、最初のフィールド（nnn）がクラスを決定します。

0 ～ 127 の場合クラス A となり、ネットワークアドレスの最初のフィールドのみ使用されます。
128～191の場合はクラスBとなり、ネットワークアドレスの最初から2つのフィールドのみ使用されます。
192～223の場合はクラスCとなり、ネットワークアドレスの最初から3つのフィールドのみ使用されます。

設定・表示項目

Subnet Address

本機に直接接続しているネットワークの IP アドレス。

設定方法

[Routing Protocol] → [RIP] → [Network Addresses] をクリックします。RIP をサポートさせるインタフェースをすべて追加します。[Apply] をクリックします。

各ネットワークインタフェースへの RIP の設定

RIP ルーティングプロセスに組み込む各インタフェースに対し、受信に使用するプロトコルメッセージの種類（RIP のバージョン）と送信に使用するプロトコルメッセージの種類（RIP バージョンまたは互換性モード）、プロトコルメッセージのループバックを回避する方法、および認証機能の使用または不要（認証機能は RIPv2 メッセージの送受信時のみ適用されます）を設定します。

機能解説

送信 / 受信プロトコルの種類の設定

- ここで各インタフェースに設定する受信のための RIP のバージョン（Receive Version）または送信のためのバージョン（Send Version）は、RIP：General Settings 画面の Global RIP Version フィールドで設定した値より優先されます。
- Receive Version は次の選択肢から設定できます。

－ローカルネットワークですべてのルータがRIPv1またはRIPv2のどちらか一方だけを使用している場合は、それぞれ ”RIPv1” または ”RIPv2” を設定します。
－ローカルネットワークでルータが RIPv1 と RIPv2 の両方を使用している場合は、“RIPv1 or RIPv2” を設定します。

－特定のインタフェースのルーティングテーブルに動的に保存させたくない場合は、“Do Not Receive” を設定します。（静的にのみルーティングさせたいインタフェースの場合など）

- Send Version は次の 3 つの選択肢から設定できます。

－ローカルネットワークのすべてのルータがRIPv1またはRIPv2のどちらか一方だけを使用している場合は、それぞれ ”RIPv1” または ”RIPv2” を設定します。

－ネットワークの他のルータに経路情報をブロードキャストする際、RIPv2 で通常要求されるマルチキャストではなく、RIPv2 の広告リストを使用する場合は “RIPv1 Compatible” を設定します。（このモードを使用すると、RIPv1 のルータはプロトコルメッセージを受信でき、RIPv2 のルータは RIPv2 で提供される追加情報（サブネットマスク、ネクストホップ、および認証情報）を受信できます。

－ネットワークに接続している他のルータから広告される経路情報を受動的にモニタリングするだけの場合は、“Do Not Send” を設定します。

ループバックの回避

レイヤ 2 スイッチがループ発生の回避にスパニングツリーアルゴリズムを使用するように、ルータも、通信データのエンドレスな再送の原因となるループを回避する手法を採用しています。プロトコルパケットがループに取り込まれると、リンクは輻輳し、プロトコルパケットは破棄されます。しかし、ネットワークはゆっくりと新たなステートに収束していきます。RIP は次の 3 つの手法を使用してネットワークトポロジの変化時により高速に収束させるようにし、ほとんどのループの発生を回避します。

- スプリットホライズン
  その経路情報を送信してきたインタフェースポートには経路情報を広告しません。
- ポイズンリバース
  その経路情報を送信してきたインタフェースポートに経路情報を広告するが、距離ベクトル型のメトリックは無限大に設定します。（これにより収束時間を短縮できます）
- トリガアップデート
  経路が変化した際はいつでも、短い遅延時間経てアップデートメッセージを広告するが、周期的なサイクルで待つことはありません。

プロトコルメッセージの認証

RIPv1 はセキュアなプロトコルではありません。UDP ポート 520 番からプロトコルメッセージを送信するデバイスは、隣接するデバイスからそのデバイスがルータであることを知られてしまいます。認証方式を導入しない場合、ネットワーク全体に、悪意のある、または望まれないプロトコルメッセージが簡単に伝搬します。RIPv2 は簡単なパスワードによって認証をサポートしています。ルータが認証メッセージを交換するよう設定されている場合、送信側は転送されるすべてのプロトコルパケットにパスワードを付加し、受信側では受信したすべてのパケットに承認されたパスワードが含まれているかをチェックします。受信したメッセージのパスワードが正しくない場合、そのメッセージは破棄されます。

設定・表示項目

VLAN

設定する VLAN の ID（1-4093）

Receive Version

インタフェースで受信する RIP のバージョン。

－ RIPv1：RIPv1 パケットのみを受信。

－ RIPv2：RIPv2 パケットのみを受信。

－ RIPv1 or RIPv2：RIPv1 または RIPv2 パケットを受信。（初期設定）

－ Do Not Receive：RIP パケットの受信を拒否。

（初期設定は、[RIP] → [General Settings] メニューの画面の Global RIP Version フィールドの選択肢に準じます。（RIPv1 の場合 " RIPv1 or RIPv2"、RIPv2 の場合 "RIPv2"））

Send Version

インタフェースから送信する RIP のバージョン。

- RIPv1：RIPv1 パケットのみを送信。
- RIPv2：RIPv2 パケットのみを送信。
- RIPv1 Compatible：他のルータへの経路情報のブロードキャストには RIPv2 を使用（初期設定）
- Do Not Send：RIP のアップデート情報を送信しない。

（初期設定は、[RIP] → [General Settings] メニューの画面の Global RIP Version フィールドの選択肢に準ずる。（RIPv1 の場合 " RIPv1 Compatible"、RIPv2 の場合 "RIPv2"））

Instability Preventing

ネットワークトポロジの変化時に収束時間を短縮させ、ソースルータに RIP プロトコルメッセージがループバックすることを回避させる手法を設定します。（初期設定：Split Horizon）

- None：手法を設定しません。ループが発生した場合、経路が到達不可能であると判断される前に、経路のホップ数が無限大（16）になるまで徐々に 1 ずつ増加します。
- Split Horizon：送信してきたインタフェースには経路情報の伝搬を行いません。
- Poison Reverse：送信してきたインタフェースに経路情報の伝搬を行いますが、距離ベクトル型のメトリックを無限大に設定します。（より高速に収束します）

Authentication Type

プロトコルメッセージの交換に認証を使用するか否かを設定します。（初期設定：No Authentication）

- No Authentication：認証を使用しません。
- Simple Password：承認されたパスワードを使用して、インタフェースは他のルータとの経路情報の交換を行います。（この選択肢は RIPv2 のみに適用されることに注意してください）

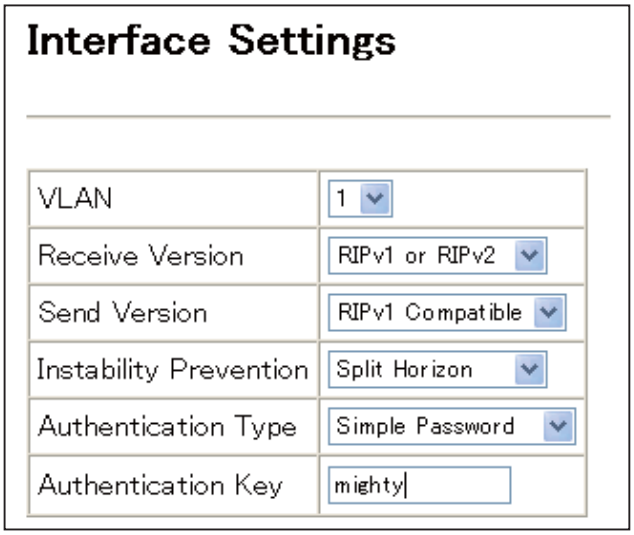
Authentication Key

RIPv2 パケット認証のためのパスワードを設定します。認証が正しく機能するためには、送受信双方のインタフェースが同じパスワードを使用する必要があります。（範囲：1-16 桁の半角文字列。大文字小文字を識別します）

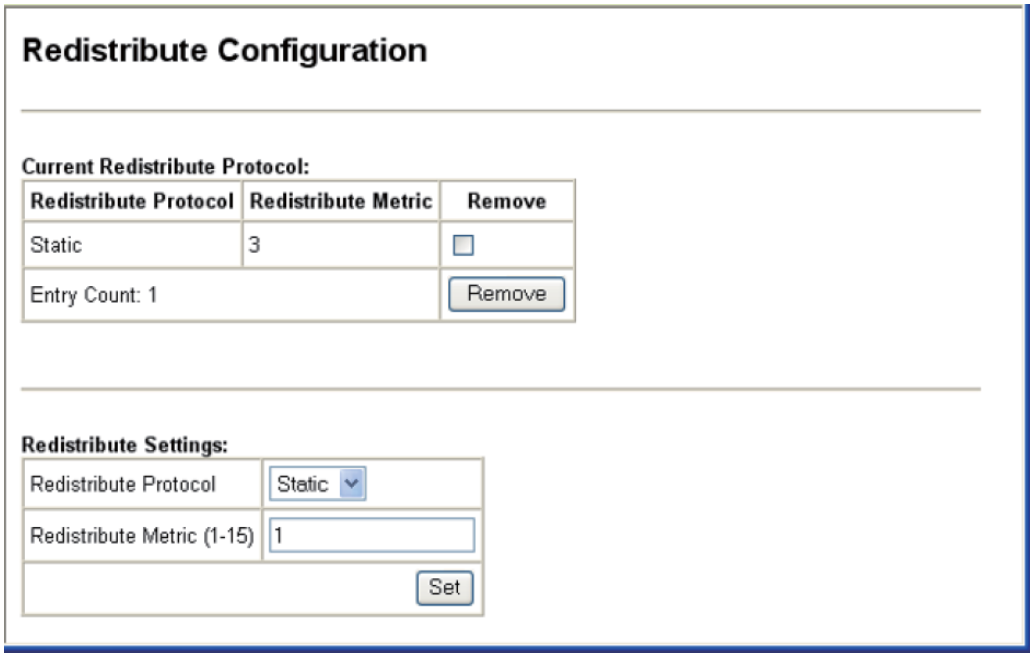
設定方法

[Routing Protocol] → [RIP] → [Interface Settings] をクリックします。受信、送信、それぞれに RIP プロトコルメッセージの種類を選択し、（ネットワークトポロジの安定性確保のた

め）高速な収束とループバック回避を提供する手法を選択し、認証の種類とそのパスワードを設定します。[Apply] をクリックします。



他のドメインからのルーティン情報を再配布



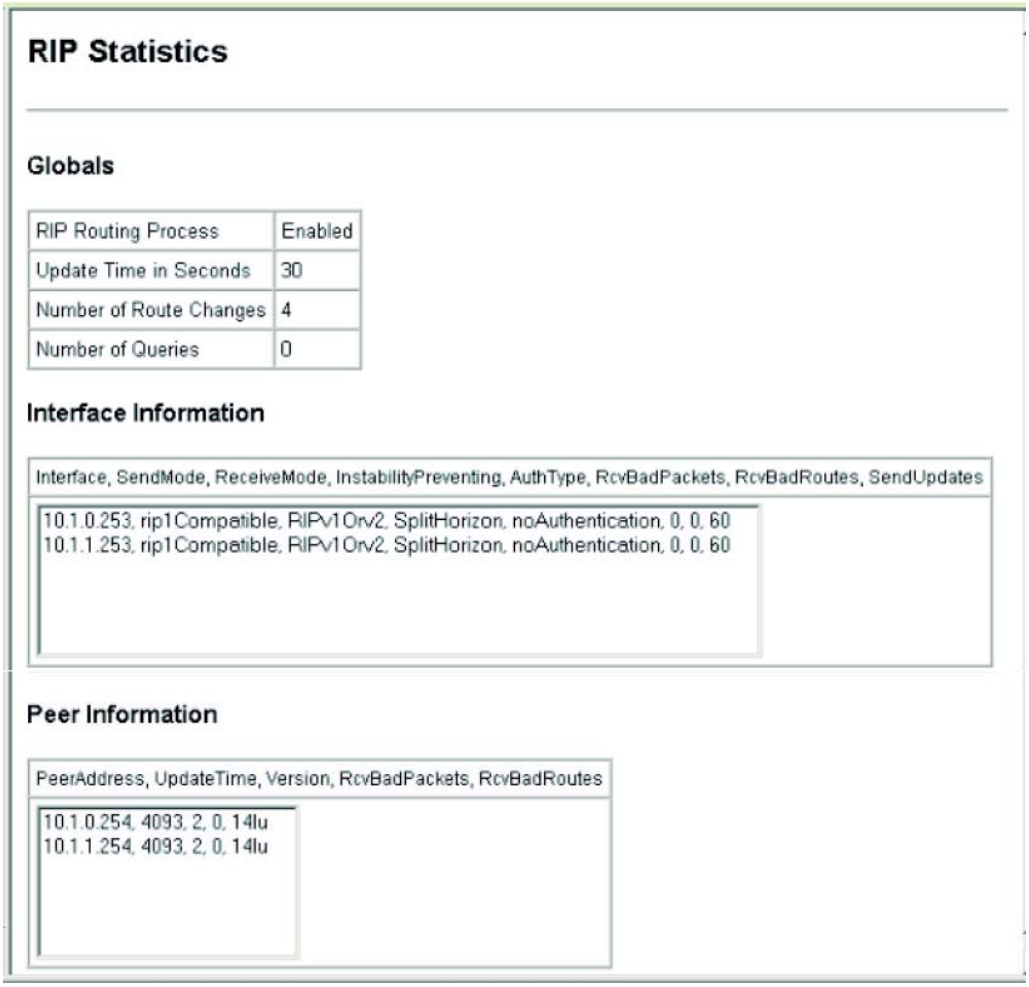
RIP の情報と統計情報の表示

RIP の現時点でのグローバルな設定内容についての基本的な情報、経路の変更や照会についての統計情報、RIP が有効なルータのインタフェース情報、および既知のピアの RIP デバイスについての情報を表示できます。

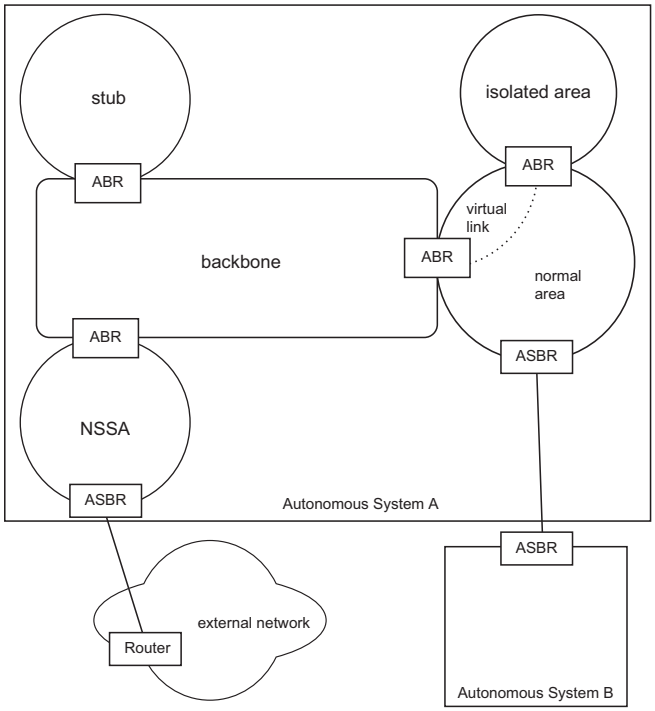
項目	内容
Globals	
RIP Routing Process	RIP の有効 / 無効の表示
Update Time in Seconds	RIP が経路情報を広告する間隔（初期設定：30 秒）
Number of Route Changes	経路情報が変更された回数
Number of Queries	本機がルーティングデータベースの照会を受けた回数
Interface Information	
Interface	インタフェースの IP アドレス
SendMode	このインタフェースが送信する RIP のバージョン（none、RIPv1、RIPv2、rip1Compatible）
ReceiveMode	このインタフェースが受信する RIP のバージョン（none、RIPv1、RIPv2、RIPv1Orv2）
InstabilityPreventing	スプリットホライズン、ポイズンリバースまたは安定性の確保手段はいずれも選択していない、についての表示
AuthType	単純なパスワードによる認証か、認証設定していないかについての表示
RcvBadPackets	受信した、RIP エラーパケット数
RcvBadRoutes	受信した、障害のある経路の数
SendUpdates	経路の変更が発生した数
Peer Information	
PeerAddress	RIP の隣接ルータの IP アドレス
UpdateTime	ピアの隣接ルータから直前に経路情報を受信した時間
Version	ピアの隣接ルータから RIPv1 または RIPv2 どちらのパケットを受信したか
RcvBadPackets	ピアの隣接ルータから受信した、RIP エラーパケット数
RcvBadRoutes	ピアの隣接ルータから受信した、障害のある経路の数

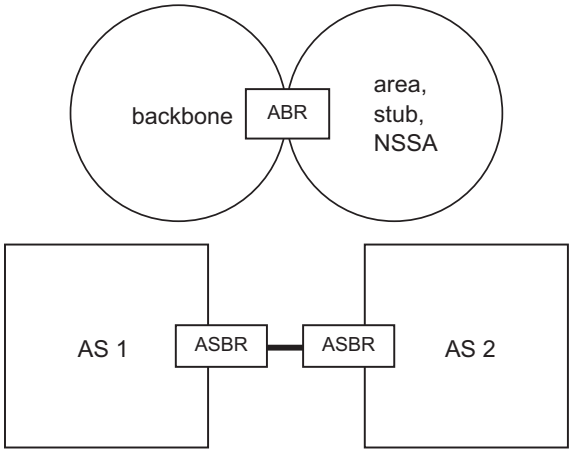
設定方法

[Routing Protocol] → [RIP] → [Statistics] をクリックします。



3.18.2 OSPF の設定





OSPF の設定

設定・表示項目

OSPF Routing Process

全ての IP インタフェースで、OSPF ルーティングを有効 / 無効（初期設定：無効）

OSPF Router ID

OSPF ルータ ID（初期設定：一番低いインタフェースアドレス）

Version Number

本機は OSPF バージョン 2 のみサポート

Area Border Router

エリア境界ルータ

Rfc1583 Compatible

RFC 1583 (OSPFv1) **を使用して、サマリー ルートのコストを計算します。**(Default:Disabled)

OSPF Hold Time (seconds)

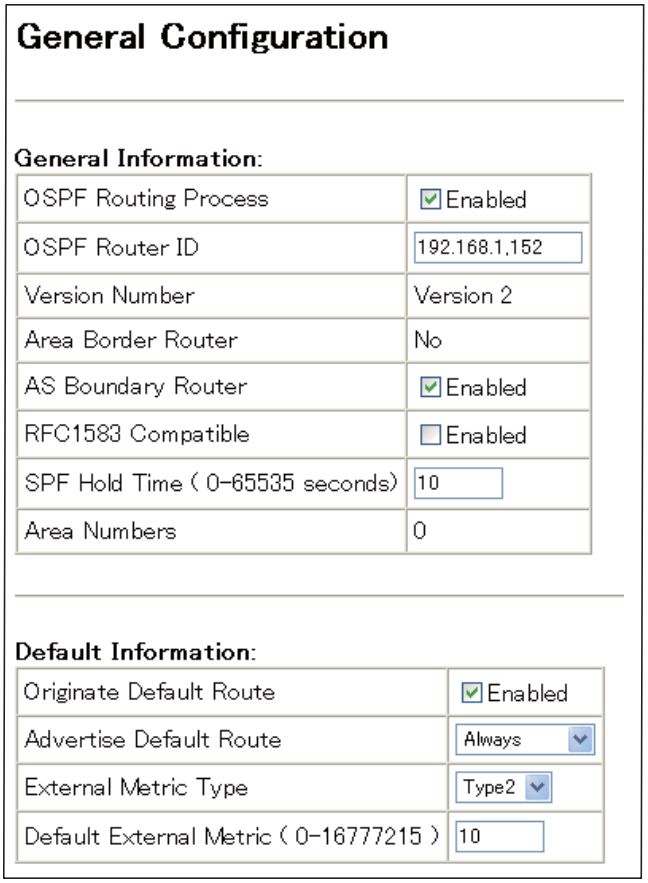
OSPF **ホールドタイム** (**範囲：**0-65535 **秒　初期設定：**10 **秒**)

Area Numbers

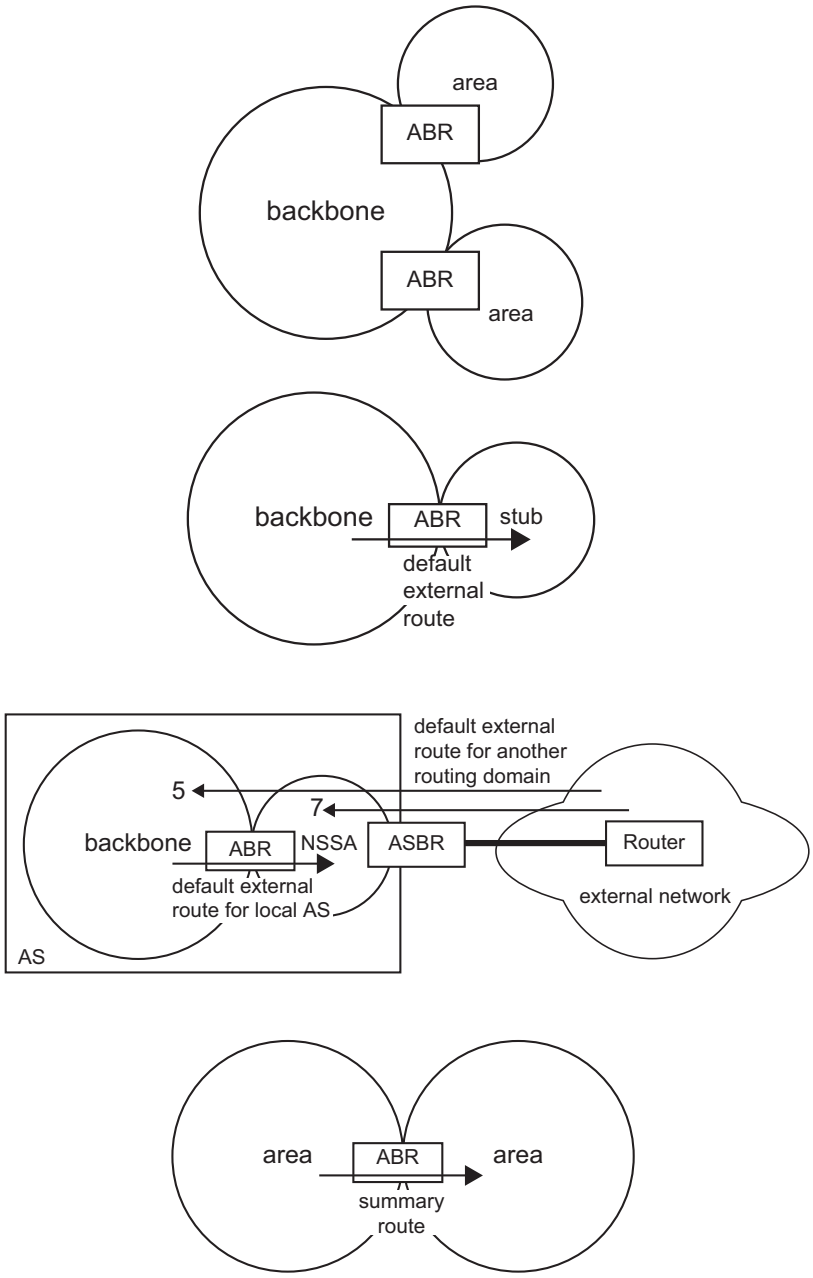
OSPF **エリア番号**

設定方法

[Routing Protocol] → [OSPF] → [General Configuration] **をクリックします。**



OSPF エリアの設定



設定・表示項目

Area ID

エリア ID（stub **または** NSSA）

Area Type

normal area, stub area, or not-so-stubby area(NSSA) **を指定。**

エリア ID 0.0.0.0 **はバックボーンにデフォルトで設定されます。(** **初期設定：**Normal area)

Default Cost

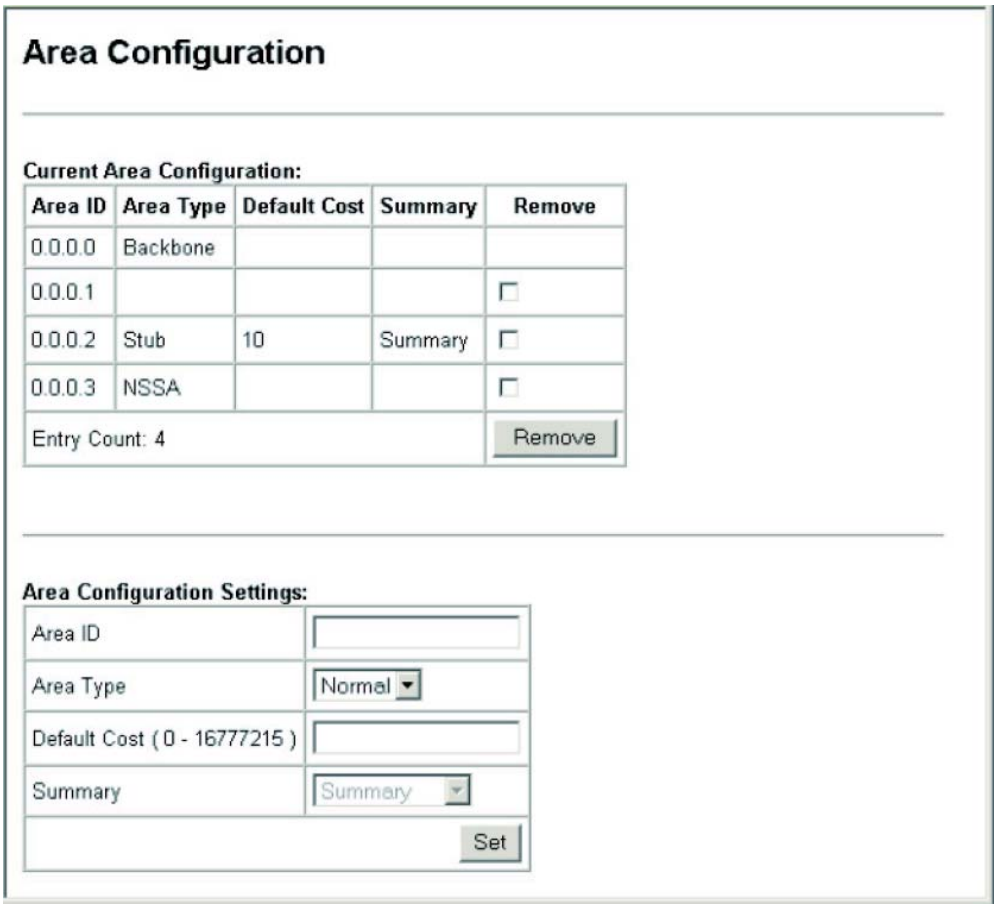
デフォルトサマリルートのコスト (**範囲：**0-16777215　**初期設定：**1)

Summary

- **スタブ内のすべてのルータは、同じエリア** ID **で構成されている必要があります。**
- **ルーティング テーブル スペースは、タイプ** 4 AS **サマリー** LSA **およびタイプ** 5 **外部** LSA **をブロックすることにより、スタブ内に保存されます。このコマンドのデフォルト設定では、ローカル エリアまたは自律システム外部の宛先へのデフォルト ルートをアドバタイズするタイプ** 3 **サマリー** LSA **をブロックすることにより、スタブを完全に分離します。**(Default: Summary).

設定方法

[Routing Protocol] → [OSPF] → [Area Configuration] **をクリックします。**



OSPF エリアレンジの設定

設定・表示項目

Area ID

ルートを要約するエリアを識別します

(エリア ID **は、**IP **アドレスと同じ形式である必要があります)。**

Range Network

要約するルートのベース アドレスです。

Range Netmask

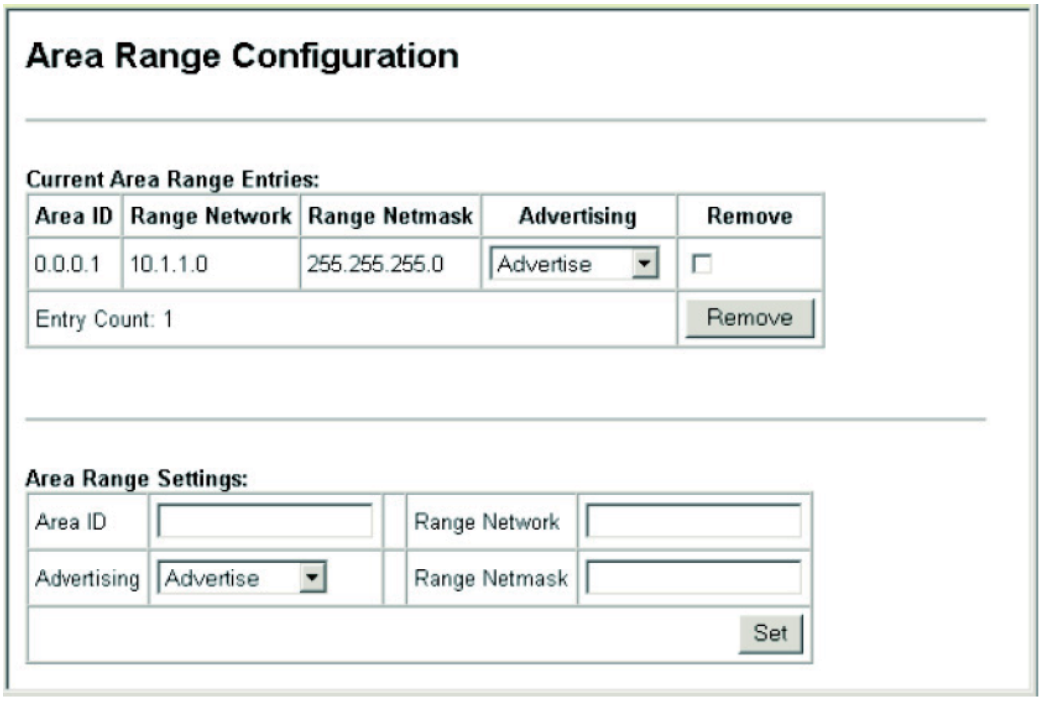
サマリー ルートのネットワーク マスクです。

Advertising

指定されたアドレス範囲をアドバタイズします。(Default: Advertise)

設定方法

[Routing Protocol] → [OSPF] → [Area Range Configuration] をクリックします。



OSPF インタフェースの設定

設定・表示項目

VLAN ID

VLAN ID を指定

Interface IP

インタフェースの IP アドレスを指定

Area ID

エリア ID を指定

Designated Router

このエリアの Designated ルータ

Backup Designated Router

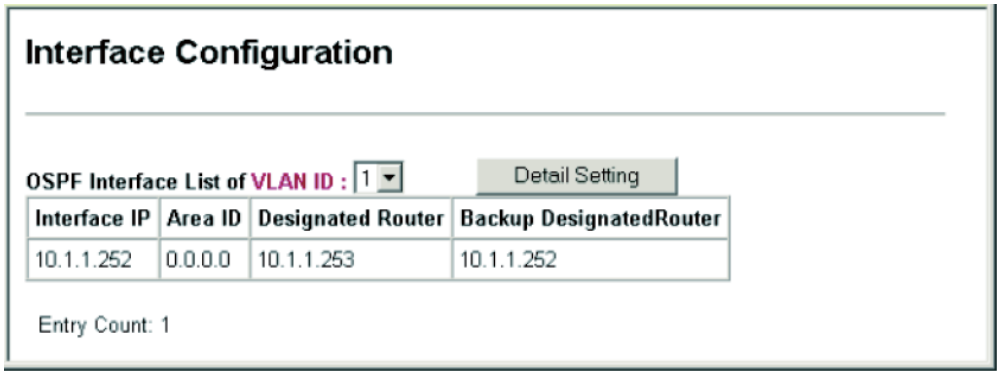
このエリアの Designated バックアップルータ

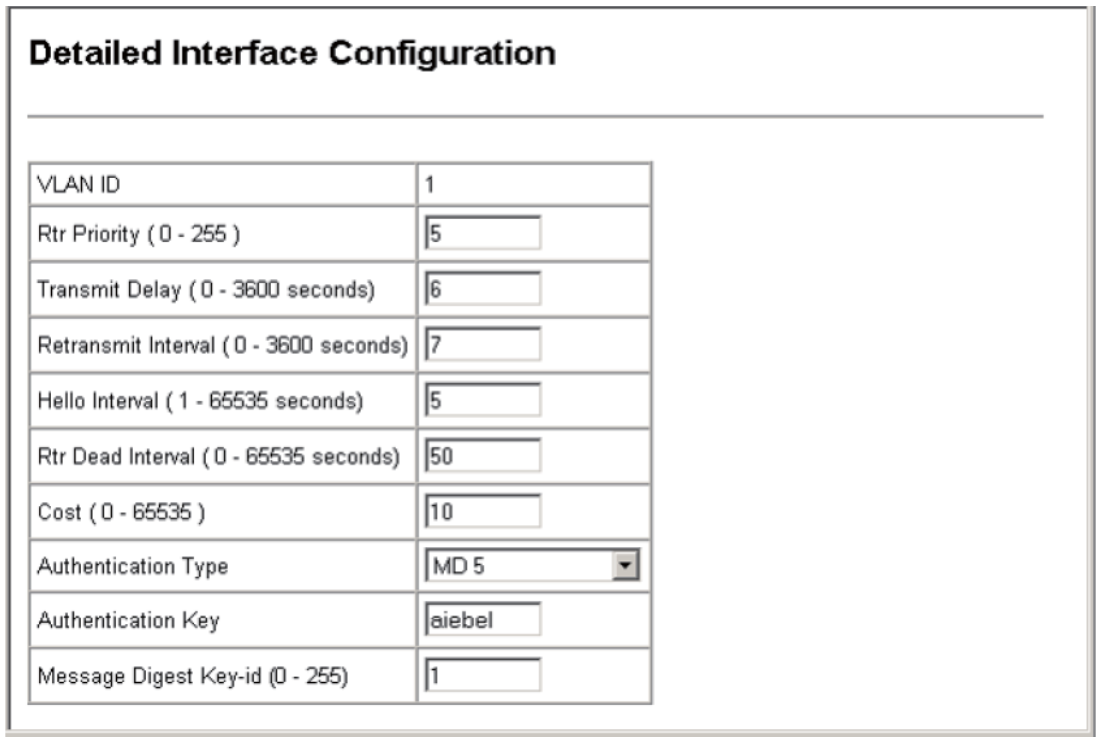
Entry Count

この VLAN にアサインされている IP インタフェースの数

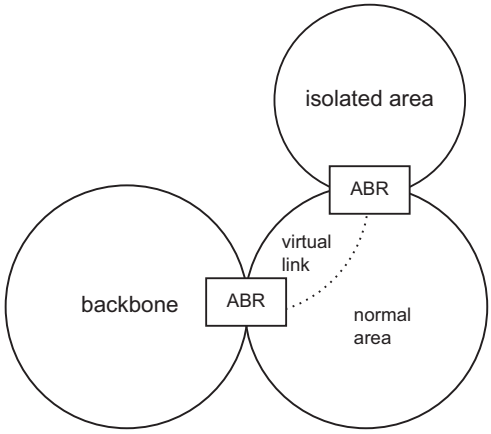
設定方法

[Routing Protocol] → [OSPF] → [Interface Configuration] **をクリックします。**





バーチャルリンクの設定



設定・表示項目

Area ID

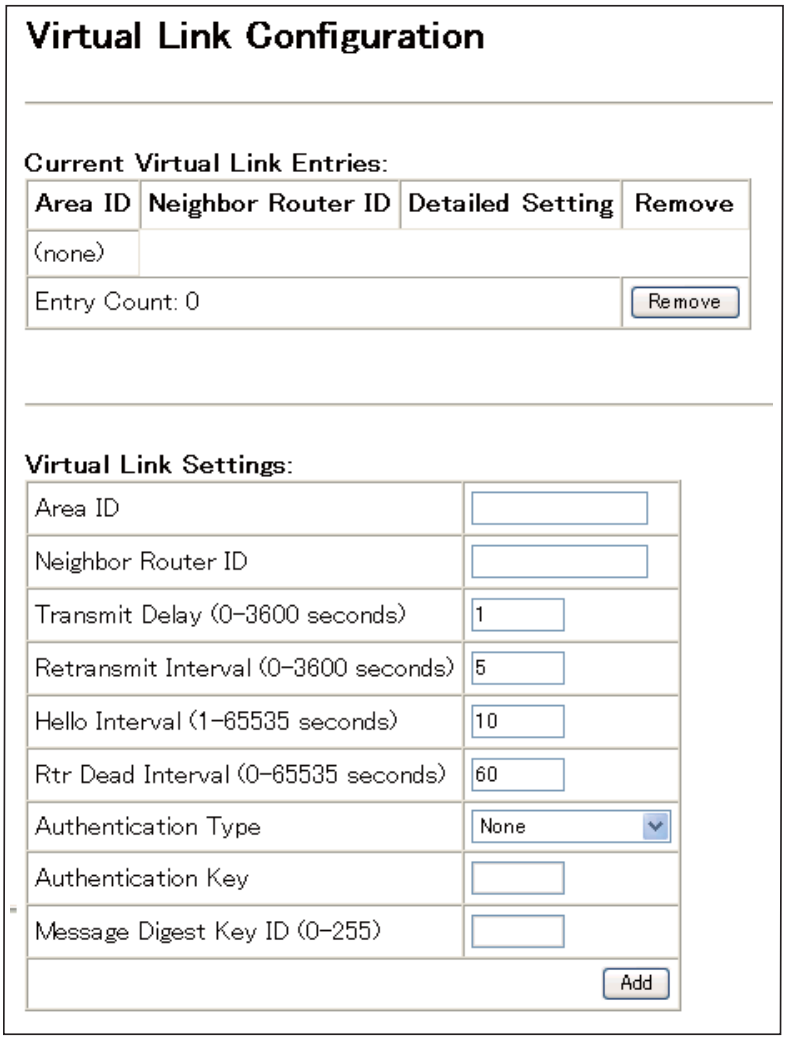
area-id - **仮想リンクのトランジット エリアの識別子です**
（エリア ID **は、**IP **アドレスと同じ形式である必要があります）。**

Neighbor Router ID

仮想リンクの隣接ルータのルータ ID **です。このルータは、仮想リンクの**
他方の端にあるバックボーンとトランジット エリア両方に隣接するエリア境界ルータ（ABR**）である必要があります。**

設定方法

[Routing Protocol] → [OSPF] → [Virtual Link Configuration] をクリックします。



ネットワークエリアアドレスの設定

設定・表示項目

IP Address

エリアに追加するインタフェースの IP アドレス

Netmask

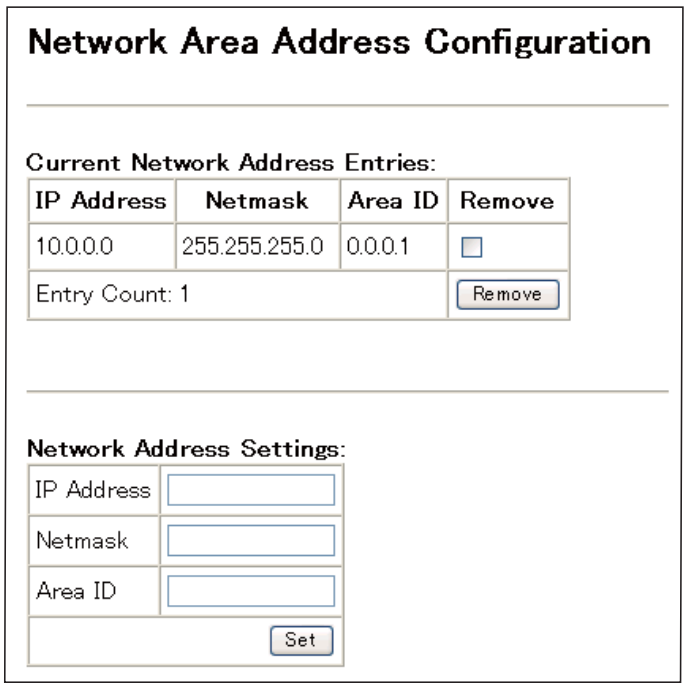
エリアに追加するインタフェースのネットマスク .

Area ID

エリア ID を指定 (エリア ID は IP アドレスのフォームになります)

設定方法

[Routing Protocol] → [OSPF] → [Network Area Address Configuration.] をクリックします。



サマリアドレスの設定

設定・表示項目

IP Address

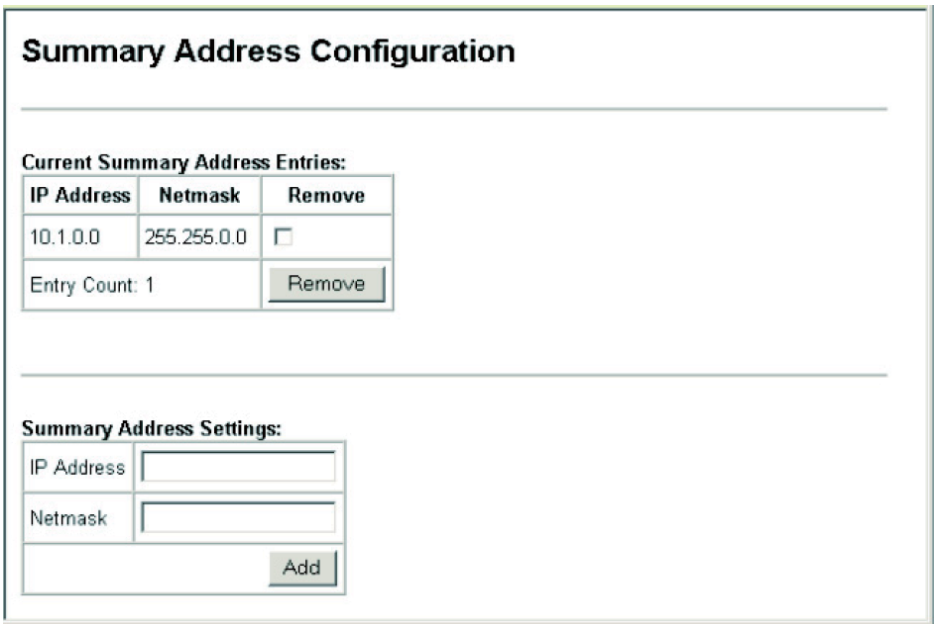
アドレス範囲をカバーするサマリー アドレスです。

Netmask

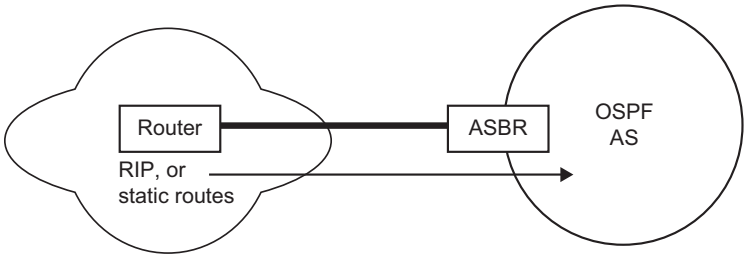
サマリー ルートのネットワーク マスクです。

設定方法

[Routing Protocol] → [OSPF] → [Summary Address Configuration] をクリックします。



外部ルートの再配布



設定・表示項目

Redistribute Protocol

外部ルーティングプロトコルタイプを指定します。（オプション：RIP、Static　**初期設定：**RIP

Redistribute Metric Type

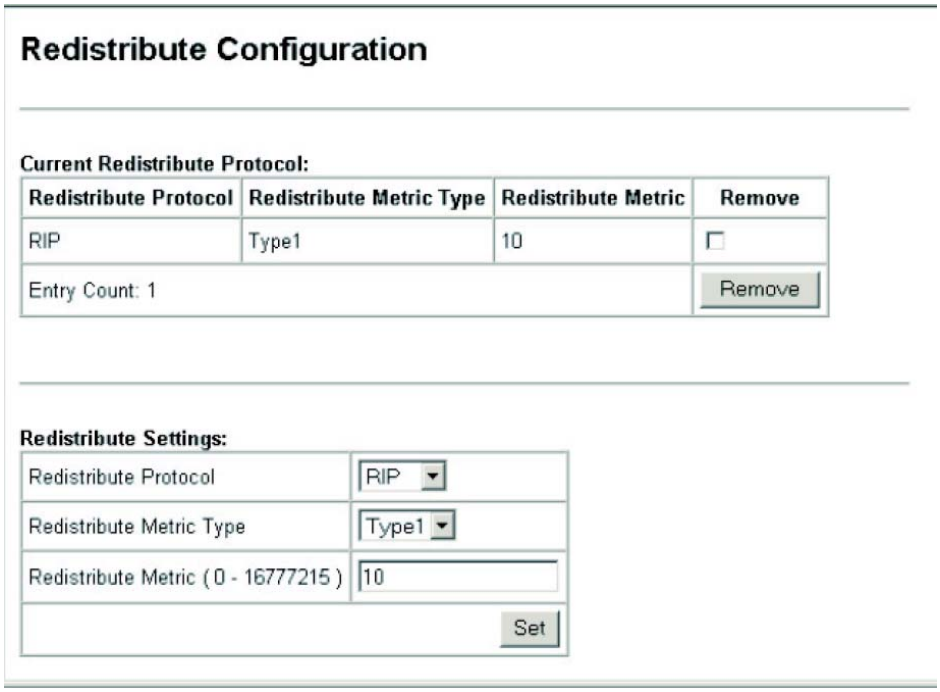
メトリックタイプを指定（オプション：Type 1, Type 2　**初期設定：**Type 1)

Redistribute Metric Type

メトリックタイプの再配布（範囲：1-65535　**初期設定：**10)

設定方法

[Routing Protocol] → [OSPF] → [Redistribute Configuration] **をクリックします。**



NSSA の設定

設定・表示項目

Area ID

NSSA の識別子です（エリア ID は、IP アドレスと同じ形式である必要があります）。.

