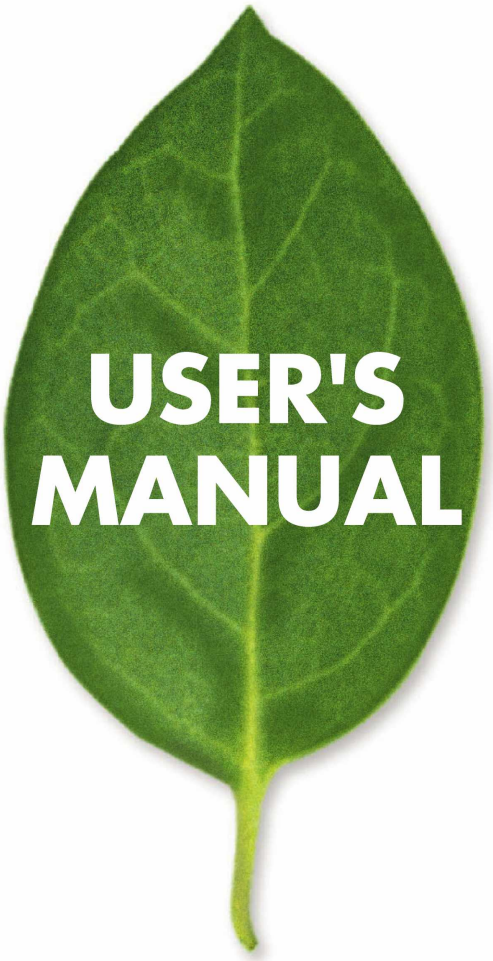

ギガビット WEB スマートプラススイッチ

SWP-0412/0420G

PLANEX COMMUNICATIONS INC.

Federal Communications Commission (FCC：米国連邦通信委員会)ステートメント

本製品は、FCC規則の第15部に準拠しています。運用上、以下の2つの条件を前提とします。

- 本製品が、有害な電波干渉の原因にならないこと
- 意図しない結果を運用に及ぼす可能性のある電波干渉を含め、本製品があらゆる電波干渉に対応すること

本製品が、FCC規則の第15部に従い、クラスAデジタルデバイスの制限に準拠していることは、テストおよび検証済みです。これらの制限は、住宅における導入事例において、有害な電波干渉に対して適切な保護を提供する目的で規定されています。本製品は電磁波を発生、使用、外部に放射するため、製造元の指示どおりに設置して使用しない場合は、無線通信を妨害する可能性があります。ただし、特定の導入事例で干渉が発生しないことを保証するものではありません。本製品がラジオまたはテレビの視聴に有害な電波干渉を引き起こし、本製品の電源をオン/オフすることで電波干渉の有無を確認できる場合、以下の単一または複数の対策によりユーザ側で電波干渉を補正することをおすすめします。

- 受信アンテナの向きまたは位置を変える。
- 本製品と受信機器の間隔を空ける。
- 受信機器を接続しているコンセントとは別系統のコンセントに本製品を接続する。
- 販売業者またはラジオ/テレビの専門技術者に問い合わせる。

警告! FCCの規定に準拠するため、グラフィックカードとモニタの接続にはシールドケーブルを使用する必要があります。コンプライアンス当事者によって明示的に承認されていない変更または修正を本製品に対して行った場合、本製品の使用する権限は取り消される可能性があります。

Canadian Department of Communications (CDC：カナダ通信省)ステートメント

本デジタル装置は、Canadian Department of Communicationsの電磁波障害規制で規定されている、デジタル装置からの電波雑音の放射に関するクラスAの制限を超えていません。

本クラスAデジタル装置は、カナダのICES-003に準拠しています。

第1章 はじめに

SWP-0412/0420G管理WEBスマートプラススイッチをお買い上げ頂き誠にありがとうございます。本製品をご利用いただくと、使いやすく高機能なユーザインタフェースを介して、LAN (ローカルエリアネットワーク)を管理することが可能になります。

本書では、SWP-0412/0420G WEB スマートプラススイッチの設定方法、および本製品を最大限に活用する上で必要な設定のカスタマイズ方法について解説します。