Default Information Originate

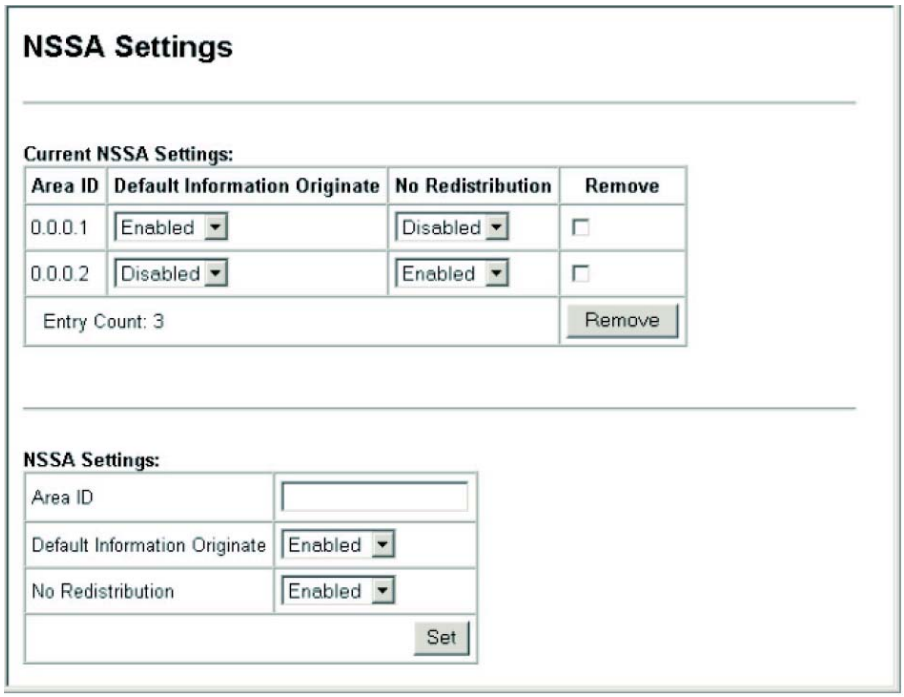
ルータが NSSA エリア境界ルータ（ABR）または NSSA 自律システム境界ルータ（ASBR）である時、このパラメータを指定すると、NSSA に対するタイプ -7 デフォルト LSA が生成されます。このデフォルトは、NSSA ABR には AS 内の他エリアに対するルートを、また NSSA ASBR には AS 外部のエリアに対するルートを提供します。

No Redistribution

ルータが NSSA のエリア境界ルータ（ABR）であり、なおかつ redistribute コマンドを使って（NSSA にではなく）ノーマル エリアにのみルートをインポートしたい場合、このキーワードを使用します。すなわち、このキーワードでは、NSSA ABR が（他のエリアのルータを介して学習された）外部ルーティング情報を NSSA へアドバタイズするのを防ぎます。

設定方法

[Routing Protocol] → [OSPF] → [NSSA Settings] をクリックします。



リンクステートデータベース情報の表示

設定・表示項目

Area ID

エリア ID を指定 (エリア ID は IP アドレスのフォームになります)

Link ID

リンク ID

Self-Originate

LSA の originated を表示

LS Type

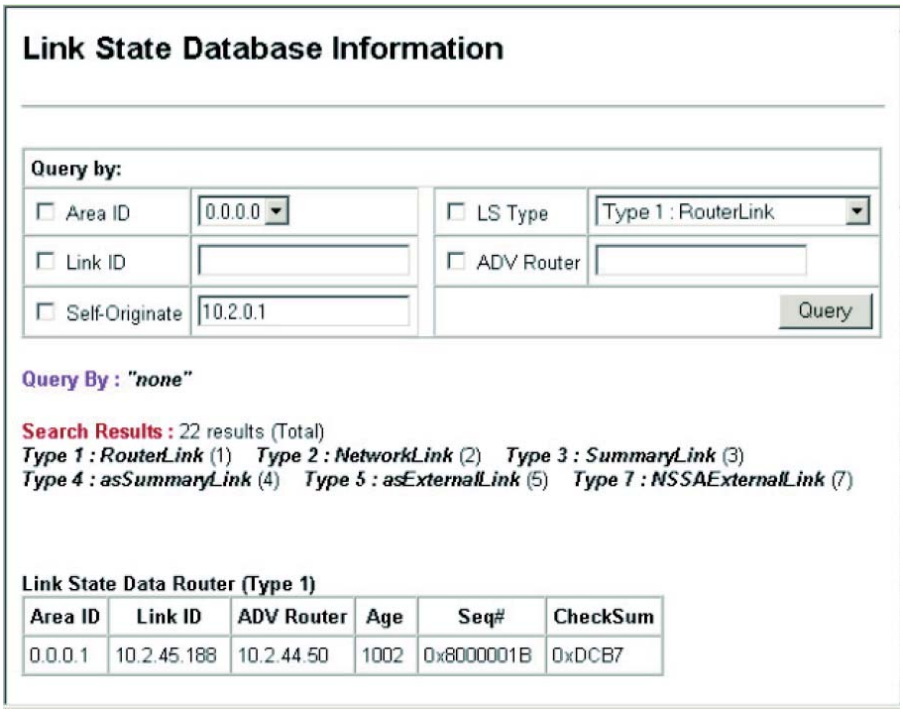
LSA タイプ (オプション：Type 1-5, 7)。

Adv Router

アドバタイジングルータの IP アドレス。

設定方法

[Routing Protocol] → [OSPF] → [Link State Database Information] をクリックします。



ボーダールータ情報の表示

設定・表示項目

Destination

宛先ルータの識別子

Next Hop

宛先へのネクスト ホップの IP アドレス

Cost

このルートのリンク メトリック

Type

宛先のルータ タイプ（ABR、ASBR、または両方）

Rte Type

ルート タイプ。イントラ エリアまたはエリア間ルート（INTRA または INTER）のいずれか。.

Area

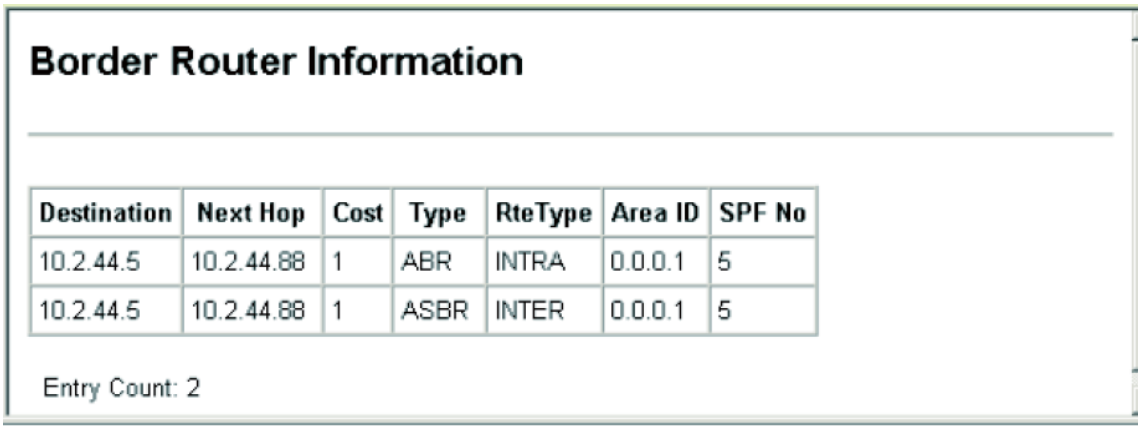
このルートが学習されたエリア。

SPF No

このルートに対して SPF （最短パス優先）アルゴリズムが実行された回数。

設定方法

[Routing Protocol] → [OSPF] → [Border Router Information] をクリックします。



隣接ルータ情報の表示

設定・表示項目

ID

隣接ルータ ID

Priority

隣接ルータプライオリティ

State

OSPF の状態と識別フラグです。各状態は、次のとおりです。

- Down ：接続がダウンしています。
- Attempt：接続はダウンしているが、コンタクトが試みられています
  （非ブロードキャスト ネットワーク用）
- Init：Hello パケットは受信されたが、通信はまだ確立されていません。
- Two-way ：双方向通信が確立しています。
- ExStart：隣接ルータ間の隣接性を初期化しています。
- Exchange：データベース記述を交換しています。
- Loading ：LSA データベースを交換しています。
- Full：隣接ルータは完全に隣接関係にあります。

各識別フラグは次のとおりです。

D －ダイナミック隣接ルータです。

S － スタティック隣接ルータです。

DR － 指定ルータです。

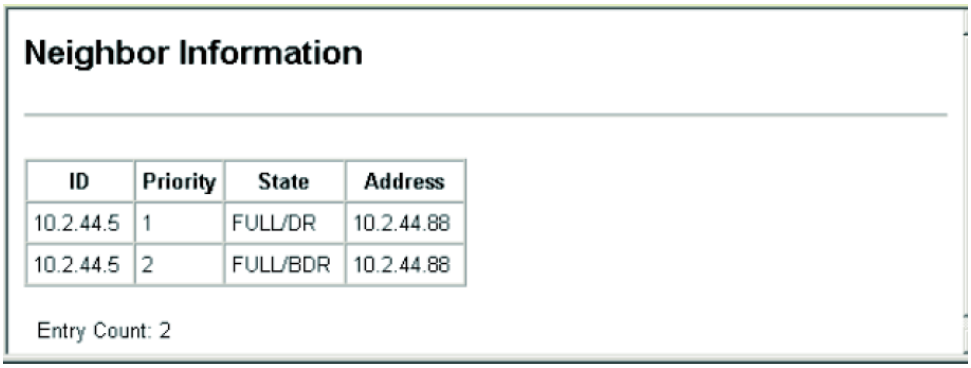
BDR － バックアップ指定ルータです。

Address

このインタフェースの IP アドレス。

設定方法

[Routing Protocol] → [OSPF] → [Neighbor Information] をクリックします。



4. コマンドラインインタフェース

4.1 コマンドラインインタフェースの利用

4.1.1 コマンドラインインタフェースへのアクセス

コンソールポート、又はネットワークから Telnet **経由で管理インタフェースにアクセスする場合、**Unix **のコマンドに似たコマンドキーとパラメータのプロンプト（コマンドラインインタフェース** /CLI**）により本機の設定を行います。**

4.1.2 コンソール接続

コンソールポートへの接続は以下の手順で行います。

（1**）コンソールプロンプトでユーザ名とパスワードを入力します。初期設定のユーザ名は** "admin" **と** "guest"**、パスワードも同じく** "admin" **と** "guest" **となっています。管理者ユーザ名とパスワード（初期設定ではどちらも** "admin"**）を入力した場合、**CLI **には** "Console#" **と表示され** Privileged Exec **モードとなります。一方ゲストユーザ名とパスワード（初期設定ではどちらも** "guest"**）を入力した場合、**CLI **には** "Console>" **と表示され** Normal Exec **モードとなります。**

（2**）ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。**

（3**）終了時には** "quit" **又は** "exit" **コマンドを使用しセッションを終了します。**

コンソールポートからシステムに接続すると以下のログイン画面が表示されます。

```
Username: admin
Password:

      CLI session with the FXC9024XG is opened.
      To end the CLI session, enter [Exit].

Console#
```

4.1.3 Telnet 接続

Telnet を利用するとネットワーク経由での管理が可能となります。Telnet を行うには管理端末側と本機側のどちらにも IP アドレスを事前に設定する必要があります。また、異なるサブネットからアクセスする場合にはデフォルトゲートウェイもあわせて設定する必要があります。

[注意] 工場出荷時には、本機は DHCP サーバー経由で IP アドレスが割り振られる設定になっています。

IP アドレスとデフォルトゲートウェイの設定例は以下の通りです。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

本機を外部と接続されたネットワークに接続する場合には、登録された IP アドレスを設定する必要があります。独立したネットワークの場合には内部で自由に IP アドレスを割り当てることができます。

本機の IP アドレスを設定した後、以下の手順で Telnet セッションを開始することができます。

（1）リモートホストから Telnet コマンドと本機の IP アドレスを入力します。

（2）プロンプト上でユーザ名とパスワードを入力します。Privileged Exec モードの場合には "Vty-0#" と表示されます。Normal Exec モードの場合には "Vty-0>" と表示されます。

（3）ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。

（4）終了時には "quit" 又は "exit" コマンドを使用しセッションを終了します。

```
Username: admin
Password:

      CLI session with the FXC9024XG is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

[注意] 同時に最大 4 セッションまでの Telnet 接続が可能です。

4.2 コマンド入力

4.2.1 キーワードと引数

CLI コマンドはキーワードと引数のグループから構成されます。キーワードによりコマンドを決定し、引数により設定パラメータを入力します。

例えば、"show interfaces status ethernet 1/5" というコマンドの場合、"show interfaces" と "status" というキーワードがコマンドなり、"ethernet" と "1/5" がそれぞれインタフェースとユニット / ポートを指定する引数となります。

以下の手順でコマンドの入力を行います。

- 簡単なコマンドを入力する場合は、コマンドキーワードを入力します。
- 複数のコマンドを入力する場合は、各コマンドを必要とされる順番で入力します。例えば Privileged Exec コマンドモードを有効にして、起動設定を表示するためには、以下のようにコマンドを入力します。

```
Console>enable
Console#show startup-config
```

- パラメータを必要とするコマンドを入力する場合は、コマンドキーワードの後に必要なパラメータを入力します。例えば、管理者パスワードを設定する場合には、以下のようにコマンドを入力します。

```
Console(config)#username admin password 0 smith
```

4.2.2 コマンドの省略

CLI ではコマンドの省略を行うことができます。例えば "configuration" というコマンドを "con" と入力するだけでもコマンドとして認識されます。但し、省略したものが複数のコマンドとなり得る場合には、システムから再度コマンドの入力を要求されます。

4.2.3 コマンドの補完

コマンドを入力している途中で Tab キーを押すと、CLI が自動的にコマンドの残りを補完し、キーワードが入力されます。例えば "logging history" コマンドを入力する際に、"log" と入力して Tab キーを押すと "logging" とキーワードがすべて入力されます。

4.2.4 コマンド上でのヘルプの表示

コマンド上で "help" コマンドを入力することで、簡単なヘルプが表示されます。また "?" と入力するとキーワードやパラメータのコマンド文法が表示されます。

コマンドの表示

コマンド上で "?" と入力すると、現在のコマンドクラスの第一階層にあるすべてのキーワードが表示されます。また特定のコマンドのキーワードを表示することもできます。例えば "show ?" と入力すると、"show" コマンド内で使用できるコマンド一覧が表示されます。

```
Console#show ?
  access-group       Access groups
  access-list        Access lists
  arp                Information of ARP cache
  bridge-ext         Bridge extension information
  calendar           Date and time information
  class-map          Display class maps
  clock
  dns                DNS information
  dot1q-tunnel       dot1q-tunnel
  dot1x              802.1x content
  garp               GARP properties
  gvrp               GVRP interface information
  history            History information
  hosts              Host information
  interfaces         Interface information
  ip                 IP information
  ipv6               IPv6 information
  lacp               LACP statistics
  line               TTY line information
  lldp               LLDP
  log                Login records
  logging            Login setting
  mac                MAC access list
  mac-address-table  Configuration of the address table
  management         Management IP filter
  map                Maps priority
  policy-map         Display policy maps
  port               Port characteristics
  port-channel       Port channel
  process            Device process
  protocol-vlan      Protocol-VLAN information
  public-key         Public key information
  pvlan              Private VLAN information
  queue              Priority queue information
  radius-server      RADIUS server information
  rip                RIP
  rmon               rmon
  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
  tech-support       Technical information
  users              Information about terminal lines
  version            System hardware and software versions
  vlan               Virtual LAN settings
  vrrp               Shows VRRP
Console#show
```

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

```
Console#show interfaces ?
  counters       Interface counters information
  protocol-vlan  Protocol-VLAN information
  status         Interface status information
  switchport     Interface switchport information
Console#show interfaces
```

4.2.5 キーワードの検索

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

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

4.2.6 コマンドのキャンセル

多くのコマンドにおいて、コマンドの前に "no" と入力することでコマンド実行の取り消し、又は初期設定へのリセットを行うことができます。例えば、"logging" コマンドではホストサーバにシステムメッセージを保存します。"no logging" コマンドを使用するとシステムメッセージの保存が無効となります。

本マニュアルでは、各コマンドの解説で "no" を利用してコマンドのキャンセルができる場合にはその旨の記載がしてあります。

4.2.7 コマンド入力履歴の利用

CLI では入力されたコマンドの履歴が保存されています。「↑」キーを押すことで、以前入力した履歴が表示されます。表示された履歴は、再びコマンドとして利用することができる他、履歴に表示されたコマンドの一部を修正して利用することもできます。

また、"show history" コマンドを使用すると最近利用したコマンドの一覧が表示されます。

4.2.8 コマンドモード

コマンドセットは Exec と Configuration クラスによって分割されます。Exec コマンドは情報の表示と統計情報のリセットを主に行います。一方の Configuration コマンドでは、設定パラメータの変更や、スイッチの各種機能の有効化などを行えます。

これらのクラスは複数のモードに分けら、使用できるコマンドはそれぞれのモード毎に異なります。"?" コマンドを入力すると、現在のモードで使用できるすべてのコマンドの一覧が表示されます。コマンドのクラスとモードは以下の表の通りです。

クラス	モード	
Exec	Normal Privileged	
Configuration	Global?	Access Control List Class Map DHCP Interface Line Multiple Spanning Tree Policy Map Router VLAN Database

?Global Configuration モードへは、Privileged Exec モードの場合のみアクセス可能です。他の Configuration モードを使用する場合は、Global Configuration モードになる必要があります。

4.2.9 Exec コマンド

コンソールへの接続にユーザ名 "guest" でログインした場合、Normal Exec モード（ゲストモード）となります。この場合、一部のコマンドしか使用できず、コマンドの使用に制限があります。すべてのコマンドを使用するためには、再度ユーザ名 "admin" でセッションを開始するか、"enable" コマンドを使用して Privileged Exec モード（管理者モード）へ移行します（管理者モード用のパスワードを設定している場合には別途パスワードの入力が必要です）

Normal Exec モードの場合にはコマンドプロンプトの表示が "Console>" と表示されます。
Privileged Exec モードの場合には "Console#" と表示されます。

Privileged Exec モードにアクセスするためには、以下のコマンドとパスワードを入力します。

```
Username: admin
Password:

      CLI session with the FXC9024XG is opened.
      To end the CLI session, enter [Exit].

Console#
```

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

      CLI session with the FXC9024XG is opened.
      To end the CLI session, enter [Exit].

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

4.2.10 Configuration コマンド

Configuration コマンドは Privileged Exec（管理者）モード内のコマンドで、本機の設定変更を行う際に使用します。これらのコマンドはランニングコンフィグレーションのみが変更され、再起動時には保存されません。

電源を切った場合にもランニングコンフィグレーションを保存するためには、"copy running-config startup-config" コマンドを使用します。

Configuration コマンドは複数の異なるモードがあります。

- **Global Configuration** — "hostname"、"snmp-server community" コマンドなどシステム関連の設定変更を行うためのモードです。
- **Access Control List Configuration** — パケットフィルタリングを行なうためのモードです。
- **Class Map Configuration** — DiffServe クラスマップを作成するためのモードです。
- **DHCP Configuration** — DHCP サーバの設定を行います。
- **Interface Configuration** — "speed-duplex" や "negotiation" コマンドなどポート設定を行うためのモードです。
- **Line Configuration** — "parity" や "databits" などコンソールポート関連の設定を行うためのモードです。
- Multiple Spanning Tree Configuration— 選択された MSTP インスタンスの設定を行うためのモードです。
- **Policy Map Configuration** — DiffServe ポリシーマップを設定します。
- **Router Configuration** — ルーティングプロトコルのグローバル設定を行います。
- **VLAN Configuration** — VLAN グループを設定するためのモードです。

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

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

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

モード	コマンド	プロンプト	ページ
Line	Line {console | vty}	Console(config-line)#	P270
Access Control List	access-list ip standard access-list ip extended access-list ip mac	Console(config-std-acl) Console(config-ext-acl) Console(config-mac-acl)	P367 P367 P372
Class Map	class map	Console(config-cmap)	P498
DHCP	ip dhcp pool	Console(config-dhcp)	P531
Interface	Iinterface {ethernet *port* | port-channel *id* | vlan *id*}	Console(config-if)#	P378
MSTP	spanning-tree mst-configuration	Console(config-mstp)#	P429
Policy Map	policy map	Console(config-pmap)	P501
router	router rip	Console(config-router)	P575
VLAN	vlan database	Console(config-vlan)	P454

以下の例では、Interface Configuration **モードにアクセスし、その後** Privileged Exec **モードに戻る動作を行っています。**

```
Console(config)#interface ethernet 1/5
Console(config-if)#exit
Console(config)#
```

4.2.11 コマンドラインプロセス

CLI のコマンドでは大文字と小文字の区別はありません。他のコマンドとパラメータの区別ができればコマンドとパラメータの省略をすることができます。また、コマンドの補完をするためにタブ・キーを使用することや、コマンドの一部と "?" コマンドを利用して関連するコマンドを表示させることもできます。

その他に、以下の表のキー入力を使用することもできます。

キー操作	機能
Ctrl-A	カーソルをコマンドラインの一番前に移動します。
Ctrl-B	カーソルを 1 文字左に移動します。
Ctrl-C	現在のタスクを終了し、コマンドプロンプトを表示します。
Ctrl-E	カーソルをコマンドラインの最後に移動します。
Ctrl-F	カーソルを 1 文字右に移動します。
Ctrl-K	カーソルから行の最後までの文字を削除します。
Ctrl-L	現在のコマンド行を新しい行で繰り返します。
Ctrl-N	コマンド入力履歴の次のコマンドを表示します。
Ctrl-P	最後に入力したコマンドを表示します。
Ctrl-R	現在のコマンド行を新しい行で繰り返します。
Ctrl-U	入力した行を削除します。
Ctrl-W	入力した最後のワードを削除します。
Esc-B	カーソルを 1 文字戻します。
Esc-D	カーソルから文字の最後までを削除します。
Esc-F	文字カーソルを進めます。
Delete 又は backspace	コマンド入力を間違えた際に削除します。

4.3 コマンドグループ

システムコマンドは機能別に以下の表の通り分類されます：

コマンドグループ	内容	ページ
General	Privileged Exec モードへのアクセスやシステムの再起動、CLI からのログアウトなど基本的なコマンド	P244
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	P252
Simple Network Management Protocol	SNMP の設定	P306
User 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	P323
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	P366
Interface	Trunk、LACP や VLAN などを各ポートの設定	P378
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	P392
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	P404
Rate Limit	通信の最大送受信帯域のコントロール	P406
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	P407
Spanning Tree	STA 設定	
VLANs	各ポートの VLAN グループの設定及びプライベート VLAN、プロトコル VLAN の設定	P454
Class of Seervice	タグ無しフレームへのポートプライオリティの設定、Strict プライオリティまたは wrr の設定、その他プライオリティの設定	P482
Quality of Service	Diff Serv の設定	P497
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	P508
Domain Name Server	DNS サーバの設定	P522
Dynamic Host Configuration Protocol	DHCP クライアント、リレー、サーバ機能の設定	P531
IP Interface	管理アクセス用 IP アドレスの設定	P559
IP Routing	静的および動的ユニキャストルーティングの設定	P567
Router Redundancy	プライマリ・バックアップルータを作成し、ルータ冗長を設定	P548

本章内の表で用いられるコマンドモードは以下の括弧内のモードを省略したものです。

ACL（Access Control List Configuration）

CM（Class Map Configuration）

DC（DHCP Server Configuration）

GC（Global Configuration）

IC（Interface Configuration）

LC（Line Configuration）

MST（Multiple Spanning Tree）

NE（Normal Exec）

PE（Normal Exec）

PM（Policy Map Configuration）

RC（Router Configuration）

VC（VLAN Database Configuration）

4.4 General（一般コマンド）

コマンド	機能	モード	ページ
enable	Privileged モードの有効化	NE	P244
disable	Privileged モードから Normal モードへの変更	PE	P246
configure	Global Configuration モードの有効化	PE	P247
show history	コマンド履歴バッファの表示	NE,PE	P248
reload	本機の再起動	PE	P249
prompt	CLI プロンプトのカスタマイズ	GC	P249
end	Privileged Exec モードへの変更	GC,IC, LC,VC	P250
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	P250
quit	CLI セッションを終了	NE,PE	P251

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 P238 「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、P325 「enable password」を参照して下さい）
- プロンプトの最後に "#" が表示されている場合は、Privileged Exec モードを表します。

例

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

関連するコマンド

disable（P246）
enable password（P325）

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 P238 「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（P245）

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 P238 「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（P250）

show history

保存されているコマンドの履歴を表示する際に利用します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

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

例

本例では、コマンド履歴として保存されているコマンドを表示しています。

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

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

Console#
```

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

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

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

reload

システムの再起動を行う際に利用します。

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

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

システム全体の再起動を行います。

例

本機の再起動方法を示しています。

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

prompt

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

初期設定

Console

コマンドモード

Global 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)#prompt RD2
RD2(config)#
```

end

Privileged モードに戻る際に利用します。

初期設定

なし

コマンドモード

Global Configuration
Interface Configuration
Line Configuration
VLAN Database Configuration

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:
```

4.5 システム管理

このコマンドはシステムログ、ユーザ名、パスワード、Web **インタフェースの設定に使用されます。また、他のシステム情報の表示や設定を行えます。**

コマンド	機能	ページ
Device Designation	**本機を特定する情報設定**	P252
System Status	**管理者やシステムバージョン、システム情報の表示**	P254
Frame Size	**ジャンボフレームサポートの有効化**	P261
File Management	**コードイメージまたは設定ファイルの管理**	P262
Line	**シリアルポートのパラメータを設定**	P270
Event logging	**エラーメッセージのログをコントロール**	P283
SMTP Alerts	SMTP**、**E **メールアラートの設定**	P291
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**	P295

4.5.1 Device Designation コマンド

コマンド	機能	モード	ページ
hostname	**ホスト名の設定**	GC	P253
snmp-server contact	**システムコンタクト者の設定**	GC	P309
snmp-server location	**システムロケーションの設定**	GC	P309
switch renumber	**スタックユニットのリナンバリング**	PE	P253

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)#
```

switch renumber

スイッチユニットの識別番号をリセットします。すべてのスタック番号は、非ループスタック用に、トップユニットから開始して連続的に付けられるか、ループスタック用にマスターユニットから開始します。

文法

switch all renumaber

初期設定

- **非ループスタッキング用：トップユニットが** 1
- **ループスタッキング用：マスターユニットが** 1

コマンドモード

Global Configuration

例

```
Console#switch all renumber
Console#
```

4.5.2 システム情報の表示

コマンド	機能	モード	ページ
show startup-config	フラッシュメモリ内のスタートアップ設定ファイルの内容の表示	PE	P254
show running-config	実行中の設定ファイルの表示	PE	P256
show system	システム情報の表示	NE,PE	P258
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	P259
show version	システムバージョン情報の表示	NE,PE	P260

show startup-config

システム起動用に保存されている設定ファイルを表示するためのコマンドです。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 実行中の設定ファイルと、起動用ファイルの内容を比較する場合には "show running-config" コマンドを一緒に使用して下さい。
- キーコマンドモードの設定が表示されます。各モードのグループは "!" によって分けられて configuration モードと対応するモードが表示されます。このコマンドでは以下の情報が表示されます：
  - スタック内のそれぞれのスイッチの MAC アドレス
  - SNTP サーバの設定
  - SNMP コミュニティ名
  - ユーザ（ユーザ名及びアクセスレベル）
  - VLAN データベース（VLAN ID, VLAN 名及び状態）
  - 各インタフェースの VLAN 設定状態
  - MSTP インスタンス（名前、インタフェース）
  - VLAN に設定された IP アドレス
  - レイヤ 4Precedence 設定
  - ルーティングプロトコル設定
  - 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...
!<stackingDB>0000000000000000</stackingDB>
!<stackingMac>01_00-17-2e-0f-e2-a0_01</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!
phymap 00-17-2e-0f-e2-a0 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
!
SNTP server
!
snmp-server community public ro
snmp-server community private rw
!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
VLAN database
 VLAN 1 name DefaultVlan media ethernet state active
!
spanning-tree MST configuration
!
interface VLAN 1
 IP address 192.168.1.2 255.255.255.0
!
interface ethernet 1/1
.
.
.
interface ethernet 1/26
 no negotiation
!
IP name-server 192.168.1.1
IP domain-lookup
!
IP route 0.0.0.0 0.0.0.0 192.168.1.1 metric 1
!
no spanning-tree
!
line console
!
line VTY
!
end
!
Console#
```

関連するコマンド

show running-config (P256)

show running-config

現在実行中の設定ファイルを表示するためのコマンドです。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 起動用ファイルと、実行中の設定ファイルの内容を比較する場合には "show startup-config" コマンドを一緒に使用して下さい。
- キーコマンドモードの設定が表示されます。各モードのグループは "!" によって分けられて configuration モードと対応するモードが表示されます。このコマンドでは以下の情報が表示されます。
  - スタック内のそれぞれのスイッチの MAC アドレス
  - SNTP サーバの設定
  - SNMP コミュニティ名
  - ユーザ（ユーザ名及びアクセスレベル）
  - VLAN データベース（VLAN ID, VLAN 名及び状態）
  - 各インタフェースの VLAN 設定状態
  - MSTP インスタンス（名前、インタフェース）
  - VLAN に設定された IP アドレス
  - レイヤ 4Precedence 設定
  - ルーティングプロトコル設定
  - 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 running-config
building running-config, please wait...
!<stackingDB>0000000000000000</stackingDB>
!<stackingMac>01_00-17-2e-0f-e2-a0_01</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!
phymap 00-17-2e-0f-e2-a0 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
!
SNTP server
!
snmp-server community public ro
snmp-server community private rw
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
VLAN database
 VLAN 1 name DefaultVlan media ethernet state active
!
spanning-tree MST configuration
!
interface VLAN 1
 IP address 192.168.1.2 255.255.255.0
!
interface ethernet 1/1
.
.
.
interface ethernet 1/26
 no negotiation
!
IP name-server 192.168.1.1
IP domain-lookup
!
IP route 0.0.0.0 0.0.0.0 192.168.1.1 metric 1
!
no spanning-tree
!
line console
!
line VTY
!
end
!
Console#
```

関連するコマンド

show startup-config (P254)

show system

システム情報を表示するためのコマンドです。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- **このコマンドによって表示される項目の説明は** P20 **「システム情報の表示」を参照してください。**
- "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: 10/100/1000 L3 SWITCH
System OID String: 1.3.6.1.4.1.25574.20.70
System Information
 System Up Time:          0 days, 0 hours, 19 minutes, and 20.4
seconds
 System Name:             [NONE]
 System Location:         [NONE]
 System Contact:          [NONE]
 MAC Address (Unit1):     00-17-2E-0F-E2-A0
 Web Server:              Enabled
 Web Server Port:         80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:           Enable
 Telnet Server Port:      23
 Jumbo Frame:             Disabled
 Jumbo Frame Size:        1522

 POST Result:
DUMMY Test 1 ................. PASS
DRAM Test .................... PASS
PCI Device 1 Test ............ PASS
I2C Bus Initialization ....... PASS
Fan Speed Test ............... PASS

Done All Pass.
Console#
```

show users

コンソール及び Telnet **で接続されているユーザの情報を表示するためのコマンドです。**
ユーザ名、接続時間及び Telnet **接続時の** IP **アドレスを表示します。**

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

コマンドを実行したユーザは行の先頭に "*" が表示されています。

例

```
Console#show users
 Username accounts:
   Username Privilege Public-Key
   -------- --------- ----------
   admin      15        None
   guest       0        None
   steve      15        RSA

Online users:
 Line         Username  Idle time (h:m:s)  Remote IP addr.
 -----------  --------  -----------------  ---------------
  0   console   admin            0:14:14
* 1     VTY 0   admin            0:00:00   192.168.1.19
  2     SSH 1   steve            0:00:06   192.168.1.19

Web online users:
 Line        Remote IP addr Username Idle time (h:m:s).
 ----------- -------------- -------- ------------------
1      HTTP   192.168.1.19   admin            0:00:00

Console#
```

show version

ハードウェアとソフトウェアのバージョン情報を表示するためのコマンドです。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

このコマンドによって表示される項目の説明は P21 **「ハードウェア及びソフトウェアバージョンの表示」を参照してください。**

例

```
Console#show version
Unit 1
 Serial Number:           A833001521
 Hardware Version:        R02
 EPLD Version:            1.06
 Number of Ports:         26
 Main Power Status:       Up
 Redundant Power Status:  Not present

Agent (Master)
 Unit ID:                 1
 Loader Version:          1.0.0.1
 Boot ROM Version:        1.0.0.9
 Operation Code Version:  2.3.0.6

Console#
```

4.5.3 フレームサイズコマンド

コマンド	機能	モード	ページ
jumbo frame	ジャンボフレームの利用	GC	P261

jumbo frame

ジャンボフレームの使用を有効にします。"no" を前に置くことで無効となります。

文法

jumbo frame
no jumbo frame

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 本機で最大 9216byte までのジャンボフレームに対応することで効率的なデータ転送を実現します。通常 1500byte までのイーサネットフレームに比べジャンボフレームを使用することで各パケットのオーバヘッドが縮小されます。
- ジャンボフレームを使用する場合は、送信側及び受信側（サーバや PC 等）がどちらも本機能をサポートしている必要があります。また Full-Duplex 時には 2 つのエンドノード間のスイッチのすべてが本機能に対応している必要があります。Half-Duplex 時にはコリジョンドメイン内の全てのデバイスが本機能に対応している必要があります。
- ジャンボフレームを使用すると、ブロードキャスト制御の最大しきい値が毎秒 64 パケットに制限されます。（詳細は、P386 「switchport broadcast packet-rate」コマンドを参照して下さい）
- ジャンボフレームの現在の設定内容は ”show system” コマンドで確認ができます。

例

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

4.5.4 ファイル管理（ Flash/File ）

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

コマンド	機能	モード	ページ
copy	**コードイメージや設定ファイルのフラッシュメモリへのコピーや** TFTP **サーバ間のコピー**	PE	P262
delete	**ファイルやコードイメージの削除**	PE	P266
dir	**フラッシュメモリ内のファイルの一覧の表示**	PE	P267
whichboot	**ブートファイルの表示**	PE	P268
boot system	**システム起動ファイル、イメージの設定**	GC	P269

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 | unit}

copy running-config {file | startup-config | tftp}

copy startup-config {file | running-config | tftp}

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

- *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）**
- unit — **ユニットの指定**

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 [*unit*:] *filename*

- *filename* — 設定ファイル又はイメージファイル名
- *unit* — ユニットの指定 （範囲：1-8）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 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。
- ユニットの指定の後にはコロン（:）が必要です。

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（P267）
delete public-key（P347）

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 { [*unit* :] [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。
- *unit*— ユニットの指定 （範囲：1-8）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 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:
         D1001                       Boot-Rom Image   Y     1531028
         V330754                     Operation Code   Y     4408104
         Factory_Default_Config.cfg  Config File      N         455
         startup                     Config File      Y        3649
         startup1.cfg                Config File      N        3649
-----------------------------------------------------------------------
                                          Total free space: 25690112
Console#
```

whichboot

現在、本機がどのファイルから起動されているかを表示します。

文法

whichboot

初期設定

なし

コマンドモード

Privileged Exec

例

本例は、すべてのファイル情報の表示を示しています。

```
Console#whichboot
                     File name     File type      Startup  Size (byte)
--------------------------------   -------------- ------- ----------
 Unit1:
                       D1001        Boot-Rom Image     Y    1531028
                      V330754       Operation Code     Y    4408104
                      startup       Config File        Y       3649
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 [*unit:*]{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
- *filename* — **ファイル又はイメージ名**
- *unit*— **ユニットの指定（範囲：**1-8）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **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（P267）
whitchboot（P268）

4.5.5 Line （ラインコマンド）

VT100 互換のデバイスを使用し、シリアルポート経由で本機の管理プログラムにアクセスすることができます。本コマンドはシリアルポート接続及び Telnet 端末との接続の設定を行うために使用されます。

コマンド	機能	モード	ページ
line	コンソール接続の設定及び line configuration モードの開始	GC	P271
login	コンソール接続時のパスワードの有効化	LC	P272
password	コンソール接続時のパスワードの設定	LC	P273
timeout login response	CLI のログイン入力待ち時間の設定	LC	P274
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	P275
password-thresh	パスワード入力時のリトライ数の設定	LC	P276
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	P277
databits	各文字あたりのデータビットの設定	LC	P278
parity	パリティビット生成の設定	LC	P278
speed	ボーレートの設定	LC	P280
stopbits	1byte あたりのストップビット値の設定	LC	P281
disconnect	Line 接続を終了	PE	P281
show line	ターミナル接続の設定情報を表示	NE,PE	P282

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（P282）
show users（P259）

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。
  ー 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。
  ー login local を選択した場合、"usaname" コマンドを使用して指定したユーザ名とパスワードを使用してユーザ認証が行なわれます。この場合、管理インタフェースは入力したユーザのユーザレベルに応じて Normal Exec (NE) モード又は Privileged Exec (PE) モードのどちらかになります。
  ー 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（P324）
password（P273）

password

コンソール接続のためのパスワードの設定を行います。"no" を前に置くことでパスワードを削除します。

文法

password {0 | 7} *password*

no password

- {0 | 7} — "0" **は平文パスワードを、**"7" **は暗号化されたパスワードとなります。**
- password — **コンソール接続用のパスワード（最大** 8 **文字（平文時）、**32 **文字（暗号化時）。大文字と小文字は区別されます）。**

初期設定

パスワードは設定されていません

コマンドモード

Line Configuration

コマンド解説

- **パスワードの設定を行うと、接続時にパスワードを要求するプロンプトが表示されます。正しいパスワードを入力するとログインできます。**"password-thresh" **コマンドを使用し、パスワード入力時のリトライ数を設定することができます。**
- **暗号化されたパスワードはシステム起動時に設定ファイルを読み込む場合や** TFTP **サーバにダウロードする場合のためにテキスト（平文）パスワードとの互換性があります。暗号化されたパスワードを手動で生成する必要はありません。**

例

```
Console(config-line)#password 0 secret
Console(config-line)#
```

関連するコマンド

login（P272）
password-thresh（P276）

timeout login response

CLI からのログイン入力のタイムアウト時間を設定します。"no" を前に置くことで初期設定に戻します。

文法

timeout login response { *seconds* }

no timeout login response

- *seconds* — タイムアウト時間（秒）（範囲：0-300 秒、0：タイムアウト設定なし）

初期設定

- CLI：無効（0 秒）
- Telnet：300 秒

コマンドモード

Line Configuration

コマンド解説

- 設定時間内にログインが検知されなかった場合、接続は切断されます。
- 本コマンドはコンソール接続と Telnet 接続の両方に有効となります。
- Telnet のタイムアウトを無効にすることはできません。
- タイムアウトを指定せずコマンドを実行した場合、初期設定に戻します。

例

本例ではタイムアウト時間を 120 秒（2 分）に設定しています。

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

関連するコマンド

silent-time (P277)
exec-timeout (P275)

exec-timeout

ユーザ入力のタイムアウト時間の設定を行います。"no" を前に置くことでタイムアウト時間の設定を削除します。

文法

exec-timeout { *seconds* }

no exec-timeout

- seconds — **タイムアウト時間（秒）**（0 - 65535（秒）、0：**タイムアウト設定なし**）

初期設定

CLI：**タイムアウト設定なし**

Telnet：600 **秒**（10 **分**）

コマンドモード

Line Configuration

コマンド解説

- **設定時間内に入力が行なわれた場合、接続は維持されます。設定時間内に入力がなかった場合には接続は切断され、ターミナルは待機状態となります。**
- **本コマンドはコンソール接続と** Telnet **接続の両方に有効となります。**
- Telnet **のタイムアウトを無効にすることはできません。**

例

本例ではタイムアウト時間を 120 **秒（**2 **分）に設定しています。**

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

ログイン時のパスワード入力のリトライ回数の設定に使用するコマンドです。"no" を前に置くことで指定したリトライ回数は削除されます。

文法

password-thresh *threshold*

no password-thresh

- *threshold* — リトライ可能なパスワード入力回数（設定範囲：1-120、0：回数の制限をなくします）

初期設定

3 回

コマンドモード

Line Configuration

コマンド解説

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

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 (P277)

silent-time

ログインに失敗し、"password-thresh" **コマンドで指定したパスワード入力のリトライ数を超えた場合にログイン要求に反応をしない時間を設定するためのコマンドです。**"no" **を前に置くことで設定されている値を削除します。**

文法

silent-time *seconds*

no silent-time

- *seconds* — **コンソールの無効時間（秒）（設定範囲：**0-65535**、**0**：コンソールを無効にしない）**

初期設定

コンソールの応答無効時間は設定されていません。

コマンドモード

Line Configuration

例

本例ではコンソール無効時間を 60 **秒に設定しています。**

```
Console(config-line)#silent-time 60
Console(config-line)#
```

関連するコマンド

password-thresh (P276)

databits

コンソールポートで生成される各文字あたりのデータビットの値を設定するためのコマンドです。"no" を前に置くことで初期設定に戻します。

文法

databits { 7 | 8 }

no databits

- 7 — 7 データビット
- 8 — 8 データビット

初期設定

8 データビット

コマンドモード

Line Configuration

コマンド解説

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

例

本例では 7 データビットに設定しています。

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

関連するコマンド

parity（P278）

parity

パリティビットの設定のためのコマンドです。"no" を前に置くことで初期設定に戻します。

文法

parity { none | even | odd }

no parity

- none — **パリティ無し**
- even — **偶数パリティ**
- odd — **奇数パリティ**

初期設定

パリティ無し

コマンドモード

Line Configuration

コマンド解説

接続するターミナルやモデムなどの機器によっては個々のパリティビットの設定を要求する場合があります。

例

本例では no parity **を設定しています。**

```
Console(config-line)#parity none
Console(config-line)#
```

speed

ターミナル接続のボーレートを指定するためのコマンドです。本設定では送受信両方の値を指定します。"no" を前に置くことで初期設定に戻します。

文法

speed *bps*

no speed

- *bps* — ボーレートを bps で指定（9600, 57600, 38400, 19200, 115200 bps）

初期設定

auto

コマンドモード

Line Configuration

コマンド解説

シリアルポートに接続された機器でサポートされているボーレートを指定してください。一部のボーレートは本機ではサポートしていない場合があります。サポートされていない値を指定した場合にはメッセージが表示されます。

例

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（**範囲** :0-4）

コマンドモード

Privileged Exec

コマンド解説

セッション ID"0" **を指定するとコンソール接続を終了させます。その他のセッション** ID **を指定した場合には** SSH **又は** Telnet **接続を終了させます。**

例

```
Console#disconnect 1
Console#
```

関連するコマンド

show users（P259）
show ssh（P351）

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:             auto
  Databits:             8
  Parity:               none
  Stopbits:             1

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

4.5.6 Event Logging コマンド

コマンド	機能	モード	ページ
logging on	エラーメッセージログの設定	GC	P283
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	P284
logging host	syslog を送信するホストの IP アドレスの設定	GC	P285
logging facility	リモートで syslog を保存する際のファシリティタイプの競って尾	GC	P285
logging trap	リモートサーバへの重要度にもとづいてた syslog メッセージの保存	GC	P286
clear log	ログバッファのクリア	PE	P286
show logging	ログ関連情報の表示	PE	P288
show log	ログメッセージの表示	PE	P290

logging on

エラーメッセージのログを取るためのコマンドです。デバッグ又はエラーメッセージをログとして保存します。"no" を前に置くことで設定を無効にします。

文法

[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 (P284)
clear logging (P286)

logging history

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

文法

logging history { flash | ram } *level*

no logging history { flash | ram }

- flash — **フラッシュメモリに保存されたイベント履歴**
- ram — RAM **に保存されたイベント履歴**
- *level* — **レベルは以下の表の通りです。選択した** Level **から** Level0 **までのメッセージが保存されます（範囲：**0-7**）**

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

? **現在のファームウェアでは** 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 7 - 0)

コマンドモード

Global Configuration

コマンド解説

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

例

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

logging host

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

文法

[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

- 設定できるホスト IP アドレスの最大数は 5 です。

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

[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。(16-23)

初期設定

23

コマンドモード

Global Configuration

コマンド解説

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

例

```
Console(config)#logging facility 19
Console(config)#
```

logging trap

syslog サーバに送信するメッセージの種類を指定することができます。"no" を前に置くことで初期設定に戻します。

文法

logging trap *level*

no logging trap

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

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

初期設定

無効（レベル：7-0）

コマンドモード

Global Configuration

コマンド解説

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

例

```
Console(config)#logging trap 3
Console(config)#
```

clear log

ログをバッファから削除するコマンドです。

文法

clear log [flash | ram]

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

初期設定

Flash and RAM

コマンドモード

Privileged Exec

例

```
Console#clear log
Console#
```

関連するコマンド

show logging（P288）

show logging

システム、イベントメッセージに関するログを表示します。

文法

show logging {flash | ram | sendmail | trap}

- flash — フラッシュメモリに保存されたイベント履歴
- ram — RAM に保存されたイベント履歴
- sendmail — SMTP イベントハンドラの設定を表示 (P293)
- trap — syslog サーバに送信されたメッセージ