1.1 L2管理機能

- 10BASE-T/100BASE-TX/1000BASE-T自動検出ギガビットイーサネットポート
- 4つのスモールフォームファクタ(SFP)ギガビットインタフェースコンバータ(ミニGBIC)スロット
- トランスペアレントブリッジ
- ハードウェア補助のエージング対応4K MACアドレスキャッシュ
- 802.3xフロー制御
- 802.1Qベースのタグ付きVLAN、最大256系統のVLAN
- 802.1pクラスオブサービス、ポート単位に4つのキュー
- 802.3adリンク集合(手動)、最大7トランクグループ
- ポートミラーリング
- 802.1XおよびRADIUS
- RMON:4グループをサポート(1、2、3、9)
- SNMP v1、v2c
- MIB-II
- ファン、システム温度、電圧に対応するエンタープライズMIB
- Telnetリモートログイン
- ファームウエア更新および設定バックアップ用のFTP
- コンソール、Telnetから利用可能なコマンドラインインタプリタ
- WEB GUI
- ポートリンクステータスを示すLED
- LEDシステム

1.2 本書の表記規則

1.2.1 表記

- 頭字語については、本文および用語集の初出時に定義を記載します。
- SWP-0412/0420Gスイッチは、略して「当スイッチ」と呼称します。

・ 用語LANおよびネットワークは同義的に使用され、単一のサイトでイーサネット接続されたコンピュータを指します。

1.2.2 書体

・ 斜体はコマンドラインインタプリタのパラメータを表します。
・ 太字体のテキストはメニューおよびドロップダウンリストから選択する項目、およびプログラムからユーザに入力を促すテキスト文字列を表します。

1.2.3 シンボル

本書では、特定の指示や説明に対するユーザの注意を促すために、以下のアイコンを使用します。

注意: 現在のトピックに関する説明や追加情報を記載します。

定義: 多くのユーザにとって特殊であると思われる用語や頭字語について説明します。該当する用語は、用語集にも記載されています。

警告: 個人の安全やシステムの整合性に関連するメッセージを含む、重要度の高いメッセージを記載します。

第2章 SWP-0412/0420Gについて

2.1 パッケージ内容

SWP-0412/0420Gスイッチパッケージには以下の品目が同梱されています。
・SWP-0412/0420G
・電源ケーブル
・コンソールインタフェース(DB9)用のヌルモデムケーブル
・ラック設置キット(#6-32ネジ×6、ブラケット×2)
・保証書
・CD-ROM(ユーザーズ・マニュアル)
・安全に関する説明書

2.2 フロントパネル

フロントパネルには、システム、ファン、およびポートのステータスを示すLEDインジケータが装備されています。

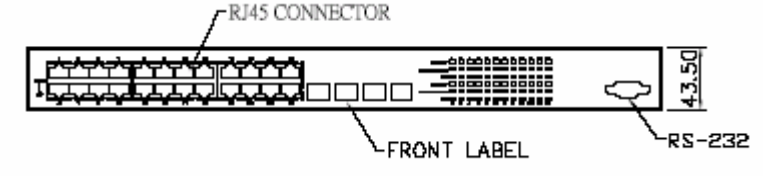

図1.フロントパネル

表1.フロントパネルのラベルとLED

ラベル	カラー	ステータス	説明
POWER	緑色	点灯	ユニットの電源がオン
		点滅	自己診断テスト、INIT (初期化)、またはダウンロード中
	橙色	点灯	温度または電圧の異常
	消灯		電源がオフ
10/100/1000 port status	緑色	点灯	リンク(RJ-45またはSFP)が存在、ポートが有効
		点滅	データの転送/受信中
	消灯		イーサネットリンクが存在しない
10/100/1000 port	緑色	点灯	1000Mbps

speed	橙色	点灯	100Mbps
	消灯		10Mbpsまたはリンクが存在しない
10/100/1000 port duplex	緑色	点灯	全二重
	橙色	点灯	半二重
	消灯		リンクが存在しない

2.3 リアパネル

当スイッチのリアパネルには、データおよび電源の接続用ポートが装備されています。

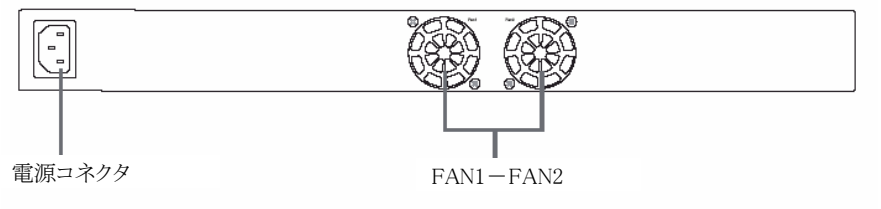

図2.リアパネル

表2.リアパネルのラベル

番号	ラベル	説明
1	電源コネクタ	電源ケーブルに接続
2	FAN1- FAN2	システムファン

2.4 技術仕様

表3.技術仕様

機能	
対応規格	IEEE802.3：10BASE-T
	IEEE802.3u：100BASE-TX
	IEEE802.3ab：1000BASE-T
	IEEE802.3z：1000BASE-SX/LX
	IEEE802.3x：フローコントロール
	IEEE802.1Q：TagVLAN
	IEEE802.1p：QoS
	IEEE802.3ad：LACP
	IEEE802.1X：ユーザ認証
ポート構成	SWP-0412G
	RJ-45コネクタ×16： 10BASE-T、100BASE-TX、1000BASE-T
	SWP-0420G
	RJ-45コネクタ×24： 10BASE-T、100BASE-TX、1000BASE-T
	（オートネゴシエーション、AutoMDI/MDI-X対応）
	拡張スロット（MiniGBIC用）x4
スイッチング方式	ストア&フォワード
ネットワークケーブル	UTP/STP LANケーブル
	10Mbps：カテゴリ3以上、100Mbps：カテゴリ5以上、 1000Mbps：カテゴリ5e以上
パケットバッファ	256KB
スイッチングファブリック	32Gbps (SWP-0412G) / 48Gbps (SWP-0420G)
MACアドレス登録数	4000個（全ポート合計）
スループット（64Byte）	10BASE-T：各ポート14,881パケット/秒
	100BASE-TX：各ポート148,810パケット/秒
	1000BASE-T/SX/LX：各ポート1,488,095パケット/秒
フローコントロール	全二重：IEEE802.3x、半二重：バックプレッシャー
ジャンボフレーム	最大フレームサイズ：約6,000Bytes without CRC
VLAN	TagVLAN
	TagVLAN PVID範囲:1～4094
	最大VLANグループ数：256（IP設定可能VLAN数：1）

機能	
Trunk	最大 8 ポート、7 グループ
QoS	4 レベル
	対応アルゴリズム：Strict
	対応 QoS 方式：CoS
SNMP	v1/v2c
	Trap v1/v2
	MIB II/Ethernet MIB/Bridge MIB/PrivateMIB
RMON	Statistics/History/Alarm/Event （1、2、3、9 グループ）
ポートミラーリング	Tx、Rx、Both
その他機能	EAP-MD5、EAP-TLS、VCT、RADIUS
ハードウェア仕様	
LED	SYSTEM、Link/Act、1000/100/10M、FDX
冷却ファン	搭載
MTBF	110,000 時間(SWP-0412G) / 88,000 時間(SWP-0420G)
電源	AC100V 50/60Hz
消費電力	最大 38W
外形寸法	442（W）×44（H）×200（D）mm
重量	2.3kg (SWP-0412G) / 2.5kg(SWP-0420G)
19 インチラック	対応
動作時環境	温度：0～40℃
	湿度：35～85%（結露なきこと）
保存時環境	温度：-20～70℃
	湿度：0～95%（結露なきこと）
取得承認規格	CE、FCC Class A、VCCI Class A
その他	
対応 OS	Windows XP/2000/Me/98SE
各種設定方法	Telnet、WEB ブラウザ(要 JAVA 環境)、コンソール
保証期間	1 年間

■注意事項

※Trunk 接続は LACP には対応しません。Static 構成のみ対応します。

※拡張スロットは RJ-45 コネクタとのコンボポート。

※IEEE802.1X については EAP-MD5,EAP-TLS でのユーザ認証の動作を確認しています。

※製品仕様は予告無く変更する場合があります。あらかじめご了承ください。

※最新情報は、弊社ホームページ（http://www.planex.co.jp）を参照ください。

第3章 クイックスタートガイド

本章では、SWP-0412/0420Gの環境を設定する基本的な手順について解説します。
『SWP-0412/0420G Installation Guide』もご覧ください。