初期設定

なし

コマンドモード

Privileged Exec

例

本例では、syslog が有効で、フラッシュメモリのメッセージレベルは "errors"（初期値 3-0）、RAM へのメッセージレベルは "debugging"（初期値 7-0）と設定してあり、1 つのサンプルエラーが表示されています。

```
Console#show logging flash
Syslog logging:          Enable
History logging in FLASH: level errors
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
Console#
```

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

本例では、トラップ機能の設定を表示しています。

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type: Debugging messages
REMOTELOG server IP address: 1.2.3.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

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

関連するコマンド

show logging sendmail (P294)

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}

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

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

メモリに保存されたシステム / イベントメッセージを表示します。タイムスタンプ、メッセージレベル、プログラムモジュール、機能、及びイベント番号を表示します。

例

本例では、RAM に保存しているサンプルメッセージを表示しています。

```
Console#show log ram
[1] 00:01:30 2001-01-01
  "VLAN 1 link-up notification."
  level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
  "Unit 1, Port 1 link-up notification."
  level: 6, module: 5, function: 1, and event no.: 1
Console#
```

4.5.7 SMTP アラートコマンド

SMTP イベントハンドル及びアラートメッセージの SMTP サーバ及びメール受信者への送信の設定を行います。

コマンド	機能	モード	ページ
logging sendmail host	アラートメッセージを受信する SMTP サーバ	GC	P291
logging sendmail level	アラートメッセージのしきい値設定	GC	P292
logging sendmail source-email	メールの ”From” 行に入力されるアドレスの設定	GC	P292
logging sendmail destination-email	メール受信者の設定	GC	P293
logging sendmail	SMTP イベントハンドリングの有効化	GC	P293
show logging sendmail	SMTP イベントハンドラ設定の表示	NE,PE	P294

logging sendmail host

アラートメッセージを送信する SMTP サーバを指定します。

"no" を前に置くことで SMTP サーバの設定を削除します。

文法

[no] logging sendmail host *ip_address*

- *ip_address* — アラートが送られる SMTP サーバの IP アドレス

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 最大 3 つの SMTP サーバを指定できます。複数のサーバを指定する場合は、サーバ毎にコマンドを入力して下さい。
- e-mail アラートを送信する場合、本機はまず接続を行ない、すべての e-mail アラートを順番に 1 通ずつ送信した後、接続を閉じます。
- 接続を行なう場合、本機は前回の接続時にメールの送信が成功したサーバへの接続を試みます。そのサーバでの接続に失敗した場合、本機はリストの次のサーバでのメールの送信を試みます。その接続も失敗した場合には、本機は周期的に接続を試みます（接続が行なえなかった場合には、トラップが発行されます）

例

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

アラートメッセージのしきい値の設定を行ないます。

文法

logging sendmail level *level*

- *level* — システムメッセージレベル (P286)。設定した値からレベル 0 までのメッセージが送信されます（設定範囲：0-7、初期設定：7）

初期設定

Level 7

コマンドモード

Global Configuration

コマンド解説

イベントしきい値のレベルを指定します。設定したレベルとそれ以上のレベルのイベントが指定したメール受信者に送信されます（例：レベル 7 にした場合はレベル 7 から 0 のイベントが送信されます）

例

本例ではレベル 3 からレベル 0 のシステムエラーがメールで送信されます。

```
Console(config)#logging sendmail level 3
Console(config)#
```

logging sendmail source-email

メールの "From" 行に入力されるメール送信者名を設定します。

文法

l**ogging sendmail source-email** *email-address*

- *email-address* — アラートメッセージの送信元アドレス（設定範囲：0-41 文字）

初期設定

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

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

logging sendmail destination-email

アラートメッセージのメール受信者を指定します。
"no" を前に置くことで受信者を削除します。

文法

logging sendmail destination-email *email-address*

no logging sendmail destination-email *email-address*

- *email-address* — アラートメッセージの送信先アドレス（設定範囲：1-41 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

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

例

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

logging sendmail

SMTP イベントハンドラを有効にします。"no" を前に置くことで機能を無効にします。

文法

[no] logging sendmail

初期設定

無効

コマンドモード

Global Configuration

例

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

show logging sendmail

SMTP イベントハンドラの設定を表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show logging sendmail
SMTP servers
-------------------------------------------------
192.168.1.19
SMTP minimum severity level: 7

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

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

SMTP status: Enable

Console#
```

4.5.8 Time コマンド

NTP 又は SNTP タイムサーバを指定することによりシステム時刻の動的な設定を行なうことができます。

コマンド	機能	モード	ページ
sntp client	特定のタイムサーバからの時刻の取得	GC	P296
sntp server	タイムサーバの指定	GC	P297
sntp poll	リクエスト送信間隔の設定	GC	P298
sntp update-time	即座に時刻アップデートを行うため、リクエストを送信	GC	P298
show sntp	SNTP 設定の表示	NE,PE	P299
clock timezone	本機内部時刻のタイムゾーンの設定	GC	P300
clock timezone-pre-defined	既定義のタイムゾーンを設定	GC	P301
clock summertime (date)	サマータイムを設定	GC	P302
clock summertime (predefined)	既定義のサマータイムを設定	GC	P303
clock summertime (recurring)	サマータイム（循環）を設定	GC	P304
show clock	タイムゾーンおよびサマータイム設定を表示	PE	P304
calendar set	システム日時の設定	PE	P304
show calendar	現在の時刻及び設定の表示	NE,PE	P305

sntp client

"sntp client" コマンドにより指定した NTP 又は SNTP タイムサーバへの SNTP クライアントリクエストを有効にします。"no" を前に置くことで SNTP クライアントリクエストを無効にします。

文法

[no] sntp client

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 本機の内部時刻の設定を正確に保つことにより、システムログの保存の際に日時を正確に記録することができます。時刻の設定がされていない場合、起動時の時刻（00:00:00, Jan. 1, 2001）が初期設定の時刻となり、そこからの時間経過となります。
- 本コマンドによりクライアント時刻リクエストが有効となり "sntp poll" コマンドにより設定した間隔で、"sntp servers" コマンドにより指定されたサーバにリクエストを行ないます。

例

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time: Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
SNTP status:Enabled
SNTP server:10.1.0.19.0.0.0.0.0.0.0.0
Current server:10.1.0.19
Console#
```

関連するコマンド

sntp server (P297)
sntp poll (P298)
show sntp (P299)

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（設定可能数：1-3）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

SNTP クライアントモード時の時刻同期リクエストを送信するタイムサーバの指定を行ないます。本機はタイムサーバに対して応答を受信するまで要求を送信します。"sntp poll" コマンドに基づいた間隔でリクエストを送信します。

例

```
Console(config)#sntp server 10.1.0.19
Console#
```

sntp poll

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

文法

sntp poll *hours*

no sntp poll

- *seconds* — リクエスト間隔（設定範囲：6-16384 秒）

初期設定

16 秒

コマンドモード

Global Configuration

コマンド解説

SNTP クライアントモード時にのみ有効となります。

例

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

関連するコマンド

sntp client (P296)

sntp update-time

時刻を更新する為、設定された SNTP サーバへ即座にリクエストを送ります。

コマンドモード

Global Configuration

例

```
Console(config)#sntp update-time
Console(config)#
```

関連するコマンド

sntp client （P296）
sntp server （P297）

show sntp

SNTP クライアントの設定及び現在の時間を表示し、現地時間が適切に更新されているか確認します。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

現在時刻、SNTP クライアントモード時の時刻更新リクエスト送信間隔、現在の SNTP モードを表示します。

例

```
Console#show sntp
Current time: Dec 23 05:13:28 2002
Poll interval: 16
Current mode: unicast
SNTP status:Enabled
SNTP server:137.92.140.80.0.0.0.0.0.0.0.0
Current server:137.92.140.80
Console#
```

clock timezone

本機内部時刻のタイムゾーンの設定を行ないます。

文法

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

- *name* — **タイムゾーン名（範囲：**1-29 **文字）**
- *hours* — UTC **との時間差（時間）（範囲：**1-12 **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（P299）

clock timezone-predefined

スイッチ内部時計のために、既定義タイムゾーンの設定をおこないます。
"no" **を前に置くことで、設定を初期値に戻します。**

文法

clock timezone-predefined *off-set city*
no clock taimezone-predefined

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

初期設定

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

コマンドモード

Global Configuration

例

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

関連するコマンド

show sntp（P299）

clock summer-time (date)

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

文法

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

no clock summer-time

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

初期設定

無効

コマンドモード

Global Configuration

例

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

関連するコマンド

show sntp（P299）

clock summer-time (predefined)

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

文法

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

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

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

既定義のサマータイムパラメータ

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

例

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

関連するコマンド

show sntp（P299）

clock summer-time (recurring)

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

文法

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

no clock summer-time

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

初期設定

無効

コマンドモード

Global Configuration

例

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

関連するコマンド

show sntp（P299）

show clock

タイムゾーンおよびサマータイム設定を表示します。

コマンドモード

Privileged Exec

例

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

calendar set

システム時刻の設定を行ないます。

文法

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

- *hour* — 時間（範囲：0 - 23）
- *min* — 分（範囲 0 - 59）
- *sec* — 秒（範囲 0 - 59）
- *day* — 日付（範囲：1-31）
- *month* — 月：**january | february | march | april | may | june | july | august | september | october | november | december**
- *year* — 年（西暦 4 桁、設定範囲：2001-2100）

初期設定

なし

コマンドモード

Privileged Exec

例

本例ではシステム時刻を 15:12:34, February 1st, 2002 に設定しています。

```
Console#calendar set 15:12:34 1 February 2002
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
15:12:34 February 1 2002
Console#
```

4.6 SNMP

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

コマンド	機能	モード	ページ
snmp-server	SNMP サーバーを有効化	GC	P306
show snmp	SNMP の設定情報を表示	NE,PE	P307
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	P308
snmp-server contact	システムコンタクト情報の設定	GC	P309
snmp-server location	システム設置情報の設定	GC	P309
snmp-server host	SNMP メッセージを受信するホストの設定	GC	P310
snmp-server enable traps	SNMP メッセージを受信するホストの有効化	GC	P312
snmp-server engine-id	エンジン ID の設定	GC	P313
show snmp engine-id	エンジン ID の表示	PE	P313
snmp-server view	ビューの設定	GC	P315
show snmp view	ビューの表示	PE	P315
snmp-server group	グループの追加と、ユーザーをビューへマッピング	GC	P317
show snmp group	グループの表示	PE	P318
snmp-server user	SNMP v3 グループへユーザーの追加	GC	P320
show snmp user	SNMP v3 ユーザーの表示	PE	P322

snmp-server

SNMPv3 エンジンおよび、その他全ての管理クライアントサービスを有効にします。

"no" を前に置くことでサービスを無効にします。

文法

[no] snmp-server

初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server
Console(config)#
```

show snmp

SNMP のステータスを表示します。

文法

show snmp

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

本コマンドを使用することで、コミュニティ名に関する情報、及び SNMP **の入出力データの数が** "snmp-server enable traps" **コマンドが有効になっていなくても表示されます。**

例

```
Console#show snmp

SNMP traps:
Authentication: enabled
Link-up-down: enabled

SNMP communities:
1. private, and the privilege is read-write
2. public, and the privilege is read-only

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

SNMP logging: disabled
Console#
```

snmp-server community

SNMP 使用時のコミュニティ名を設定します。"no" を前に置くことで個々のコミュニティ名の削除を行います。

文法

snmp-server community *string* **{ ro | rw }**

no snmp-server community *string*

- *string* — SNMP プロトコルにアクセスするためのパスワードとなるコミュニティ名（最大 32 文字、大文字小文字は区別されます。最大 5 つのコミュニティ名を設定できます）
- **ro** — 読み取りのみ可能なアクセス。ro に指定された管理端末は MIB オブジェクトの取得のみが行えます
- **rw** — 読み書きが可能なアクセス。rw に指定された管理端末は MIB オブジェクトの取得及び変更が行えます

初期設定

- public — 読み取り専用アクセス (ro)。MIB オブジェクトの取得のみが行えます
- private — 読み書き可能なアクセス (rw)。管理端末は MIB オブジェクトの取得及び変更が行えます

コマンドモード

Global Configuration

コマンド解説

"snmp-server community" コマンドは SNMP **を有効にします。"no snmp-server community" コマンドは** SNMP **を無効にします。**

例

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

システムコンタクト情報の設定を行います。"no" を前に置くことでシステムコンタクト情報を削除します。

文法

snmp-server contact *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)#
```

snmp-server location

システム設置場所情報の設定を行います。"no" を前に置くことでシステム設置場所情報を削除します。

文法

snmp-server location *text*

no snmp-server location

- *text* — **システム設置場所の解説（最大 255 文字）**

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server location Room 23
Console(config)#
```

snmp-server host

SNMP メッセージを受け取るホストの指定を行います。"no" を前に置くことでホストを削除します。

文法

snmp-server host *host-addr* **inform** {**retry** *retries* | **timeout** *seconds* } *community-string* **version [1 | 2c | 3 {auth | noauth | priv }] udp-port** *port*

no snmp-server host *host-addr*

- *host-addr* — SNMP メッセージを受け取るホストのアドレス（最大 5 つのホストを設定できます）
- **inform** — インフォームを使用（version2c と 3 でのみ使用可）
  - **retry** *retries* ー 再送を行う最大回数（0-255 回　初期設定：3 回）
  - **timeout** *seconds* ー 再送までの待ち時間（0-2147483647 センチセカンド　初期設定：1500 センチセカンド）
- *community-string* — メッセージとともに送られるコミュニティ名。本コマンドでもコミュニティ名の設定が行えますが、"snmp-server community" コマンドを利用して設定することを推奨します（最大 32 文字）
- **version** — トラップバージョンを指定します（範囲：v1,v2c,v3）

ー **auth | noauth |priv** ー v3 使用時に設定します。

- *port* — トラップマネージャが使用する UDP ポートを指定（1-65535　初期設定：162）

初期設定

Host Address：なし　　SNMP バージョン：1

通知：トラップ　　UDP ポート：162

コマンドモード

Global Configuration

コマンド解説

- "snmp-server host" コマンドを使用しない場合は、SNMP メッセージは送信されません。SNMP メッセージの送信を行うためには必ず "snmp-server host" コマンドを使用し最低 1 つのホストを指定して下さい。複数のホストを設定する場合にはそれぞれに "snmp-server host" コマンドを使用してホストの設定を行って下さい。
- "snmp-server host" コマンドは "snmp-server enable traps" コマンドとともに使用されます。"snmp-server enable traps" コマンドではどのような SNMP メッセージを送信するか指定します。ホストが SNMP メッセージを受信するためには最低 1 つ以上の "snmp-server enable traps" コマンドと "snmp-server host" コマンドが指定されホストが有効になっている必要があります。
- 一部のメッセージタイプは "snmp-server enable traps" コマンドで指定することができず、メッセージは常に有効になります。
- スイッチは初期設定でトラップメッセージの通知を行いますが、トラップメッセージの受け取り側はスイッチへ応答を送りません。その為、十分な信頼性は確保できません。イン

フォームを使用することにより、重要情報がホストに受け取られるのを保証することが可能です。

[注意] インフォームを使用した場合、スイッチは応答を受け取るまでの間、情報をメモリ内に保持しなくてはならないため多くのシステムリソースを使用します。またインフォームはネットワークトラフィックにも影響を与えます。これらの影響を考慮した上で、トラップまたはトラップ通知の使用を決定してください。

- SNMPv3 ホストを指定している場合、トラップマネージャのコミュニティ名は、SNMP ユーザー名として解釈されます。SNMPv3 認証または暗号化オプションを使用している際には（authNoPriv または authPriv）、最初に P320 「snmp-server user」でユーザー名を定義してください。ユーザー名が定義されていない場合、認証パスワードおよびプライバシーパスワードが存在せず、スイッチはホストからのアクセスを許可しません。
尚、SNMPv3 ホストを no authentication（noAuth）として設定している場合には、SNMP ユーザーアカウントは自動的に生成されますので、スイッチはホストからのアクセスを許可します。

例

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

関連するコマンド

snmp-server enable traps (P312)

snmp-server enable traps

SNMP のトラップメッセージの送信を有効化します。"no" を前に置くことで機能を無効にします。

文法

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

- **authentication** — 認証時に不正なパスワードが送信された場合にトラップが発行されます
- **link-up-down** — Link-up 又は Link-down 時にトラップが発行されます

初期設定

authentication 及び link-up-down トラップを通知

コマンドモード

Global Configuration

コマンド解説

- snmp-server enable traps" コマンドを使用しない場合、一切のメッセージは送信されません。SNMP メッセージを送信するためには最低 1 つの "snmp-server enable traps" コマンドを入力する必要があります。キーワードを入力せずにコマンドを入力した場合にはすべてのメッセージが有効となります。キーワードを入力した場合には、キーワードに関連するメッセージのみが有効となります。
- "snmp-server host" コマンドは "snmp-server enable traps" コマンドとともに使用されます。"snmp-server host" コマンドでは SNMP メッセージを受け取るホストを指定します。ホストが SNMP メッセージを受信するためには最低 1 つ以上の "snmp-server host" コマンドが指定されホストが有効になっている必要があります。

例

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

関連するコマンド

snmp-server host (P310)

snmp-server engine-id

エンジン ID の設定を行います。
エンジン ID はデバイス内のエージェントを固有に識別するためのものです。
"no" を前に置くことでエンジン ID を初期設定値に戻します。

文法

[no] snmp-server engine-id { local | remote *IP Address* **}** *engineid-string*

- **local** — スイッチ上の SNMP エンジンを指定
- **remote** — リモートデバイス上の SNMP エンジンを指定
- *IP Address* — リモートデバイスの IP アドレス
- *engineid-string* — エンジン ID（範囲：1-26　16 進数文字）

初期設定

スイッチの MAC アドレスを基に自動的に生成されます

コマンドモード

Global Configuration

コマンド解説

- SNMP エンジンはメッセージ再送、遅延およびダイレクションを防止します。エンジン ID はユーザパスワードと組み合わせて、SNMPv3 パケットの認証と暗号化を行うためのセキュリティキーを生成します。
- リモートエンジン ID は SNMPv3 インフォームを使用する際に必要です。（詳しくは P310 「snmp-server host」を参照してください）リモートエンジン ID は、リモートホストでユーザに送られた認証と暗号化パケットのセキュリティダイジェストを計算するために使用されます。SNMP パスワードは信頼できるエージェントのエンジン ID を使用してローカライズされます。インフォームの信頼できるエージェントはリモートエージェントです。したがってプロキシリクエストまたはインフォームを送信する前に、リモートエージェントの SNMP エンジン ID を変更を行う必要があります。
- ローカルエンジン ID はスイッチにたいして固有になるように自動的に生成されます。これをデフォルトエンジン ID とよびます。ローカルエンジン ID が削除または変更された場合、全ての SNMP ユーザーはクリアされます。そのため既存のユーザーの再構成を行う必要があります。

例

```
Console(config)#snmp-server engineID local 12345
Console(config)#snmp-server engineID remote 54321 192.168.1.19
Console(config)#
```

show snmp engine-id

設定中の SNMP エンジン ID を表示します

文法

show snmp engine-id

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
Local SNMP engineID	**ローカルエンジン** ID **を表示**
Local SNMP engineBoots	**前回エンジン** ID **の設定が行われてから、エンジンの（再）初期化が行われた回数を表示**
Remote SNMP engineID	**リモートデバイスのエンジン** ID **を表示**
IP address	**リモートエンジンの** IP **アドレスを表示**

例

```
Console#show snmp engine-id
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1
Remote SNMP engineID                              IP address
80000000030004e2b316c54321                      192.168.1.19
Console#
```

関連するコマンド

snmp-server engine-ID (P313)

snmp-server view

このコマンドでは、ビューの追加を行います。"no" を前に置くことでビューを削除します。

文法

[no] snmp-server view *view-name oid-tree* { **included** | **excluded** }

- *view-name* — ビューの名前（1-64 文字）
- *oid-tree* — 参照可能にする MIB ツリーの OID。ストリングの特定の部分に、ワイルドカードを使用してマスクをかけることができます
- **included** — *oid-tree* で指定した OID を参照可能な範囲に含む
- **excluded** — *oid-tree* で指定した OID を参照可能な範囲に含まない

初期設定

デフォルトビュー（全ての MIB ツリーへのアクセスを含む）

コマンドモード

Global Configuration

コマンド解説

- 作成されたビューは、MIB ツリーの指定された範囲へのユーザアクセスを制限するために使用されます。
- デフォルトビューは全体の MIB ツリーへのアクセスを含みます。

例

MIB-2 を含む View を設定

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

MIB-2 インタフェーステーブル、ifDescr を含む View を設定。ワイルドカードは、このテーブル内のすべてのインデックス値を選択するのに使用されます。

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2
  included
Console(config)#
```

MIB-2 インタフェーステーブルを含む View を設定。マスクはすべてのインデックスエントリーを選択します。

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
  included
Console(config)#
```

show snmp view

SNMP ビューを表示します。

文法

show snmp view

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
View Name	ビュー名
Subtree OID	参照可能な MIB ツリーの OID
View Type	OID で表示される MIB ノードがビューに含まれてるか（included）、含まれていないか（excluded）
Storage Type	このエントリーのストレージタイプ
Row Status	ビューの状態

例

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: nonvolatile
Row Status: active
View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active
Console#
```

snmp-server group

SNMP グループ追加と、SNMP ユーザーのビューへのマッピングを行います。
"no" を前に置くことでグループを削除します。

文法

[no] snmp-server group *groupname* **[v1 | v2c | v3 { auth | noauth |priv }] read** *readview* **write** *writeview* **notify** *notify view*

- *groupname* — SNMP グループ名
- **v1 | v2c | v3** — 使用する SNMP バージョンを選択します

  ー **auth | noauth |priv** ー v3 使用時に設定します。
- *readview* — Read アクセスのビューを設定します（1-64 文字）
- *writeview* — write アクセスのビューを設定します（1-64 文字）
- *notify view* — 通知ビューを設定します（1-64 文字）

初期設定

Default groups: public5 (read only), private6 (read/write)

readview - 全てのオブジェクトは Internet OID space (1.3.6.1) に属します

writeview - なし

notifyview - なし

コマンドモード

Global Configuration

コマンド解説

- SNMP グループは、所属するユーザーのアクセスポリシーを定義します。
- authentication が有効時は、「snmp-server user」で、MD5 または SHA どちらかの認証方式を選択してください。
- privacy が有効時は、DES56bit 暗号化方式が使用されます。

例

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

show snmp group

本機は 4 つのデフォルトグループを提供します。

- SNMPv1 read-only access
- read/write access
- SNMPv2c read-only access
- read/write access

文法

show snmp group

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
groupname	**グループ名**
security model	**セキュリティモデル**
readview	read **ビュー**
writeview	write **ビュー**
notifyview	**通知ビュー**
storage-type	**このエントリーのストレージタイプ**
Row Status	**ビューの状態**

例

```
Console#show snmp group
Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#
```

snmp-server user

SNMP ユーザーをグループへ追加します。

"no" を前に置くことでユーザーをグループから除きます。

文法

snmp-server user *username groupname* **[remote** *ip-address*] **{ v1 | v2c | v3 }**

[auth { md5 | sha } *auth-password* **[priv des56** *priv-password*] **]**

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

- *username* — ユーザー名（1-32 文字）
- *groupname* — グループ名（1-32 文字）
- **remote** — リモートデバイス上の SNMP エンジンを選択します
- *ip-address* — リモートデバイスの IP アドレス
- **v1 | v2c | v3** — SNMP バージョンの選択します
- **auth** — 認証を使用します
- **md5 | sha** — MD5 または SHA 認証を選択します
- *auth-password* — 認証用パスワード
- **priv des56** — DES56bit データ暗号化方式を使用します
- *priv-password* — 暗号化用パスワード。暗号化オプションが使用されていない場合はプレーンテキストを入力してください。暗号化オプションが使用されている場合は暗号化パスワードを入力してください。

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- リモートユーザーの設定を行う前に、「snmp-server engine-id」コマンドで、リモートエンジン ID の設定を行ってください。その後に「snmp-server user」を使用しユーザーと、ユーザーが所属するリモートデバイスの IP アドレスを設定してください。リモートエージェントのエンジン ID はユーザーのパスワードから認証 / プライバシーのダイジェストを計算するのに使用されます。
- SNMP パスワードは、信頼できるエージェントのエンジン ID を使用してローカライズされます。トラップ通知の信頼できる SNMP エージェントはリモートエージェントです。そのため、プロキシリクエストまたはトラップ通知を送信する前にリモートエージェントの SNMP エンジン ID を設定する必要があります。

例

```
Console(config)#snmp-server user steve group r&d v3 auth md5
greenpeace priv des56 einstien
Console(config)#snmp-server user mark group r&d remote
192.168.1.19 v3 auth md5 greenpeace priv des56 einstien
Console(config)#
```

show snmp user

SNMP ユーザー情報を表示します。

文法

show snmp user

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
EngineId	エンジン ID
User Name	ユーザー名
Authentication Protocol	認証プロトコル
Privacy Protocol	暗号化方式
storage-type	このエントリーのストレージタイプ
Row Status	ビューの状態
SNMP remote user	リモートデバイス上の SNMP エンジンに所属するユーザー

例

```
Console#show snmp user
EngineId: 0100000000000000000000000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active
SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active
Console#
```

4.7 ユーザ認証

システム管理のためのユーザログインはローカル及び認証サーバを用いたユーザ認証が利用可能です。

また、IEEE802.1X **を利用したポートベース認証によるユーザのネットワークへのアクセス管理も可能です。**

コマンドグループ	機能	ページ
User Accounts	**ユーザー名とパスワードの設定**	P323
Authentication Sequence	**ログイン認証方式と優先順位の設定**	P326
RADIUS Client	RADIUS **サーバ認証の設定**	P328
TACACS+ Client	TACACS+ **サーバ認証の設定**	P333
Web Server setting	Web **ブラウザからの管理アクセスを有効化**	P336
Telnet Server setting	Telnet **サーバからの管理アクセスを有効化**	P340
Secure Shell Settings	Telnet **接続に** SSH **を設定**	P341
Port Security	**ポートへのセキュアアドレスの設定**	P353
Port Authentication	EEE802.1X **によるポート認証の設定**	P355
Management IP Filter	**管理アクセスを許可される** IP **アドレスを設定**	P364

4.7.1 ユーザーアクセスコマンド

管理アクセスのための基本的なコマンドです。管理アクセスに関するその他の設定に関しては、P273 **「**password**」や** P326 **「認証コマンド」、**P355 **「**802.1x **ポート認証コマンド」があります。**

コマンド	機能	モード	ページ
username	**ログインするためのユーザ名の設定**	GC	P324
enable password	**各アクセスレベルのパスワードの設定**	GC	P325

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

- **初期設定のアクセスレベルは** Normal Exec **レベルです。**
- **初期設定のユーザ名とパスワードは以下の通りです。**

ユーザ名	アクセスレベル	パスワード
guest admin	0 15	guest admin

コマンドモード

Global Configuration

コマンド解説

暗号化されたパスワードはシステム起動時に設定ファイルを読み込む場合や TFTP **サーバにダウロードする場合のためにテキスト（平文）パスワードとの互換性があります。暗号化されたパスワードを手動で生成する必要はありません。**

例

本例は、ユーザへのアクセスレベルとパスワードの設定を示しています。

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

enable password

Normal Exec レベルから Privileged Exec レベルに移行する際に使用します。"no" を前に置くことで初期設定に戻ります。

安全のためパスワードは初期設定から変更してください。変更したパスワードは忘れないようにして下さい。

文法

enable password [level *level***] {0 | 7}** *password*

no enable password [level *level***]**

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

初期設定

初期設定レベル 15

初期設定パスワード "super"

コマンドモード

Global Configuration

コマンド解説

- パスワードを空欄にすることはできません。P245 「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 (P245)

authentication enabled (P327)

4.7.2 認証コマンド

本機のシステムへの管理アクセスに対するユーザ認証には、3 つの認証方法から指定することが可能です。

この項では、コマンドの認証方法とシーケンスを定義する方法について解説します。

コマンド	機能	モード	ページ
Authentication login	認証方法と優先順位の設定	GC	P326
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	P326

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

コマンドモード

Global Configuration

コマンド解説

- RADIUS では UDP、TACACS+ では TCP を使用します。UDP はベストエフォート型の接続ですが、TCP は接続確立型の接続となります。また、RADIUS 暗号化はクライアントからサーバへのアクセス要求パケットのパスワードのみが暗号化されます。
- RADIUS 及び TACACS+ ログイン認証は各ユーザ名とパスワードに対しアクセスレベルを設定することができます。ユーザ名とパスワード、アクセスレベルは認証サーバ側で設定することができます。
- 3 つの認証方式を 1 つのコマンドで設定することができます。例えば、"authentication login radius tacacs local" とした場合、ユーザ名とパスワードを RADIUS サーバに対し最初に確認します。RADIUS サーバが利用できない場合、TACACS+ サーバにアクセスします。TACACS+ サーバが利用できない場合はローカルのユーザ名とパスワードを利用します。

例

```
Console(config)#authentication login radius
Console(config)#
```

関連するコマンド

username (P324)

authentication enable

"enable" コマンド（P245）で Exec モードから Privileged Exec モードへ変更する場合の、ログイン認証方法及び優先順位を設定します。"no" を前に置くことで初期設定に戻します。

文法

authentication enable {[local] [radius] [tacacs]}

no authentication enable

- **local** — ローカル認証を使用します
- **radius** — RADIUS サーバ認証を使用します
- **tacacs** — TACACS+ サーバ認証を使用します

初期設定

Local のみ

コマンドモード

Global Configuration

コマンド解説

- RADIUS では UDP、TACACS+ では TCP を使用します。UDP はベストエフォート型の接続ですが、TCP は接続確立型の接続となります。また、RADIUS 暗号化はクライアントからサーバへのアクセス要求パケットのパスワードのみが暗号化されます。
- RADIUS 及び TACACS+ ログイン認証は各ユーザ名とパスワードに対しアクセスレベルを設定することができます。ユーザ名とパスワード、アクセスレベルは認証サーバ側で設定することができます。
- 3 つの認証方式を 1 つのコマンドで設定することができます。例えば、"authentication enable radius tacacs local" とした場合、ユーザ名とパスワードを RADIUS サーバに対し最初に確認します。RADIUS サーバが利用できない場合、TACACS+ サーバにアクセスします。TACACS+ サーバが利用できない場合はローカルのユーザ名とパスワードを利用します。

例

```
Console(config)#authentication enable radius
Console(config)#
```

関連するコマンド

enable password (P245) — コマンドモード変更のためのパスワードの設定

4.7.3 Radius クライアントコマンド

RADIUS(Remote Authentication Dial-in User Service) は、ネットワーク上の RADIUS 対応デバイスのアクセスコントロールを認証サーバにより集中的に管理することができます。認証サーバは複数のユーザ名 / パスワードと各ユーザの本機へのアクセスレベルを管理するデータベースを保有しています。

コマンド	機能	モード	ページ
radius-server host	RADIUS サーバの設定	GC	P329
radius-server port	RADIUS サーバのポートの設定	GC	P330
radius-server key	RADIUS 暗号キーの設定	GC	P330
radius-server retransmit	リトライ回数の設定	GC	P331
radius-server timeout	認証リクエストの間隔の設定	GC	P331
show radius-server	RADIUS 関連設定情報の表示	PE	P332

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

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

- *index* — **サーバを** 5 **つまで設定できます。指定したサーバの順に、サーバが応答するかタイムアウトがくるまでリクエストを送信します。**
- *host_ip_address* — RADIUS **サーバの** IP **アドレス**
- *auth_port* — RADIUS **サーバの認証用** UDP **ポート番号（範囲：**1-65535**）**
- *key* — **クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入れられません（最大** 48 **文字）**
- *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**）**
- *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）**

初期設定

- auth-port：1812
- timeout：5 **秒**
- retransmit：2

コマンドモード

Global Configuration

例

```
Console(config)#radius-server 1 host 192.168.1.20 auth-port 181 timeout
10 retransmit 5 key green
Console(config)#
```

radius-server 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 48 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

リトライ数を設定します。"no" **を前に置くことで初期設定に戻します。**

文法

radius-server retransmit *number_of_retries*

no radius-server retransmit

- *number_of_retries* — RADIUS **サーバに対するログインアクセスをリトライできる回数（範囲：**1-30**）**

初期設定

2

コマンドモード

Global Configuration

例

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

RADIUS **サーバへの認証要求を送信する間隔を設定します。**"no" **を前に置くことで初期設定に戻します。**

文法

radius-server timeout *number_of_seconds*

no radius-server timeout

- *number_of_seconds* — **サーバからの応答を待ち、再送信を行うまでの時間（秒）(範囲：**1-65535)

初期設定

5

コマンドモード

Global Configuration

例

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

現在の RADIUS サーバ関連の設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show radius-server

Remote RADIUS server configuration:

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

Server 1:
 Server IP address: 192.168.1.1
 Communication key with RADIUS server: *****
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5

Console#
```

4.7.4 TACACS+ クライアントコマンド

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

コマンド	機能	モード	ページ
tacacs-server host	TACACS+ サーバの設定	GC	P333
tacacs-server port	TACACS+ サーバのポートの設定	GC	P334
tacacs-server key	TACACS+ 暗号キーの設定	GC	P334
show tacacs-server	TACACS+ 関連設定情報の表示	GC	P335

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 48 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server key green
Console(config)#
```

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#
```

4.7.5 Web サーバーコマンド

コマンド	機能	モード	ページ
ip http port	Web インタフェースに使用するポートの設定	GC	P336
ip http server	管理用 Web インタフェースの使用	GC	P337
ip http secure-server	セキュア HTTP（HTTPS）サーバの使用	GC	P338
ip http secure-port	HTTPS 接続に使用するポートの設定	GC	P339

ip http port

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

文法

ip http port *port-number*

no ip http port

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

初期設定

80

コマンドモード

Global Configuration

例

```
Console(config)#ip http port 769
Console(config)#
```

関連するコマンド

ip http server（P337）
show system（P258）

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（P336）
show system（P258）

ip http secure-server

Web インタフェースを使用し本機への暗号化された安全な接続を行うために、Secure Socket Layer (SSL) を使用した Secure hypertext transfer protocol (HTTPS) を使用するためのコマンドです。"no" を前に置くことで本機能を無効にします。

文法

ip http secure-server

no ip http secure-server

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- HTTP 及び HTTPS サービスはそれぞれのサービスを個別に有効にすることが可能です。
- HTTPS を有効にした場合は Web ブラウザのアドレスバーに https://device [: ポート番号] と入力します。
- HTTPS を有効にした場合、以下の手順で接続が確立されます：
  - クライアントはサーバのデジタル証明書を使用し、サーバを確証します。
  - クライアントおよびサーバは、接続のために使用する 1 セットのセキュリティ・プ ロトコルを協定します。
  - クライアントおよびサーバは、データを暗号化し解読するためのセッション・キーを生成します。
- クライアントとサーバ間の暗号化されたアクセスが確立した場合、Internet Explorer 5.x 以上及び Netscape Navigator 6.2 以上、Mozilla Firefox 2.0.0.0 以上のステータスバーに鍵マークが表示されます。

？セキュアサイト証明の詳細は P59 「サイト証明書の設定変更」を参照して下さい。

例

```
Console(config)#ip http secure-server
Console(config)#
```

関連するコマンド

ip http secure-port（P339）
copy tftp https-certificate（P262）

ip http secure-port

Web インタフェースからの HTTPS/SSL 接続で使用する UDP ポートを設定することができます。"no" を前に置くことで初期設定に戻ります。

文法

ip http secure-port *port_number*

no ip http secure-port

- *port_number* — HTTPS/SSL に使用する UDP ポート番号 (1-65535)

初期設定

443

コマンドモード

Global Configuration

コマンド解説

- HTTP と HTTPS で同じポートは設定できません。
- HTTPS ポート番号を設定した場合、HTTPS サーバにアクセスするためには URL にポート番号を指定する必要があります。(https://device:[ポート番号])

例

```
Console(config)#ip http secure-port 1000
Console(config)#
```

関連するコマンド

ip http secure-server（P338）
show system（P258）

4.7.6 Telnet サーバーコマンド

コマンド	機能	モード	ページ
ip telnet server	管理用 Telnet インタフェースの使用	GC	P340

ip telnet server

Telnet から本機の設定、及び設定情報の閲覧を可能にします。

"no" を前に置くことで本機能は無効となります。

文法

ip telnet server [port *port-number*]
no ip telnet server [port *port-number*]

- Port — Telnet インタフェースに使用される TCP ポート
- *port_number* — ブラウザインタフェースに使用される TCP ポート番号 （範囲：1-65535）

初期設定

サーバー：有効
サーバーポート：23

コマンドモード

Global Configuration

例

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

4.7.7 Secure Shell コマンド

Secure Shell (SSH) は、それ以前からあったバークレーリモートアクセスツールのセキュリティ面を確保した代替としてサーバ / クライアントアプリケーションを含んでいます。また、SSH は Telnet に代わる本機へのセキュアなリモート管理アクセスを提供します。

クライアントが SSH プロトコルによって本機と接続する場合、本機はアクセス認証のためにローカルのユーザ名およびパスワードと共にクライアントが使用する公開暗号キーを生成します。さらに、SSH では本機と SSH を利用する管理端末の間の通信をすべて暗号化し、ネットワーク上のデータの保護を行ないます。

ここでは、SSH サーバを設定するためのコマンドを解説します。

なお、SSH 経由での管理アクセスを行なうためには、クライアントに SSH クライアントをインストールする必要があります。

[注意] 本機では SSH Version1.5 と 2.0 をサポートしています。

コマンド	機能	モード	ページ
ip ssh server	SSH サーバの使用	GC	P344
ip ssh timeout	SSH サーバの認証タイムアウト設定	GC	P345
ip ssh authentication -retries	クライアントに許可するリトライ数の設定	GC	P346
ip ssh server-key size	SSH サーバキーサイズの設定	GC	P346
copy tftp public-key	ユーザ公開キーの TFTP サーバから本機へコピー	PE	P262
delete public-key	特定ユーザの公開キーの削除	PE	P347
ip ssh crypto host-key generate	ホストキーの生成	PE	P348
ip ssh crypto zeroize	RAM からのホストキーの削除	PE	P349
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	P350
disconnect	ライン接続の終了	PE	P281
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	P350
show ssh	SSH セッション状態の表示	PE	P351
show public-key	特定のユーザ又はホストの公開キーの表示	PE	P352
show users	SSH ユーザ、アクセスレベル、公開キータイプの表示	PE	P259

本機の SSH サーバはパスワード及びパブリックキー認証をサポートしています。SSH クライアントによりパスワード認証を選択した場合、認証設定ページで設定したパスワードにより本機内、RADIUS、TACACS+ のいずれかの認証方式を用います。クライアントがパブリックキー認証を選択した場合には、クライアント及び本機に対して認証キーの設定を行なう必要があります。公開暗号キー又はパスワード認証のどちらかを使用するに関わらず、本機上の認証キー（SSH ホストキー）を生成し、SSH サーバを有効にする必要があります。

SSH サーバを使用するには以下の手順で設定を行ないます。

(1) **ホストキーペアの生成** — "ip ssh crypto host-key generate" **コマンドによりホスト パブリック / プライベートキーのペアを生成します。**

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

10.1.0.54 1024 35
15684995401867669259333946775054617325313674890836547254150202455931998685443583616519999233297817660658309561082591321289023376546801726272571413428762941301196195566782595664104869574278881462065194174677298486546861571773939016477935594230357741309802273708779454524083971752646358058176716709574804776117

(3) **クライアント公開キーの本機への取り込み** — P4-69"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。クライアントへはこれらのキーを使用し、認証が行なわれます。現在のファームウェアでは以下のような** UNIX **標準フォーマットのファイルのみ受け入れることが可能です。**

1024 35
13410816856098939210409449201554253476316419218729589211431738800555361616310517759408386863110929123222682851925437460310093718772119969631781366277414168985132049117204830339254324101637997592371449011938006090253948408482717819437228840253311595213486102290297898272135326713162943253281891504530639391664 3 steve@192.168.1.19

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

(5) **SSH サービスの有効化** — "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) **認証** — **以下の認証方法の内** 1 **つが使用されます。**

- **パスワード認証（**SSH1.5 **または** V2 **クライアント）**

  a. **クライアントが自身のパスワードをサーバへ送ります。**

  b. **本機はクライアントのパスワードと、メモリに保管されている物を比較します。**

  c. **一致した場合、接続が許可されます。**

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

- **パブリックキー認証**－ SSH **クライアントが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。このプロセスの間に、以下の交換が行われます。**

  SSH1.5 クライアントの認証

  a. **クライアントが自身の** RSA **パブリックキーをサーバへ送ります。**

b. スイッチはクライアントのパブリックキーと、メモリに保管されている物を比較します。

c. 一致した場合、スイッチは Challenge としてランダム 256 ビット文字列を生成するために、そのシークレットキーを使用し、この文字列をユーザーのパブリックキーと共に暗号化します。その後、これをクライアントに送信します。

d. クライアントはそのプライベートキーを、Challenge 文字列を解読するために使用し、MD5 チェックサムを計算した後スイッチへ送り返します。

SSH v2 クライアントの認証

a. DSA パブリックキー認証が受容できるか否かを決定するために、クライアントは最初にスイッチへ問い合わせを行います。

b. 指定したアルゴリズムがスイッチでサポートされる場合、認証プロセスを続けるようクライアントへ知らせます。さもなければリクエストは拒絶されます。

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

d. サーバがメッセージを受信した際、それは供給されたキーが認証のために受容できるか否かを調べ、もしそうであるならば今度は署名が正しいか否かを調べます。両方のチェックが成功した場合、クライアントは認証されます。

[注意] SSH サーバは最大 4 つのクライアントセッションをサポートします。クライアントセッションの最大数は、点在と Telnet セッションと SSH セッションの両方を含みます。

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

[no] ip ssh server

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 最大 4 セッションの同時接続をサポートします。最大セッション数は Telnet 及び SSH の合計数です。
- SSH サーバはクライアントとの接続を確立する際に DAS 又は RAS を使ったキー交換を行います。その後、DES (56-bit) または 3DES (168-bit) を用いてデータの暗号化を行います。
- SSH サーバを有効にする前に、ホストキーを生成する必要があります。

例

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

関連するコマンド

ip ssh crypto host-key generate (P348)

show ssh (P351)

ip ssh timeout

SSH サーバのタイムアウト時間を設定します。"no" を前に置くことで初期設定に戻ります。

文法

ip ssh timeout *seconds*

no ip ssh timeout

- *seconds* — SSH 接続調整時のクライアント応答のタイムアウト時間（設定範囲：1-120）

初期設定

10 秒

コマンドモード

Global Configuration

コマンド解説

タイムアウトは SSH 情報交換時のクライアントからの応答を本機が待つ時間の指定を行ないます。SSH セッションが確立した後のユーザ入力のタイムアウトは vty セッションへの "exec-timeout" コマンドを使用します。

例

```
Console(config)#ip ssh timeout 60
Console(config)#
```

関連するコマンド

exec-timeout (P275)

show ip ssh (P350)

ip ssh authentication-retries

SSH サーバがユーザの再認証を行なう回数を設定します。"no" を前に置くことで初期設定に戻ります。

文法

ip ssh authentication-retries *count*
no ip ssh authentication-retries

- *count* — インタフェースがリセット後、認証を行なうことができる回数（設定範囲：1-5）

初期設定

3

コマンドモード

Global Configuration

例

```
Console(config)#ip ssh authentication-retries 2
Console(config)#
```

関連するコマンド

show ip ssh (P350)

ip ssh server-key size

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

文法

ip ssh server-key size *key-size*

no ip ssh server-key size

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

初期設定

768 bits

コマンドモード

Global Configuration

コマンド解説

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

例

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

delete public-key

特定のユーザパブリックキーを削除します。

文法

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

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

初期設定

DSA 及び RSA キーの両方の削除

コマンドモード

Privileged Exec

例

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

ip ssh crypto host-key generate

パブリック及びプライベートのホストキーペアの生成を行ないます。

文法

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

- **dsa** — DSA（Version2）キータイプ
- **rsa** — RSA（Version1）キータイプ

初期設定

DSA 及び RSA キーペア両方の生成

コマンドモード

Privileged Exec

コマンド解説

- 本コマンドはホストキーペアをメモリ (RAM) に保存します。" ip ssh save host-key" コマンドを使用してホストキーペアをフラッシュメモリに保存できます。
- 多くの SSH クライアントは接続設定時に自動的にパブリックキーをホストファイルとして保存します。そうでない場合には、手動で管理端末のホストファイルを作成し、ホスト公開キーを置く必要があります。
- SSH サーバは、接続しようとするクライアントとセッションキー及び暗号化方法を取り決めるためにホストキーを使用します。

例

```
Console#ip ssh crypto host-key generate dsa
Console#
```

関連するコマンド

ip ssh crypto zeroize （P349）
ip ssh save host-key （P350）

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（P348）
ip ssh save host-key（P350）

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 (P348)

show ip ssh

このコマンドを使用することで SSH サーバの設定状況を閲覧することができます。

コマンドモード

Privileged Exec

例

```
Console#show ip ssh
SSH Enabled - version 1.99
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

show ssh

現在の SSH **サーバへの接続状況を表示します。**

コマンドモード

Privileged Exec

例

```
Console#show ssh
Connection Version  State            Username  Encryption
0          2.0   Session-Started admin    ctos aes128-cbc-hmac-md5
                                              stoc aes128-cbc-hmac-md5
Console#
```

項目	解説
Session	**セッション番号** (0-3)
Version	SSH **バージョン番号**
State	**認証接続状態（値：**Negotiation-Started, Authentication-Started,Session-Started**）**
Username	**クライアントのユーザ名**
Encryption	**暗号化方式はクライアントとサーバの間で自動的に情報交換を行ない設定します。** SSH v1.5 **の選択肢：**DES, 3DES SSH v2.0 **の選択肢は** client-to-server (ctos) **及び** server-to-client (stoc) **の** 2 **種類の方式をサポートします：** aes128-cbc-hmac-sha1、aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1、3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1、aes128-cbc-hmac-md5 aes192-cbc-hmac-md5、aes256-cbc-hmac-md5 3des-cbc-hmac-md5、blowfish-cbc-hmac-md5 **用語集：** DES — Data Encryption Standard (56-bit key) 3DES — Triple-DES (Uses three iterations of DES, 112-bit key) aes — Advanced Encryption Standard (160 or 224-bit key) blowfish — Blowfish (32-448 bit key) cbc — cypher-block chaining sha1 — Secure Hash Algorithm 1 (160-bit hashes) md5 — Message Digest algorithm number 5 (128-bit hashes)

show public-key

特定のユーザ又はホストの公開キーを表示します。

文法

show public-key [user [*username*] | host]

- *username* — SSH ユーザ名（範囲：1-8 文字）

初期設定

すべての公開キーの表示

コマンドモード

Privileged Exec

コマンド解説

- パラメータを設定しない場合には、すべてのキーが表示されます。キーワードを入力し、ユーザ名を指定しない場合、すべてのユーザの公開キーが表示されます。
- RSA キーが表示された場合、最初のフィールドはホストキーサイズ (1024) となり、次のフィールドはエンコードされた公開指数 (35)、その後の値がエンコードされたモジュールとなります。DSA キーが表示された場合、最初のフィールドは SSH で使用される暗号化方式の DSS となり、その後の値がエンコードされたモジュールとなります。

例

```
Console#show public-key host
Host:
RSA:
1024 35
156849954018676692593339467750546173253136748908365472541502024559319
986854435836165199992332978176606583095861082591321289023376546801726
272571413428762941301196195566782595664104869574278881462065194174677
298486546861571773939016477935594230357741309802273708779454524083971
752646358058176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/
Dg0h2HxcYV44sXZ2JXhamLK6P8bvuiyacWbUW/
a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfvJlPdOkFgzLGMinvSNYQwiQXbKT
BH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEAsy
5YWDC99ebYHNRj5kh47wY4i8cZvH+/
p9cnrfwFTMU01VFDly3IR2G395NLy5Qd7ZDxfA9mCOfT/
yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/
Kjw6BmiFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/
ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOyDbsloBfPuSAb4oAsyjKXKVYNLQkTLZ
fcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2 o/
dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475
S7 w0W
Console#
```

4.7.8 ポートセキュリティコマンド

ポートへのポートセキュリティ機能を使用できるようにします。ポートセキュリティ機能を使用すると、ポートにおける最大学習数に達した際に MAC アドレスの学習を止めます。そして、そのポートの動的 / 静的なアドレステーブルに既に登録されているソース MAC アドレスの受信フレームのみネットワークへのアクセスを許可します。そのポートでも他のポートからも学習されていない不明なソース MAC アドレスの受信フレームは破棄します。学習されていない MAC アドレスを送信するデバイスがあった場合、この動作はスイッチで検知され、自動的にそのポートを無効にし、SNMP トラップメッセージを送信します。

コマンド	機能	モード	ページ
port security	ポートセキュリティの設定	IC	P353
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	P407
show mac-address-table	フォワーディングデータベースのエントリ表示	PE	P409

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 0 は無効です）

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：
  - 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（P384）
mac-address-table static（P407）

4.7.9 802.1x ポート認証コマンド

本機では IEEE802.1X (dot1x) のポートベースアクセスコントロールをサポートし、ID とパスワードによる認証により許可されないネットワークへのアクセスを防ぐことができます。クライアントの認証は RADIUS サーバにより EAP(Extensible Authentication Protocol) を用いて行われます。

コマンド	機能	モード	ページ
dot1x system-auth-control	dot1x をスイッチ全体に有効に設定	GC	P355
dot1x default	dot1x の設定値をすべて初期設定に戻します。	GC	P356
dot1x max-req	認証プロセスを初めからやり直す前に認証プロセスを繰り返す最大回数	GC	P356
dot1x port-control	ポートへの dot1x モードの設定	IC	P357
dot1x operation-mode	dot1x ポートへの接続可能ホスト数の設定	IC	P358
dot1x re-authenticate	特定ポートへの再認証の強制	PE	P359
dot1x re-authentication	全ポートへの再認証の強制	GC	P359
dot1x timeout quiet-period	max-req を超えた後、クライアントの応答を待つ時間	GC	P360
dot1x timeout re-autheperiod	接続済みクライアントの再認証間隔の設定	GC	P360
dot1x timeout tx-period	認証中の EAP パケットの再送信間隔の設定	GC	P361
show dot1x	dot1x 関連情報の表示	PE	P362

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

[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 P357 「dot1x port-control」で "auto" に設定されている場合にのみ有効です。
- "multi-host" を設定すると、ポートに接続するホストのうちの 1 台のみが認証の許可を得られれば、他の複数のホストもネットワークへのアクセスが可能になります。逆に、接続するホスト再認証に失敗したり、EAPOL ログオフメッセージを送信した場合、他のホストも認証に失敗したことになります。

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x re-authenticate

全ポート又は特定のポートでの再認証を強制的に行います。

文法

dot1x re-authenticate [*interface*]

- i*nterface*
  - **ethernet** *unit/port*
    - *unit* — **ユニット番号 （範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**

コマンドモード

Privileged Exec

例

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

dot1x re-authentication

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

文法

dot1x re-authentication
no dot1x re-authentication

コマンドモード

Interface Configuration

例

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

dot1x timeout quiet-period

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

文法

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period

- *seconds* — 秒数（範囲：1-65535 秒）

初期設定

60 秒

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod

接続されたクライアントに再認証を要求する間隔を設定します。

文法

dot1x timeout re-authperiod *seconds*
no dot1x timeout re-authperiod

- *seconds* — 秒数（範囲：1-65535 秒）

初期設定

3600 秒

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

dot1x timeout tx-period

認証時に EAP **パケットの再送信を行う間隔を設定します。**"no" **を前に置くことで初期設定に戻します。**

文法

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

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

初期設定

30 **秒**

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

show dot1x

本機または特定のインタフェースのポート認証に関連した設定状態の表示を行います。

文法

show dot1x [statistics] [interface *interface***]**

- *interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号 （範囲：1-8）
    - *port* — ポート番号（範囲：1-26）

コマンドモード

Privileged Exec

コマンド解説

本コマンドで表示されるのは以下の情報です。

- *Global 802.1X Parameters* — 本機全体に対する、802.1X ポート認証の有効 / 無効
- *802.1X Port Summary* — 各インタフェースのアクセスコントロールの設定値
  - Status — ポートアクセスコントロールの管理状態
  - Operation Mode — P358 「dot1x operation-mode」の設定値
  - Mode — dot1x port-control で設定する dot1x モード (P357)
  - 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 (P359)
  - reauth-period - 接続されたクライアントに再認証を要求する間隔 (P360)
  - 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 (P360)
  - tx-period - 認証時に EAP パケットの再送信を行う間隔 (P361)
  - 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 (P356)
  - 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 (P358)
  - 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 (P357)
  - 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
.
.
1/52        disabled   Single-Host    ForceAuthorized   n/a
802.1X Port Details
802.1X is disabled on port 1/1
802.1X is enabled on port 1/2
  reauth-enabled: Enable
  reauth-period: 1800
  quiet-period: 30
  tx-period: 40
  supplicant-timeout: 30
  server-timeout: 10
  reauth-max: 2
  max-req: 5
Status              Authorized
Operation mode      Single-Host
Max count           5
Port-control        Auto
Supplicant          00-12-cf-49-5e-dc
Current Identifier 3
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 1/52
Console#
```

4.7.10 管理 IP フィルターコマンド

コマンド	機能	モード	ページ
management	管理アクセスを許可する IP アドレスを設定	GC	P364
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	P365

management

本機では管理アクセスに接続を許可するクライアントの IP アドレスの設定を行なうことができます。"no" を前に置くことで設定を削除します。

文法

[no] management {all-client | http-client | snmp-client | telnet-client}

start-address **[***end-address***]**

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

初期設定

全アドレス

コマンドモード

Global Configuration

コマンド解説

- 設定以外の無効な IP アドレスから管理アクセスに接続された場合、本機は接続を拒否し、イベントメッセージをシステムログに保存し、トラップメッセージの送信を行ないます。
- SNMP、Web ブラウザ、Telnet アクセスへの IP アドレス又は IP アドレス範囲の設定は合計で最大 5 つまで設定可能です。
- SNMP、Web ブラウザ、Telnet の同一グループに対して IP アドレス範囲を重複して設定することはできません。異なるグループの場合には IP アドレス範囲を重複して設定することは可能です。
- 設定した IP アドレス範囲から特定の IP アドレスのみを削除することはできません。IP アドレス範囲をすべて削除し、その後設定をし直して下さい。
- IP アドレス範囲の削除は IP アドレス範囲の最初のアドレスだけを入力しても削除することができます。また、最初のアドレスと最後のアドレスの両方を入力して削除することも可能です。

例

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なっています。

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

show management

管理アクセスへの接続が許可されている IP アドレスを表示します。

文法

show management {all-client | http-client | snmp-client |telnet-client}

- **all-client** — SNMP/Web **ブラウザ** /Telnet **クライアントの** IP **アドレス**
- **http-client** — Web **ブラウザクライアントの** IP **アドレス**
- **snmp-client** — SNMP **クライアントの** IP **アドレス** .
- **telnet-client** — Telnet **クライアントの** IP **アドレス**

コマンドモード

Privileged Exec

例

```
Console#show management all-client
Management Ip Filter
Http-Client:
Start ip address End ip address
-----------------------------------------------
1. 192.168.1.19 192.168.1.19
2. 192.168.1.25 192.168.1.30

Snmp-Client:
Start ip address End ip address
-----------------------------------------------
1. 192.168.1.19 192.168.1.19
2. 192.168.1.25 192.168.1.30

Telnet-Client:
Start ip address End ip address
-----------------------------------------------
1. 192.168.1.19 192.168.1.19
2. 192.168.1.25 192.168.1.30

Console#
```

4.8 ACL（Access Control Lists）

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

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

コマンド	機能	ページ
IP ACLs	IP アドレス、TCP/UDP ポート番号、TCP コントロールコードに基づく ACL の設定	P366
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	P372
ACL Information	ACL 及び関連するルールの表示。各ポートの ACL の表示	P376

4.8.1 IP ACL コマンド

この節のコマンドで、IP アドレス、TCP/UDP ポート番号、プロトコルタイプ、TCP コントロールコードを基にした ACL の設定を行います。
IP ACL を設定するには、最初に必要な許可、または拒否ルールを含むアクセスリストを作成することから始め、その後にアクセスリストを 1 つ以上のポートにバインドします。

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	P367
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	P368
permit,deny	ソース又はディスティネーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号に基づくフィルタリング	EXT-ACL	P369
show ip access-list	設定済み IP ACL のルールの表示	PE	P370
ip access-group	IP ACL へのポートの追加	IC	P371
show ip access-group	IP ACL に指定したポートの表示	PE	P371

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

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

- **standard** — ソース IP アドレスに基づくフィルタリングを行う ACL
- **extended** — ソース又はディスティネーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号に基づくフィルタリングを行う ACL
- *acl_name* — ACL 名（最大 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（P368）
ip access-group（P371）
show ip access-list（P370）

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

[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（**P367**）

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* [*bitmask*]] [destination-port *dport* [*port-bitmask*]]

[**no**] {**permit** | **deny**} tcp

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

{any | *destination address-bitmask* | host *destination*}

[precedence *precedence*] [tos *tos*] [dscp *dscp*]

[source-port sport [*bitmask*]] [destination-port *dport* [*port-bitmask*]]

[control-flag *control-flags flag-bitmask*]

- *protocol-number* — **特定のプロトコル番号（範囲：**0-255**）**
- *source* — **ソース** IP **アドレス**
- *destination* — **ディスティネーション** IP **アドレス**
- *address-bitmask* — **アドレスビットマスク**
- host — **特定の** IP **アドレスの指定**
- *precedence*— Precedence **レベル（範囲：**0-7**）**
- *tos* — ToS **レベル（範囲：**0-7**）**
- *dscp* — DSCP **プライオリティレベル（**0-63**）**
- *sport* — **プロトコル** * **ソースポート番号（範囲：**0-65535**）**
- *dscp* — DSCP **プライオリティレベル（範囲：**0-63**）**
- *port-bitmask* — **ポートビットマスク**
- *control-flags* —TCP **ヘッダの** 14 **バイト内フラッグビットを指定する** 10 **進数（範囲：**0-63**）**
- *flag-bitmask* — **フラッグビットマスク**

初期設定

なし

コマンドモード

Extended ACL

コマンド解説

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

例

本例では、ソースアドレスがサブネット 10.7.1.x 内の場合、すべての入力パケットを許可します。

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

本例では、ディスティネーション TCP ポート番号 80 のクラス C アドレス 192.168.1.0 からすべてのディスティネーションアドレスへの TCP パケットを許可します。

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
destination-port 80
Console(config-ext-acl)##
```

関連するコマンド

access-list ip（P367）

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（4 文字以上 15 文字以内）

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（P368）
ip access-group（P371）

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

[no] ip access-group *acl_name* **in**

- *acl_name* — 最大 16 文字
- **in** — 入力パケットへのリスト

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 1 つのポートは 1 つの ACL のみ設定可能です。
- ポートがすでに ACL を設定済みで、他の ACL をバインドした場合、新しくバインドした ACL が有効となります。

例

```
Console(config)#int eth 1/25
Console(config-if)#ip access-group david in
Console(config-if)#
```

関連するコマンド

show ip access-list （P370）

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 (P371)

4.8.2 MAC ACL コマンド

コマンド	機能	モード	ページ
access-list mac	MAC ACL の作成と configuration mode への移行	GC	P372
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	P373
show mac access-list	設定済み MAC ACL のルールの表示	PE	P375
mac access-group	MAC ACL へのポートの追加	IC	P375
show mac access-group	MAC ACL に指定したポートの表示	PE	P376

access-list mac

MAC アドレスリストを追加し、MAC ACL 設定モードに移行します。"no" を前に置くことで指定した ACL を削除します。

文法

access-list mac *acl_name*
no access-list mac *acl_name*

- *acl_name* — ACL 名（最大 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)（P368）
mac access-group（P371）
show mac access-list（P370）

permit,deny（MAC ACL）

MAC ACL へのルールの追加を行います。MAC ソース / ディスティネーションアドレス、イーサネットプロトコルタイプによりフィルタリングを行います。"no" を前に置くことでルールを削除します。

文法

[**no**] {**permit** | **deny**}
{any |host *source*|*source address-bitmask*}
{any | host *destination* | *destination address-bitmask*}
[vid *vid vid-bitmask*] [ethertype *protocol* [*protocol-bitmask*]]

? 初期設定は Ethernet2 パケットです。

[**no**] {**permit** | **deny**} tagged-eth2
{any |host *source*|*source address-bitmask*}
{any | host *destination* | *destination address-bitmask*}
[vid *vid vid-bitmask*] [ethertype *protocol* [*protocol-bitmask*]

[**no**] {**permit** | **deny**} untagged-eth2
{any |host *source*|*source address-bitmask*}
{any | host *destination* | *destination address-bitmask*}
[ethertype *protocol* [*protocol-bitmask*]

[**no**] {**permit | deny**} **tagged-802.3**
{**any |host** *source*|*source address-bitmask*}
{**any | host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*]

[**no**] {**permit** | **deny**} untagged-802.3
{any |host *source*|*source address-bitmask*}
{any | host *destination* | *destination address-bitmask*}

protocol-number — 特定のプロトコル番号（範囲：0-255）

- tagged-eth2 — タグ付きイーサネット 2 パケット
- untagged-eth2 — タグ無しイーサネット 2 パケット定
- tagged-802.3 — タグ付きイーサネット 802.3 パケット
- untagged-802.3 — タグ無しイーサネット 802.3 パケット
- any — すべての MAC ソース / ディスティネーションアドレス
- host — 特定の MAC アドレス
- *source* — ソース MAC アドレス
- *destination* — ビットマスクを含むディスティネーション MAC アドレス範囲
- *address-bitmask* — MAC アドレスのビットマスク（16 進数）
- *vid* — VLAN ID（範囲：1-4093）
- *vid* — VLAN ビットマスク（範囲：1-4093）
- *protocol* — イーサネットプロトコル番号（範囲：600-fff 16 進数）
- *protocol -bitmask*— プロトコルビットマスク（範囲：600-fff 16 進数）

初期設定

なし

コマンドモード

MAC ACL

コマンド解説

- 新しいルールはリストの最後に追加されます。
- イーサネットタイプオプションは Ethernet II のフィルタにのみ使用します。
- イーサネットプロトコルタイプのリストは RFC 1060 で定義されていますが、一般的なタイプは以下の通りです。
  - 0800(IP)
  - 0806(ARP)
  - 8137(IPX)

例

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

関連するコマンド

access-list mac (P372)

show mac access-list

MAC ACL のルールを表示します。

文法

show mac access-list [*acl_name*]

- *acl_name* — ACL 名（最大 16 文字）

コマンドモード

Privileged Exec

例

```
Console#show mac access-list
MAC access-list jerry:
   permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

関連するコマンド

permit, deny（P373）
mac access-group（P375）

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

[no] mac access-group *acl_name* **in**

- *acl_name*— ACL 名（最大 16 文字）
- **in** — 入力パケットへのリスト

コマンドモード

Privileged Exec

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

関連するコマンド

show mac access-list（P375）

show mac access-group

MAC ACL に指定されたポートを表示します。

コマンドモード

Privileged Exec

例

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
Console#
```

関連するコマンド

mac access-group （P375）

4.8.3 ACL 情報の表示

コマンド	機能	モード	ページ
show access-list	全ての ACL と関連するルールの表示	PE	P376
show access-group	ソース IP アドレスが一致するパケットのフィルタリング	PE	P377

show access-list

すべての ACL とユーザ定義マスクを含む関連するルールを表示します。

コマンドモード

Privileged Exec

コマンド解説

- ACL がインタフェースに結合されると、ルールが表示される順序は関連するマスクによって決定されます。

例

```
Console#show access-list
IP standard access-list david:
 permit host 10.1.1.21
 permit 168.92.16.0 255.255.240.0
IP extended access-list bob:
 permit 10.7.1.1 255.255.255.0 any
 permit 192.168.1.0 255.255.255.0 any destination-port 80 80
IP access-list jerry:
 permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
 permit any any
Console#
```

show access-group

ACL のポートの指定を表示します。

コマンドモード

Privileged Executive

例

```
Console#show access-group
Interface ethernet 1/1
 IP access-list jerry in
.
.
.
Interface ethernet 1/26
 IP access-list jerry in
Console#
```

4.9 インタフェース

コマンド	機能	モード	ページ
interface	本機の DHCP クライアント ID の指定	GC	P378
description	インタフェースタイプの設定及び interface configuration モードへの変更	IC	P379
speed-duplex	インタフェースの解説	IC	P380
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	P381
capabilities	オートネゴシエーション無効時の通信速度、通信方式の設定	IC	P382
flowcontrol	インタフェースへのフローコントロール設定	IC	P383
media-type	コンボポートの強制ポートタイプの設定	IC	P384
shutdown	インタフェースを無効化	IC	P384
switchport broadcast packet-rate	ロードキャストストームコントロールの設定	IC	P386
clear counters	インタフェースの統計情報のクリア	PE	P387
show interfaces status	インタフェースの設定状況を表示	NE,PE	P388
show interfaces counters	インタフェースの統計情報の表示	NE,PE	P389
show interfaces switchport	インタフェースの管理、運用状況の表示	NE,PE	P390

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 （範囲：1-8）
    - *port* — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)
  - vlan *vlan-id* — VLAN ID (1-4093)

初期設定

なし

コマンドモード

Global Configuration

例

本例では 24 番ポートの指定を行っています。

```
Console(config)#interface ethernet 1/24
Console(config-if)#
```

description

各インタフェースの解説を行います。"no" を前に置くことで解説を削除します。

文法

description *string*

no description

- *string* — 設定や監視作業を行いやすくするための各ポートの接続先などのコメントや解説（範囲：1-64 文字）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

本例は、24 番ポートに解説を加えている設定です。

```
Console(config)#interface ethernet 1/24
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

オートネゴシエーションを無効にした場合の通信速度及び通信方式の設定が行えます。"no" **を前に置くことで初期設定に戻します。**

文法

speed-duplex {1000full | 100full | 100half | 10full | 10half }
no speed-duplex

- 1000full — 1000 Mbps full-duplex **固定**
- 100full — 100 Mbps full-duplex **固定**
- 100half — 100 Mbps half-duplex **固定**
- 10full — 10 Mbps full-duplex **固定**
- 10half — 10 Mbps half-duplex **固定**

初期設定

- **初期設定ではオートネゴシエーションが有効になっています。**
- **オートネゴシエーションが無効の際、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。また、**"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（P381）
capabilities（P382）

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（P382）
speed-duplex（P380）

capabilities

オートネゴシエーション時のポートの通信方式を設定します。

"no" **を前に置きパラメータを設定することで指定したパラメータの値を削除します。パラメータを設定せず** "no" **を前に置いた場合には初期設定に戻ります。**

文法

capabilities [1000full | 100full | 100half | 10full | 10half | flowcontrol | symmetric]

no capabilities { 1000full | 100full | 100half | 10full | 10half | flowcontrol | symmetric }

- **1000full** — 1000Mbps full-duplex **通信**
- **100full** — 100Mbps full-duplex **通信**
- **100half** — 100Mbps half-duplex **通信**
- **10full** — 10Mbps full-duplex **通信**
- **10half** — 10Mbps half-duplex **通信**
- **flowcontrol —** flow control **サポート**
- **symmetric**—**フローコントロールからポーズフレームを送受信(本機では**symmetric **ポーズフレームのみがサポートされています)。(ギガビット環境のみ)**

初期設定

- 100BASE-TX：10half, 10full, 100half, 100full
- 1000BASE-T：10half, 10full, 100half, 100full, 1000full
- SFP：1000full

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

"negotiation" **コマンドを使用しオートネゴシエーションが有効になっている場合、**"capabilites" **コマンドで指定された内容に基づき最適な通信方式でリンクを行います。オートネゴシエーションが無効の場合には** "speed-duplex" **コマンドと** "flowcontrol" **コマンドを使用して手動で通信方式を設定する必要があります。**

例

本例では 5 **番ポートに** 100half, 100full **に設定しています。**

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#
```

flow control

フローコントロールを有効にします。"no" を前に置くことでフローコントロールを無効にします。

文法

flowcontrol
no flowcontrol

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- フローコントロールを使用するとスイッチのバッファ容量がいっぱいになった場合に通信のロスが発生するのを防ぐことができます。フローコントロールを有効にした場合、full-duplex では IEEE802.3x 準拠、half-duplex ではバックプレッシャを用いてフローコントロールを行います。"negotiation" コマンドを使用しオートネゴシエーションを有効にした場合、"capabilities" コマンドによりフローコントロールを使用するか決定されます。オートネゴシエーション時にフローコントロールを有効にするためには各ポートの機能 (Capabilities) に "flowcontrol" を含める必要があります。
- flowcontrol" コマンド又は "no flowcontrol" コマンドを使用してフローコントロールを固定設定する場合には、"no negotiation" コマンドを使用してオートネゴシエーションを無効にする必要があります。
- ハブ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 （P381）
capabilities (flowcontrol, symmetric)（P382）

media-type

21-26 番ポートの強制 / 優先設定を行ないます。"no" を前に置くことで初期設定に戻ります。

文法

media-type *mode*

no media-type

- *mode*
  - > copper-forced — 標準の RJ-45 ポートを使用
  - > sfp-forced — オプションの SFP ポートを使用（モジュールが搭載されていない場合も含む）
  - > sfp-preferred-auto — RJ-45 ポートのリンクが有効な場合、RJ-45 ポートを優先

初期設定

sfp-preferred-auto

コマンドモード

Interface Configuration (Ethernet)

例

本例では 5 番ポートを無効にしています。

```
Console(config)#interface ethernet 1/48
Console(config-if)#media-type copper-forced
Console(config-if)#
```

shutdown

インタフェースを無効にします。"no" を前に置くことでインタフェースを有効にします。

文法

shutdown
no shutdown

初期設定

すべてのインタフェースが有効になっています。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

コリジョンの発生などによる異常な動作を回避するなどの目的や、セキュリティの目的でポートを無効にすることができます。問題が解決した場合や、ポートを使用する場合には再度ポートを有効にすることができます。

例

本例では 5 番ポートを無効にしています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport 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 (Kbyte/ 秒) （範囲：500-262143）

初期設定

有効（全ポート）

パケットレートの上限：500 パケット / 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 500
Console(config-if)#
```

clear counters

インタフェースの統計情報をクリアします。

文法

clear counters *interface*

- *Interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号 （範囲：1-8）
    - *port* — ポート番号（範囲：1-26）
  - **port-channel** channel-id (範囲：1-32)

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 （範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id (**範囲：**1-32)
  - vlan *vlan-id* — VLAN ID (1-4093)

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:              1000T
  Mac Address:            00-17-2E-0F-E2-A5
 Configuration:
  Name:
  Port Admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full, 1000full
  Broadcast Storm:        Enabled
  Broadcast Storm Limit:  500 packets/second
  Flow Control:           Disabled
  LACP:                   Disabled
  Port Security:          Disabled
  Max MAC Count:          0
  Port Security Action:   None
  Media Type:             None
  Jumbo Frame state:      DISABLE
  Jumbo Frame size:       1522
 Current Status:
  Link Status:            Down
  Operation Speed-duplex: 1000full
  Flow Control Type:      None
Console#
```

show interfaces counters

インタフェースの統計情報を表示します。

文法

show interfaces counters [*interface*]

- *Interface*
  - **ethernet** *unit/port*
    - *unit* — **ユニット番号（範囲：**1-8）
    - *port* — **ポート番号（範囲：**1-26）
  - **port-channel** channel-id（**範囲：**1-32）

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: 0, Octets Output: 0
  Unicast Input: 0, Unicast Output: 0
  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: 0
  Broadcast Input: 0, Broadcast Output: 0
 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
  Frames Too Long: 0, Carrier Sense Errors: 0
  Symbol Errors: 0
 RMON Stats:
  Drop Events: 0, Octets: 0, Packets: 0
  Broadcast PKTS: 0, Multi-cast PKTS: 0
  Undersize PKTS: 0, Oversize PKTS: 0
  Fragments: 0, Jabbers: 0
  CRC Align Errors: 0, Collisions: 0
  Packet Size <= 64 Octets: 0, Packet Size 65 to 127 Octets: 0
  Packet Size 128 to 255 Octets: 0, 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（範囲：**1-8）
    - *port* — **ポート番号（範囲：**1-26）
  - **port-channel** channel-id (**範囲：**1-32）

初期設定

すべてのインタフェースを表示

コマンドモード

Normal Exec, Privileged Exec

例

本例は 23 **番ポートの情報を表示しています。**

```
Console#show interfaces switchport ethernet 1/23
Information of Eth 1/23
 Broadcast Threshold:           Enabled, 500 packets/second
 LACP Status:                   Disabled
 Ingress Rate Limit:            Disabled, 1000M bits per second
 Egress Rate Limit:             Disabled, 1000M bits per second
 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:
 802.1Q-tunnel Status:          Disable
 802.1Q-tunnel Mode:            NORMAL
 802.1Q-tunnel TPID:            8100(Hex)
Console#
```

コマンド解説

項目	解説
Broadcast threshold	ブロードキャストストーム制御機能の有効 / 無効の表示。有効時にはしきい値を表示（P386 参照）
Lacp status	LACP の有効 / 無効（P394 参照）
Ingress/Egress rate limit	入力 / 出力帯域制御の有効 / 無効。現在の設定（P406 参照）
VLAN membership mode	トランク又は Hybrid のメンバーモードを表示（P463 参照）
Ingress rule	イングレスフィルタの有効 / 無効の表示（P465 参照）
Acceptable frame type	VLAN フレームは、全てのフレームタイプか、タグフレームのみ受け取り可能か（P464 参照）
Native VLAN	デフォルトポート VLAN ID の表示（P466 参照）
Priority for untagged traffic	タグなしフレームへの初期設定のプライオリティの表示（P482 参照）
Gvrp status	GVRP の有効 / 無効（P455 参照）
Allowed Vlan	参加している VLAN の表示。"(u)" はタグなし、"(t)" はタグ（P467 参照）
Forbidden Vlan	GVRP によって動的に参加できない VLAN の表示（P468 参照）
802.1Q-tunnel Status	このインタフェース上で 802.1Q トンネルが使用可能か否かを表示（P471 参照）
802.1Q-tunnel Mode	トンネルモードが 802.1Q トンネルまたは 802.1Q トンネルアップリンクを表示（P472 参照）
802.1Q-tunnel TPID	学習およびスイッチパケットに使用されるタグプロトコル識別子を表示（P473 参照）

4.10 リンクアグリゲーション

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

本機では最大 32 トランクグループをサポートします。

2 つの 1000Mbps ポートをトランクした場合、full duplex 時には最大 4Gpbs のバンド幅となります。

コマンド	機能	モード	ページ
Manual Configuration Commands			
interface port-channel	interface configuration モードへの移動とトランク設定	GC	P378
channel-group	トランクへのポートの追加	IC	P393
Dynamic Configuration Command			
lacp	現在のインタフェースでの LACP の設定	IC	P394
lacp system-priority	ポート LACP システムプライオリティの設定	IC (Ethernet)	P396
lacp admin-key	ポートアドミンキーの設定	IC (Ethernet)	P397
lacp admin-key	ポートチャンネルアドミンキーの設定	IC(Port Channel)	P398
lacp port-priority	LACP ポートプライオリティの設定	IC (Ethernet)	P399
Trunk Status Display Command			
show interfaces status port-channel	トランク情報の表示	NE,PE	P388
show lacp	LACP 関連情報の表示	PE	P400

トランク設定ガイドライン

- ループを防ぐため、ネットワークケーブルを接続する前にトランクの設定を完了させて下さい。
- 各トランクは最大 8 ポートまでトランク可能です。
- トランクの両端のポートはトランクポートとして設定される必要があります。
- トランクに参加するすべてのポートは、通信速度、duplex モード、フローコントロール、VLAN、CoS などすべて同一の設定である必要があります。
- port-channel を使用し VLAN からの移動、追加、削除する場合、トランクされたすべてのポートは１つのものとして扱われます。
- STP、VLAN および IGMP の設定は、指定したポートチャンネルを使用しすべてのトランクに設定することができます。

LACP 設定ガイドライン

ポートを同一ポートチャンネルに設定するには以下の条件に一致する必要があります。

- ポートは同一の LACP システムプライオリティの必要があります

- ポートは同一のポートアドミンキーの必要があります (Ethernet Interface)
- チャンネルグループが形成される場合に、ポートチャンネルアドミンキーをセットしなければ、このキーは、グループのインタフェースのポートアドミンキーと同一の値に設定されます。
- ポートチャンネルアドミンキーを設定する場合には、ポートアドミンキーはチャンネルグループへの参加が可能な同じ値を設定する必要があります。
- リンクが落ちた場合、LACP ポートプライオリティはバックアップリンクを選択します。

channel-group

トランクにポートを追加します。"no" を前に置くことでポートをトランクからはずします。

文法

channel-group *channel-id*

no channel-group

- *channel-id* — トランク ID（範囲：1-32）

初期設定

現在のポートがそのトランクに追加されます。

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 静的トランクの設定を行う場合、対向のスイッチは Cisco EtherChannel 標準と互換性がなくてはいけません。
- " no channel-group" コマンドを使うことでポートグループをトランクからはずします。
- " no interfaces port-channel" コマンドを使うことでスイッチからトランクを削除します。

例

本例では、trunk 1 を生成し、11 番ポートをメンバーに加えています。

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

IEEE802.3ad 準拠の LACP を現在のインタフェースに対して設定します。"no" を前に置くことで本機能を無効にします。

文法

lacp
no lacp

初期設定

無効 (Disabled)

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- LACP トランクの両端は固定設定もしくはオートネゴシエーションにより full duplex に設定されている必要があります。
- LACP を使用したトランクは自動的に使用可能なポートチャンネル ID を割り当てられます。
- 対向のスイッチも接続するポートで LACP を有効にしている場合、トランクは自動的に有効になります。
- 8 つ以上のポートが同じ対向のスイッチに接続されて、LACP が有効になっている場合、追加されるポートはスタンバイモードとなり、他のアクティブなリンクが落ちた場合にのみ有効となります。

例

本例では、11 **から** 13 **番ポートの** LACP **を有効にしています。**"show interfaces status port-channel 1" **コマンドを使用し、**Trunk1 **が対向の機器と確立されていることを確認することができます。**

```
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
Port type:                 100TX
Mac address:               00-00-e8-00-00-0b
Configuration:
Name:
Port admin:                Up
Speed-duplex:              Auto
Capabilities:              10half, 10full, 100half, 100full,
Flow control status:     Disabled
Port security:             Disabled
Max MAC count:             0
Current status:
Created by:                lACP
Link status:               Up
Operation speed-duplex: 100full
Flow control type:       None
Member Ports: Eth1/11, Eth1/12, Eth1/13,
Console#
```

lacp system-priority

ポートの LACP **システムプライオリティの設定を行います。**"no" **を前に置くことで初期設定に戻します。**

文法

lacp {actor | partner} **system-priority** *priority*

no lacp {actor | partner} **system-priority**

- actor — **リンクアグリゲーションのローカル側**
- partner — **リンクアグリゲーションのリモート側**
- *priority* — **プライオリティは、リンクアグリゲーショングループ** (LAG) **メンバーシップを決定し、又** LAG **接続時に他のスイッチが本機を識別するために使用します（範囲：**0-65535）

初期設定

32768

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **同一** LAG **に参加するポートは同一システムプライオリティに設定する必要があります。**
- **システムプライオリティは本機の** MAC **アドレスと結合し** LAG ID **となります。**ID **は他のシステムとの** LACP **接続時の特定の** LAG **を表すために使用されます。**
- **リモート側のリンクが確立されると、**LACP **運用設定は使用されている状態です。パートナーの** LACP **設定は運用状態ではなく管理状態を表し、今後** LACP **がパートナーと確立される際に使用されます。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key（Ethernet Interface）

ポートの LACP **アドミニストレーションキーの設定を行います。**"no" **を前に置くことで初期設定に戻します。**

文法

lacp {actor | partner} admin-key *key*

no lacp {actor | partner} admin-key

- **actor** — **リンクアグリゲーションのローカル側**
- **partner** — **リンクアグリゲーションのリモート側**
- *key* — **ポートアドミンキーは同じ** LAG **のポートが同一の値を設定する必要があります（範囲：**0-65535）

初期設定

0

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **同じ** LAG **に参加するには、**LACP **システムプライオリティが一致し、**LACP **ポートアドミンキーが一致し、**LACP **ポートチャンネルキーが一致した場合となります。**
- **ポートチャンネルアドミンキーを設定する場合には、ポートアドミンキーはチャンネルグループへの参加が可能な同じ値を設定する必要があります。**
- **リモート側のリンクが確立されると、**LACP **運用設定は使用されている状態です。パートナーの** LACP **設定は運用状態ではなく管理状態を表し、今後** LACP **がパートナーと確立される際に使用されます。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp admin-key（Port Channel）

ポートチャンネル LACP アドミニストレーションキーの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

lacp admin-key *key*

no lacp admin-key

- *key* — ポートアドミンキーは同じ LAG のポートが同一の値を設定する必要があります（範囲：0-65535）

初期設定

0

コマンドモード

Interface Configuration (Port Channel)

コマンド解説

- 同じ LAG に参加するには、LACP システムプライオリティが一致し、LACP ポートアドミンキーが一致し、LACP ポートチャンネルアドミンキーが一致した場合となります。
- チャンネルグループが形成され、ポートチャンネルアドミンキーが設定されていない場合、ポートアドミンキーと同一の値に設定されます。LAG がポートチャンネルアドミンキーを使用しない場合には 0 にリセットされます。

例

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp port-priority

LACP ポートプライオリティの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

lacp {actor | partner} **port-priority** *priority*

no lacp {actor | partner} **port-priority**

- actor — リンクアグリゲーションのローカル側
- partner — リンクアグリゲーションのリモート側
- *priority* — バックアップリンクに使用する LACP ポートプライオリティ（範囲：0-65535）

初期設定

32768

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 低い値が高いプライオリティを示します。
- アクティブなポートがダウンした場合、高いプライオリティを持ったポートがバックアップとなります。複数のポートが同じプライオリティの場合には低いポート番号のポートがバックアップリンクとなります。
- リモート側のリンクが確立されると、LACP 運用設定は使用されている状態です。パートナーの LACP 設定は運用状態ではなく管理状態を表し、今後 LACP がパートナーと確立される際に使用されます。

例

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

show lacp

LACP 情報の表示を行います。

文法

show lacp [*port-channel*] {counters | internal | neighbors | sys-id }

- *port-channel* — **リンクアグリゲーショングループ** ID（**範囲：**1-8）
- counters — LACP **プロトコルメッセージの統計情報**
- internal — **ローカルサイドの運用状況と設定情報**
- neighbors — **リモートサイドの運用状況と設定情報**
- sys-id— **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。

4.11 ミラーポート

ミラーポート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	P404
show port monitor	ミラーポートの設定の表示	PE	P404

port monitor

ミラーセッションの設定を行います。"no" を前に置くことでミラーセッションをクリアします。

文法

port monitor *interface* [*rx* | *tx* | *both*]
no port monitor *interface*

- *interface* − ethernet *unit/port* (source port)
  - − *unit* — ユニット番号 （範囲：1-8）
  - − *port* — ポート番号（範囲：1-26）
- *rx* — 受信パケットのミラー
- *tx* — 送信パケットのミラー
- *both*— 受信 / 送信パケットのミラー

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, destination port)

コマンド解説

- ソースポートからディスティネーションポートに通信をミラーし、リアルタイムでの通信分析を行えます。ディスティネイションポートにネットワーク解析装置（Sniffer 等) 又は RMON プローブを接続し、通信に影響を与えずにソースポートのトラフィックを解析することができます。
- ディスティネーションポートは Ethernet インタフェースに設定します。
- ソース及びディスティネーションポートの通信速度は同じ必要があります。同じ通信速度でない場合には通信がソースポートから落とされます。
- 単一のミラーセッションのみを作成することができます。
- ディスティネーションポートとソースポートは同一の VLAN に所属している必要があります。

例

本例では 6 番から 11 番ポートへのミラーを行います。

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

show port monitor

ミラー情報の表示を行います。

文法

show port monitor [*interface*]

- i*nterface*
  - **ethernet** *unit/port*
    - *unit* — **ユニット番号（範囲：**1-8）
    - *port* — **ポート番号（範囲：**1-26）

初期設定

すべてのセッションを表示

コマンドモード

Privileged Exec

コマンド解説

本コマンドを使用することで現在設定されているソースポート、ディスティネーションポート、ミラーモード (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
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
Destination port(listen port):Eth1/1
Source port(monitored port) :Eth1/6
Mode :RX/TX
Console#
```

4.12 帯域制御

帯域制御機能では各インタフェースの送信及び受信の最大速度を設定することができます。帯域制御は各ポート / トランク毎に設定可能です。

帯域制御を有効にすると、通信はハードウェアにより監視され、設定を超える通信は破棄されます。設定範囲内の通信はそのまま転送されます。

コマンド	機能	モード	ページ
rate-limit	ポートの入出力の最大帯域の設定	IC	P406

rate-limit

特定のインタフェースの帯域制御レベルを設定します。帯域を設定せずに本コマンドを使用すると初期値が適用されます。"no" を前に置くことで本機能を無効とします。

文法

rate-limit < input | output > [*rate*]
no rate-limit < input | output >

- **input** — 入力帯域（レート）
- **output** — 出力帯域（レート）
- *rate* — 最大値（1-1000Mbps）

初期設定

Gigabit イーサネット：1000Mbps

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 600
Console(config-if)#
```

4.13 アドレステーブル

MAC アドレステーブルに対するアドレスフィルタリング、現在エントリーされているアドレスの表示、テーブルのクリア、エージングタイムの設定を行います。

コマンド	機能	モード	ページ
mac-address-table static	VLAN ポートへの MAC アドレスの静的なマッピング	GC	P407
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	P408
show mac-address-table	転送データベースに登録された情報の表示	PE	P409
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	P410
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	P410

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 （範囲：1-8）
    - *port* — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)
- vlan *vlan-id* — VLAN ID (1-4093)
- *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 （範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
- port-channel *channel-id***（範囲：**1-8**）**
- *vlan-id* — VLAN ID (1-4093)
- **sort — アドレス、**VLAN**、インタフェースによる並び替え**

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show mac-address-table
  Interface MAC Address VLAN Type
  --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de 1 Delete-on-reset
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 (10-1000000 の値。0 に設定した場合はエージングを無効にします)

初期設定

300（秒）

コマンドモード

Global Configuration

コマンド解説

エージングタイムは動的転送情報を本機に保持する時間を表します。

例

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

アドレステーブルのエージングタイムを表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

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

4.14 LLDP コマンド

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

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

コマンド	機能	モード	ページ
lldp	スイッチで LLDP を有効	GC	P412
lldp holdtime-multiplier	TTL(time-to-live) 値の設定	GC	P413
lldp notification-interval	LLDP の変更に関する SNMP 通知送信の間隔を設定	GC	P414
lldp refresh-interval	LLDP 配信の転送間隔を設定	GC	P414
lldp reinit-delay	LLDP ポートが無効またはリンクダウン時の再初期化までの待ち時間を設定	GC	P415
lldp tx-delay	ローカル LLDP MIB の変数に変化が起こった後に、アドバタイズメントを送信するまでの時間を設定します	GC	P415
lldp admin-status	LLDP メッセージの送信・受信のモードを有効	IC	P416
lldp admin-status	LLDP メッセージの送信・受信のモードを有効	IC	P416
lldp notification	LLDP 変更の SNMP トラップ通知送信を有効	IC	P417
lldp basic-tlv port-description	TLV Type “port-description“ を設定	IC	P418
lldp basic-tlv system-capabilities	TLV Type “system-capabilities“ を設定	IC	P418
lldp basic-tlv system-description	TLV Type “system-description“ を設定	IC	P419
lldp basic-tlv system-name	TLV Type “system-name“ を設定	IC	P420
lldp dot1-tlv proto-ident*	lldp dot1-TLV“ proto-ident“ を設定	IC	P420
lldp dot1-tlv proto-vid*	lldp dot1-TLV“ proto-vid“ を設定	IC	P421
lldp dot1-tlv pvid*	lldp dot1-TLV“pvid“ を設定	IC	P421
lldp dot1-tlv vlan-name*	lldp dot1-TLV“vlan-name“ を設定	IC	P422
lldp dot3-tlv link-agg	lldp dot3-TLV“link-agg“ を設定	IC	P422
lldp dot3-tlv mac-phy	lldp dot3-TLV“mac-phy“ を設定	IC	P423

lldp dot3-tlv max-frame	lldp dot3-TLV“max-frame“ を設定	IC	P423
lldp dot3-tlv poe	dot3-tlv “poe” を設定	IC	P424
show lldp config	LLDP 設定の表示	PE	P425
show lldp info local-device	LLDP ローカルデバイス情報を表示	PE	P426
show lldp info remote-device	LLDP リモートデバイス情報を表示	PE	P427
show lldp info statistics	LLDP 統計情報を表示	PE	P428

lldp

スイッチで LLDP を有効にします。"no" を前に置くことで機能を無効にします。

文法

lldp

no lldp

初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#lldp
Console(config)#
```

lldp holdtime-multiplier

LLDP のアドバタイズメントで送信された Time-To-Live（TTL）値を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

- *value* - TTL 値を設定します。TTL は秒で表され、下の数式で計算します。
  Transmission Interval × Hold Time Multiplier ≦ 65536
  （範囲：2-10）

初期設定

Holdtime multiplier：4

TTL：4×30 = 120 秒

コマンドモード

Global Configuration

コマンド解説

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

例

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

lldp notification-interval

LLDP MIB の変更を行い、SNMP 通知が送信されるまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp notification-interval *seconds*

no lldp notification-interval

- *seconds* - SNMP 通知が送られる周期的な間隔を指定します
  （範囲：5 ～ 3600 秒　初期設定 5 秒）

初期設定

5 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp notification-interval 30
Console(config)#
```

lldp refresh-interval

LLDP アドバタイズが送信されるまでの間隔を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp refresh-interval *seconds*

no lldp refresh-delay

- *seconds* - LLDP アドバタイズが送信されるまでの間隔を指定します
  （範囲：5 ～ 32768 秒）

初期設定

30 秒

コマンドモード

Global Configuration

コマンド解説

refresh-interval× Hold Time Multiplier ≦ 65536

例

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

lldp reinit-delay

LLDP ポートが無効になるかリンクダウンした後、再初期化を試みるまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp reinit-delay *seconds*

no lldp reinit-delay

- *seconds* - 再初期化を試みるまでの時間を指定します（範囲：1-10 秒）

初期設定

2 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay

ローカル LLDP MIB の変数に変化が起こった後に引き続き、アドバタイズメントを送信するまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp tx-delay *seconds*

no lldp tx-delay

- *seconds* - アドバタイズメントを送信するまでの時間を設定を指定します（範囲：1-8192 秒）

初期設定

2 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status

個別のインターフェースに対し、メッセージの内容を指定するために LLDP **ポート・トランクの設定を行います。**"no" **を前に置くことでこの機能を無効にします。**

文法

lldp admin-status < rx-only | tx-only | tx-rx >

no lldp admin-status

- rx-only - LLDP PDUs. **受信のみ**
- tx-only - LLDP PDUs. **送信のみ**
- tx-rx - LLDP PDUs. **送受信**

初期設定

tx-rx

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp notification

LLDP 変更について SNMP トラップ通知の送信を可能にします。"no" を前に置くことでこの機能を無効にします。

文法

lldp notification
no lldp notification

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

lldp basic-tlv management-ip-address

LLDP 有効ポートで "management-ip-address" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv management-ip-address

no lldp basic-tlv management-ip-address

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- management-ip-address には、スイッチの IPv4 アドレスが含まれます。スイッチに管理用のアドレスがない場合、アドレスはスイッチの CPU の MAC アドレスが、このアドバタイズメントを送信するポートの MAC アドレスになります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description

LLDP 有効ポートで "port-description" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv port-description
no lldp basic-tlv port-description

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- port-description には、RFC2863 の ifDescr オブジェクトで規定されています。これには製造者、スイッチの製品名、インターフェースのハードウェアとソフトウェアのバージョンが含まれます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

lldp basic-tlv system-capabilities

LLDP 有効ポートで "system-capabilities" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv system-capabilities
no lldp basic-tlv system-capabilities

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- system-capabilities には、システムの主な機能が含まれます。この情報には機能自体が有効かどうかは関係ありません。この TLV によってアドバタイズされる情報は IEEE802.1AB 規格に記述されています。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description

LLDP 有効ポートで "system-description" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv system-description

no lldp basic-tlv system-description

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

system-description は RFC3418 の sysDescr オブジェクトで規定されています。システムのハードウェア、オペレーティングソフト、ネットワーキングソフトのフルネームとバージョンが含まれています。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name

LLDP 有効ポートで "system-name" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv system-name
no lldp basic-tlv system-name

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- System-name は RFC3418 の sysName オブジェクトで規定されています。システムの管理用に割り当てられた名前が含まれます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dot1-tlv proto-ident

LLDP 有効ポートで "proto-ident" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv proto-ident
no lldp dot1-tlv proto-ident

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

lldp dot1-tlv proto-vid

LLDP 有効ポートで "proto-vid" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv proto-vid
no lldp dot1-tlv proto-vid

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ポートベースおよびプロトコルベース VLAN 情報をアドバタイズします。
  詳細については P462 「VLAN インタフェースの設定」および P477 「プロトコル VLAN の設定」を参照してください。

例

```
Console(config)#inter ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

lldp dot1-tlv pvid

LLDP 有効ポートで "pvid" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv pvid
no lldp dot1-tlv pvid

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- PVID 情報をアドバタイズします。
  詳細については P466 「switchport native vlan」を参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

lldp dot1-tlv vlan-name

LLDP 有効ポートで "vlan-name" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv vlan-name
no lldp dot1-tlv vlan-name

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 指定したインタフェースが割り当てられた、全ての VLAN 名をアドバタイズします。VLAN については P467 「switchport allowed vlan」および P478 「protocol-vlan protocol-group (Configuring Groups)」を参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg

LLDP 有効ポートで "link-agg" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot3-tlv link-agg
no lldp dot3-tlv link-agg

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- リンクアグリゲーションステータスをアドバタイズします。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy

LLDP 有効ポートで "mac-phy" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot3-tlv mac-phy
no lldp dot3-tlv mac-phy

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- MAC/PHY 設定およびステータスをアドバタイズします。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv max-frame

LLDP 有効ポートで "max-frame" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot3-tlv max-frame
no lldp dot3-tlv max-frame

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 最大フレームサイズ情報をアドバタイズします。フレームサイズについての詳細は P261 「フレームサイズコマンド」を参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp dot3-tlv poe

LLDP 有効ポートで "PoE”（Power-over-Ethernet）のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot3-tlv poe
no lldp dot3-tlv poe

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- This option advertises Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class.

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv poe
Console(config-if)
```

show lldp config

全てのポートの LLDP **設定を表示します。**

文法

show lldp config [detail *interface*]

- *detail* — **設定サマリを表示**
- *interface*
  - ethernet *unit/port*
    - *unit* — **ユニット番号（範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
  - port-channel *channel-id*（**範囲：**1-32**）**

コマンドモード

Privileged Exec

例

```
Console#show lldp config

LLDP Global Configuration

 LLDP Enabled                  : Yes
 LLDP Transmit interval        : 30 sec.
 LLDP Hold Time Multiplier     : 4
 LLDP Delay Interval           : 2 sec.
 LLDP Re-initialization Delay : 2 sec.
 LLDP Notification Interval    : 5 sec.


LLDP Port Configuration
 Port     Admin Status Notification Enabled
 -------- ------------ --------------------
 Eth 1/1  Tx-Rx        False
 Eth 1/2  Tx-Rx        False
 Eth 1/3  Tx-Rx        False
 Eth 1/4  Tx-Rx        False
 Eth 1/5  Tx-Rx        False
 Eth 1/6  Tx-Rx        False
 Eth 1/7  Tx-Rx        False
 Eth 1/8  Tx-Rx        False
 Eth 1/9  Tx-Rx        False
 Eth 1/10 Tx-Rx        False
Console#
```

show lldp info local-device

スイッチについての情報を表示します。

文法

show lldp info local-device [detail interface]

- *detail* — **詳細情報を表示**
- *interface*
  - ethernet *unit/port*
    - *unit* — **ユニット番号（範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
  - port-channel *channel-id*（**範囲：**1-32**）**

コマンドモード

Privileged Exec

例

```
Console#show lldp info local-device

 LLDP Local System Information
  Chassis Type                : MAC Address
  Chassis ID                  : 00-12-CF-F3-DE-46
  System Name                 :
  System Description          : FXC3110
  System Capabilities Support : Bridge, Router
  System Capabilities Enabled : Bridge, Router

 LLDP Port Information
  Port    PortID Type      PortID            Port Description
 -------- ---------------- ----------------- --------------------------------
-
 Eth 1/1  MAC Address      00-12-CF-F3-DE-47 Ethernet Port on unit 1, port 1
 Eth 1/2  MAC Address      00-12-CF-F3-DE-48 Ethernet Port on unit 1, port 2
 Eth 1/3  MAC Address      00-12-CF-F3-DE-49 Ethernet Port on unit 1, port 3
 Eth 1/4  MAC Address      00-12-CF-F3-DE-4A Ethernet Port on unit 1, port 4
 Eth 1/5  MAC Address      00-12-CF-F3-DE-4B Ethernet Port on unit 1, port 5
 Eth 1/6  MAC Address      00-12-CF-F3-DE-4C Ethernet Port on unit 1, port 6
 Eth 1/7  MAC Address      00-12-CF-F3-DE-4D Ethernet Port on unit 1, port 7
 Eth 1/8  MAC Address      00-12-CF-F3-DE-4E Ethernet Port on unit 1, port 8
 Eth 1/9  MAC Address      00-12-CF-F3-DE-4F Ethernet Port on unit 1, port 9
 Eth 1/10 MAC Address     00-12-CF-F3-DE-50 Ethernet Port on unit 1, port 10
Console#
```

show lldp info remote-device

ローカルスイッチの指定されたポートに接続された、LLDP が有効のデバイスについての詳細情報を表示します。

文法

show lldp info remote-device [detail interface]

- *detail* — **詳細情報を表示**
- *interface*
  - ethernet *unit/port*
    - *unit* — **ユニット番号（範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
  - port-channel *channel-id*（**範囲：**1-32**）**

コマンドモード

Privileged Exec

例

```
Console#show lldp info remote-device
LLDP Remote Devices Information
Interface | ChassisId PortId SysName
--------- + ----------------- ----------------- -----------------
----
Eth 1/1 | 00-01-02-03-04-05 00-01-02-03-04-06
Console#show lldp info remote-device detail ethernet 1/1
LLDP Remote Devices Information Detail
---------------------------------------------------------------
Local PortName : Eth 1/1
Chassis Type : MAC Address
Chassis Id : 00-01-02-03-04-05
PortID Type : MAC Address
PortID : 00-01-02-03-04-06
SysName :
SysDescr : 24PORT GIGABIT L2 INTELLIGENT SWITCH
PortDescr : Ethernet Port on unit 1, port 1
SystemCapSupported : Bridge
SystemCapEnabled : Bridge
Remote Management Address :
00-01-02-03-04-05 (MAC Address)
Console#
```

show lldp info statistics

このスイッチに接続されている LLDP **が有効なすべてのデバイスの統計を表示します。**

文法

show lldp info statistics [detail interface]

- *detail* — **詳細情報を表示**
- *interface*
  - ethernet *unit/port*
    - *unit* — **ユニット番号（範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
  - port-channel *channel-id*（**範囲：**1-32**）**

コマンドモード

Privileged Exec

例

```
Console#show lldp info statistics

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 0 seconds
  New Neighbor Entries Count         : 0
  Neighbor Entries Deleted Count     : 0
  Neighbor Entries Dropped Count     : 0
  Neighbor Entries Ageout Count      : 0

  Port     NumFramesRecvd NumFramesSent NumFramesDiscarded
  -------- -------------- ------------- ------------------
  Eth 1/1               0             0                  0
  Eth 1/2               0             0                  0
  Eth 1/3               0             0                  0
  Eth 1/4               0             0                  0
  Eth 1/5               0             0                  0
  Eth 1/6               0             0                  0
  Eth 1/7               0             0                  0
  Eth 1/8               0             0                  0
  Eth 1/9               0             0                  0
  Eth 1/10              0             0                  0
Console#
```

4.15 スパニングツリー

本機へのスパニングツリーアルゴリズム (Spanning Tree Algorithm/STA) **の設定と、選択したインタフェースへの** STA **の設定を行うコマンドです。**

コマンド	機能	モード	ページ
spanning-tree	**スパニングツリープロトコルの有効化**	GC	P430
spanning-tree mode	STP/RSTP/MSTP **モードの選択**	GC	P431
spanning-tree forward-time	**スパニングツリーブリッジ転送時間の設定**	GC	P432
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	P433
spanning-tree max-age	**スパニングツリーブリッジ最長時間の設定**	GC	P434
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	P435
spanning-tree path-cost method	RSTP/MSTP **のパスコスト方法の設定**	GC	P436
spanning-tree transmission-limit	RSTP/MSTP **の送信リミットの設定**	GC	P437
spanning-tree-mst-configuration	MSTP **設定モードの変更**	GC	P437
mst vlan	**スパニングツリーインスタンスへの** VLAN **の追加**	MST	P438
mst priority	**スパニングツリーインスタンスのプライオリティの設定**	MST	P439
name	MST **名の設定**	MST	P440
revision	MST **リビジョンナンバーの設定**	MST	P441
max-hops	BPDU **が破棄される前最大ホップ数の設定**	MST	P442
spanning-tree spanning-disabled	**インタフェースのスパニングツリーの無効化**	IC	P442
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	P443
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	P444
spanning-tree edge-port	**エッジポートへのポートファストの有効化**	IC	P445
spanning-tree portfast	**インタフェースのポートファストの設定**	IC	P446
spanning-tree link-type	RSTP/MSTP **のリンクタイプを設定**	IC	P447
spanning-tree mst cost	MST **インスタンスのパスコストの設定**	IC	P448
spanning-tree mst port-priority	MST **インスタンスプライオリティの設定**	IC	P449
spanning-tree protocol-migration	**適切な** BPDU **フォーマットの再確認**	PE	P450
show spanning-tree	**スパニングツリーの設定を表示**	PE	P451
show spanning-tree mst configuration	MST **設定の表示**	PE	P453

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

[no] spanning-tree

初期設定

STA 有効

コマンドモード

Global Configuration

コマンド解説

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

例

本例では STA を有効にしています。

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

spanning-tree mode

STP のモードを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree mode { stp | rstp | mstp }

no spanning-tree mode

- stp — Spanning Tree Protocol（IEEE 802.1D 準拠）
- rstp — Rapid Spanning Tree Protocol（IEEE 802.1w 準拠）
- mstp— mstp - Multiple Spanning Tree（IEEE 802.1s 準拠）

初期設定

rstp

コマンドモード

Global Configuration

コマンド解説

- Spanning Tree Protocol(STP)
  スイッチ内部では RSTP を用いますが、外部へは IEEE802.1D 準拠の BPDU の送信のみを行います。
- Rapid Spanning Tree Protocol(RSTP)
  RSTP は以下の入ってくるメッセージの種類を判断し STP 及び RSTP のいずれにも自動的に対応することができます。
  - STP Mode — ポートの移行遅延タイマーが切れた後にIEEE802.1D BPDUを受け取ると、本機は IEEE802.1D ブリッジと接続していると判断し、IEEE802.1D BPDU のみを使用します。
  - RSTP Mode — IEEE802.1D BPDU を使用し、ポートの移行遅延タイマーが切れた後に RSTP BPDU を受け取ると、RSTP は移行遅延タイマーを再スタートさせ、そのポートに対し RSTP BPDU を使用します。
- Multiple Spanning Tree Protocol(MSTP)
  - ネットワーク上で MSTP を有効にするには、接続された関連するブリッジにおいても同様の MSTP の設定を行ない、スパニングツリーインスタンスに参加することを許可する必要があります。
  - スパニングツリーインスタンスは、互換性を持つ VLAN インスタンスを持つブリッジにのみ設定可能です。
  - スパニングツリーモードを変更する場合、変更前のモードのスパニングツリーインスタンスをすべて止め、その後新しいモードにおいて通信を再開します。スパニングツリーのモード変更時には通信が一時的に遮断されるので注意して下さい。

例

本例では RSTP を使用する設定をしています。

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

spanning-tree forward-time

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

文法

spanning-tree forward-time *seconds*

no spanning-tree forward-time

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

初期設定

15**（秒）**

コマンドモード

Global Configuration

コマンド解説

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

例

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

spanning-tree hello-time

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

文法

spanning-tree hello-time *time*

no spanning-tree hello-time

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

初期設定

2**（秒）**

コマンドモード

Global Configuration

コマンド解説

設定情報の送信を行う間隔を設定するためのコマンドです。

例

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

spanning-tree max-age

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

文法

spanning-tree max-age *seconds*
no spanning-tree max-age

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

初期設定

20**（秒）**

コマンドモード

Global Configuration

コマンド解説

設定変更を行う前に設定情報を受け取るまでの最大待ち時間（秒）。

指定ポートを除くすべてのポートが設定情報を一定の間隔で受け取ります。タイムアウトした STP **ポートは付属する** LAN **のための指定ポートになります。そのポートがルートポートの場合、ネットワークに接続された他のポートがルートポートとして選択されます。**

例

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

spanning-tree priority

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

文法

spanning-tree priority *priority*
no spanning-tree priority

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

初期設定

32768

コマンドモード

Global Configuration

コマンド解説

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

例

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

spanning-tree pathcost method

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

文法

spanning-tree pathcost method { long | short }
no spanning-tree pathcost method

- long — 1-200,000,000 までの 32 ビットの値
- short — 1-65535 までの 16 ビットの値

初期設定

long

コマンドモード

Global Configuration

コマンド解説

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

例

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

spanning-tree transmission-limit

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

文法

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

- *count* — 転送リミットの秒数（範囲：1-10 秒）

初期設定

3

コマンドモード

Global Configuration

コマンド解説

本コマンドでは BPDU の最大転送レートを制限します。

例

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

spanning-tree mst-configuration

MST 設定モードに移行します。

初期設定

- MST インスタンスに VLAN がマッピングされていません
- リジョン名は本機の MAC アドレスです

コマンドモード

Global Configuration

例

```
Console(config)#spanning-tree mst-configuration
Console(config-mstp)#
```

関連するコマンド

mst vlan（P438）
mst priority（P439）
name（P440）
revision（P441）
max-hops（P442）

mst vlan

スパニングツリーインスタンスに VLAN を追加します。"no" を前に置くことで特定の VLAN を削除します。VLAN を指定しない場合にはすべての VLAN を削除します。

文法

mst *instance_id* **vlan** *vlan-range*
no mst *instance_id* **vlan** *vlan-range*

- *instance_id* — MST インスタンス ID（範囲：0-4094）
- *vlan-range* — VLAN 範囲（範囲：1-4093）

初期設定

なし

コマンドモード

MST Configuration

コマンド解説

- 本コマンドによりスパニングツリーに VLAN をグループ化します。MSTP は各インスタンスに対し特定のスパニングツリーを生成します。これによりネットワーク上に複数のパスを構築し、通信のロードバランスを行い、単一のインスタンスに不具合が発生した場合に大規模なネットワークの障害が発生することを回避すると共に、不具合の発生したインスタンスの新しいトポロジーへの変更を迅速に行ないます。
- 初期設定では、MST リジョン内のすべてのブリッジと LAN に接続されたすべての VLAN が内部スパニングツリー (MSTI 0) に割り当てられています。本機では最大 58 のインスタンスをサポートしています。但し、同一インスタンスのセットにより同一 MSTI 内のすべてのブリッジ、及び同一 VLAN のセットにより同一インスタンスを形成する必要があります。RSTP は単一ノードとして各 MSTI を扱い、すべての MSTI を Common Spanning Tree として接続する点に注意して下さい。

[注意] MST の設定を行う際には、事前に spanning-tree mode を mstp に選択してください。（P431 「spanning-tree mode」を参照）

例

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

mst priority

スパニングツリーインスタンスのプライオリティを設定します。"no" **を前に置くことで初期設定に戻します。**

文法

mst *instance_id* **priority** *priority*

no mst *instance_id* **priority**

- *instance_id* — MST **インスタンス** ID**（範囲：**0-4094**）**
- *priority* — MST **インスタンスのプライオリティ**
  (0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

初期設定

32768

コマンドモード

MST Configuration

コマンド解説

- MST **プライオリティはルートデバイス、特定のインスタンスの代理ブリッジの決定に使用されます。一番高いプライオリティを持ったデバイスが** MSTI **ルートデバイスとなります。すべてのデバイスが同じプライオリティの場合、**MAC **アドレスが一番小さいデバイスがルートデバイスとなります。**
- **プライオリティを** 0 **に設定することにより本機を** MSTI **のルートデバイスに、**16384 **に設定することにより代理デバイスに設定できます。**

例

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

name

本機の設置されている MST リジョン名の設定を行ないます。"no" を前に置くことで名前を削除します。

文法

name *name*

- *name* — スパニングツリー名 (32 文字以内)

初期設定

本機の MAC アドレス

コマンドモード

MST Configuration

コマンド解説

MST リジョン名とリビジョンナンバーは唯一の MST リジョンを指定するために使用されます。(本機のようなスパニングツリー対応機器である) ブリッジは 1 つの MST リジョンにのみ属すことができます。同じリジョン内のすべてのブリッジはすべて同じ MST インスタンスの設定をする必要があります。

例

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

関連するコマンド

revision (P441)

revision

本機の MST **設定のリビジョンナンバーの設定を行ないます。**"no" **を前に置くことで初期設定に戻ります。**

文法

revision *number*

- *number* — **スパニングツリーのリビジョンナンバー（範囲：**0-65535**）**

初期設定

0

コマンドモード

MST Configuration

コマンド解説

MST **リジョン名とリビジョンナンバーは唯一の** MST **リジョンを指定するために使用されます。（本機のようなスパニングツリー対応機器である）ブリッジは** 1 **つの** MST **リジョンにのみ属すことができます。同じリジョン内のすべてのブリッジはすべて同じ** MST **インスタンスの設定をする必要があります。**

例

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

関連するコマンド

name（P440）

max-hops

BPDU が破棄される前の MST 内での最大ホップ数を設定します。"no" を前に置くことで初期設定に戻ります。

文法

max-hops *hop-number*

- *hop-number* — MST の最大ホップ数（設定範囲：1-40）

初期設定

20

コマンドモード

MST Configuration

コマンド解説

MSTI リジョンは STP と RSTP プロトコルでは単一のノードとして扱われます。従って MSTI リジョン内の BPDU のメッセージエイジは変更されません。しかし、リジョン内の各スパニングツリーインスタンス及びインスタンスを接続する内部スパニングツリー (IST) は、BPDU を広げるためブリッジの最大数を指定するために hop カウントを使用します。各ブリッジは BPDU を渡す前に hop カウントを 1 つ減らします。hop カウントが 0 になった場合にはメッセージは破棄されます。

例

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

spanning-tree spanning-disabled

特定のポートの STA を無効にします。"no" を前に置くことで再び STA を有効にします。

文法

[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。

- Gigabit Ethernet：2,000-200,000
- 10G Ethernet：200-20,000

初期設定

- Gigabit Ethernet ：10,000
- 10G Ethernet：1,000

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

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

例

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

spanning-tree port-priority

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

文法

spanning-tree port-priority *priority*
no spanning-tree port-priority

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

初期設定

128

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

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

例

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

関連するコマンド

spanning-tree cost (P443)

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

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

関連するコマンド

spanning-tree portfast（P446）

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

[no] spanning-tree portfast

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **本コマンドは選択したポートに対しファストスパニングツリーモードの設定を行います。このモードでは、ポートは学習ステートをパスして、フォワーディングを行います。**
- **エンドノードではループを発生しないため、スパニングツリーステートの変更を通常よりも早く行うことができます。ファストフォワーディングは、エンドノードのサーバ、ワークステーションに対し** STP **によるタイムアウトを軽減します（ファストフォワーディングは** LAN **のエンドノードのデバイス又は** LAN **のエンドのブリッジに接続されたポートにのみ有効にして下さい）**
- **本コマンドは** "spanning-tree 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（P445）

spanning-tree link-type

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

文法

spanning-tree link-type {auto | point-to-point | shared}

no spanning-tree link-type

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

初期設定

auto

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

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

例

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

spanning-tree mst cost

MST のインスタンスのパスコストの設定を行ないます。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree mst *instance_id* **cost** *cost*

no spanning-tree mst *instance_id* **cost**

- *instance_id* — MST インスタンス ID（範囲：0-4094）
- *cost* — インタフェースへのパスコストの値（ショートパスコスト：1-65535　ロングパスコスト：1-200,000,000　0 は自動設定 ）
  推奨する値は P443 を参照してください。

初期設定

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021D-2004 standard exceeds 65,535, the default is set to 65,535. The default path costs are listed in Table 33-3 on page 33-12.

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 各スパニングツリーインスタンスは VLAN ID に関連付けられます。
- 本コマンドはデバイス間の MSTA のパスを最適に決定するためのコマンドです。従って、速度の速いポートに対し小さい値を設定し、速度の遅いポートに対し大きな値を設定します。
- パスコストはインタフェースプライオリティより優先されます。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

関連するコマンド

spanning-tree mst port-priority （P449）

spanning-tree mst port-priority

MST インスタンスのインタフェースプライオリティの設定を行ないます。"no" を前に置くことで初期設定に戻ります。

文法

spanning-tree mst *instance_id* **port-priority** *priority*

no spanning-tree mst *instance_id port-priority*

- *instance_id* — MST インスタンス ID（範囲：0-4094）
- *priority* — ポートの優先順位（16 間隔で 0-240 の値）

初期設定

128

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

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

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

関連するコマンド

spanning-tree mst cost（**P448**）

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（範囲：**1-8）
    - *port* — **ポート番号（範囲：**1-26）
  - **port-channel** *channel-id*（**範囲：**1-32）

コマンドモード

Privileged Exec

コマンド解説

本機が設定、トポロジーチェンジ BPDU **を含む** STP BPDU **を検知した場合、該当するポートは自動的に** STP **互換モードにセットされます。**"spanning-tree protocol-migration" **コマンドを使用し、手動で選択したポートに対して最適な** BPDU **フォーマット（**RSTP **又は** STP **互換）の再確認を行うことができます。**

例

```
Console#spanning-tree protocol-migration ethernet 1/5
Console#
```

show spanning-tree

STP の設定内容を表示します。

文法

show spanning-tree

show spanning-tree ethernet *unit / port*

show spanning-tree port-channel *channel-id*

show spanning-tree mst *instance-id*

- **ethernet** *unit/port*
  - *unit* — ユニット番号（範囲：1-8）
  - *port* — ポート番号（範囲：1-26）
- **port-channel** *channel-id*（範囲：1-32）

- **mst** *instance-id* （範囲：0-4094）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- パラメータを使わず "show spanning-tree" コマンドを使用した場合、ツリー内の各インタフェースのための本機のスパニングツリー設定が表示されます。
- "show spanning-tree interface" コマンドを使用した場合、指定したインタフェースのスパニングツリー設定のみ表示されます。

例

```
Console#show spanning-tree
Spanning-tree information
----------------------------------------------------------------
Spanning tree mode:                MSTP
Spanning tree enable/disable:      enable
Instance:                          0
Vlans configuration:               1-4093
Priority:                          32768
Bridge Hello Time (sec.):          2
Bridge Max Age (sec.):             20
Bridge Forward Delay (sec.):       15
Root Hello Time (sec.):            2
Root Max Age (sec.):               20
Root Forward Delay (sec.):         15
Max hops:                          20
Remaining hops:                    20
Designated Root:                   32768.0.0000ABCD0000
Current root port:                 1
Current root cost:                 10000
Number of topology changes:        1
Last topology changes time (sec.): 22
Transmission limit:                3
Path Cost Method:                  long
----------------------------------------------------------------
Eth 1/ 1 information
----------------------------------------------------------------
Admin status:                      enable
Role:                              root
State:                             forwarding
External admin path cost:          10000
Internal admin cost:               10000
External oper path cost:           10000
Internal oper path cost:           10000
Priority:                          128
Designated cost:                   200000
Designated port:                   128.24
Designated root:                   32768.0.0000ABCD0000
Designated bridge:                 32768.0.0030F1552000
Fast forwarding:                   disable
Forward transitions:               1
Admin edge port:                   enable
Oper edge port:                    disable
Admin Link type:                   auto
Oper Link type:                    point-to-point
Spanning Tree Status:              enable ...
```

show spanning-tree mst configuration

MST の設定を表示します。

文法

show spanning-tree mst configuration

コマンドモード

Privileged Exec

例

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
-------------------------------------------------------------
Configuration name:XSTP REGION 0
Revision level:0

Instance Vlans
-------------------------------------------------------------
   1      2
Console#
```

4.16 VLAN

VLAN はネットワーク上のどこにでも位置することができますが、あたかもそれらが物理的な同一セグメントに属するかのように動作し、通信を行うポートのグループです。

ここでは VLAN 関連コマンドを使用し、指定するポートの VLAN グループの生成、メンバーポートの追加、VLAN タグ使用法の設定、自動 VLAN 登録の有効化を行います。

コマンドグループ	機能	ページ
GVRP and Bridge Extension	GVRP の設定	P454
Editing VLAN Groups	VLAN 名、VID、状態を含む VLAN の設定	P460
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	P462
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	P469
802.1Q Tunneling	802.1Q トンネリング（QinQ）の設定	P470
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	P475
Configuring Protocol VLANs	フレームタイプおよびプロトコルを基にした Protocol-based VLAN の設定	P477

4.16.1 GVRP の設定

GARP VLAN Registration Protocol(GVRP) はスイッチが自動的にネットワークを介してインタフェースを VLAN メンバーとして登録するために VLAN 情報を交換する方法を定義します。各インタフェース又は本機全体への GVRP の有効化の方法と、Bridge Extension MIB の設定の表示方法を説明しています。

コマンド	機能	モード	ページ
bridge-ext gvrp	本機全体に対し GVRP を有効化	GC	P455
show bridge-ext	bridge extension 情報の表示	PE	P456
switchport gvrp	インタフェースへの GVRP の有効化	IC	P456
switchport forbidden vlan	インタフェースへの登録禁止 VLAN の設定	IC	P468
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	P457
garp timer	選択した機能への GARP タイマーの設定	IC	P458
show garp timer	選択した機能への GARP タイマーの表示	NE,PE	P459

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

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

例

```
Console#show bridge-ext
Max support vlan numbers:                256
Max support vlan ID:                      4094
Extended multicast filtering services: No
Static entry individual port:           Yes
VLAN learning:                             IVL
Configurable PVID tagging:               Yes
Local VLAN capable:                       No
Traffic classes:                           Enabled
Global GVRP status:                        Enabled
GMRP:                                        Disabled
Console#
```

switchport gvrp

ポートの GVRP を有効に設定します。"no" を前に置くことで機能を無効にします。

文法

[no] switchport gvrp

初期設定

無効

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 （範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
  - port-channel *channel-id*（**範囲：**1-32）

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 (P459)

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 （範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
  - port-channel *channel-id*（**範囲：**1-32**）**

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 (P458)

4.16.2 VLAN グループの設定

コマンド	機能	モード	ページ
vlan database	VLAN database モードに入り、VLAN の設定を行う	GC	P460
VLAN	VID,VLAN 名、ステートなど VLAN の設定	VC	P461

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 (P469)

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：1-4093）
- **name** — 識別するための VLAN 名
- *vlan-name* — 1-32 文字
- **media ethernet** — イーサネットメディアの種類
- **state** — VLAN のステートの識別
  - ー **active** — VLAN の実行
  - ー **suspend** — VLAN の中断。中断中の VLAN はパケットの転送を行いません。

初期設定

初期設定では VLAN 1 が存在し、active 状態です。

コマンドモード

VLAN Database Configuration

コマンド解説

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

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 (P469)

4.16.3 VLAN インタフェースの設定

コマンド	機能	モード	ページ
interface vlan	VLAN を設定するための Interface 設定モードへの参加	IC	P462
switchport mode	インタフェースの VLAN メンバーモードの設定	IC	P463
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	P464
switchport ingress-filtering	インタフェースへの入力フィルタの有効化	IC	P465
switchport native vlan	インタフェースの PVID(native VLAN) の設定	IC	P466
switchport allowed vlan	インタフェースに関連した VLAN の設定	IC	P467
switchport gvrp	インタフェースへの GVRP の有効化	IC	P456
switchport forbidden vlan	インタフェースの登録を禁止する VLAN の設定	IC	P468
switchport priority default	タグなし受信フレームのポートプライオリティの設定	IC	P484

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：1-4093）

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 (P469)

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 { hybrid | trunk }
no switchport mode

- hybrid — ハイブリッド VLAN インタフェースを指定。ポートはタグ付及びタグなしフレームを送信します。
- trunk — VLAN トランクに使用されるポートを指定します。トランクは 2 つのスイッチ間の直接接続で、ポートはソース VLAN を示すタグ付フレームを送信します。デフォルト VLAN に所属するフレームもタグ付フレームを送信します。

初期設定

すべてのポートは hybrid に指定され、VLAN 1 が PVID に設定されています。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

本例では、1 番ポートの configuration モードの設定を行い、switchport モードを hybrid に指定しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

switchport acceptable-frame-types

ポートの受け入れ可能なフレームの種類を指定します。"no" **を前に置くことで初期設定に戻します。**

文法

switchport acceptable-frame-types {all | tagged}

no switchport acceptable-frame-types

- all — **タグ付、タグなしのすべてのフレームを受け入れます。**
- tagged — **タグ付フレームのみを受け入れます。**

初期設定

すべてのフレームタイプ

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

すべてのフレームを許可する設定にした場合、タグなし受信フレームはデフォルト VLAN **に指定されます。**

例

本例では 1 **番ポートにタグ付フレームのみを許可する設定にしています。**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

関連するコマンド

switchport mode（P463）

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

[no] switch port ingress-filtering

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- イングレスフィルタリングはタグ付フレームにのみ有効です。
- イングレスフィルタリングが有効の場合、メンバーでない VLAN へのタグがついたフレームを受信すると、そのフレームは捨てられます。
- イングレスフィルタリングは GVRP や STP などの VLAN と関連のない BPDU フレームには影響を与えません。但し、VLAN に関連した GMRP などの BPDU フレームには影響を与えます。

例

本例では、1 番ポートを指定し、イングレスフィルタリングを有効にしています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

ポートへのデフォルト VLAN ID である PVID の設定を行います。"no" を前に置くことで初期設定に戻します。

文法

switchport native vlan *vlan-id*

no switchport native vlan

- *vlan-id* — ポートへのデフォルト VLAN ID（範囲：1-4093）

初期設定

VLAN 1

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- PVID を設定するためには、対象のポートが指定する PVID と同じ VLAN に所属しており、またその VLAN がタグなしである必要があります。
- 受け入れ可能なフレームタイプを "all" にしている場合か、switchport モードを "hybrid" にしている場合、入力ポートに入るすべてのタグなしフレームには PVID が挿入されます。

例

本例では PVID を VLAN3 として 1 番ポートに設定しています。

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

switchport allowed vlan

選択したインタフェースの VLAN グループの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

switchport allowed vlan { add *vlan-list* [tagged | untagged] | remove *vlan-list* }

no switchport allowed vlan

- add *vlan-list* — 追加する VLAN の ID のリスト
- remove *vlan-list* — 解除する VLAN の ID のリスト
- *vlan-list* — 連続しない VLAN ID をカンマで分けて入力（スペースは入れない）。連続する ID はハイフンで範囲を指定（範囲：1-4093）

初期設定

すべてのポートが VLAN 1 に参加

フレームタイプはタグなし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- switchport モードが " trunk" に設定されている場合、インタフェースをタグ付メンバーとしてしか VLAN に設定できません。
- インタフェースの switchport mode が "hybrid" に設定されている場合、インタフェースを最低 1 つの VLAN にタグなしメンバーとして設定する必要があります。
- スイッチ内では常にフレームはタグ付となっています。タグ付及びタグなしパラメータはインタフェースへ VLAN を加えるとき使われ、出力ポートでフレームのタグをはずすか保持するかを決定します。
- ネットワークの途中や対向のデバイスが VLAN をサポートしていない場合、インタフェースはこれらの VLAN をタグなしメンバーとして加えます。1 つの VLAN にタグなしとして加え、その VLAN がネイティブ VLAN となります。
- インタフェースの禁止リスト上の VLAN が手動でインタフェースに加えられた場合、VLAN は自動的にインタフェースの禁止リストから削除されます。
- ポートへの接続装置にかかわらず、タグなし VLAN へメンバーを追加することができます。初期設定では VLAN1 となります。
  各ポートは 1 つのタグ無し VLAN にしか所属ができないので、もし 2 つ目の VLAN がタグなしと定義された場合、もう一方の VLAN は自動的にタグつきに変更されます。またポートの PVID もこの VLAN ID へ変更されます。

例

本例では、1 番ポートのタグ付 VLAN 許可リストに 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：1-4093）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- GVRP で自動的に VLAN に加えられることを防ぐためのコマンドです。
- インタフェース上で VLAN が許可 VLAN にセットされている場合、同じインタフェースの禁止 VLAN リストに加えることはできません。

例

本例では 1 番ポートを VLAN 3 に加えることを防いでいます。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

4.16.4 VLAN 情報の表示

コマンド	機能	モード	ページ
show vlan	VLAN 情報の表示	NE,PE	P469
show interfaces status vlan	特定 VLAN インタフェースの状態の表示	NE,PE	P388
show interfaces switchport	インタフェースの管理、運用状態の表示	NE,PE	P390

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：1-4093）
- 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、P476 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#
```

4.16.5 IEEE802.1Q トンネリングの設定

IEEE 802.1Q トンネリング（QinQ）機能を使用することにより、サービス プロバイダは複数の VLAN を設定しているカスタマを、1 つの VLAN を使用してサポートできます。カスタマの VID は保持されるため、さまざまなカスタマからのトラフィックは、同じ VLAN 上に存在するように見える場合でも、サービスプロバイダのインフラストラクチャ内では分離されています。QinQ トンネリングでは、VLAN 内 VLAN 階層を使用して、タグ付きパケットに再度タグ付けを行うこと（ダブルタギングとも呼ばれます）によって、VLAN スペースを拡張します。

この節では、QinQ トンネリングの設定に使用されるコマンドについて説明します。

コマンド	機能	モード	ページ
dot1q-tunnel system-tunnel-control	スイッチをノーマルモードまたは QinQ モードに設定	GC	P471
switchport dot1q-tunnel mode	インタフェースを QinQ トンネルポートに設定	IC	P472
switchport dot1q-tunnel tpid	トンネルポートの TPID（Tag Protocol Identifier）値を設定	IC	P473
show dot1q-tunnel	QinQ トンネルポートの設定を表示	PE	P474
show interfaces switchport	QinQ ポートステータスを表示	PE	P390

QinQ の一般的な設定ガイド

（1）スイッチを QinQ モードに設定（dot1q-tunnel system-tunnel-control P471）

（2）SPVLAN を作成（vlan P461）

（3）QinQ トンネルアクセスポートを dot1Q トンネルアクセスモードに設定
（switchport dot1q-tunnel mode P472）

（4）トンネルアクセスポートの Tag Protocol Identifier (TPID) 値を設定。このステップは、接続されているクライアントが、802.1Q タグ付きフレームの識別に非標準 2-byte イーサタイプを使用している場合に必要です。
（switchport dot1q-tunnel tpid　P473）

（5）QinQ トンネルアクセスポートをタグ無しメンバーとして SPVLAN に追加
（switchport allowed vlan　P467）

（6）QinQ トンネルアクセスポートの SPVLAN ID をネイティブ VID として設定
（switchport native vlan　P466）

（7）QinQ トンネルアップリンクポートを dot1Q トンネルアップリンクモードに設定
（switchport dot1q-tunnel mode　P472）

（8）QinQ トンネルアップリンクポートをタグ付きメンバーとして SPVLAN に追加
（switchport allowed vlan　P467）

QinQ の制限事項

- トンネルアップリンクポートのネイティブ VLAN とトンネルアクセスポートは同一には出来ませんが、同じサービス VLAN を両方のトンネルポートタイプに設定することは可能です。
- トンネルポートでは IGMP スヌーピングを有効に出来ません。
- スパニングツリープロトコルが有効時に、スパニングツリー構造がツリーの中断を克服するために自動で再配置された場合、トンネルアクセスまたはトンネルアップリンクポートは無効になります。これらのポートではスパニングツリーを無効にすることが賢明です。

dot1q-tunnel system-tunnel-control

スイッチが QinQ モードで動作するよう設定を行います。"no" を前に置くと QinQ オペレーティングモードを無効にします。

文法

[no]dot1q-tunnel system-tunnel-control

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

QinQ インタフェース設定が機能するために、QinQ トンネルモードをスイッチで有効にしてください。

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

関連するコマンド

show dot1q-tunnel（P474）
show interfaces switchport（P390）

switchport dot1q-tunnel mode

インタフェースを QinQ **トンネルポートとして設定します。**"no" **を前に置くことでインタフェースの** QinQ **を無効にします。**

文法

switchport dot1q-tunnel mode < access | uplink >
no switchport dot1q-tunnel mode

- access — **ポートを** 802.1Q **トンネルアクセスポートに設定**
- uplink — **ポートを** 802.1Q **トンネルアップリンクポートに設定**

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- switchport dot1q-tunnel mode **インタフェースコマンドを使用する前に、**dot1q-tunnel system-tunnel-control **コマンド（**P471**）を使用して** QinQ **トンネリングを有効にする必要があります。**
- **トンネルアップリンクポートがカスタマからのパケットを受信した際、カスタマタグ（**1 **つ以上のタグレイヤがあるか否かにかかわらず）は内側に保持され、サービスプロバイダのタグが外側のタグに付加されます。**
- **トンネルアップリンクポートがサービスプロバイダからのパケットを受信した際、外側のサービスプロバイダタグは取り除かれ、パケットは内側のタグが示す** VLAN **へ渡されます。内側のタグが見つからない場合、パケットはアップリンクポートに定義されたネイティブ** VLAN **へ渡されます。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

関連するコマンド

show dot1q-tunnel（P474）
show interfaces switchport（P390）

switchport dot1q-tunnel tpid

トンネルポートの Tag Protocol Identifier (TPID) 値を設定します。"no" を前に置くことで設定を初期値へ戻します。

文法

switchport dot1q-tunnel tpid *tpid*
no switchport dot1q-tunnel tpid

- *tpid* — 802.1Q カプセル化のイーサタイプ値を設定。この識別子は 802.1Q タグ付きフレームの識別に非標準 2-byte を選択するために使用します。標準イーサタイプ値は 0x8100（範囲：0800-FFFF16 進数）

初期設定

0x8100

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- "switchport dot1q-tunnel tpid" コマンドは選択されたインタフェースのカスタム 802.1Q イーサタイプ値を設定します。
  この機能は本機へ、802.1Q タグ付きフレームの識別に標準 0x8100 イーサタイプを使用しないサードパーティ製スイッチとインタオペレートすることを許可します。
  例えば、0x1234 はトランクポートのカスタム 802.1Q イーサタイプとして設定され、このイーサタイプを含む入力フレームは、イーサタイプフィールドに続くタグに含まれる VLAN へ、標準的 802.1Q トランクとして割り当てられます。
  その他のイーサタイプを持つポートへ到着したフレームはタグ無しフレームとして見られ、このポートのネイティブ VLAN へ割り当てられます。
- スイッチの全てのポートは同じイーサタイプに設定されます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

関連するコマンド

show interfaces switchport（P390）

show dot1q-tunnel

QinQ トンネルポート情報を表示します。

コマンドモード

Privileged Exec

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel

Current double-tagged status of the system is Enabled

The dot1q-tunnel mode of the set interface 1/1 is Access mode,
TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/2 is Uplink mode,
TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/3 is Normal mode,
TPID is 0x8100.
.
.
.
```

関連するコマンド

switchport dot1q-tunnel mode（P472）

4.16.6 プライベート VLAN の設定

プライベート VLAN はポートベースのセキュリティと VLAN 内のポート間の独立が行えます。ここでは、プライベート VLAN の設定のためのコマンドの解説を行ないます。

コマンド	機能	モード	ページ
pvlan	プライベート VLAN の設定と有効化	GC	P475
show pvlan	プライベート VLAN の設定の表示	PE	P476

pvlan

プライベート VLAN の有効化と設定を行ないます。"no" を前に置くことでプライベート VLAN を無効にします。

文法

pvlan [up-link *interface-list* down-link *interface-list*]

no pvlan

- up-link — アップリンクインタフェースの指定
- down-link — ダウンリンクインタフェースの指定

初期設定

プライベート VLAN は設定されていません

初期設定

Global Configuration

コマンド解説

- プライベート VLAN はポートベースのセキュリティと VLAN 内のポート間の独立が行えます。ダウンリンクポートの通信はアップリンクポートとの間でのみ行なうことができます。
- プライベート VLAN と通常の VLAN は両方を設定し共存させることが可能です。
- パラメータを入力せずに "pvlan" コマンドを使用するとプライベート VLAN が有効になります。"no pvlan" コマンドを使用すると無効になります。

例

本例ではプライベート VLAN を有効にし、12 番ポートをアップリンクに、5-8 番ポートをダウンリンクに設定しています。

```
Console(config)#pvlan
Console(config)#pvlan up-link ethernet 1/12 down-link ethernet 1/5-8
Console(config)#
```

show pvlan

プライベート VLAN **の設定を表示します。**

コマンドモード

Privileged Exec

例

```
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/12
Down-link port:
 Ethernet 1/5
 Ethernet 1/6
 Ethernet 1/7
 Ethernet 1/8
Console#
```

4.16.7 プロトコル VLAN の設定

通常の VLAN では、プロトコル毎の VLAN グループの形成を容易に行なうことはできません。そのため、特定のプロトコルに関連するすべての機器が通信を行えるよう、特殊なネットワーク機器を使用して異なる VLAN 間の通信をサポートする必要があります。
しかし、このような方法では、セキュリティと容易な設定が可能な VLAN のメリットを失ってしまいます。

そのような問題を回避するため、本機では物理的なネットワークの構成を、プロトコルを基にした論理的 VLAN のネットワーク構成とすることが可能なプロトコルベース VLAN 機能を提供します。ポートがフレームを受信した際、受信フレームのプロトコルタイプに応じて VLAN メンバーシップが決定されます。

コマンド	機能	モード	ページ
protocol-vlan protocol-group	プロトコルグループの作成及びサポートプロトコルの指定	GC	P478
protocol-vlan protocol-group	プロトコルグループの VLAN へのマッピング	IC	P479
show protocol-vlan protocol-group	プロトコルグループの設定の表示	PE	P480
show interfaces protocol-vlan protocol-group	プロトコルグループにマッピングされたインタフェースと関連する VLAN の表示	PE	P481

プロトコル VLAN の設定は以下の手順で行ないます。

（1）使用するプロトコルのための VLAN グループを作成します。主要なプロトコル毎に VLAN の作成を行なうこと推奨します。また、この時点ではポートメンバーの追加を行なわないで下さい。

（2）VLAN に設定するプロトコル毎のグループを "protocol-vlan protocol-group" コマンド (General Configuration mode) を利用して生成します。

（3）適切な VLAN に各インタフェースのプロトコルを "protocol-vlan protocol-group" コマンド (Interface Configuration mode) を利用してマッピングします。

protocol-vlan protocol-group (Configuring Groups)

プロトコルグループの作成及び特定のプロトコルのグループへの追加を行ないます。"no" **を前に置くことでプロトコルグループを削除します。**

文法

protocol-vlan protocol-group *group-id* [{ add | remove } frame-type *frame* protocol-type *protocol*]

no protocol-vlan protocol-group *group-id*

- *group-id* — **プロトコルグループ** ID**（設定範囲：**1-2147483647**）**
- *frame* — **プロトコルのフレームタイプ（選択肢：**ethernet,rfc_1042, snap_8021h, snap_other, llc_other**）**
- *protocol* — **プロトコルタイプ。フレームタイプが** llc_other **のフレームの選択肢は** ipx_raw **です。その他のフレームタイプの場合は** ip, arp, rarp **です。（範囲：**0801-FFFF 16 **進数）**

初期設定

プロトコルグループ未設定

コマンドモード

Global Configuration

例

プロトコルグループ "1" **を作成し、フレームタイプを** "Ethernet"**、プロトコルタイプを** "IP" **及び** "ARP" **に設定しています。**

```
Console(config)#protocol-vlan protocol-group 1 add frame-type
 ethernet protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type
 ethernet protocol-type arp
Console(config)#
```

protocol-vlan protocol-group (Configuring Interfaces)

インタフェースにおいてプロトコルグループを VLAN にマッピングします。"no" を前におくことでインタフェースのプロトコルのマッピングを解除します。

文法

protocol-vlan protocol-group *group-id* vlan *vlan-id*

no protocol-vlan protocol-group *group-id* vlan

- *group-id* — プロトコルグループ ID（設定範囲：1-2147483647）
- *vlan-id* — 致したプロトコルの通信が転送される VLAN（設定範囲：1-4093）

初期設定

プロトコルグループはインタフェースにマッピングされていません。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- インタフェースの設定を行なって下さい。他の VLAN コマンドを使用した場合、設定したインタフェースはすべてのプロトコルタイプの通信を関連した VLAN に対して行います。
- フレームがプロトコル VLAN に割り当てられたポートに入力する場合、以下の方法で処理されます。
  - フレームにタグ付フレームの場合、タグの情報に基づき処理されます。
  - フレームがタグなしフレームで、プロトコルタイプが一致した場合、フレームは適切な VLAN に転送されます。
  - フレームがタグなしフレームで、プロトコルタイプが一致しない場合、フレームはインタフェースのデフォルト VLAN に転送されます。

例

本例では、1 番ポートに入ってきた通信でプロトコルグループ 1 と一致する通信が VLAN2 にマッピングしています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

プロトコルグループに関連したフレーム及びプロトコルタイプの表示

文法

show protocol-vlan protocol-group [*group-id*]

- *group-id* — **プロトコルグループ** ID（**設定範囲：**1-2147483647）

初期設定

すべてのプロトコルグループを表示

コマンドモード

Privileged Exec

例

プロトコルグループ 1 **が** Ethernet、IP **に設定されていることを表示しています。**

```
Console#show protocol-vlan protocol-group
ProtocolGroup ID     Frame Type   Protocol Type
------------------ ------------- ---------------
                1     ethernet           08 00
Console#
```

show interfaces protocol-vlan protocol-group

選択したインタフェースのプロトコルグループと VLAN **のマッピング情報を表示します。**

文法

show interfaces protocol-vlan protocol-group [*interface*]

- *Interface*
  - **ethernet** *unit/port*
    - *unit* — **ユニット番号 （範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
- **－ port-channel** channel-id (**範囲：**1-32)

初期設定

すべてのプロトコルグループを表示

コマンドモード

Privileged Exec

例

1 番ポートに入ってきた通信でプロトコルグループ 1 **と一致する通信が** VLAN2 **にマッピングされています。**

```
Console#show interfaces protocol-vlan protocol-group
   Port      ProtocolGroup ID   Vlan ID
---------- ------------------ -----------
   Eth 1/1                 1       vlan2
Console#
```

4.17 プライオリティ

通信の過密によりパケットがスイッチにバッファされた場合、通信の優先権を持つデータパケットを明確にすることができます。本機は各ポートに 4 段階のプライオリティキューを持つ CoS をサポートします。

ポートの最高プライオリティキューの付いたデータパケットは、より低いプライオリティのキューのパケットよりも先に送信されます。各ポートに対しデフォルトプライオリティ、各キューの重みの関連、フレームプライオリティタグのマッピングをスイッチのキューに付けることができます。

コマンドグループ	機能	ページ
Priority（Layer 2）	タグなしフレームへのデフォルトプライオリティの設定、キューウエイトの設定、CoS タグのハードウェアキューへのマッピング	P482
Priority（Layer 3 and 4 ）	TCP ポート、IP DSCP タグの CoS 値への設定	P489

4.17.1 プライオリティコマンド（Layer 2）

コマンド	機能	モード	ページ
queue mode	キューモードを "strict" 又は " Weighted Round-Robin (WRR)" に設定	GC	P483
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	P484
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	P485
queue cos map	プライオリティキューに Class of Service(CoS) を指定	IC	P486
show queue mode	現在のキューモードを表示	PE	P487
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	P487
show queue cos-map	CoS マップの表示	PE	P488
show interfaces switchport	インタフェースの管理、運用ステータスの表示	PE	P390

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 0-7 にそれぞれスケジューリングウエイト 1、2、4、6、8、10、12、14 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 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 *weight0...weight7*
no queue bandwidth

- *weight0...weight7* - キュー 0 ～ 7 の WRR スケジューラで使用される重みの比率（範囲：1-15)

初期設定

1、2、4、6、8、10、12、14 がそれぞれキュー 0-7 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（P487）

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 0-7 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
  - 0-7 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	4	5	6	7
キュー	2	0	1	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

```
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#
```

show queue mode

現在のキューモードを表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show queue mode

Queue mode: wrr
Console#
```

show queue bandwidth

ラウンドロビン（WRR）バンド幅を表示します。

文法

show queue bandwidth [*interface*]

- *Interface*
  - ethernet *unit/port*
    - *unit* — ユニット番号 （範囲：1-8）
    - *port* — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)

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 （範囲：1-8）
    - *port* — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
CoS Value     : 0 1 2 3 4 5 6 7
Priority Queue: 0 0 0 1 2 2 3 3
Console#
```

4.17.2 プライオリティコマンド（Layer 3 and 4）

コマンド	機能	モード	ページ
map ip port	サービスマッピングの TCP/UDP クラスを有効化	GC	P489
map ip port	TCP/UDP ソケットを CoS にマップ	IC	P490
map ip precedence	IP precedence の CoS マッピングの有効化	GC	P490
map ip precedence	IP precedence 値を CoS キューへマッピング	IC	P491
map ip dscp	IP DSCP の CoS マッピングの有効化	GC	P492
map ip dscp	IP DSCP 値を CoS キューへマッピング	IC	P493
show map ip port	IP ポートマップの表示	IC	P493
show map ip precedence	IP Precedence マップの表示	PE	P495
show map ip dscp	IP DSCP マップの表示	PE	P498

map ip port（Global Configuration）

IP 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を解除します。

文法

[no] map ip port

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- プライオリティマッピングの優先順位は IP ポート、IP Precedence/DSCP/ToS、デフォルトポートプライオリティです。

例

```
Console(config)#map ip port
Console(config)#
```

map ip port（interface Configuration）

IP ポートプライオリティマッピングの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

map ip port [*port-number* cos *cos-queue*]

no map ip port [*port-number*]

- *port-number* — 16-bit TCP/UDP ポート番号（範囲：0-65535）
- *cos-queue* — CoS 値（範囲：0-7）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
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 マッピングを設定します。"no" を前に置くことで設定を解除します。

文法

[no] map ip precedence

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence（interface Configuration）

IP precedence プライオリティマッピングの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

map ip precendence [*ip-precedence-value* cos *cos-value*]

no map ip precedence

- *ip-precedence-value* — 3bit precedence 値（範囲：0-7）
- *cos-queue* — CoS 値（範囲：0-7）

初期設定

以下はデフォルトプライオリティマッピング値になります。

IP Precedence 値	0	1	2	3	4	5	6	7
CoS 値	0	1	2	3	4	5	6	7

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
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

[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 DSCP、ポートプライオリティです。

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 DSCP、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を表示します。**

文法

show map ip port [*interface*]

- i*nterface*
  - ethernet *unit/port*
    - *unit* — **ユニット番号 （範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id (**範囲：**1-32)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip port
TCP port mapping status: disabled

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

show map ip precedence

IP ポートプライオリティマップを表示します。

文法

show map ip precedence [*interface*]

- i*nterface*
  - ー ethernet *unit/port*
    - ー *unit* — **ユニット番号 （範囲：**1-8**）**
    - ー *port* — **ポート番号（範囲：**1-26**）**
  - ー port-channel channel-id (**範囲：**1-32)

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: disabled

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

関連するコマンド

map ip precedence（P490）

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 （範囲：**1-8**）**
    - *port* — **ポート番号（範囲：**1-26**）**
  - port-channel channel-id (**範囲：**1-32)

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

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

関連するコマンド

map ip dscp（Global Configuration）（P492）
map ip dscp（Interface Configuration）（P493）

4.18 Quality of Service

この章で記載されているコマンドは QoS(Quality of Service) 機能の基準とサービスポリシーを構成するために使用されます。DiffServ(Differentiated Services) 機能は、ネットワーク上を流れるフレームの 1 つの単位を特定のトラフィックの要件に合致させるため、ネットワークリソースを優先する管理機能を提供します。それぞれのパケットはアクセスリスト、IP Precedence、DSCP、VLAN リストをベースにしたネットワークの中のエントリによって分類されます。アクセスリストを使用することにより、それぞれのパケットが含んでいるレイヤ 2 ～ 4 の情報を元にトラフィックの選別を許可します。設定されたネットワークポリシーをベースにして、異なる種類のトラフィックに対し、異なる種類の転送のために印を付けることができます。

コマンド	機能	モード	ページ
class-map	クラスマップを作成	GC	P498
match	クラス分類のためトラフィックに使う条件を定義	CM	P499
rename	クラスマップの名前を再定義	CM	P500
description	クラスマップの説明を指定	CM	P500
policy-map	ポリシーマップを作成	GC	P501
class	ポリシー上で実行するクラスを設定	PM	P502
rename	クラスマップの名前を再定義	PM	P500
description	クラスマップの記述を指定	PM	P500
set	IP パケットに適用する CoS、DSCP、IP Precedence の値を設定	PM-C	P503
police	クラス分けされたトラフィックに制限を設定	PM-C	P504
service-policy	ポリシーマップをインターフェースに適用	IC	P505
show class-map	クラスマップの情報を表示	PE	P506
show policy-map	ポリシーマップの情報を表示	PE	P507
show policy-map interface	インターフェースに設定されたポリシーマップの情報を表示	PE	P507

特定の入力トラフィックにポリシーを設定する方法は下記の通りです。

（1）class-map コマンドを使用してクラスの名前を設定し、クラスマップコンフィグレーションモードに入ります。

（2）アクセスリスト、DSCP と IP Precedence の値、VLAN 情報を基にトラフィックをフィルタするため match コマンドを使用します。

（3）match コマンドで指定した条件でのトラフィックのフィルタを有効にするため、ACL を設定します。

（4）ポリシーの名前を指定し、ポリシーマップコンフィグレーションモードに入るため、policy-map コマンドを使用します。

（5）クラスマップをポリシーマップに割り当てるために class コマンドを使用し、ポリシーマップ・クラスコンフィグレーションモードに入ります。ポリシーマップには複数のクラス設定を含めることができます。

（6）クラス情報と一致するトラフィックに QoS の値を設定するため set コマンドを使用します。また帯域幅とバーストレートを制限するため police コマンドを使用します。police コマンドではトラフィックが指定したレートを越えたとき、そのトラフィックを破棄するか、トラフィックの DSCP の値を減少させるよう設定できます。

（7）インターフェースにポリシーマップを割り当てるため、service-policy コマンドを使用します。

[注意] クラスマップごとに最大 16 個のルールを設定することができます。ポリシーマップには複数のクラスを設定することもできます。

[注意] ポリシーマップを作成する前にクラスマップを作成してください。作成しない場合、ポリシールールのクラスマップを選択することはできません。

class-map

このコマンドはクラスマップを作成し、クラスマップコンフィグレーションモードに移行します。no **を付けるとクラスマップを削除し、グローバルコンフィグレーションモードに戻ります。**

文法

[no] class-map *class-map-name* [match-any]

- match-any — **クラスマップの条件のうちいずれか** 1 **つに一致するトラフィックを対象**
- *class-map-name* — **クラスマップ名（**1-16 **文字）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **最初にこのコマンドを実行してクラスマップを作成し、クラスマップコンフィグレーションモードに入ります。次に入力トラフィックの分類条件を** match **コマンドで指定します。**
- 1 **つのクラスマップあたり最大** 16 **個、**match **コマンドを実行することができます。**
- **クラスマップは、パケットの分類、タグの付与、帯域幅の制限をインターフェースに対して行うため、ポリシーマップと同時に使用されます。**

例

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

関連するコマンド

show class map (P506)

match

このコマンドはトラフィックを分類するために使用する条件を設定します。

文法

[no] match {access-list *acl-name* | ip dscp *dscp* | ip precedence *ip-precedence* | vlan *vlan*}

- *acl-name* — **アクセスコントロールリスト名**（1-16 **文字**）
- *dscp* — DSCP **値**（0-63）
- *ip-precedence* — IP Precedence **値**（0-7）
- *vlan* — VLAN ID（1-4094）

初期設定

なし

コマンドモード

Class Map Configuration

コマンド解説

- **最初に** class-map **コマンドを実行してクラスマップを作成し、クラスマップコンフィグレーションモードに入ります。次にこのクラスマップ上で合致させたい入力パケット中の値を** match **コマンドで指定します。**
- 1 **つのクラスマップあたり** 1 **つの** match **コマンドのみ入力することができま**

例

“rd_class#1,” **という名前のクラスマップを作成し、**DSCP **値** 3 **をマークします。**

```
Console(config)#class-map rd_class#1_ match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

“rd_class#2,” **という名前のクラスマップを作成し、**IP Precedence **値** 5 **をマークします。**

```
Console(config)#class-map rd_class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

“rd_class#3,” **という名前のクラスマップを作成し、**VLAN1 **をマークします。**

```
Console(config)#class-map rd_class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

rename

クラスマップまたはポリシーマップの名前を再定義します。

文法

rename *map-name*

map-name — **クラスマップまたはポリシーマップの名前（範囲：**1-16 **文字）**

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

description

クラスマップまたはポリシーマップの説明を入力します。

文法

description *string*

string — **クラスマップまたはポリシーマップの説明（範囲：**1-64 **文字）**

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description matches packets marked for DSCP service
  value 3
Console(config-cmap)#
```

policy-map

このコマンドはポリシーマップを作成し、ポリシーマップコンフィグレーションモードに入ります。no を付けるとポリシーマップは削除され、グローバルコンフィグレーションモードに戻ります。

文法

[no] policy-map *policy-map-name*

- *policy-map-name* — ポリシーマップ名（1-16 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- ポリシーマップの名前を設定するために policy-map コマンドを使用します。次にクラスマップで指定された条件に合致するトラフィックにポリシーを設定するため、class コマンドを使用します。
- ポリシーマップに複数のクラス設定を含めることができます。
- ポリシーマップを作成する前にクラスマップを作成する必要があります。

例

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

class

このコマンドはポリシーマップが実行するクラスマップを指定し、ポリシーマップ・クラスコンフィグレーションモードに入ります。no を付けるとクラスマップを削除し、ポリシーマップコンフィグレーションモードに戻ります。

文法

[no] class *class-map-name*

- *class-map-name* — クラスマップ名（1-16 文字）

初期設定

なし

コマンドモード

Policy Map Configuration

コマンド解説

- ポリシーマップの設定を行うために policy-map コマンドを使用し、ポリシーマップコンフィグレーションモードに入ります。次にポリシーマップ・クラスコンフィグレーションモードに入るために class コマンドを使用します。そして最後に、set コマンドと police コマンドを使用して設定を行います。
  - set －コマンドは受信した IP パケットをクラス分けします。
  - police －コマンドは最大スループット、バーストレート、ポリシーに反した場合の動作を定義します。
- 1 つのクラスマップあたり最大 16 個のルールを設定できます。また、ポリシーマップには複数のクラスを所属させることができます。

例

この例では "rd_policy" という名前のポリシーを作成し、class コマンドを使って前もって設定されたクラス "rd_class" を設定しています。次に set コマンドを使用して受信された入力パケットのクラス分けを行い、police コマンドで平均帯域幅を 100,000kbps、バーストレートを 1522bytes に制限し、それに反したパケットを破棄するよう設定しています。

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

set

このコマンドは match **コマンドで設定した条件に合致したパケットに** CoS、DSCP、IP Precedence **の値を** IP **パケットに付加します。**no **を付けるとトラフィックのクラス分けを取り止めます。**

文法

[no] set {cos *new-cos* | ip dscp *new-dscp* | ip precedence *new-precedence*}

- *new-cos* — **新しく付加する** CoS **の値（**0-7**）**
- *new-dscp* — **新しく付加する** DSCP **の値（**0-63**）**
- *new-precedence* — **新しく付加する** IP Precedence Value（0-7）

初期設定

なし

コマンドモード

Policy Map Configuration

例

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

police

このコマンドはクラス分けされたトラフィックにポリサを設定します。no **を付けるとポリサの適用を取り止めます。**

文法

[no] police *rate-kbps burst-byte* [exceed-action {drop | set}]

- *rate-kbps* — 1 **秒あたりの転送レート（単位：**kbps　**範囲：**1 ～ 100,000kbps）
- *burst-byte* — **バーストレート** (**範囲：**64-1522 bytes)
- drop — **設定した帯域幅とバーストレートを超えたパケットは破棄する。**
- set — **設定した帯域幅とバーストレートを超えたパケットに** DSCP **の値を設定する。**

初期設定

drop

コマンドモード

Policy Map Configuration

コマンド解説

- **各アクセスリスト（**Standard ACL、Extended ACL、MAC ACL**）のそれぞれに最大** 64 **個のポリサを構成できます。**
- **ポリシングはトークンバケットを基にしています。バケットの深さ（バケットがオーバーフローする前の最大バーストレート）は** burst-byte **オプションで指定します。またバケットから移動するトークンの平均レートは** rate-kbps **オプションで指定します。**

例

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

service-policy

このコマンドはインターフェースの入力キューに policy-map **コマンドで定義されたポリシーマップを割り当てます。**no **を付けるとこのインターフェースからポリシーマップの割り当てを外します。**

文法

[no] service-policy input *policy-map-name*

- input — **入力トラフィックにインタフェースを適用**
- *policy-map-name* — **ポリシーマップ名（**1-16 **文字）**

初期設定

インタフェースにポリシーマップは未適用

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **インターフェースには** 1 **つのポリシーマップのみ割り当てることができます。**
- **最初にクラスマップを定義し、次にポリシーマップを設定し、最後に** service-policy **コマンドを使用して必要なインターフェースにポリシーマップを関連付けてください。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd_policy
Console(config-if)#
```

show class-map

このコマンドは match コマンドで設定した QoS のクラスマップを表示します。

文法

show class-map [*class-map-name*]

- *class-map-name* — クラスマップ名（1-16 文字）

初期設定

全てのクラスマップを表示

コマンドモード

Privileged Exec

例

```
Console#show class-map
Class Map match-any rd_class#1
Match ip dscp 3
Class Map match-any rd_class#2
Match ip precedence 5
Class Map match-any rd_class#3
Match vlan 1
Console#
```

show policy-map

このコマンドは QoS のポリシーマップを表示します。

文法

show policy-map [*policy-map-name* [class *class-map-name*]]

- *policy-map-name* — ポリシーマップ名（1-16 文字）
- *class-map-name* — クラスマップ名（1-16 文字）

初期設定

全てのポリシーマップおよびクラスマップを表示

コマンドモード

Privileged Exec

例

```
Console#show policy-map
Policy Map rd_policy
class rd_class
set ip dscp 3
Console#show policy-map rd_policy class rd_class
Policy Map rd_policy
class rd_class
set ip dscp 3
Console#
```

show policy-map interface

このコマンドはインターフェースに割り当てられたサービスポリシーを表示します。.

文法

show policy-map interface *interface* **input**

- *Interface*
  - ethernet *unit/port*
    - *unit* — ユニット番号 （範囲：1-8）
    - *port* — ポート番号（範囲：1-26）
  - port-channel channel-id (範囲：1-32)

コマンドモード

Privileged Exec

例

```
Console#show policy-map interface ethernet 1/5
Service-policy rd_policy input
Console#
```

4.19 マルチキャストフィルタリング

IGMP (Internet Group Management Protocol) を使用し、特定のマルチキャストサービスを受けたいホストに対してクエリを実行します。リクエストしているホストが所属するポートを特定し、それらのポートにのみデータを送ります。マルチキャストサービスを受け取り続けるために、隣接するマルチキャストスイッチ / ルータにサービスリクエストを伝搬します。

コマンドグループ	機能	ページ
IGMP Snooping	IGMP snooping 又は静的設定によるマルチキャストグループの設定。IGMP バージョンの設定、設定状態、マルチキャストサービスグループやメンバーの表示	P508
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	P515
Static Multicast Interface	静的マルチキャストルータポートの設定	P520

4.19.1 IGMP Snooping コマンド

コマンド	機能	モード	ページ
ip igmp snooping	IGMP snooping を有効化	GC	P509
ip igmp snooping vlan static	インタフェースを、マルチキャストグループのメンバとして追加	GC	P510
ip igmp snooping version	IGMP バージョンを設定	GC	P511
ip igmp snooping immediate-leave	ポートで Leave パケットが受信され、親 VLAN で immediate-leave が有効の場合、マルチキャストサービスのメンバーポートを直ちに削除	GC	P512
show ip igmp snooping	IGMP スヌーピングとクエリの設定を表示	PE	P513
show mac-address-table multicast	IGMP スヌーピング MAC マルチキャストリストの表示	PE	P514

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

[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：**1-4093）
- *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** （**範囲：**1-8）
    - *port* — **ポート番号**（**範囲：**1-26）
  - **port-channel** *channel-id*（**範囲：**1-32）

初期設定

なし

コマンドモード

Global Configuration

例

本例ではポートにマルチキャストグループを静的に設定しています。

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
ethernet 1/5
Console(config)#
```

ip igmp snooping version

IGMP snooping のバージョンを設定します。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping version {1 | 2 | 3 }

no ip igmp snooping version

- 1 — IGMP Version1
- 2 — IGMP Version2
- 3 — IGMP Version3

初期設定

IGMP Version 2

コマンドモード

Global Configuration

コマンド解説

- サブネット上のすべてのシステムが同じバージョンをサポートする必要があります。もし既存のデバイスが Version 1 しかサポートしていない場合、本機に対しても Version 1 を設定します。
- "ip igmp query-max-response-time" コマンド及び "ip igmp router-port-expire-time" コマンドは Version 2 でしか使えません。

例

本例では IGMP Version 1 に設定しています。

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping immediate-leave

ポートで leave packet **が受信され、**immediate-leave **が親** VLAN **で有効になっている時、マルチキャストサービスのメンバーポートをただちに削除します。**"no" **を前に置くことで初期設定に戻します。**

文法

[no] ip igmp snooping immediate-leave

初期設定

無効

コマンドモード

Interface Configuration（VLAN）

コマンド解説

- immediate-leave **が使用されない場合、**IGMPv2/v3 **グループが** leave **メッセージを受信した時、マルチキャストルータ（またはクエリア）はグループ指定クエリメッセージを送信します。タイムアウト期間の内にホストがクエリに返答しない場合に限り、ルータ / クエリはグループのトラフィック転送を停止します。（このリリースのタイムアウトは現在** Last Member Query Interval **によって定義されています（**1 **秒に固定）***RFC2236 **で定義される信頼関数（**2 **に固定））**
- **このコマンドは** IGMP **スヌーピング有効で、**IGMPv2 **または** IGMPv3 **スヌーピングが使用されている時のみ効果があります。**

例

```
Console(config-if-vlan1)#ip igmp snooping immediate-leave
Console(config-if-vlan1)#
```

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

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 { *interface* | user | igmp-snooping | *multicast-address* }

- *interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号 （範囲：1-8）
    - *port* — ポート番号（範囲：1-26）
  - **port-channel** *channel-id*（範囲：1-32）
- user— ユーザーに設定されたマルチキャストエントリのみを表示
- igmp-snooping— IGMP スヌーピングで学習されたエントリのみを表示
- *multicast-address* —IP マルチキャストグループアドレス
  （範囲：224.0.0.0- 239.255.255.255）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

メンバーの種類は選択したオプションにより IGMP 又は USER を含む表示がされます。

例

本例では VLAN 1 で IGMP snooping により登録されたマルチキャストエントリを表示しています。

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
VLAN M'cast IP addr. Member ports Type
---- --------------- ------------ -------
   1       224.1.2.3      Eth1/11    IGMP
Console#
```

4.19.2 IGMP Query コマンド（Layer2）

コマンド	機能	モード	ページ
ip igmp snooping querier	IGMP snooping クエリアとしての動作の有効化	GC	P515
ip igmp snooping query-count	クエリーカウントの設定	GC	P516
ip igmp snooping query-interval	クエリー間隔の設定	GC	P517
ip igmp snooping query-maxrsponse-time	レポート遅延の設定	GC	P518
ip igmp snooping rouoter-port-expire-time	クエリータイムアウトの設定	GC	P519

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

[no] ip igmp snooping querier

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

有効にした場合、本機はクエリアとして機能します。クエリアはマルチキャストトラフィックを受け取る必要があるかどうか、ホストに質問します。

例

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-coount

クエリーカウントの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping query-count *count*

no ip igmp snooping query-count

- *count* — マルチキャストグループからクライアントを除外する前に、スイッチからクエリ送信する最大回数（範囲：2-10）

初期設定

2 回

コマンドモード

Global Configuration

コマンド解説

クエリーカウントではマルチキャストクライアントからの応答をクエリアが待つ回数を定めます。クエリアが本コマンドで定義された数のクエリーを送り、クライアントからの応答がなかった場合、" ip igmp snooping query-max-response-time" コマンドで指定したカウントダウンタイマーがスタートします。

カウントダウンが終わり、クライアントからの応答がない場合、クライアントがマルチキャストグループからはずれたと判断されます。

例

本例では、クエリーカウントを 10 に設定しています。

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

関連するコマンド

ip igmp snooping query-max-response-time (P518)

ip igmp snooping query-interval

クエリの送信間隔を設定します。"no" **を前に置くことで初期設定に戻します。**

文法

ip igmp snooping query-interval *seconds*

no ip igmp snooping query-interval

- *seconds* — IGMP **クエリを送信する間隔（範囲：**60-125)

初期設定

125**（秒）**

コマンドモード

Global Configuration

例

本例ではクエリ間隔を 100 **秒に設定しています。**

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

クエリの送信間隔を設定します。"no" **を前に置くことで初期設定に戻します。**

文法

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

- *seconds* — IGMP **クエリを送信する間隔（範囲：**5-25)

初期設定

10**（秒）**

コマンドモード

Global Configuration

コマンド解説

- **本機能を有効にするには** IGMP v2 **を使用する必要があります。**
- **クエリ後のマルチキャストクライアントからの正式な回答があるまでの待ち時間を設定します。クエリアが送信するクエリ数を** " ip igmp snooping query-count" **コマンドを使用して設定している場合、クライアントからの応答がないとカウントダウンタイマーが本コマンドで設定した値でスタートします。カウントダウンが終わり、クライアントからの応答がない場合、クライアントがマルチキャストグループからはずれたと判断されます。**

例

本例では、最大返答時間を 20 **秒に設定しています。**

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

ip igmp snooping router-port-expire-time

クエリータイムアウト時間の設定を行います。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

- *seconds* — クエリーパケットを受信していたルータポートが無効になると判断される前の待機時間（範囲：300-500（秒））

初期設定

300（秒）

コマンドモード

Global Configuration

コマンド解説

本機能を有効にするには IGMP v2 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（P511）

4.19.3 静的マルチキャストルーティングコマンド

コマンド	機能	モード	ページ
ip igmp snooping VLAN mrouter	マルチキャストルータポートの追加	GC	P520
show ip igmp snooping mrouter	マルチキャストルータポートの表示	PE	P521

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：1-4093）
- *Interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号 （範囲：1-8）
    - *port* — ポート番号（範囲：1-26）
  - **port-channel** channel-id (範囲：1-32)

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：1-4093）

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#
```

4.20 DNS

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

DNS は "ip name-server" コマンドを使用し最低 1 つのネームサーバを指定しなければ有効にすることはできません。また、ドメインルックアップは " ip domain-lookup" コマンドにより有効にします

コマンド	機能	モード	ページ
ip host	静的ホスト名－アドレスマッピング	GC	P523
clear host	ホスト名－アドレステーブルからのエントリの削除	PE	P524
ip domain-name	不完全なホスト用のデフォルトドメイン名の設定	GC	P525
ip domain-list	不完全なホスト用のデフォルトドメイン名リストの設定	GC	P526
ip name-server	ホスト名－アドレス変換のための 1 つ又は複数のネームサーバの指定	GC	P527
ip domain-lookup	DNS によるホスト名－アドレス変換の有効化	GC	P528
show hosts	静的ホスト名－アドレスマッピングテーブルの表示	PE	P529
show dns	DNS サービスの設定の表示	PE	P529
show dns cache	DNS キャッシュのエントリの表示	PE	P530
clear dns cache	DNS キャッシュのエントリのクリア	PE	P530

ip host

DNS テーブルのホスト名と IP アドレスのマッピングの静的設定を行ないます。
"no" を前に置くことでエントリを削除します。

文法

ip host *name address1* [*address2 … address8*]

no ip host *name address1* [*address2 … address8*]

- *name* — ホスト名（設定範囲：1-64 文字）
- *address1* — 関連する IP アドレス
- *address2 … address8* — 関連する IP アドレス（追加分）

初期設定

静的エントリなし

コマンドモード

Global Configuration

コマンド解説

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

例

2 つのアドレスをホスト名にマッピングしています。

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
  rd5
Inet address
  10.1.0.55 192.168.1.55
Alias
Console#
```

clear host

DNS テーブルのエントリを削除します。

文法

clear host {*name* | *}

- *name* — ホスト名（設定範囲：1-64 文字）
- * — すべてのエントリを削除

初期設定

なし

コマンドモード

Privileged Exec

例

本例ではすべての DNS テーブルのエントリを削除しています。

```
Console(config)#clear host *
Console(config)#
```

ip domain-name

不完全なホスト名に追加するデフォルトドメイン名を設定します。
"no" を前に置くことでドメイン名を削除します。

文法

ip domain-name *name*

no ip domain-name

- *name* — **ホスト名。ドメイン名とホスト名の間のドット (.) は入力しないで下さい（設定範囲：**1-64 **文字）**

例

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
Name Server List:
Console#
```

関連するコマンド

ip domain-list（P526）
ip name-server（P527）
ip domain-lookup（P528）

ip domain-list

このコマンドは、不完全なホスト名に追加するドメイン名のリストを設定します。"no" を前に置くことでリストからドメイン名を削除します。

文法

ip domain-list *name*
no ip domain-list *name*

- *name* — ホスト名。ドメイン名とホスト名の間のドット (.) は入力しないで下さい（設定範囲：1-64 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- ドメイン名はリストの最後に追加されます。
- 本機の DNS サーバが不完全なホスト名を受信し、ドメイン名リストが指定された場合、本機は追加するリスト内の各ドメイン名をホスト名に加え、一致する特定のネームサーバを確認して、ドメインリストにより動作します。
- ドメインリストがない場合、デフォルトドメイン名が使用されます。ドメインリストがある場合には、デフォルトドメイン名は使用されません。

例

本例では、現在のリストに 2 つのドメイン名を追加し、その後リストを表示しています。

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
   DNS disabled
Default Domain Name:
   .sample.com
Domain Name List:
   .sample.com.jp
   .sample.com.uk
Name Server List:
Console#
```

関連するコマンド

ip domain-name（P525）

ip name-server

ドメイン名解決のために 1 つ又は複数のドメインネームサーバのアドレスを指定します。"no" を前に置くことでリストからネームサーバを削除します。

文法

ip name-server *server-address1* [*server-address2 … server-address6*]
no ip name-server *server-address1* [*server-address2 … server-address6*]

- *server-address1* — **ドメインネームサーバの** IP **アドレス**
- *server-address2 … server-address6* — **ドメインネームサーバの** IP **アドレス（追加分）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

応答を受信するまで、又はリストの最後に到達するまで、リスト内のネームサーバに対して順番にリクエストを送信します。

例

応答を受信するまで、又はリストの最後に到達するまで、リスト内のネームサーバに対して順番にリクエストを送信します。

```
Console(config)#ip domain-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
   DNS disabled
Default Domain Name:
   .sample.com
Domain Name List:
   .sample.com.jp
   .sample.com.uk
Name Server List:
192.168.1.55
10.1.0.55
Console#
```

関連するコマンド

ip domain-name（**P525**）
ip domain-lookup（**P528**）

ip domain-lookup

DNS ホスト名・アドレス変換を有効にします。"no" を前に置くことで DNS を無効にします。

文法

[no] ip domain-lookup

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- DNS を有効にする前に最低 1 つのネームサーバを指定する必要があります。
- すべてのネームサーバが削除された場合には DNS は自動的に無効になります。

例

本例では、DNS を有効にし、設定を表示しています。

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

関連するコマンド

domain-name（P538）
ip name-server（P539）

show hosts

静的ホスト名－アドレスマッピングテーブルを表示します。

コマンドモード

Privileged Exec

例

以前に設定されたエントリと同じアドレスがマッピングされた場合、ホスト名はエイリアスとして表示されます。

```
Console#show hosts

Hostname
  rd5
Inet address
  10.1.0.55 192.168.1.55
Alias
  1.rd6
Console#
```

show dns

DNS サーバの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

show dns cache

DNS キャッシュの内容を表示します。

コマンドモード

Privileged Exec

例

```
NO   FLAG TYPE IP             TTL DOMAIN
0     4   CNAME 10.2.44.96    893 pttch_pc.accton.com.tw
1     4   CNAME 10.2.44.3     898 ahten.accton.com.tw
2     4   CNAME 66.218.71.84 298 www.yahoo.akadns.net
3     4   CNAME 66.218.71.83 298 www.yahoo.akadns.net
4     4   CNAME 66.218.71.81 298 www.yahoo.akadns.net
5     4   CNAME 66.218.71.80 298 www.yahoo.akadns.net
6     4   CNAME 66.218.71.89 298 www.yahoo.akadns.net
7     4   CNAME 66.218.71.86 298 www.yahoo.akadns.net
8     4   ALIAS POINTER TO:7 298 www.yahoo.com
Console#
```

項目	解説
NO	各リソースレコードのエントリ番号
FLAG	キャッシュエントリのフラグは常に "4"
TYPE	標準的又はプライマリ名が指定された「CNAME」、既存のエントリと同じ IP アドレスをマッピングされている多数のドメイン名が指定された「ALIAS」
IP	レコードに関連した IP アドレス
TTL	ネームサーバにより報告された生存可能時間
DOMAIN	レコードに関連するドメイン名

clear dns cache

DNS キャッシュのすべての値をクリアします。

コマンドモード

Privileged Exec

例

```
Console#clear dns cache
Console#show dns cache
NO      FLAG      TYPE     IP     TTL     DOMAIN
Console#
```

4.21 DHCP

コマンドグループ	機能	ページ
DHCP Client	DHCP クライアントの設定	P531
DHCP Relay	DHC リレーの設定	P533
DHCP Server	DHCP サーバーの設定	P535

4.21.1 DHCP Client

DHCP (Dynamic Host Configuration Protocol) クライアントの設定を行ないます。任意の VLAN インタフェースに対して DHCP を使用し、IP アドレスを自動的に設定することが可能です。

コマンド	機能	モード	ページ
ip dhcp client-identifier	本機の DHCP クライアント ID の指定	IC	P531
ip dhcp restart client	BOOTP 又は DCHP クライアントリクエストの送信	PE	P532

ip dhcp client-identifier

インタフェースに対して DHCP クライアント ID の指定をします。"no" を前に置くことで ID を削除します。

文法

ip dhcp client-identifier {text *text* | hex *hex*}

no ip dhcp client-identifier

- *text* — テキスト（範囲：1-15 文字）
- *hex* — 16 進数値

初期設定

なし

コマンドモード

Interface Configuration (VLAN)

コマンド解説

DHCP サーバと接続する際のクライアント ID として使用されます。ID タイプは DHCP サーバの要求に依存します。

例

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

関連するコマンド

ip dhcp restart client（P532）

ip dhcp restart client

BOOTP 又は DHCP リクエストを送信するためのコマンドです。

初期設定

なし

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- ip address コマンドで BOOTP 又は DHCP モードを選択した場合に、IP インタフェースに対して BOOTP 又は DHCP クライアントリクエストを発行します。
- DHCP はサーバに対し使用可能であれば最後に取得したアドレスの使用を要求します。
- BOOTP 又は DHCP サーバが他のドメインに移動していた場合、指定されるアドレスは新しいドメインに基づいたアドレスとなります。

例

本例では、本機が再度同じアドレスを取得しています。

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
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: Dhcp.
Console#
```

関連するコマンド

ip address（P560）

4.21.2 DHCP Relay

コマンド	機能	モード	ページ
ip dhcp restart relay	DHCP リレーエージェントを有効化	IC	P531
ip dhcp relay server	DHCP サーバアドレスを指定	IC	P532

ip dhcp restart relay

指定した VLAN **で** DHCP **リレーを有効にします。**"no" **を前に置くことで無効にします。**

文法

[no] ip dhcp relay

初期設定

無効

コマンドモード

Interface Configuration (VLAN)

例

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay
Console(config-if)#end
Console#show ip interface

Vlan 1 is up, addressing mode is Dhcp
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

ip dhcp relay server

スイッチのリレーエージェントに使用される、DHCP **サーバのアドレスを指定します。**"no" **を前に置くことで全てのアドレスを消去します。**

文法

ip dhcp relay server *address1* [*address2* [*address3* ...]]

no ip dhcp relay server

- *address* — DHCP **サーバの** IP **アドレス（**1-3 **アドレス）**

初期設定

なし

コマンドモード

Interface Configuration (VLAN)

例

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

4.21.3 DHCP Server

コマンド	機能	モード	ページ
service dhcp	スイッチで DHCP サーバ機能を有効化	GC	P536
ip dhcp excluded-address	DHCP サーバが除外する DHCP クライアントの IP アドレスを指定	GC	P536
ip dhcp pool	DHCP サーバーの DHCP アドレスプールを設定	GC	P536
netowork	DHCP アドレスプールのサブネット番号およびマスクを設定	DC	P537
default-router	DHCP クライアントのデフォルトルータリストを指定	DC	P538
domain-name	DHCP クライアントのドメインネームを指定	DC	P538
dns-server	DHCP クライアントで使用可能な DNS サーバを指定	DC	P539
next-server	DHCP クライアントのブーとプロセスで、次のサーバを設定	DC	P539
bootfile	DHCP クライアントのデフォルトブートイメージを指定	DC	P540
netbios-name-server	DHCP クライアントで使用可能な NetBios ネームサーバを指定	DC	P541
netbios-node-type	DHCP クライアントの NetBIos ノードタイプを設定	DC	P542
lease	DHCP クライアントにアサインされた IP アドレスの継続時間を設定します。	DC	P543
host*	IP アドレスおよびネットワークマスクを、マニュアルで DHCP クライアントにバインド	DC	P544
client-identifier*	DHCP クライアントのクライアント識別子を指定	DC	P545
hardware-address*	DHCP クライアントのハードウェアアドレスを指定	DC	P546
clear ip dhcp binding	DHCP サーバデータベースから自動アドレスを削除	PE	P547
show ip dhcp binding	DHCP サーバーのアドレスバインディングを表示	PE, NE	P547

* これらのコマンドは、マニュアルでクライアントにアドレスをバインドする際に使用します。

service dhcp

スイッチで DHCP サーバを有効にします。"no" を前に置くことで DHCP サーバを無効にします。

文法

[no] service dhcp

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#service dhcp
Console(config)#
```

ip dhcp excluded-address

DHCP サーバが除外する DHCP クライアントを指定します。"no" を前に置くことで指定したアドレスを削除します。

文法

ip dhcp excluded-address *low-address* [*high-address*]
no ip dhcp excluded-address

- *low-address* — 除外する IP アドレスまたは、除外されるアドレス範囲の最初のアドレス。
- *low-address* — 除外されるアドレス範囲の最後のアドレス。

初期設定

全ての IP プールアドレスはアサイン可能

コマンドモード

Global Configuration

例

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```

ip dhcp pool

DHCP アドレスプールの設定を行うとともに、DHCP プール設定モードへ移行します。"no" を前に置くことでアドレスプールを削除します。

文法

ip dhcp pool *name*

no ip dhcp pool

- *name* — **プール名（範囲：**1-8 **文字）**

初期設定

DHCP **アドレスプールは設定されていません**

コマンドモード

Global Configuration

例

```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

関連するコマンド

network (P537)

host (P544)

netowork

DHCP **アドレスプールに、サブネット番号およびマスクを設定します。**"no" **を前に置くことで設定した値を削除します。**

文法

netowork *network-number* **[** *mask* **]**

no network

- *network-number* — DHCP **サアドレスプールの** IP **アドレス**
- *mask* — DHCP **アドレスプールのサブネット番号、マスク**

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#
```

default-router

DHCP プールのデフォルトルータを指定します。"no" を前に置くことで設定された値を削除します。

文法

default-router *address1* [*address2*]

no default-router

- *address1* — プライマリルータの IP アドレス
- *address2* — 代替ルータの IP アドレス

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#default-router 10.1.0.54 10.1.0.64
Console(config-dhcp)#
```

domain-name

DHCP クライアントのドメイン名を指定します。"no" を前に置くことで設定したドメイン名を削除します。

文法

domain-name *domain*
no domain-name

- *domain* — クライアントのドメイン名を指定します。（範囲：1-32 文字）

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

dns-server

DHCP クライアントで利用可能な、DNS サーバを指定します。"no" を前に置くことでサーバーをリストから削除します。

文法

dns server *address1* [*address2*]

no dns server

- *address1* — プライマリ DNS サーバのアドレスを指定
- *address2* — 代替 DNS サーバのアドレスを指定

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

next-server

DHCP クライアントのブートプロセスの、次のサーバを設定します。"no" を前に置くことでブートサーバーリストから削除します。

文法

next-server *address*
no next-server *address*

- *address* — IP アドレスを指定します。

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

関連するコマンド

bootfile（P540）

bootfile

DHCP クライアントのデフォルトブートイメージの名前を指定します。このファイルは next-server コマンドで指定された TFTP サーバに置かれます。"no" を前に置くことでブートイメージファイル名を削除します。

文法

bootfile *filename*

no bootfile

- *filename* — デフォルトブートイメージファイル名

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

関連するコマンド

next-server（P539）

netbios-name-server

DHCP クライアントで利用可能な、NetBIOS WINS ネームサーバを設定します。"no" を前に置くことでサーバリストから NetBIOS 名を削除します。

文法

netbios-name-server *address1* [*address2*]

no netbios-name-server

- *address1* — プライマリ NetBIOS WINS ネームサーバ名を指定
- *address2* — 代替 NetBIOS WINS ネームサーバ名を指定

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

関連するコマンド

netbios-node-type (P542)

netbios-node-type

DHCP クライアントの、NetBIOS ノードタイプを指定します。"no" を前に置くことで設定した NetBIOS ノードタイプを削除します。

文法

netbios-node-type *type*

no netbios-node-type

- *type* — NetBIOS ノードタイプを指定
  - broadcast
  - hybrid（推奨）
  - mixed
  - peer-to-peer

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

関連するコマンド

netbios-name-server（P541）

lease

DHCP クライアントにアサインされた IP アドレスの継続時間を設定します。"no" を前に置くことで初期値にもどします。

文法

lease {*days* [*hours*][*minutes*] | *infinite*}

no lease

- *days* — 日数を指定（範囲：0-364）
- *hours* — 時間を指定（範囲：0-23）
- *minutes* — 分を指定（範囲：0-59）
- *infinite* — 期限無し。このオプションは通常 host コマンドによって、BOOTP クライアントへ手動でアドレスをバウンドする際に使用します。

初期設定

1 日

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

host

DHCP クライアントへ手動でバインドする際に、IP アドレスおよびネットワークマスクを指定します。"no" を前に置くことで設定した IP アドレスを削除します。

文法

host *address* [*mask*]

no host

- *address* — クライアントの IP アドレスを指定します。
- *mask* — クライアントのネットワークマスクを指定します。

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

関連するコマンド

client-identifier（P545）
hardware-address（P546）

client-identifier

DHCP クライアントの識別子を指定します。"no" を前に置くことで設定したクライアント識別子を削除します。

文法

client-identifier {text *text* | hex *hex*}
no client-identifier

- *text* — クライアント識別子を指定します。（範囲：1-15 文字）
- *text* — 16 進数の値

初期設定

なし

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#client-identifier text steve
Console(config-dhcp)#
```

関連するコマンド

host （P544）

hardware-address

DHCP クライアントのハードウェアアドレスを指定します。"no" を前に置くことで設定したハードウェアアドレスを削除します。

文法

hardware-address *hardware-address type*

no hardware-address

- *hardware-address* — クライアントデバイスの MAC アドレスを指定
- *type* — クライアントデバイスで使用されるプロトコル
  - ethernet
  - ieee802
  - fddi

初期設定

タイプが未指定の場合、デフォルトプロトコルは Ethernet になります。

コマンドモード

DHCP Pool Configuration

例

```
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#
```

関連するコマンド

host（P544）

clear ip dhcp binding

DHCP サーバーデータベースから、バインドされた自動アドレスを削除します。

文法

clear ip dhcp binding {*address* | * }

- *address* — アドレスを指定
- * — 全ての自動バインディングを削除

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#clear ip dhcp binding *
Console#
```

関連するコマンド

show ip dhcp binding (P547)

show ip dhcp binding

DHCP サーバ上のバインディングアドレスを表示します。

文法

show ip dhcp binding [*address*]

- *address* — IP アドレスを指定

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show ip dhcp binding

     IP              MAC         Lease  Time       Start
                                (dd/hh/mm/ss)
-------------- ----------------- ---------------- -----------
192.1.3.21    00-00-e8-98-73-21            86400 Dec 25 08:01:57 2002
Console#
```

4.22 VRRP

ルータ冗長性プロトコルは、プライマリ ルータおよび複数のバックアップ ルータをサポートするために、仮想 IP アドレスを使用します。
マスター ルータに障害が発生した時にワークロードを引き継ぐように、バックアップ ルータを構成することができます。また、トラフィック ロードを共有するように構成することもできます。ルータ冗長性の主な目的は、プライマリ ゲートウェイの障害発生時に、固定ゲートウェイで構成されたホスト デバイスがネットワーク コネクティビティを保持できるようにすることです。

コマンド グループ	機能	ページ
Virtual Router Redundancy Protocol	VRRP のインタフェース設定を構成します。	P548

4.22.1 仮想ルータ冗長性プロトコル（VRRP）コマンド

コマンド	機能	モード	ページ
vrrp ip	VRRP を有効にし、仮想ルータの IP アドレスを設定します。	IC	P549
vrrp authentication key	他のルータから受信した VRRP パケットの認証に使用されるキーを構成します。	IC	P550
vrrp priority	VRRP グループ内でのこのルータのプライオリティを設定します。	IC	P551
vrrp timers advertise	マスター仮想ルータの連続するアドバタイズメントの間隔を設定します。	IC	P552
vrrp preempt	現在のマスター仮想ルータよりも高いプライオリティを持つルータが VRRP グループに参加した時、このルータがマスター仮想ルータとして処理を引き継ぐように構成します。	IC	P553
show vrrp	VRRP ステータス情報を表示します。	PE	P554
show vrrp interface	指定インタフェースの VRRP ステータス情報を表示します。	PE	P556
show vrrp router counters	VRRP 統計情報を表示します。	PE	P556
show vrrp interface counters	指定インタフェースの VRRP 統計情報を表示します。	PE	P557
clear vrrp router counters	VRRP ルータの統計情報をクリアします。	PE	P558
clear vrrp interface counters	VRRP インタフェースの統計情報をクリアします。	PE	P558

vrrp ip

インタフェース上の仮想ルータ冗長性プロトコル（VRRP）を有効にし、仮想ルータの IP アドレスを指定します。"no" を前に置くことで、インタフェース上の VRRP が無効になり、IP アドレスが仮想ルータから削除されます。

文法

[no] vrrp *group* **ip** *ip-address*

- *group* — 仮想ルータ グループを識別（範囲 : 1-255）
- *ip-address* — 仮想ルータの IP アドレス

初期設定

仮想ルータ グループは構成されていません。

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 仮想ルータ グループに参加しているすべてのルータのインタフェースは、同じ IP サブネットに属する必要があります。
- 仮想ルータに割り当てられる IP アドレスは、オーナーになるルータ上で予め構成されている必要があります。すなわち、このコマンドで指定された IP アドレスは、仮想ルータ グループの 1 台の、かつ唯一のルータ上にすでに存在している必要があります。また、仮想ルータ アドレスのネットワーク マスクはオーナーから派生します。また、オーナーは、グループ内のマスター仮想ルータとしての役割も果たします。
- 現在の VLAN インタフェース上で複数のセカンダリ アドレスを構成した場合、このコマンドを secondary キーワードとともに使用することで、仮想ルータによってサポートされる任意のセカンダリ アドレスを追加することができます。
- このコマンドを入力すると、VRRP は即座に有効になります。VRRP の他のパラメータ（認証、プライオリティ、アドバタイズメント間隔てなど）をカスタマイズする必要がある場合、最初にこれらのパラメータを構成してから、VRRP を有効にしてください。

例

このコマンドでは、VRRP グループのオーナーとして VLAN 1 のプライマリ インタフェースを使用して、VRRP グループ 1 を作成し、グループのメンバーとしてセカンダリ インタフェースを追加します。

```
Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#
```

vrrp authentication key

他のルータから受信した VRRP パケットの認証に使用されるキーを指定します。"no" を前に置くことで、認証が無効になります。

文法

vrrp *group* **authentication** *key*

no vrrp *group* **authentication**

- *group* — 仮想ルータ グループを識別（範囲 : 1-255）
- *key*— 認証ストリング（範囲 : 1-8 英数字文字）。

初期設定

定義されているキーはありません。

初期設定

なし

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 同じ VRRP グループ内のすべてのルータは、同じ認証キーで構成されている必要があります。
- グループ内の別のルータから VRRP パケットが受信されると、その認証キーは、このルータ上で構成されたストリングと比較されます。キーが合致すれば、メッセージは受理されます。合致しない場合、パケットは廃棄されます。
- プレーン テキスト認証では、現実的なセキュリティは何も提供されません。プレーンテキストは、誤設定されたルータが VRRP に参加することを防ぐためにのみサポートされています。

例

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

vrrp priority

VRRP グループ内でのこのルータのプライオリティを設定します。"no" を前に置くことで、設定を初期値に戻します。

文法

vrrp *group* **priority** *level*

no vrrp *group* **priority**

- *group* — VRRP グループを識別（範囲 : 1-255）
- *level*— VRRP グループ内でのこのルータのプライオリティを設定（範囲 : 1-254）

初期設定

100

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 仮想ルータに使用されるのと同じ IP アドレスの物理インタフェースを持つルータが、マスター仮想ルータになります。現在のマスターが故障した時には、最も高いプライオリティを持つバックアップ ルータがマスター ルータになります。元のマスタールータが障害から回復すると、アクティブなマスター ルータとして再び処理を引き継ぎます。
- 2 つまたはそれ以上のルータが同じ VRRP プライオリティで構成されている場合、現在のマスターの故障時には、最も高い IP アドレスを持つルータが、新規マスター ルータとして選出されます。
- vrrp preempt コマンドによりバックアップ プリエンプト機能が有効になっており、現在マスターとして動作しているルータよりも高いプライオリティを持つバックアップルータがオンラインになった場合、このバックアップ ルータが新規マスターとして処理を引き継ぎます。ただし、元のマスター（VRRP IP アドレスのオーナー）がオンラインに戻ると、常にマスターとしての制御を再開します。

例

```
Console(config-if)#vrrp 1 priority 1
Console(config-if)#
```

関連するコマンド

vrrp preempt（P553）

vrrp timers advertise

マスター仮想ルータが、マスターとしてのその状態を通信するためのアドバタイズメントを送信する間隔を設定します。"no" を前に置くことで、設定を初期値に戻します。

文法

vrrp *group* **timers advertise** *interval*

no vrrp *group* **timers advertise**

- *group* — VRRP **グループを識別（範囲** : 1-255）
- *level*— **マスター仮想ルータがアドバタイズメントを行う間隔（範囲** : 1-255 **秒）**

初期設定

1 **秒**

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- **現在のマスター仮想ルータからの** VRRP **アドバタイズメントには、そのプライオリティとマスターとしての現在の状態に関する情報が含まれています。**
- VRRP **アドバタイズメントは、マルチキャスト アドレス** 224.0.0.8 **へ送信されます。**
- **マルチキャスト アドレスを使用すると、指定** VRRP **グループに参加していないネットワーク デバイスによって処理される必要のあるトラフィックの量を削減できます。**
- **マスター ルータがアドバタイズメントの送信を停止すると、バックアップ ルータは、プライオリティに基づいてマスター ルータの候補となります。マスターとして処理を引き継ごうとする前の** dead **間隔の値は、**hello **間隔の** 3 **倍に** 0.5 **秒を加えたものになります。**

例

```
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#
```

vrrp preempt

現在マスターとして動作しているルータよりも高いプライオリティを持つルータが VRRP グループに参加した時、このルータがマスター仮想ルータとして処理を引き継ぐように構成します。"no" を前に置くことで、プリエンプションが無効になります。

文法

vrrp *group* **preempt** [delay *seconds*]

no vrrp *group* **preempt**

- *group* — VRRP グループを識別（範囲 : 1-255）
- *seconds*— マスターになる宣言を発行するまでの待機時間です（範囲 : 0-120 秒）。

初期設定

プリエンプション : 有効
待機時間 : 0 秒

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- プリエンプト機能が有効になっており、このバックアップ ルータが現在マスターとして動作しているルータよりも高いプライオリティを持つ場合、新規マスターとして処理を引き継ぎます。ただし、元のマスター（VRRP IP アドレスのオーナー）がオンラインに戻ると、常にマスターとしての制御を再開します。
- この遅延を設定することにより、新規ルータが制御を引き継ぐ前に、現在のマスターからアドバタイズメント メッセージを受信するための追加の時間を与えることができます。マスターになろうとしているルータがオンラインになった時、（新規ルータが）現在のアクティブ ルータを実際にプリエンプトする前に、この遅延時間により、ルーティング テーブルの情報を収集する時間が与えられます。

例

```
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#
```

関連するコマンド

vrrp priority（P551）

show vrrp

VRRP のステータス情報を表示します。

文法

show vrrp [brief | *group*]

- brief — このルータ上のすべての VRRP グループに関するサマリー情報を表示
- *group* — VRRP グループを識別します（範囲 : 1-255）

初期設定

なし

コマンド モード

Privileged Exec

コマンド解説

- キーワードを指定せずに、このコマンドを使用すると、このルータ上で構成されたすべての VRRP グループのステータス情報が完全にリスト表示されます。
- このコマンドを brief キーワードとともに使用すると、このルータ上で構成されたすべての VRRP グループのステータスに関する要約情報が表示されます。
- 特定のグループに関するステータス情報を表示するには、グループ番号を指定します。

例

この例では、すべてのグループに関するステータス情報をリスト表示します。

```
Console#show vrrp
  Vlan 1 - Group 1,
  state                          Master
  Virtual IP address            192.168.1.6
  Virtual MAC address            00-00-5E-00-01-01
  Advertisement interval         5 sec
  Preemption                     enabled
  Min delay                       10 sec
  Priority                        1
  Authentication                 SimpleText
  Authentication key             bluebird
  Master Router                  192.168.1.6
  Master priority                 255
  Master Advertisement interval  5 sec
  Master down interval            15
Console#
```

項目	解説
State	このインタフェースの VRRP 役割（マスターまたはバックアップ）です。
Virtual IP address	仮想 IP アドレスのオーナーから派生する仮想 MAC アドレスです。
Virtual MAC address	経路情報が変更された回数
Advertisement interval	マスター仮想ルータが、マスターとしての自身の役割をアドバタイズする間隔です。
Preemption	より高いプライオリティのルータが、現在マスターとして動作しているルータをプリエンプトできるか表示します。
Min delay	より高いプライオリティのルータが、現在マスターとして動作しているルータをプリエンプトするまでの遅延時間です。
Priority	このルータのプライオリティです。
Authentication	パケットの検証に使用される認証モードです。
Authentication key	他のルータから受信した VRRP パケットの認証に使用されるキーです。
Master Router	グループ マスターとして現在動作しているルータの IP アドレスです。
Master priority	グループ マスターとして現在動作しているルータのプライオリティです。
Master Advertisement interval	VRRP マスター上で構成されるアドバタイズメント間隔です。
Master down interval	VRRP マスター上で構成される、ダウン間隔です（ この間隔は、ローカル設定に関わらず、グループ内のすべてのルータで使用されます）。

この例では、すべてのグループに関するステータス情報を簡潔にリスト表示します。

```
Console#show vrrp brief
Interface Grp State Virtual addr Int Pre Prio
-----------------------------------------------------------------
vlan 1    1   Master 192.168.1.6   5   E   1
Console#
```

項目	解説
Interface	VLAN インタフェース
Grp	VRRP グループ
State	このインタフェースの VRRP 役割（マスターまたはバックアップ）です。
Virtual addr	この VRRP グループを識別する仮想アドレスです。
Int	マスター仮想ルータが、マスターとしての自身の役割をアドバタイズする間隔です。
Pre	より高いプライオリティのルータが、現在マスターとして動作しているルータをプリエンプトできるか表示します。
Prio	このルータのプライオリティです。

show vrrp interface

このコマンドでは、指定した VRRP インタフェースのステータス情報を表示します。

文法

show vrrp interface vlan *vlan-id* { brief }

- *vlan-id* — 構成された VLAN インタフェースの識別子（範囲 : 1 ～ 4094）
- brief — このルータ上のすべての VRRP グループに関するサマリー情報を表示

初期設定

なし

コマンドモード

Privileged Exec

例

この例では、VLAN 1 に関するステータス情報を完全にリスト表示します。

```
Console#show vrrp interface vlan 1
  Vlan 1 - Group 1,
  state Master
  Virtual IP address 192.168.1.6
  Virtual MAC address 00-00-5E-00-01-01
  Advertisement interval 5 sec
  Preemption enabled
  Min delay 10 sec
  Priority 1
  Authentication SimpleText
  Authentication key bluebird
  Master Router 192.168.1.6
  Master priority 1
  Master Advertisement interval 5 sec
  Master down interval 15
Console#
```

* 表示される項目に関する説明は、「show vrrp（P554）」を参照してください。

show vrrp router counters

VRRP プロトコル パケット内のエラーに対するカウンタを表示します。

コマンド モード

Privileged Exec

例

```
Console#show vrrp router counters
  Total Number of VRRP Packets with Invalid Checksum : 0
  Total Number of VRRP Packets with Unknown Error : 0
  Total Number of VRRP Packets with Invalid VRID : 0
Console#
```

[注意]　未知のエラーは、未知または非サポート対象のバージョン番号で受信された VRRP パケットを示すことに注意してください。

show vrrp interface counters

指定グループまたはインタフェースで発生した VRRP **プロトコル イベントとエラーのカウンタを表示します。**

文法

show vrrp *group* **interface** vlan *interface* **counters**

- *group* — VRRP **グループを識別（範囲** : 1-255）
- *interface* — **構成された** VLAN **インタフェースの識別子（範囲** : 1-4094）

初期設定

なし

コマンド モード

Privileged Exec

例

```
Console#show vrrp 1 interface vlan 1 counters
  Total Number of Times Transitioned to MASTER : 6
  Total Number of Received Advertisements Packets : 0
  Total Number of Received Error Advertisement Interval Packets : 0
  Total Number of Received Authentication Failures Packets : 0
  Total Number of Received Error IP TTL VRRP Packets : 0
  Total Number of Received Priority 0 VRRP Packets : 0
  Total Number of Sent Priority 0 VRRP Packets : 5
  Total Number of Received Invalid Type VRRP Packets : 0
  Total Number of Received Error Address List VRRP Packets : 0
  Total Number of Received Invalid Authentication Type VRRP Packets : 0
  Total Number of Received Mismatch Authentication Type VRRP Packets : 0
  Total Number of Received Error Packet Length VRRP Packets : 0
Console#
```

clear vrrp router counters

VRRP システムの統計情報をクリアします。

コマンド モード

Privileged Exec

例

```
Console#clear vrrp router counters
Console#
```

clear vrrp interface counters

指定したグループおよびインタフェースの VRRP **システム統計情報をクリアします。**

文法

clear vrrp *group* interface i*nterface* counters

- *group* — VRRP **グループを識別（範囲** : 1-255）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#clear vrrp 1 interface 1 counters
Console#
```

4.23 IP インタフェース

IP アドレスは本機へのネットワーク経由での管理用アクセスの際に使用されます。初期設定では DHCP を使用して IP アドレスの取得を行う設定になっています。IP アドレスは手動で設定することも、又 BOOTP/DHCP サーバから電源投入時に自動的に取得することもできます。また、他のセグメントから本機へのアクセスを行うためにはデフォルトゲートウェイの設定も必要となります。

コマンドグループ	機能	ページ
Basic IP Configuration	インタフェースへ IP アドレス、デフォルトゲートウェイを設定	P559
Address Resolution Protocol (ARP)	静的、動的、プロキシ ARP の設定	P564

4.23.1 基本 IP 設定

コマンド	機能	モード	ページ
ip address	本機への IP アドレスの設定	IC	P560
ip default-gateway	本機と管理端末を接続するためのゲートウェイ設定の表示	GC	P561
show ip interface	本機の IP 設定の表示	PE	P562
show ip redirects	本機のデフォルトゲートウェイ設定の表示	PE	P562
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	P563

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 } { secondary }

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**
- dhcp — IP **アドレスを** DHCP **から取得**
- secondary — **セカンダリ** IP **アドレスを指定**

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。**

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（P565）

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 (P562)

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（P562）

show ip redirects

デフォルトゲートウェイの設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

関連するコマンド

ip default-gateway（P561）

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

サイズ 32bytes、カウント 5 回

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:
Å@Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

関連するコマンド

interface（P378）

4.23.2 ARP

コマンド	機能	モード	ページ
arp	本機への IP アドレスの設定	GC	P564
arp-timeout	本機と管理端末を接続するためのゲートウェイ設定の表示	GC	P565
clear arp-cache	BOOTP/DHCP クライアントリクエストの送信	PE	P565
show arp	本機の IP 設定の表示	NE, PE	P566
ip-proxy-arp	本機のデフォルトゲートウェイ設定の表示	VC	P566

arp

ARP キャッシュの静的エントリを追加します。"no" を前に置くことでキャッシュからエントリを削除します。

文法

arp *ip-address hardware-address*

no arp *ip-address*

- *ip-address* — IP アドレスを指定します。
- *hardware-address* — ハードウェアアドレスを指定します。

初期設定

エントリなし

コマンドモード

Global Configuration

例

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

関連するコマンド

clear arp-cache（P565）
show arp（P566）

arp-timeout

ARP キャッシュの動的エントリ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値にもどします。

文法

arp-timeout *seconds*
no arp-timeout

- *seconds* — 動的エントリが ARP キャッシュに残存する時間（範囲：300-86400　86400 は一日）

初期設定

1200 秒（20 分）

コマンドモード

Global Configuration

例

```
Console(config)#arp-timeout 900
Console(config)#
```

clear arp-cache

すべての動的エントリを ARP キャッシュのから削除します。

コマンドモード

Privileged Exec

例

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp

ARP キャッシュのエントリを表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show arp
Arp cache timeout: 1200 (seconds)
  IP Address        MAC Address        Type     Interface
---------------  ----------------- --------- -----------
       10.1.0.0  ff-ff-ff-ff-ff-ff  other         1
     10.1.0.254  00-00-ab-cd-00-00  other         1
     10.1.0.255  ff-ff-ff-ff-ff-ff  other         1
   123.20.10.123 02-10-20-30-40-50  static        2
    345.30.20.23 09-50-40-30-20-10  dynamic       3

Total entry : 5
Console#
```

ip-proxy-arp

プロキシ ARP を有効にします。"no" を前に置くことで無効にします。

文法

[no] ip proxy-arp

初期設定

無効

コマンドモード

Interface Configuration (VLAN)

例

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

4.24 IP ルーティング

本機は IP ルーティング機能をサポートしており、ルーティングパスの管理は、静的な経路の設定（P567）、または RIP による動的な設定（P574）により可能になります。IP ルーティング機能を有効に設定（していると、本機はワイヤスピードを実現するルータ同様に動作するため、異なる IP インタフェースを介した VLAN 間通信や、外部 IP ネットワークへのトラフィックのルーティングを行います。しかし、本機の初期設定ではルーティング機能は設定されていません。ルーティング機能を使用するには、既存のルータ製品のように、最初にこれらの設定を行う必要があります。

工場出荷時の設定では、ポートはすべて単一の VLAN に所属し、レイヤ 2 機能のみを使用するようになっています。そのため、まず、各ユーザグループまたはトラフィックのアプリケーション別に VLAN を作成し、同じグループに所属するすべてのポートを各 VLAN に割り当て、それから各 VLAN に IP インタフェースを設定する必要があります。ネットワークを複数の異なる VLAN に分けることによって、レイヤ 2 レベルで分割されているサブネットワークで分けることができます。同一サブネット内でやり取りされるトラフィックは、レイヤ 2 のスイッチング機能を使用して通信されます。そして、必要な場合には、レイヤ 3 のスイッチング機能を使用して VLAN 間通信ができることになります。

各 VLAN はレイヤ 3 での仮想的なインタフェースに相当します。この仮想インタフェースに対してネットワークアドレスを設定しさえすれば、トラフィックは、異なるサブネット間でレイヤ 3 レベルでルーティングされるようになります。

コマンドグループ	機能	ページ
Global Routing Configuration	静的または動的ルーティングのための、グローバルパラメータの設定および、ルーティングテーブルや、情報交換のためにしようされるプロトコルの統計の表示。	P567
Routing Information Protocol （RIP）	グローバルまたはインタフェースで RIP のパラメータを設定	P574
Open Shortest Path First （OSPF）	グローバルまたはインタフェースで OSPF のパラメータを設定	P574

4.24.1 グローバルルーティング設定

コマンド	機能	モード	ページ
IP routing	静的または動的 IP ルーティングを有効化	GC	P568
IP route	静的ルートの設定	GC	P569
clear ip route	ルーティングテーブルから、指定したエントリを削除	PE	P570
show ip route	ルーティングテーブル内の指定したエントリを表示	PE	P571
show ip host-route	周知のルートと関連付けられたインタフェースの表示	PE	P572
show ip traffic	IP、ICMP、UDP、TCP および ARP プロトコルの統計情報を表示	PE	P572

IP routing

IP ルーティングを有効にします。"no" を前に置くことで 無効にします。

文法

[no] ip routing

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- **このコマンドは、静的 / 動的両方のユニキャストルーティングに影響します。**
- **IP ルーティングを有効にすると、すべての IP パケットは静的にまたは RIP により動的にルーティングされ、非 IP プロトコル（NetBuei、NetWare、AppleTalk など）のパケットは MAC アドレスでスイッチングされます。IP ルーティングを無効にすると、すべてのパケットは、MAC アドレスのみでフィルタリングとフォワーディングされてスイッチングされます。**

例

```
Console(config)#ip routing
Console(config)#
```

ip route

静的ルートの設定を行います。"no" を前に置くことで、設定された静的ルートを削除します。

文法

ip route { *destination-ip netmask* | default } { *gateway* } [metric *metric*]

no ip route { *destination-ip netmask* | default | * }

- *destination-ip* — **送信先ネットワークの** IP **アドレス、サブネットマスクまたはホスト**
- *netmask* — IP **サブネットに関連するネットワークマスク。このマスクは、特定のサブネットにルーティングするために使用するホストアドレスのビットを識別します**
- default — **このエントリをデフォルトルートにする。**
- *gateway* — **このルートのゲートウェイ** IP **アドレス**
- *metric* — **このインタフェースの** RIP **コストを選択（範囲：**1-5 **初期設定** 1）
- * — **全ての静的ルーティングテーブルのエントリを削除。**

初期設定

静的ル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

- **本機は、最大** 64 **の静的エントリを設定することができます。**
- **もし、静的および動的パスが同じ最低コストを所持する場合、静的パスが動的パスよりも優先されます。**

例

本例では、すべてのトラフィックをサブネット 192.168.1.10 **でルータ** 192.168.5.254 **へ転送します。**

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

clear ip route

IP ルーティングテーブルから、動的学習エントリを削除します。

文法

clear ip route { *network* [*netmask*] | * }

- *network* — ネットワークサブネットアドレス
- *netmask* — IP サブネットに関連するネットワークマスク。このマスクは、特定のサブネットにルーティングするために使用する、ホストアドレスのビットを識別します。
- * — 全ての静的ルーティングテーブルのエントリを削除。

初期設定

全ての動的ルーティングテーブルのエントリを削除。

コマンドモード

Privileged Exec

コマンド解説

- 本コマンドは、動的学習ルートのみ削除を行います。
- "no ip address" コマンドはローカルインタフェースを削除するために使用します。
- "no ip route" コマンドは静的ルートを削除するために使用します。

例

```
Console#clear ip route 10.1.5.0
Console#
```

show ip route

IP ルーティングテーブル情報を表示します。

文法

show ip route [config | *address* [*netmask*]]

- config — 全ての静的ルーティングエントリを表示します。
- *address* — 送信先ネットワークの IP アドレス、サブネットワーク、ホスト
- *netmask* — IP サブネットに関連するネットワークマスク。このマスクは、特定のサブネットにルーティングするために使用する、ホストアドレスのビットを識別します。

コマンドモード

Privileged Exec

例

```
Console#show ip route

   Ip Address       Netmask       Next Hop    Protocol  Metric Interface
--------------- -------------- ------------- ---------- ------ ---------
        0.0.0.0        0.0.0.0   10.2.48.102     static      0         1
      10.2.48.2  255.255.252.0    10.2.48.16      local      0         1
       10.2.5.6  255.255.255.0     10.2.8.12        RIP      1         2
       10.3.9.1  255.255.255.0    10.2.9.254 OSPF-intra      2         3

Total entry: 4
Console#
```

項目	解説
IP Address	送信先ネットワーク、サブネットワークまたはホストの IP アドレス。IP アドレス 0.0.0.0 は本機のデフォルトゲートウェイを示すことに注意してください。
Netmask	IP サブネットに関連付けられているネットマスク。このマスクは、特定のサブネットにルーティングされる際に使用されるホストアドレスのビットを識別します
Next Hop	経路のネクストホップ（ゲートウェイ）の IP アドレス
Protocol	経路情報を生成した方法 / プロトコル名。（表示項目：local、static、RIP）
Metric	インタフェースのコスト
Interface	VLAN インタフェース

show ip host-route

既知ルータに関連付けられたインタフェースを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip host-route
Total count: 0
 IP address                    Mac address        VLAN     Port
 --------------------    --------------------   ------   ------
 192.168. 1.250          00-00-30-01-01-01        3       1/ 1
  10. 2. 48. 2           00-00-30-01-01-02        1       1/ 1
  10. 2. 5. 6            00-00-30-01-01-03        1       1/ 2
  10. 3. 9. 1            00-00-30-01-01-04        2       1/ 3

Console#
```

項目	解説
IP Address	送信先ネットワーク、サブネットワークまたはホストの IP アドレス。
MAC アドレス	IP アドレスに対応したフィジカルレイヤアドレス
VLAN	この IP アドレスにつながる VLAN
Port	この IP アドレスにつながるポート

show ip traffic

UIP、ICMP、UDP、TCP および ARP プロトコルの解析情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip traffic
IP statistics:
  Rcvd:  5 total, 5 local destination
         0 checksum errors
         0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
         0 fragmented, 0 couldn't fragment
  Sent:  9 generated
         0 no route
ICMP statistics:
  Rcvd:  0 checksum errors, 0 redirects, 0 unreachable, 0 echo
         5 echo reply, 0 mask requests, 0 mask replies, 0 quench
         0 parameter, 0 timestamp
  Sent:  0 redirects, 0 unreachable, 0 echo, 0 echo reply
         0 mask requests, 0 mask replies, 0 quench, 0 timestamp
         0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd:  0 total, 0 checksum errors, 0 no port
  Sent:  0 total
TCP statistics:
  Rcvd:  0 total, 0 checksum errors
  Sent:  0 total
ARP statistics:
  Rcvd:  0 requests, 1 replies
  Sent:  1 requests, 0 replies
Console#
```

4.24.2 RIP

コマンド	機能	モード	ページ
router rip	RIP ルーティングプロトコルを有効化	GC	P575
default-metric	デフォルトメトリックを設定	RC	P576
timers basic	基本タイマーを設定	RC	P577
network	RIP ルーティングに使用されるネットワークインタフェースを指定	RC	P578
neighbor	情報を交換する、隣接ルータを定義	RC	P579
version	RIP バージョンを設定	RC	P579
redistribute	１つのドメインからもう１つまでのルートを再配布	RC	P580
ip rip receive version	RIP レシーババージョンをネットワークインタフェースに設定	IC	P581
ip rip send version	RIP センドバージョンを設定	IC	P582
ip split-horizon	Split Horizon または Poison Reverse の有効化	IC	P583
ip rip authentication key	RIPv2 パケット認証の有効化および、パスワードを設定	IC	P583
ip rip authentication mode	RIPv2 パケット認証のタイプを指定	IC	P584
show rip globals	グローバル設定および RIP 統計情報の表示	PE	P585
show ip rip	各ネットワークインタフェースごとの、RIP 設定情報の表示	PE	P586

router rip

全ての IP インタフェースで RIP ルーティングを有効にします。"no" を前に置くことで、無効にします。

文法

router rip
no router rip

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- RIP はルータが経路情報を交換する方法を定義するのに使用されます。
- 本コマンドはルータ設定モードへの移行にも使用します。

例

```
Console(config)#router rip
Console(config-router)#
```

関連するコマンド

network （P578）

default-metric

デフォルトメトリック値を設定します。"no" を前に置くことで、初期設定値にもどします。

文法

default-metric *metric-value*
no default-metric

- *metric-value* — 外部ルータにアサインされたメトリック値（範囲：0-15）

初期設定

8

コマンドモード

Privileged Exec

コマンド解説

- 静的な経路情報の再分配のメトリックが設定されていない場合、default-metric コマンド（P576）により、読み込むすべての外部経路情報に使用するメトリック値を設定します。
- 経路のメトリックは、互換性のないメトリックを含む外部の経路情報を再分配するという問題を解決するために使用されなくてはなりません。
- 他のプロトコルから RIP へ経路情報を再分配する場合、小さなメトリックを使用することを推奨します。大きなメトリックを設定すると、RIP への外部経路情報の再分配の実用性が制限されてしまいます。例えば、経路情報の再分配にメトリック 10 を設定した場合、これらの経路情報は 5 ホップ先のルータまで（ここでメトリックが最大のホップ数 15 を超過するため）しか広告されません。小さなメトリック 1 を設定することにより、RIP のドメイン内で許可された最大のホップ数で読み込まれた経路で通信することができます。しかし、小さいメトリックを採用した場合、経路でループが発生する可能性が高くなります。たとえば、複数の再分配箇所があり、ルータが同じ外部ネットワークについて、元のソースからではなく再分配ポイントから、より良いメトリックを学習するようなケースが発生します。

例

本例ではデフォルトメトリック値を 5 に設定しています。

```
Console(config-router)#default-metric 5
Console(config-router)#
```

関連するコマンド

redistribute（P580）

timers basic

RIP アップデートタイマー、タイムアウトタイマーおよび Garbage コレクションタイマーの設定を行います。"no" を前に置くことで、初期設定値にもどします。

文法

timers basic *update-seconds*
no timers basic

- *update-seconds* — アップデート情報の送信間隔を設定します。この値を 6 倍した値がタイムアウト時間として、4 倍した値がガベージコレクション時間として設定されます。（範囲：15-60 秒）

初期設定

Update: 30 秒

Timeout: 180 秒

Garbage collection: 120 秒

コマンドモード

Router Configuration

コマンド解説

- アップデートタイマーはすべての基本的な RIP プロセスを制御するのに使用される、重要なタイマーです。
- アップデートタイマーの間隔を短くしすぎると、ルータがアップデートの処理に膨大な時間を費やすことになります。一方、長くしすぎるとネットワーク構成の変更を検出しにくいルーティングプロトコルになってしまいます。
- アップデートタイマーは、同一ネットワークのすべてのルータに同じ値を設定しなくてはなりません。

例

```
Console(config-router)#timers basic 15
Console(config-router)#
```

network

RIP ルーティングプロセスに含まれる、ネットワークインタフェースを指定します。"no" を前に置くことでエントリを削除します。

文法

network *subnet-address*
no network *subnet-address*

- *subnet-address* — サブネットの IP アドレス

初期設定

ネットワークは指定されていません。

コマンドモード

Router Configuration

コマンド解説

- このコマンドで設定したインタフェースにのみ RIP のアップデート情報が送信されます
- サブネットアドレスは、設定したアドレスの最初のフィールドに基付き、クラス A、B、C のいずれかに解釈されます。つまり、サブネットアドレス nnn.xxx.xxx.xxx を入力した場合、最初のフィールド（nnn）がクラスを決定します。
  - 0 ～ 127 の場合クラス A となり、ネットワークアドレスの最初のフィールドのみ使用されます。
  - 128 ～ 191 の場合はクラス B となり、ネットワークアドレスの最初から 2 つのフィールドのみ使用されます。
  - 192 ～ 223 の場合はクラス C となり、ネットワークアドレスの最初から 3 つのフィールドのみ使用されます。

例

本例では 10.1.0.0 のネットワークインタフェースを RIP のルーティングプロセスに組み込みます。

```
Console(config-router)#network 10.1.0.0
Console(config-rou
```

neighbor

隣接ルータを定義します。"no" を前に置くことでエントリを削除します。

文法

neighbor *ip-address*

no neighbor *ip-address*

- *ip-address* — MAC アドレスにマップされた IP アドレス

初期設定

隣接ルータは定義されていません。

コマンドモード

Router Configuration

例

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

version

ルータでグローバルに使用される RIP バージョンを指定します。"no" を前に置くことで初期設定値にもどします。

文法

version {1 | 2}

no version

- 1 — RIP バージョン 1
- 2 — RIP バージョン 2

初期設定

RIP バージョン 1

コマンドモード

Router Configuration

例

```
Console(config-router)#version 2
Console(config-router)#
```

redistribute

経路情報の再分配を設定します。"no" を前に置くことでこの機能を無効にします。

文法

redistribute (static} [metric <*metric-value*>]

no redistribute (static} [metric <*metric-value*>]

- static — **静的ルート**
- *metric-value* — **メトリック値（範囲：**1-15）

初期設定

再分配：無効

メトリック値："default-metric" **コマンドで設定された値**

コマンドモード

Router Configuration

コマンド解説

- **静的な経路情報の再分配のメトリックが設定されていない場合、**default-metric **コマンド（**P576）**により、読み込むすべての外部経路情報に使用するメトリック値を設定します。**
- **経路のメトリックは、互換性のないメトリックを含む外部の経路情報を再分配するという問題を解決するために使用されなくてはなりません。**
- **他のプロトコルから** RIP **へ経路情報を再分配する場合、小さなメトリックを使用することを推奨します。大きなメトリックを設定すると、**RIP **への外部経路情報の再分配の実用性が制限されてしまいます。例えば、経路情報の再分配にメトリック** 10 **を設定した場合、これらの経路情報は** 5 **ホップ先のルータまで（ここでメトリックが最大のホップ数** 15 **を超過するため）しか広告されません。小さなメトリック** 1 **を設定することにより、**RIP **のドメイン内で許可された最大のホップ数で読み込まれた経路で通信することができます。しかし、小さいメトリックを採用した場合、経路でループが発生する可能性が高くなります。たとえば、複数の再分配箇所があり、ルータが同じ外部ネットワークについて、元のソースからではなく再分配ポイントから、より良いメトリックを学習するようなケースが発生します。**

例

本例では静的な経路情報を再分配し、これらの経路のメトリック値をすべて 3 **に設定しています。**

```
Console(config-router)#redistribute static metric 3
Console(config-router)#
```

ip rip receive version

RIP ルーティングプロセスに組み込む各インタフェースに対し、受信に使用するプロトコルメッセージの種類（RIP 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値にもどします。

文法

ip rip receive version [none | 1 | 2 | 1 2]

no ip rip receive version

- none — RIP パケットは許可しません
- 1 — RIP v 1 パケットのみ許可
- 2 — RIP v 2 パケットのみ許可
- 1 2 — RIP v 1 または RIP v 2 パケットを許可

初期設定

Global RIPv1 - RIPv1 or RIPv2 packets

Global RIPv2 - RIPv2 packets

コマンドモード

Router Configuration

コマンド解説

- Receive Version は次の選択肢から設定できます。
  - ローカルネットワークですべてのルータがRIPv1またはRIPv2のどちらか一方だけを使用している場合は、それぞれ "RIPv1" または "RIPv2" を設定します。
  - ローカルネットワークでルータが RIPv1 と RIPv2 の両方を使用している場合は、"RIPv1 or RIPv2" を設定します。
  - 特定のインタフェースのルーティングテーブルに動的に保存させたくない場合は、"Do Not Receive" を設定します。（静的にのみルーティングさせたいインタフェースの場合など）

例

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

ip rip send version

RIP ルーティングプロセスに組み込む各インタフェースに対し、送信に使用するプロトコルメッセージの種類（RIP 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値にもどします。

文法

ip rip send version [none | 1 | 2 | v2-broadcast]

no ip rip send version

- none — RIP パケットは許可しません。
- 1 — RIP v 1 パケットのみ許可。
- 2 — RIP v 2 パケットのみ許可。
- v2-broadcast — ルート情報は、他の RIPv2 ルータにブロードキャストされます。

初期設定

Global RIPv1 - ルート情報は、他の RIPv2 ルータにブロードキャスト

Global RIPv2 - RIPv2 packets

コマンドモード

Router Configuration

コマンド解説

- Send Version は次の 3 つの選択肢から設定できます
  - ローカルネットワークのすべてのルータがRIPv1またはRIPv2のどちらか一方だけを使用している場合は、それぞれ "RIPv1" または "RIPv2" を設定します。
  - ネットワークの他のルータに経路情報をブロードキャストする際、RIPv2 で通常要求されるマルチキャストではなく、RIPv2 の広告リストを使用する場合は "RIPv1 Compatible" を設定します。（このモードを使用すると、RIPv1 のルータはプロトコルメッセージを受信でき、RIPv2 のルータは RIPv2 で提供される追加情報（サブネットマスク、ネクストホップ、および認証情報）を受信できます。
  - ネットワークに接続している他のルータから広告される経路情報を受動的にモニタリングするだけの場合は、"Do Not Send" を設定します。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

関連するコマンド

redistribute（P580）

ip split-horizon

スプリットホライズン（経路情報を送信してきたインタフェースポートには経路情報を広告しない）を有効にします。"no" を前に置くことで無効にします。

文法

ip split-horizon [poison-reverse]
no ip split-horizon

- poison-reverse — その経路情報を送信してきたインタフェースポートに経路情報を広告するが、距離ベクトル型のメトリックは無限大に設定します。（これにより収束時間を短縮できます）

初期設定

split-horizon

コマンドモード

Interface Configuration(VLAN)

例

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

ip rip authentication key

インタフェースに RIPv2 パケット認証を有効化および認証キーを指定します。"no" を前に置くことで認証を無効にします。

文法

ip rip authentication key *key-string*

no ip rip authentication

- *key-string* — 認証に使用されるパスワード（範囲：1-16 文字）

初期設定

無効

コマンドモード

Interface Configuration（VLAN）

例

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication key small
Console(config-if)#
```

関連するコマンド

ip rip authentication mode（P584）

ip rip authentication mode

インタフェースに認証タイプを設定します。"no" を前に置くことで初期設定値に戻します。

[注意] 現在のファームウェアバージョンでは、シンプルパスワードのみサポートしています。

文法

ip rip authentication mode {text}
no ip rip authentication mode

- text — **シンプルパスワードを指定**

初期設定

認証無し

コマンドモード

Interface Configuration（VLAN）

コマンド解説

- **本コマンドは、動的学習ルートのみ削除を行います。**
- "no ip address" **コマンドはローカルインタフェースを削除するために使用します。**
- "no ip route" **コマンドは静的ルートを削除するために使用します。**

例

```
Console#clear ip route 10.1.5.0
Console#
```

関連するコマンド

ip rip authentication key（P583）

show rip globals

RIP のグローバル設定情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show rip globals

RIP Process: Enabled
Update Time in Seconds: 30
Number of Route Change: 0
Number of Queries: 1
Console#
```

項目	解説
RIP Process	RIP の有効 / 無効の表示
Update Time in Seconds	RIP が経路情報を広告する間隔（初期設定：30 秒）
Number of Route Changes	経路情報が変更された回数
Number of Queries	本機がルーティングデータベースの照会を受けた回数

show ip rip

RIP インタフェース設定情報を表示します。

文法

show ip rip {configuration | status | peer}

- configuration — **シインタフェースごとの** RIP **設定**
- status — **各インタフェースのルーティングメッセージのステータスを表示**
- peer — **隣接ルータの情報を表示**

初期設定

認証無し

コマンドモード

Privileged Exec

例

```
Console#show ip rip configuration

     Interface      SendMode     ReceiveMode      Poison
Authentication
--------------- --------------- ------------- --------------
------------------
    10.1.0.253   rip1Compatible   RIPv1Orv2    SplitHorizon
noAuthentication
    10.1.1.253   rip1Compatible   RIPv1Orv2    SplitHorizon
noAuthentication
Console#show ip rip status

     Interface   RcvBadPackets   RcvBadRoutes    SendUpdates
--------------- --------------- -------------- ---------------
    10.1.0.253               0              0              13
    10.1.1.253               0              0              13
Console#show ip rip peer

           Peer  UpdateTime   Version   RcvBadPackets   RcvBadRoutes
--------------- ------------ --------- --------------- -------------
    10.1.0.254          1625         2               0             0
    10.1.1.254          1625         2               0             0
Console#
```

項目	解説
show ip rip configuration	
Interface	**インタフェースの** IP **アドレス**
SendMode	**このインタフェースが送信する** RIP **のバージョン**（none、RIPv1、RIPv2、rip1Compatible）
ReceiveMode	**このインタフェースが受信する** RIP **のバージョン**（none、RIPv1、RIPv2、RIPv1Orv2）

Poison	スプリットホライズン、ポイズンリバースまたは安定性の確保手段はいずれも選択していない、についての表示
Authentication	単純なパスワードによる認証か、認証設定していないかについての表示
show ip rip status	
Interface	インタフェースの IP アドレス
RcvBadPackets	受信した、RIP エラーパケット数
RcvBadRoutes	受信した、障害のある経路の数
SendUpdates	経路の変更が発生した数
show ip rip peer	
Peer	RIP の隣接ルータの IP アドレス
UpdateTime	ピアの隣接ルータから直前に経路情報を受信した時間
Version	ピアの隣接ルータから RIPv1 または RIPv2 どちらのパケットを受信したか
RcvBadPackets	ピアの隣接ルータから受信した、RIP エラーパケット数
RcvBadRoutes	ピアの隣接ルータから受信した、障害のある経路の数

4.24.3 OSPF

コマンド	機能	モード	ページ
General Configuration			
router ospf	OSPF を有効または無効にします。	GC	P590
router-id	このデバイスのルータ ID を設定します。	RC	P591
compatible rfc1583	RFC 1583 (OSPFv1) を使用して、サマリー ルートのコストを計算します。	RC	P592
default-information originate	自律システム（Autonomous System; AS）へのデフォルトの外部ルートを生成します。	RC	P593
timers spf	連続する SPF 計算間のホールド タイムを構成します。	RC	P594
Route Metric and Summaries			
area range	ABR によってアドバタイズされるルートを要約します。	RC	P595
area default-cost	スタブまたは NSSA へ送信されるデフォルトサマリールートのコストを設定します。	RC	P596
summary-address	ASBR によってアドバタイズされるルートを要約します。	RC	P597
redistribute	1 つのルーティング ドメインから別のルーティング ドメインへルートを再配布します。	RC	P598
Area Configuration			
network area	指定したインタフェースを特定のエリアに割り当てます。	RC	P599
area stub	LSA を送信または受信できないスタブ エリアを定義します。	RC	P600
area nssa	外部ルートをインポートできる、準スタブ エリアを定義します。	RC	P601
area virtual-link	エリア境界ルータからバックボーンへの仮想リンクを定義します。	RC	P603
Interface Configuration			
ip ospf authentication	インタフェースの認証タイプを指定します。	IC	P605
ip ospf authentication-key	隣接ルータによって使用されるシンプル パスワードを割り当てます。	IC	P606
ip ospf message-digest-key	MD5 認証を有効にし、インタフェース用のキーを設定します。	IC	P607
ip ospf cost	インタフェース上でのパケット送信コストを指定します。	IC	P608
ip ospf dead-interval	Hello パケットが受信されないまま時間が経過すると、隣接ルータによってルータのダウンが宣言されるまでの間隔を設定します。	IC	P609
ip ospf hello-interval	Hello パケットの送信間隔を指定します。	IC	P610
ip ospf priority	指定ルータの決定に使用されるルータ プライオリティを設定します。	IC	P610
ip ospf retransmit-interval	リンクステート アドバタイズメント（LSA）を再送信する間隔を指定します。	IC	P611
ip ospf transmit-delay	インタフェースでリンクステート アップデート パケットを送信するまでの時間を予測します。	IC	P612
Display Information			
show ip ospf	ルーティング プロセスに関する一般情報を表示します。	PE	P613
show ip ospf border-routers	エリア境界ルータ（Area Border Router; ABR）および自律システム境界ルータ（Autonomous SystemBoundaryRouter; ASBR）のルーティング テーブル エントリを表示します。	PE	P614

show ip ospf database	データベース内の各種 LSA に関する情報を表示します。	PE	P615
show ip ospf interface	インタフェース情報を表示します。	PE	P622
show ip ospf neighbor	隣接ルータ情報を表示します。	PE	P623
show ip ospf summary-address	すべてのサマリー アドレスの再配布情報を表示します。	PE	P624
show ip ospf virtual-links	仮想リンクのパラメータと隣接状態を表示します。	PE	P624

router ospf

スイッチ上のすべての IP インタフェースで Open Shortest Path First(OSPF) を有効にします。"no" を前に置くことで、無効になります。

文法

[no] **router ospf**

コマンド モード

Global Configuration

初期設定

無効

コマンド解説

- OSPF は、ルータがルーティング テーブル情報を交換する方法を指定するのに使用されます。

例

```
Console(config)#router ospf
Console(config-router)#
```

関連するコマンド

network area （P599）

router-id

自律システム内のこのデバイスに対して一意のルータ ID **を割り当てます。**"no" **を前に置くことで、デフォルトのルータ識別方式（最も小さいインタフェース アドレス）が使用されます。**

文法

router-id *ip-address*

no router-id

- *ip-address*— IP **アドレスと同じ形式でルータ** ID **を指定します。**

コマンドモード

Router Configuration

初期設定

最も小さいインタフェース アドレス

コマンド解説

- **ルータ** ID **は、自律システム内のすべてのルータに対して一意である必要があります。最も小さいインタフェース アドレスに基づくデフォルト設定を使用することで、各ルータ** ID **が一意であることを保証できます。また、ルータ** ID **は** 0.0.0.0 **または** 255.255.255.255 **には設定できないことに注意してください。**
- **このルータが、すでに隣接ルータを登録している場合、ルータのリブート時または** norouter ospf **の後に** router ospf **コマンドを入力して手動で再起動した時、新規のルータ** ID **が使用されます。**
- **あるエリアに対する指定ルータまたはバックアップ指定ルータの候補となるルータのプライオリティ値が等しい場合、最も大きい** ID **を持つルータが選出されます。**

例

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

関連するコマンド

router ospf（P590）

compatible rfc1583

RFC 1583 (OSPFv1) を使用して、サマリー ルートのコストを計算します。"no" を前に置くことで、RFC 2328 (OSPFv2) を使用してコストを計算します。

文法

[no] compatible rfc1583

コマンドモード

Router Configuration

初期設定

RFC 1583 互換

コマンド解説

OSPF ルーティング ドメイン内のすべてのルータは、サマリー ルートの計算に同じ RFC を使用する必要があります。

例

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```

default-information originate

自律システム（Autonomous System; AS）へのデフォルトの外部ルートを生成します。"no" を前に置くことで、この機能が無効になります。

文法

default-information originate [always] [metric *interface-metric*] [metric-type *metric-type*]

no default-information originate

- always — ルータにデフォルト ルートがあるかどうかに関わらず、ローカル AS に対して常にデフォルト ルートをアドバタイズします。（P569 の「ip route」を参照）
- *interface-metric* — デフォルト ルートに割り当てられるメトリックです（範囲 : 1 ～ 65535、デフォルト : 10）
- *metric-type* — デフォルト ルートのアドバタイズに使用される外部リンクのタイプです（オプション : Type 1、Type 2、デフォルト : Type 2）

コマンドモード

Router Configuration

初期設定

無効

コマンド解説

- デフォルトの外部ルートに対するメトリックは、ASBR から出て AS 内の他のルータを通過するトラフィックのパス コストを計算するのに使用されます。
- このコマンドを使用してルーティング ドメイン（すなわち自律システム ; AS）へルートを再配布すると、このルータは自動的に自律システム境界ルータ（ASBR）になります。ただし、デフォルトでは、ASBR は、ルーティング ドメインへのデフォルトルートを生成しません。
- always キーワードを使用すると、ルータは、デフォルトの外部ルートが実際には存在しない場合でも、自身を AS へのデフォルト外部ルートとしてアドバタイズします（デフォルト ルートを定義するには、ip route コマンドを使用します）。
- always キーワードを使用しないと、ルータが AS へのデフォルト外部ルートとしてアドバタイズできるのは、redistribute コマンドにより、RIP またはスタティック ルーティングを介して外部ルートがインポートされており、このようなルートが既知である場合のみです。
- タイプ 1 ルート アドバタイズメントでは、外部ルート メトリックに内部コストを追加します。タイプ 2 ルートは、内部コスト メトリックを追加しません。タイプ 2 ルー
- トを比較する時、複数のタイプ 2 ルートが同じコストを持っている場合、内部コストはタイブレーカーとしてのみ使用されます。

例

この例では、自律システムにアドバタイズされるデフォルト外部ルートにメトリック 20 を割り当て、これをタイプ 2 外部メトリックとして送信します。

```
Console(config-router)#default-information originate metric 20
metric-type 2
Console(config-router)#
```

関連するコマンド

ip route（P569）
redistribute（P598）

timers spf

連続する 2 つの SPF （最短パス優先）計算のホールド タイムを構成します。"no" を前に置くことで、設定を初期値に戻します。

文法

timers spf *spf-holdtime*

no timers spf

- *spf-holdtime* — **連続する 2 つの SPF 計算の最小間隔です（範囲** : 0 ～ 65535 **秒）。**

コマンドモード

Router Configuration

初期設定

10 秒

コマンド解説

- SPF **ホールドタイムを** 0 **に設定すると、連続する計算間に遅延がまったくないことになります。**
- **値を小さくすると、ルータは高速に新規パスをスイッチングできますが、**CPU **処理時間がより長くかかります。**

例

```
Console(config-router)#timers spf 20
Console(config-router)#
```

area range

エリア境界ルータ（ABR）によってアドバタイズされるルートを要約します。"no" **を前に置くことで、この機能が無効になります。**

構文

[no] area *area-id* **range** *ip-address netmask* [advertise | not-advertise]

- *area-id* — **ルートを要約するエリアを識別します（エリア** ID **は、**IP **アドレスと同じ形式である必要があります）**
- *ip-address* — **要約するルートのベース アドレスです**
- *netmask* — **サマリー ルートのネットワーク マスクです**
- advertise — **指定されたアドレス範囲をアドバタイズします**
- not-advertise — **サマリーは送信されず、ルートは残りのネットワークから隠されたままです**

コマンドモード

Router Configuration

初期設定

無効

コマンド解説

- **このコマンドは、エリア間ルートをアドバタイズするのに使用されます。**
- **ルートがアドバタイズされるよう設定されている場合、ルータは、このコマンドで指定された各アドレス範囲に対して、タイプ** 3 **サマリー** LSA **を発行します。**
- **このルータは、各エリア範囲につき最大** 64 **のサマリー ルートをサポートします。**

例

この例では、10.2.x.x **の範囲内にあるすべてのエリア ルートのサマリー アドレスを作成します。**

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0
advertise
Console(config-router)#
```

area default-cost

エリア境界ルータ（ABR）からスタッブ エリアまたは準スタブ エリア（not-so-stubby area ; NSSA**）へ送信されるデフォルト サマリー ルートのコストを指定します。**"no" **を前に置くことで、割り当てられたデフォルト コストが削除されます。**

構文

area *area-id* **default-cost** *cost*

no area *area-id* **default-cost**

- *area-id* — **スタブまたは** NSSA **の識別子です。**IP **アドレスと同じ形式である必要があります**
- *cost* — **スタブまたは** NSSA **へ送信されるデフォルト サマリー ルートのコストです（範囲：**0-1677215**）**

コマンドモード

Router Configuration

初期設定

1

コマンド解説

- **ノーマル エリアに対してこのコマンドを入力すると、そのエリアはスタブに変わります。**
- **デフォルト コストが「**0**」に設定されている場合、ルータは、接続されたスタブまたは** NSSA **に対してデフォルト ルートをアドバタイズしません。**

例

```
Console(config-router)#area 10.3.9.0 default-cost 10
Console(config-router)#
```

関連するコマンド

area stub（P600）

summary-address

他のプロトコルから学習したルートを集約します。"no" を前に置くことで、サマリー アドレスが削除されます。

文法

[no] summary-address *summary-address netmask*

- *summary-address*— **アドレス範囲をカバーするサマリー アドレスです**
- *netmask*— **サマリー ルートのネットワーク マスクです**

コマンドモード

Router Configuration

初期設定

無効

コマンド解説

- **自律システム境界ルータ（ASBR）は、接続されたすべての自律システムに集約ルートをアドバタイズすることにより、他のプロトコルから学習したルートを再配布することができます。**
- **このルータは、最大 16 のタイプ 5 サマリー ルートをサポートします。**

例

この例では、192.168.x.x の範囲内に含まれるすべてのルートのサマリー アドレスを作成します。

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

関連するコマンド

area range （P595）

redistribute

他のルーティング ドメイン（プロトコル）から自律システムに外部ルーティング情報をインポートします。"no" **を前に置くことで、この機能が無効になります。**

文法

[no] redistribute [rip | static] [metric *metric-value*] [metric-type *type-value*]

- rip — **ルーティング情報プロトコル**（RIP）**からこの自律システム**（AS）**へ、外部ルートをインポートします。**
- static — **この自律システムへスタティック ルートをインポートします**
- *metric-value* — **指定したプロトコルのすべての外部ルートに割り当てられるメトリックです（範囲** : 1 ～ 65535**、デフォルト** : 10）
- *type-value*— 1 - **タイプ** 1 **外部ルート**　2 - **タイプ** 2 **外部ルート（デフォルト）**

コマンドモード

Router Configuration

初期設定

再配布 - **なし**

プロトコル - RIP **およびスタティック**

メトリック値 - 0

タイプ メトリック - 2

コマンド解説

- **このルータでは、**RIP **およびスタティック両方のルートの再配布をサポートしています。**
- OSPF **自律システム**（AS）**に外部ルートを再配布すると、ルータは自動的に自律システム境界ルータ**（ASBR）**になります。**redistribute **コマンドを** default-informationoriginate **コマンドと組み合わせて使用することにより** AS **への「デフォルト」外部ルートを生成した場合、このコマンドで指定されたメトリック値は、**default-information originate **コマンドで指定されたメトリックを上書きします。**
- **メトリック タイプは、外部** LSA **を介して、**AS **外部の宛先へのルートをアドバタイズする方法を指定します。外部ルート メトリックに内部コスト メトリックを追加するには、タイプ** 1 **を指定します。すなわち、**AS **内の任意のルータのルートのコストは、アドバタイジング** ASBR **への到達コストと、外部ルートのコストを加えたものに等しいことになります。外部ルート メトリックのみをアドバタイズするには、タイプ** 2 **を指定します。**

例

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

関連するコマンド

default-information originate（P593）

network area

このエリア内で動作する OSPF **エリアとインタフェースを定義します。**

"no" **を前に置くことで、指定インタフェースの** OSPF **が無効になります。**

文法

[no] network *ip-address netmask* **area** *area-id*

- *ip-address* — **エリアに追加するインタフェースのアドレス**
- *netmask* — **エリアに追加するアドレス範囲のネットワーク マスク**
- *area-id*— **指定アドレスまたは範囲が割り当てられるエリア。**OSPF **エリアは、共通のルーティング情報を共有するルータのグループを識別します（エリア** ID **は、**IP **アドレスと同じ形式である必要があります）**

コマンドモード

Router Configuration

初期設定

無効

コマンド解説

- **エリア** ID **は、**OSPF **ブロードキャスト エリアを一意に定義するものです。エリア** ID0.0.0.0 **は、自律システムの** OSPF **バックボーンを示します。各ルータは、直接接続または仮想リンクを介してバックボーンに接続されている必要があります。**
- 1 **つまたは複数のインタフェースをエリアに追加するには、ネットワーク マスクを使用して、ネットワーク セグメント上のすべてのルータのエリア** ID **を同じ値に設定します。**
- **ネットワーク エリア内に存在するインタフェースのプライマリ アドレスを確実に含めるようにします。そうしないと、**OSPF **は、このコマンドでカバーされるセカンダリ アドレスに対して動作しません。**
- **インタフェースは、**1 **つのエリアにのみ割り当てることができます。その後のネットワーク エリア コマンドによりアドレス範囲が重複して指定された場合、ルータは、最初のコマンドで指定されたエリアのアドレス範囲を実装し、後のコマンドで重複したエリアを無視します。ただし、より特定性の高いアドレス範囲をエリアから削除すると、このエリアをカバーする特定性の低いアドレスが指定された場合に、この範囲に属するインタフェースがアクティブのままになります。**
- **このルータは、最大** 64 **の** OSPF **ルータ インタフェースと、最大** 16 **のエリア（ノーマル トランジット エリア、スタブ、または** NSSA **のいずれかの合計）をサポートします。**

例

この例では、クラス B **アドレス** 10.1.x.x **をカバーするバックボーン** 0.0.0.0**、およびクラス** C **アドレス** 10.2.9.x **をカバーするノーマル トランジット エリア** 10.2.9.0 **を作成します。**

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area
10.1.0.0
Console(config-router)#
```

area stub

スタブ エリアを定義します。スタブを削除するには、オプション キーワードを指定せずに no 形式を使用します。サマリー属性を削除するには、サマリー キーワードを指定せずに no 形式を使用します。

文法

[no] area *area-id* **stub** [summary]

- *area-id* - スタブ エリアの識別子です（エリア ID は、IP アドレスと同じ形式である必要があります）。
- summary - エリア境界ルータ（ABR）は、スタブ エリアにサマリー リンク アドバタイズメントを送信します（デフォルト : no summary）。

コマンドモード

Router Configuration

初期設定

スタブは構成されていません。

コマンド解説

- スタブ内のすべてのルータは、同じエリア ID で構成されている必要があります。
- ルーティング テーブル スペースは、タイプ 4 AS サマリー LSA およびタイプ 5 外部 LSA をブロックすることにより、スタブ内に保存されます。このコマンドのデフォルト設定では、ローカル エリアまたは自律システム外部の宛先へのデフォルト ルートをアドバタイズするタイプ 3 サマリー LSA をブロックすることにより、スタブを完全に分離します。
- ABR によってスタブへ送信されるデフォルト サマリー ルートのコストを指定するには、area default-cost コマンドを使用します。
- このルータは、最大 16 のエリア（ ノーマル トランジット エリア、スタブ、または NSSA のいずれかの合計）をサポートします。

例

この例では、スタブ エリア 10.2.0.0 を作成し、クラス B アドレス 10.2.x.x を持つインターフェースをすべてスタブに割り当てます。

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area
10.2.0.0
Console(config-router)#
```

関連するコマンド

area default-cost（P596）

area nssa

準スタブ エリア（NSSA）を定義します。NSSA を削除するには、オプション キーワードを指定せずに no 形式を使用します。オプション属性を削除するには、関連するキーワードを指定せずに no 形式を使用します。

文法

[no] area *area-id* **nssa** [no-redistribution] [default-information-originate]

- *area-id* - NSSA の識別子です（エリア ID は、IP アドレスと同じ形式である必要があります）。
- no-redistribution - ルータが NSSA のエリア境界ルータ（ABR）であり、なおかつ redistribute コマンドを使って（NSSA にではなく）ノーマル エリアにのみルートをインポートしたい場合、このキーワードを使用します。すなわち、このキーワードでは、NSSA ABR が（他のエリアのルータを介して学習された）外部ルーティング情報を NSSA へアドバタイズするのを防ぎます。
- default-information-originate - ルータが NSSA エリア境界ルータ（ABR）または NSSA 自律システム境界ルータ（ASBR）である時、このパラメータを指定すると、NSSA に対するタイプ -7 デフォルト LSA が生成されます。このデフォルトは、NSSA ABR には AS 内の他エリアに対するルートを、また NSSA ASBR には AS 外部のエリアに対するルートを提供します。

コマンドモード

Router Configuration

初期設定

NSSA は構成されていません。

コマンド解説

- NSSA 内のすべてのルータは、同じエリア ID で構成されている必要があります。
- NSSA はスタブに似ています。この理由は、ルータが ABR である場合、default-information-originate キーワードを使用して、AS 内の他のエリアに対するデフォルト ルートを NSSA に送信できるためです。ただし、NSSA がスタブと異なる点は、ルータが ASBR である場合、default-information-originate キーワードを使用して、デフォルトの外部 AS ルート（NSSA に隣接しているが OSPF AS 内にはないルーティング プロトコル ドメイン宛）を NSSA にインポートできることです。
- NSSA にアドバタイズされる外部ルートには、OSPF を介して学習された AS 外部のネットワーク宛先のほか、デフォルト ルート、スタティック ルート、他のルーティング プロトコル（RIP など）からインポートされたルート、OSPF を実行していないルータに直接接続されたネットワークなどを含めることができます。
- NSSA 外部 LSA （タイプ 7）は、NSSA に隣接した任意の ABR によって外部 LSA （タイプ 5）に変換され、AS 内の他のエリアへ伝播されます。
- また、アンリンク スタブ エリア、すべてのタイプ 3 サマリー LSA は常に NSSA へインポートされ、内部ルートが常にタイプ 7 NSSA 外部ルートよりも優先して選択されることを保証します。
- このルータは、最大 16 のエリア（ ノーマル トランジット エリア、スタブ、または NSSA のいずれかの合計）をサポートします。

例

この例では、スタブ エリア 10.3.0.0 **を作成し、クラス** B **アドレス** 10.3.x.x **を持つインタフェースをすべて** NSSA **に割り当てます。また、ルータが** NSSA ABR **または** NSSA ASBR **の場合、**NSSA **への外部** LSA **を生成するように指示します。**

```
Console(config-router)#area 10.3.0.0 nssa
default-information-originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```

area virtual-link

仮想リンクを定義します。仮想リンクを削除するには、オプション キーワードを指定せずに no 形式を使用します。属性のデフォルト値に戻すには、要求されるキーワードを指定せずに no 形式を使用します。

文法

[no] area *area-id* **virtual-link** *router-id*

[authentication [message-digest | null]] [hello-interval *seconds*]

[retransmit-interval *seconds*] [transmit-delay *seconds*]

[dead-interval *seconds*] [[authentication-key *key*] |

[message-digest-key *key-id* md5 *key*]]

no area *area-id*

- *area-id* - 仮想リンクのトランジット エリアの識別子です（エリア ID は、IP アドレスと同じ形式である必要があります）。
- *router-id* - 仮想リンクの隣接ルータのルータ ID です。このルータは、仮想リンクの他方の端にあるバックボーンとトランジット エリア両方に隣接するエリア境界ルータ（ABR）である必要があります。
- authentication - 認証モードを指定します。キーワードの後にオプション パラメータを指定しないと、authentication-key で指定されたパスワードとともにプレーンテキスト認証が使用されます。message-digest 認証を指定する場合、message-digest-key および md5 パラメータも同時に指定する必要があります。null オプションを指定した場合、OSPF ルーティング プロトコル メッセージには認証は実行されません。
- message-digest - メッセージ ダイジェスト（MD5）認証を指定します。
- null - 使用される認証はないことを示します。
- hello-interval seconds - Hello パケット送信間の伝送遅延を指定します。Hello 間隔を小さい値に設定すると、トポロジ変更を検知する際の遅延は短縮されますが、ルーティング トラフィックは増加します。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲 : 1 ～ 65535 秒、デフォルト : 10 秒）。
- retransmit-interval seconds - ABR が仮想リンク上でリンクステート アドバタイズメント（LSA）を再送信する間隔を指定します。この送信間隔は、ルーティング情報の適切なフローを提供しつつも、不必要なプロトコル トラフィックを発生させない程度の控えめな値に設定してください。ただし、この値は、仮想リンクの値よりは大きく設定する必要があることに注意してください（範囲 : 1 ～ 3600 秒、デフォルト : 5 秒）。
- transmit-delay seconds - 仮想リンク上でリンクステート アップデート パケットを送信するのに必要な時間を、伝送遅延および伝播遅延を考慮に入れて予測します。LSA のエージには、この値が送信前に加算されます。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲 : 1 ～ 3600 秒、デフォルト : 1 秒）。
- . dead-interval seconds - ルータのダウンを宣言する前に、隣接ルータが Hello パケットを待機する時間です。この値は、自律システムに接続されたすべてのルータで同じに設定される必要があります（範囲 : 1 ～ 65535 秒、デフォルト : 4 × Hello 間隔、または 40 秒）。
- authentication-key key - プロトコル メッセージのヘッダ内の認証フィールドを生成または検証するために、仮想リンク上の隣接ルータによって使用されるプレーンテキスト パスワード（最大 8 文字）を設定します。各ネットワーク インタフェースに個別のパスワードを割り当てることができます。ただし、このキーは、同じネットワーク（自律システム）

上のすべての隣接ルータに対して同じ値に設定する必要があります。このキーは、バックボーンで認証が有効になっている時のみ使用されます。

- message-digest-key key-id md5 key - メッセージ ダイジェスト（MD5）認証を使用時、隣接ルータとこのルータ間を通過するプロトコル メッセージの認証に使用されるキー識別子とパスワードを設定します。key-id は、1 ～ 255 までの整数で、key は、最大 16 文字長の英数字ストリングです。仮想リンク上で MD5 認証が使用されている場合、自律システム内のすべてのルータ上で MD5 が有効になっている必要があります。また、キー識別子とキーは、すべてのルータに対して同じである必要があります。

コマンドモード

Router Configuration

初期設定

area-id: なし　router-id: なし　hello-interval:10 秒
retransmit-interval:5 秒　transmit-delay:1 秒　dead-interval:40 秒
authentication-key: なし　message-digest-key: なし

コマンド解説

- 自律システム全体のルーティング コネクティビティを保持するには、すべてのエリアが、バックボーン エリア（0.0.0.0）に接続されている必要があります。特定のエリアをバックボーンに接続することが物理的に不可能な場合、仮想リンクを使用することができます。仮想リンクは、分離されたエリアのバックボーンへの論理パスを提供するものです。このルータでは、最大 32 の仮想リンクを指定することができます。
- バックボーンから切断された各エリアには、トランジット エリア ID、およびバックボーンに隣接する仮想リンク隣接ルータのルータ ID が含まれている必要があります。
- このルータでは、最大 64 の仮想リンクをサポートします。

例

この例では、すべてのオプション パラメータのデフォルト値を使用して、仮想リンクを作成します。

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

この例では、MD5 認証を使用して、仮想リンクを作成します。

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
message-digest-key 5 md5 ld83jdpq
Console(config-router)#
```

関連するコマンド

show ip ospf virtual-links（P624）

ip ospf authentication

インタフェースで使用される認証タイプを指定します。プレーン テキスト（シンプル パスワード）認証を指定するには、オプション パラメータを使用せずに、こ

のコマンドを入力します。"no" を前に置くことで、デフォルトの認証なしに戻ります。

文法

ip ospf authentication [message-digest | null]

no ip ospf authentication

- message-digest - メッセージ ダイジェスト（MD5）認証を指定します。
- null - 使用される認証はないことを示します。

コマンドモード

Router Configuration

初期設定

認証なし

コマンド解説

- インタフェースにプレーン テキスト パスワード認証を指定する際は、ip ospfauthentication-key コマンドでパスワードを予め構成しておきます。インタフェースに MD5 認証を指定する際は、ip ospf message-digest-key コマンドで、メッセージダイジェスト キー ID とキーを予め構成しておきます。
- プレーンテキスト認証キー、または MD5 キー ID およびキーの使用では、自律システム全体で整合性を保つ必要があります。

例

この例では、指定インタフェースでメッセージダイジェスト認証を有効にします。

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

ip ospf authentication-key

隣接ルータによって使用されるシンプル パスワードを割り当てます。"no" を前に置くことで、パスワードが削除されます。

文法

ip ospf authentication-key *key*
no ip ospf authentication-key

- *key* - プレーン テキスト パスワードを設定します（範囲 : 1-8 文字）。

コマンドモード

Interface Configuration (VLAN)

初期設定

パスワードなし

コマンド解説

- インタフェースにプレーン テキスト パスワード認証を指定する際は、ip ospfauthentication-key コマンドでパスワードを予め構成しておきます。インタフェースに MD5 認証を指定する際は、ip ospf message-digest-key コマンドで、メッセージダイジェスト キー ID とキーを予め構成しておきます。
- 各ネットワーク インタフェース ベースで異なるパスワードを割り当てることが可能ですが、パスワードの使用では、ネットワーク（自律システム）全体のすべての隣接ルータ上で整合性を保つ必要があります。

例

この例では、指定インタフェースのパスワードを設定します。

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

ip ospf message-digest-key

指定インタフェースでメッセージダイジェスト（MD5）認証を有効にします。また、隣接ルータによって使用されるキー ID およびキーの割当てを有効にします。
"no" を前に置くことで、既存のキーが削除されます。

文法

ip ospf message-digest-key *key-id* md5 *key*

no ip ospf message-digest-key *key-id*

- *key-id* - MD5 キーのインデックス番号です（範囲 : 1-255）。
- *key* - 128 ビットのメッセージダイジェストまたは「フィンガープリント」を生成するのに使用される英数字パスワードです（範囲 : 1-16 文字）。

コマンド モード

Interface Configuration (VLAN)

初期設定

MD5 認証は無効です。

コマンド解説

- 通常、アウトバウンド パケット用の認証情報の生成および着信パケットの認証に使用されるキーは、インタフェースごとに 1 つのみです。隣接ルータ同士は、同じキー識別子とキー値を使用する必要があります。
- 新規キーに変更する時、ルータは、すべてのプロトコル メッセージの複数のコピーを、1 つは古いキーで、もう 1 つは新しいキーで送信します。すべての隣接ルータが新しいキーで、このルータへプロトコル メッセージの送信を開始すると、ルータは古いキーの使用を止めます。このロールオーバ プロセスにより、ネットワーク管理者には、ネットワーク コネクティビティを低下させることなくネットワーク上のすべてのルータをアップデートする時間の余裕ができます。すべてのネットワーク ルータが新しいキーでアップデートされると、古いキーは、セキュリティ上の理由により削除されます。

例

この例では、メッセージダイジェスト キーの識別子およびパスワードを設定します。

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```

ip ospf cost

インタフェース上でのパケット送信コストを明示的に設定します。"no" を前に置くことで、設定を初期値に戻します。

文法

ip ospf cost *cost*

no ip ospf cost

- *cost* - このインタフェースのリンク メトリックです。低速ポートを示すには、この値を大きくします（範囲 : 1- 65535）。

コマンドモード

Interface Configuration（VLAN）

初期設定

1

コマンド解説

インタフェース コストは、ポートのスピードを反映します。このルータでは、すべてのポートに対してデフォルトのコスト 1 を使用します。したがって、ギガビット モジュールをインストールする場合、すべての 100 Mbps ポートのコストを 2 以上の値にリセットする必要があります。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```

ip ospf dead-interval

Hello パケットを受信しないまま、この時間が経過すると、隣接ルータによってルータのダウンが宣言されるまでの間隔を設定します。"no" を前に置くことで、設定を初期値に戻します。

文法

ip ospf dead-interval *seconds*

no ip ospf dead-interval

- *seconds* - 隣接ルータが送信ルータのダウンを宣言する前に、Hello パケットを待機する最大時間です。この間隔は、ネットワーク上のすべてのルータに対して同じ値に設定されている必要があります（範囲 : 1-65535）。

コマンドモード

Interface Configuration (VLAN)

初期設定

40 秒、または ip ospf hello-interval コマンドにより指定された間隔の 4 倍

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

ip ospf hello-interval

インタフェース上で送信する Hello **パケットの間隔を指定します。**"no" **を前に置くことで、設定を初期値に戻します。**

文法

ip ospf hello-interval *seconds*

no ip ospf hello-interval

- *seconds* - **インタフェースから送信される** Hello **パケットの間隔です。この間隔は、ネットワーク上のすべてのルータに対して同じ値に設定されている必要があります（範囲** : 1-65535**）。**

コマンドモード

Router Configuration

初期設定

10 **秒**

コマンド解説

Hello **パケットは、送信ルータがまだアクティブであることを他のルータに通知するために使用されます。**Hello **間隔を小さい値に設定すると、トポロジ変更の検出における遅延は短縮されますが、ルーティング トラフィックは増加します。**

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

ip ospf priority

エリアの指定ルータ（DR**）およびバックアップ指定ルータ（**BDR**）を決定する際に使用されるルータ プライオリティを設定します。**"no" **を前に置くことで、設定を初期値に戻します。**

文法

ip ospf priority *priority*

no ip ospf priority

- *priority* - **このルータのインタフェース プライオリティです（範囲** : 0-255**）。**

コマンドモード

Interface Configuration（VLAN）

初期設定

1

コマンド解説

- ルータが DR または BDR として選出されないようにするには、プライオリティを 0 に設定します。0 以外の任意の値に設定すると、最も高いプライオリティのルータが DR になり、次に高いプライオリティのルータが BDR になります。2 つまたはそれ以上のルータに同じ最高のプライオリティが割り当てられている場合、より高い ID を持つルータが選出されます。
- DR がすでに存在しているエリアにこのインタフェースが追加された場合、新規ルータの持つプライオリティに関わらず、現行の DR が存続します。DR は、次に選出プロセスが初期化されるまで変更されません。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```

ip ospf retransmit-interval

リンクステート アドバタイズメント（LSA）を再送信する間隔を指定します。"no" を前に置くことで、設定を初期状態にもどします。

文法

ip ospf retransmit-interval *seconds*
no ip ospf retransmit-interval

- *seconds* - このインタフェースで LSA を再送信する間隔を設定します（範囲 : 1- 65535）。

コマンド モード

Interface Configuration (VLAN)

初期設定

5 秒

コマンド解説

ルータは、肯定応答（ACK）を受信しないと、隣接ルータに LSA を再送信します。この送信間隔は、ルーティング情報の適切なフローを提供しつつも、不必要なプロトコル トラフィックを発生させない程度の控えめな値に設定してください。この値は、仮想リンクの値より大きく設定する必要があることに注意してください。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

ip ospf transmit-delay

インタフェースでリンクステート アップデート パケットを送信するまでの時間を予測します。"no" を前に置くことで、設定を初期状態にもどします。

文法

ip ospf transmit-delay *seconds*

no ip ospf transmit-delay

- *seconds* - リンクステート アップデートを送信するまでの予測待機時間を設定します（範囲 : 1-65535）。

コマンド モード

Interface Configuration (VLAN)

初期設定

1 秒

コマンド解説

LSA のエージには、この遅延が送信前に加算されます。送信遅延を予測するには、インタフェースの送信遅延および伝播遅延を考慮に入れます。低速リンクに大きい値を使用し、リンク スピードに従って送信遅延を設定します。この送信遅延は、自律システムに接続されたすべてのルータで同じに設定される必要があります。

例

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

show ip ospf

このコマンドでは、ルーティング コンフィギュレーションに関する基本情報を表示します。

コマンド モード

Privileged Exec

例

```
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Redistributing External Routes from,
     rip with metric mapped to 10
Number of area in this router is 2
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 19 times
Area 10.1.0.0
     Number of interfaces in this area is 4
     SPF algorithm executed 19 times
Console#
```

項目	解説
Routing Process with ID	ルータ ID
Supports only single TOS (TOS0) route	タイプ オブ サービス（ToS）はサポートされていません。したがって、インタフェースごとに 1 つのコストしか割り当てることができません。
It is an router type	表示されるルータ タイプ。内部ルータ、エリア境界ルータ、自律システム境界ルータがあります。
Number of areas in this router	構成されたエリアの数
Area identifier	エリア アドレス、およびエリア タイプ（バックボーン、NSSA、またはスタブ）
Number of interfaces	このエリアに接続されたインタフェースの数
SPF algorithm executed	このエリアに対して SPF （最短パス優先）アルゴリズムが実行された回数

show ip ospf border-routers

エリア境界ルータ（ABR）または自律システム境界ルータ（ASBR）についてのルーティング テーブルのエントリを表示します。

コマンド モード

Privileged Exec

例

```
Console#show ip ospf border-routers

  Destination     Next Hop   Cost   Type   RteType   Area          SPF No
------------- ------------- ------ ----- -------- ------------- --------
  10.1.1.252     10.1.1.253       0   ABR     INTRA     10.1.0.0        3
  10.2.6.252     10.2.9.253       0   ASBR    INTER     10.2.0.0        7
Console#
```

項目	解説
Destination	宛先ルータの識別子
Next Hop	宛先へのネクスト ホップの IP アドレス
Cost	このルートのリンク メトリック
Type	宛先のルータ タイプ（ABR、ASBR、または両方）
RteType	ルート タイプ。イントラ エリアまたはエリア間ルート（INTRA または INTER）のいずれか
Area	このルートが学習されたエリア
SPF No	このルートに対して SPF （最短パス優先）アルゴリズムが実行された回数

show ip ospf database

このルータのデータベース内に保存された各種 OSPF リンクステート アドバタイズメント（LSA）に関する情報を表示します。

文法

show ip ospf [*area-id*] database [adv-router [*ip-address*]]

show ip ospf [*area-id*] database [asbr-summary] [*link-state-id*]

show ip ospf [*area-id*] database [asbr-summary] [*link-state-id*] [adv-router [*ip-address*]]

show ip ospf [*area-id*] database [asbr-summary] [*link-state-id*] [self-originate] [*link-state-id*]

show ip ospf [*area-id*] database [database-summary]

show ip ospf [*area-id*] database [external] [*link-state-id*]

show ip ospf [*area-id*] database [external] [*link-state-id*] [adv-router [*ip-address*]]

show ip ospf [*area-id*] database [external] [*link-state-id*] [self-originate] [*ip-address*]

show ip ospf [*area-id*] database [network] [*link-state-id*]

show ip ospf [*area-id*] database [network] [*link-state-id*] [adv-router [*ip-address*]]

show ip ospf [*area-id*] database [network] [*link-state-id*] [self-originate] [*link-state-id*]

show ip ospf [*area-id*] database [nssa-external] [*link-state-id*]

show ip ospf [*area-id*] database [nssa-external] [*link-state-id*] [adv-router [*ip-address*]]

show ip ospf [*area-id*] database [nssa-external] [*link-state-id*] [self-originate] [*link-state-id*]

show ip ospf [*area-id*] database [router] [*link-state-id*]

show ip ospf [*area-id*] database [[router] [adv-router [*ip-address*]]

show ip ospf [*area-id*] database [router] [self-originate] [*link-state-id*]

show ip ospf [*area-id*] database [self-originate] [*link-state-id*]

show ip ospf [*area-id*] database [summary] [*link-state-id*]

show ip ospf [*area-id*] database [summary] [*link-state-id*] [adv-router [*ip-address*]]

show ip ospf [*area-id*] database [summary] [*link-state-id*] [self-originate] [*link-state-id*]

- *area-id* - LSA 情報を閲覧したいエリアを定義します（ この項目は、IP アドレスと同じ形式で入力する必要があります）。
- adv-router - アドバタイジング ルータの IP アドレスです。入力しない場合、すべてのアドバタイジング ルータに関する情報が表示されます。
- *ip-address* - 指定ルータの IP アドレスです。アドレスを入力しない場合、ローカルルータに関する情報が表示されます。
- asbr-summary - ASBR （自律システム境界ルータ）サマリー LSA に関する情報を表示します。
- *link-state-id* - LSA によって記述されるネットワーク部分です。link-state-id には、次を入力する必要があります。

  －タイプ 3 サマリーおよび外部 LSA の IP ネットワーク番号

  －ルータのルータ ID、ネットワーク、タイプ 4 AS サマリー LSA。また、タイプ 5 ASBR 外部 LSA によってデフォルト ルートが記述される時、その link-state-id はデフォルトの宛先（0.0.0.0）に設定されることに注意してください。

- self-originate - **このルータによって送信される** LSA **を表示します。**
- database-summary - **データベース内に保存されている各エリアの各** LSA **タイプのカウント、およびデータベース内の** LSA **の総数を表示します。**
- external - **外部** LSA **に関する情報を表示します。**
- network - **ネットワーク** LSA **に関する情報を表示します。**
- nssa-external - NSSA **外部** LSA **に関する情報を表示します。**
- router - **ルータ** LSA **に関する情報を表示します。**
- summary - **サマリー** LSA **に関する情報を表示します。**

コマンド モード

Privileged Exec

例

次の例は、show ip ospf database **コマンドの出力を示します。**

```
Console#show ip ospf database


   Displaying Router Link States(Area 10.1.0.0)
       Link ID      ADV Router     Age       Seq#       Checksum
--------------- --------------- ------ ----------- -----------
     10.1.1.252      10.1.1.252     26   0X80000005       0X89A1
     10.1.1.253      10.1.1.253     23   0X80000002       0X8D9D


   Displaying Net Link States(Area 10.1.0.0)
       Link ID      ADV Router     Age       Seq#       Checksum
--------------- --------------- ------ ----------- -----------
     10.1.1.252      10.1.1.252     28   0X80000001       0X53E1
Console#
```

項目	解説
Link ID	**ルータ** ID
ADV Router	**アドバタイジング ルータ** ID
Age	LSA **のエージです（秒単位）**
Seq#	LSA **のシーケンス番号（古い重複した** LSA **の検出に使用されます）**
Checksum	LSA **の完全コンテンツのチェックサム**

次の例は、asbr-summary **キーワードを使用した場合 です。**

```
Console#show ip ospf database asbr-summary

OSPF Router with id(10.1.1.253)

            Displaying Summary ASB Link States(Area 0.0.0.0)

LS age: 433
Options: (No TOS-capability)
LS Type: Summary Links (AS Boundary Router)
Link State ID: 192.168.5.1 (AS Boundary Router's Router ID)
Advertising Router: 192.168.1.5
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0
Metric: 1

Console#
```

項目	解説
OSPF Router id	**ルータ** ID
LS age	LSA **のエージ（秒単位）**
Options	LSA **と関連付けられたオプション機能**
LS Type	AS External Links - LSA **は、**AS **外部の宛先へのルート（**AS **へのデフォルト外部ルートを含む）を記述**
Link State ID	**リンクステート** ID
Advertising Router	**アドバタイジング ルータ** ID
LS Sequence Number	LSA **のシーケンス番号（古い重複した** LSA **の検出に使用されます）**
LS Checksum	LSA **の完全コンテンツのチェックサム**
Length	LSA **の長さをバイト単位で示**
Network Mask	**ネットワークのアドレス マスク**
Metric Type	**タイプ** 1 **またはタイプ** 2 **外部メトリック**
Metrics	**リンクのコスト**

次の例は、database-summary **キーワードを使用した場合 です。**

```
Console#show ip ospf database database-summary

Area ID (10.1.0.0)
        Router Network Sum-Net Sum-ASBR External-AS External-Nssa
           2      1        1      0          0             0
Total LSA Counts : 4
Console#
```

項目	解説
Area ID	**ルータ** ID
Router	**エリア識別子**
Options	**ルータ** LSA **の数**
Network	**ネットワーク** LSA **の数**
Sum-net	**サマリ** LSA **の数**
Sum-ASBR	**サマリ** ASBR LSA **の数**
External-AS	**自立システム外部** LSA **の数**
External-Nssa	NSSA **外部ネットワーク** LSA **の数**
Total LSA Counts	LSA **の合計数**

次の例は、external **キーワードを使用した場合 です。**

```
Console#show ip ospf database external

OSPF Router with id(192.168.5.1) (Autonomous system 5)

            Displaying AS External Link States

LS age: 433
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.1.1.253 (External Network Number)
Advertising Router: 10.1.2.254
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.0.0
Metric Type: 2 (Larger than any link state path)
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0

Console#
```

項目	解説
OSPF Router id	**ルータ** ID
LS age	LSA **のエージ（秒）**
Options	LSA **と関連付けられたオプション機能**
LS Type	Network Link - LSA **は、ネットワークに接続されたルータを記述**
Link State ID	**自律システム境界ルータ（**ASBR**）のインタフェース アドレス**
Advertising Router	**アドバタイジング ルータ** ID
LS Sequence Number	LSA **のシーケンス番号（古い重複した** LSA **の検出に使用されます）**
LS Checksum	LSA **の完全コンテンツのチェックサム**
Length	LSA **の長さをバイト単位で示します**
Network Mask	**ネットワークのアドレス マスク**
Metric Type	**タイプ** 1 **またはタイプ** 2 **外部メトリック**
Metrics	**リンクのコスト**
Forward Address	**アドバタイズされた宛先へ渡されるデータのフォワーディング アドレスです（フォワーディング アドレスが** 0.0.0.0 **に設定されている場合、データはアドバタイズメントの発信元へ転送されます）**
External Route Tag	**各外部ルートに割り当てられた** 32 **ビット フィールドです（**OSPF **では使用されません。特定のアプリケーションで指定されたとおりに境界ルータ間で他の情報を通信するのに使用されます）。**

次の例は、network キーワードを使用した場合 です。

```
Console#show ip ospf database network

OSPF Router with id(10.1.1.253)

          Displaying Net Link States(Area 10.1.0.0)


Link State Data Network (Type 2)
--------------------------------

LS age: 433
Options: Support External routing capability
LS Type: Network Links
Link State ID: 10.1.1.252 (IP interface address of the Designated
Router)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0

       Attached Router: 10.1.1.252
       Attached Router: 10.1.1.253
Console#
```

項目	解説
OSPF Router id	ルータ ID
LS age	LSA のエージ（秒単位）
Options	LSA と関連付けられたオプション機能
LS Type	Network Link - LSA は、ネットワークに接続されたルータを記述
Link State ID	自律システム境界ルータ（ASBR）のインタフェース アドレス
Advertising Router	アドバタイジング ルータ ID
LS Sequence Number	LSA のシーケンス番号（古い重複した LSA の検出に使用されます）
LS Checksum	LSA の完全コンテンツのチェックサム
Length	LSA の長さをバイト単位で示します
Network Mask	ネットワークのアドレス マスク
Attached Router	ネットワークに接続されたルータ（指定ルータ自身を含む、指定ルータに完全に隣接したルータ）のリスト

次の例は、summary **キーワードを使用した場合 です。**

```
Console#show ip ospf database summary

OSPF Router with id(10.1.1.253)

            Displaying Summary Net Link States(Area 10.1.0.0)

Link State Data Summary (Type 3)
--------------------------------

LS age: 686
Options: Support External routing capability
LS Type: Summary Links(Network)
Link State ID: 10.2.6.0 (The destination Summary Network Number)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000003
LS Checksum: 0x3D02
Length: 28
Network Mask: 255.255.255.0
Metric: 1

Console#
```

項目	解説
OSPF Router id	**ルータ** ID
LS age	LSA **のエージ（秒単位）**
Options	LSA **と関連付けられたオプション機能**
LS Type	Network Link - LSA **は、ネットワークに接続されたルータを記述**
Link State ID	**自律システム境界ルータ（**ASBR**）のインタフェース アドレス**
Advertising Router	**アドバタイジング ルータ** ID
LS Sequence Number	LSA **のシーケンス番号（古い重複した** LSA **の検出に使用されます）**
LS Checksum	LSA **の完全コンテンツのチェックサム**
Length	LSA **の長さをバイト単位で示します**
Network Mask	**ネットワークのアドレス マスク**
Metrics	**リンクのコスト**

show ip ospf interface

OSPF インタフェースのサマリー情報を表示します。

文法

show ip ospf interface [vlan *vlan-id*]

- *vlan-id* - VLAN ID です（範囲：1-4093）

コマンド モード

Privileged Exec

例

```
Console#show ip ospf interface vlan 1

Vlan 1 is up
  Interface Address 10.1.1.253, Mask 255.255.255.0, Area 10.1.0.0
  Router ID 10.1.1.253, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router id 10.1.1.252, Interface address 10.1.1.252
  Backup Designated router id 10.1.1.253, Interface addr 10.1.1.253
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Console#
```

項目	解説
Vlan	物理リンクの VLAN ID とステータスです。
Interface Address	OSPF インタフェースの IP アドレス
Mask	インタフェース アドレスのネットワーク マスク
Area	このインタフェースが属している OSPF エリア
Router ID	ルータ ID
Network Type	ブロードキャスト、非ブロードキャスト、またはポイントツーポイント ネットワークのいずれか
Cost	インタフェースの送信コスト
Transmit Delay	インタフェースの送信遅延（秒単位）
State	• Disabled - このインタフェース上で OSPF は有効になっていません。 • Down . - このインタフェース上で OSPF は有効になっていますが、インタフェースがダウンしています。 • Loopback - ループバック インタフェースです。 • Waiting - ルータは DR と BDR を見つけようとしています。 • DR - 指定ルータ（Designated Router）です。 • BDR - バックアップ指定ルータ（Backup Designated Router）です。 • DRother - インタフェースはマルチアクセス ネットワーク上にありますが、DR または BDR ではありません。
Priority	ルータのプライオリティ
Designated Router	指定ルータ ID （DR ID）、および対応するインタフェース アドレス
Backup Designated Router	バックアップ指定ルータの ID と対応するインタフェース アドレス
Timer intervals	タイマー間隔（Hello 間隔、Dead 間隔、Retransmit 間隔を含む）のコンフィギュレーション設定

show ip ospf neighbor

OSPF エリア内の各インタフェース上の隣接ルータに関する情報を表示します。

文法

show ip ospf neighbor

コマンド モード

Privileged Exec

例

```
Console#show ip ospf neighbor

     ID            Pri        State           Address
--------------- ------ --------------- ---------------
     10.1.1.252      1          FULL/DR      10.1.1.252

Console#
```

項目	解説
ID	隣接ルータのルータ ID
Pri	近隣のルータプライオリティ
State	OSPF の状態と識別フラグ。各状態は、次のとおりです。 Down - 接続がダウンしています。 Attempt - 接続はダウンしているが、コンタクトが試みられています（非ブロードキャスト ネットワーク用）。 Init - Hello パケットは受信されたが、通信はまだ確立されていません。 Two-way - 双方向通信が確立しています。 ExStart - 隣接ルータ間の隣接性を初期化しています。 Exchange - データベース記述を交換しています。 Loading - LSA データベースを交換しています。 Full - 隣接ルータは完全に隣接関係にあります。 各識別フラグは次のとおりです。 D - ダイナミック隣接ルータです。 S - スタティック隣接ルータです。 DR - 指定ルータです。 BDR - バックアップ指定ルータです。

show ip ospf summary-address

すべてのサマリー アドレス情報を表示します。

文法

show ip ospf summary-address

コマンド モード

Privileged Exec

例

この例では、サマリー アドレス、および関連付けられたネットワーク マスクを表示します。

```
Console#show ip ospf summary-address
10.1.0.0/255.255.0.0
Console#
```

show ip ospf virtual-links

仮想リンクに関する詳細情報を表示します。

文法

show ip ospf virtual-links

コマンド モード

Privileged Exec

例

```
Console#show ip ospf virtual-links
Virtual Link to router 10.1.1.253 is up
Transit area 10.1.1.0
Transmit Delay is 1 sec
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Console#
```

項目	解説
Virtual Link to router	OSPF **隣接ルータとリンク状態（アップまたはダウン）**
Transit area	**仮想リンクがターゲット ルータに到達するために横断する共通エリア**
Transmit Delay	**仮想リンク上の予測送信遅延（秒単位）**
Timer intervals	**タイマー間隔（**Hello **間隔、**Dead **間隔、**Retransmit **間隔を含む）のコンフィギュレーション設定**

関連するコマンド

area virtual-link（P603）

FXC9024XG Management Guide (FXC08-DC-200011-R2.1)

初版	2008 年 7 月
2 版	2011 年 1 月
3 版	2016 年 2 月
4 版	2016 年 4 月