パート1では、SWP-0412/0420Gを平面またはラックに設置する方法について説明します。

パート2では、ハードウェアを設定する手順について説明します。

パート3では、SWP-0412/0420Gの基本設定を構成する方法について説明します。

手順を進める前に、ネットワーク管理者から以下の情報を入手してください。

- 当スイッチのIPアドレス
- ネットワークのデフォルトゲートウェイ
- ネットワークのネットワークマスク

3.1 パート1－ハードウェアの設置

電源コンセント、およびコンピュータまたはネットワークに装置を接続します。

3.1.1 スイッチを平面上に設置

当スイッチは、スイッチ自体と付属品の荷重に耐えられる水平面に設置する必要があります。当スイッチ底面のマークされた位置に4つの防振パッドを取り付けてください。

3.1.2 スイッチをラックにマウント

1. 当スイッチの両側にブラケットを取り付けて、支柱部分をスイッチに挿入します。
2. 2本のネジを挿入して締め、ラックの両側にブラケットを固定します。

3.2 パート2－スイッチの設定

電源コンセント、およびコンピュータまたはネットワークに装置を接続します。

3.2.1 コンソールポートの接続

コンソール管理を目的として当スイッチに接続する場合は、RS232C (DB9)を使用します。
WEBインタフェースを使用する場合は、イーサネットケーブルを使用してコンピュータを当スイッチに接続します。

3.2.2 コンピュータまたはLANへの接続

直接コンピュータを当スイッチのポートに接続する場合は、イーサネットケーブルを使用できます。

ハブ/スイッチを当スイッチのポートに接続する場合も、イーサネットケーブルを使用できます。

コンピュータ、ハブ、またはスイッチへの接続には、クロスオーバまたはストレートのイーサネットケーブルを使用できます。

注意: 1000BASE-Tポートへの接続には、カテゴリ5eツイストペアイーサネットケーブルを使用してください。当該ケーブルを使用しなければ、リンク速度は1Gbpsを下回ります。

3.2.3 電源ケーブルの取り付け

1. 電源ケーブルを当スイッチ背面の電源コンセントに接続し、電源ケーブルのもう一端を壁面のコンセントまたは電源タップに接続します。

2. 表4の説明と照らし合わせて、正面のLEDインジケータをチェックします。LEDが説明どおりに点灯している場合、当スイッチのハードウェアは適切に動作しています。

表4.LEDインジケータ

番号	LED	説明
1	システム	緑色の点灯は、装置の電源がオンであることを示します。このライトがオフの場合は、電源アダプタが当スイッチおよび電源に接続されているかどうかチェックしてください。
2	スイッチポート SWP-0412G:[1]－[16] SWP-0420G:[1]－[24]	緑色の点灯は装置がLANと通信可能な状態であることを示し、点滅はデバイスがLAN上のコンピュータとの間でデータの送受信中であることを示します。

3.3 パート3－管理用の基本的なスイッチ設定

ハードウェアの接続が終了したら、スイッチの基本設定を構成します。当スイッチは以下の方法で管理できます。

- WEBインタフェース:Java対応のIE5.5以降のバージョンで、当スイッチの管理に対応する一連のページが用意されています。
- コマンドラインインタフェース:コンソールポートを使用して当スイッチを管理します。

3.3.1 コンソールポートからの設定

1. 同梱のRS-232Cクロスケーブルを使用して、当スイッチ背面のコンソールポートに接続します。このポートはDB-9オスコネクタであり、データ端末装置(DTE)接続用に実

装されています。ケーブルの取り付けネジを締めて、コネクタに固定します。

端末エミュレーションソフトウェア(ハイパーターミナルなど)が動作している
コンピュータにケーブルのもう一端を接続します。

2. 端末エミュレーションソフトウェアの設定が以下のとおりであることを確認します。

   a) 適切なシリアルポート番号を選択している。
   b) データボーレートを9600に設定している。
   c) データフォーマットをパリティなし、8データビット、1ストップビットに設定している。
   d) フローコントロールなし。
   e) エミュレーションモードにVT100を設定している。

3. 端末の設定が終了すると、端末にプロンプト「(PLANEX)%」が表示されます。

4. 「login」と入力し、コマンドラインインタフェースにアクセスします。デフォルトのユーザ名は「admin」です。パスワードには「password」と入力してEnterキーを押します。

   パスワードはCLIからいつでも変更できます(セクション5.3.1を参照)。不正なアクセスからスイッチを保護するため、デフォルトのパスワードはできるだけ速やかに変更してください。

5. 以下のステップに従って、当スイッチにIPアドレスを割り当てます。

   a) 「net interface ip sw0 <IPアドレス> <ネットワークマスク>」と入力します。たとえば、スイッチのIPが192.168.10.1、ネットワークマスクが255.255.255.0である場合、「net interface ip sw0 192.168.10.1 255.255.255.0」と入力してください。
   b) ネットワークを介して当スイッチを管理する必要がある場合、デフォルトゲートウェイまたは静的ルートエントリが必要になります。図3に示すように、デフォルトのルートエントリとして「net route static add 0.0.0.0 <ネットワークゲートウェイIP> 0.0.0.0 1」を入力します。

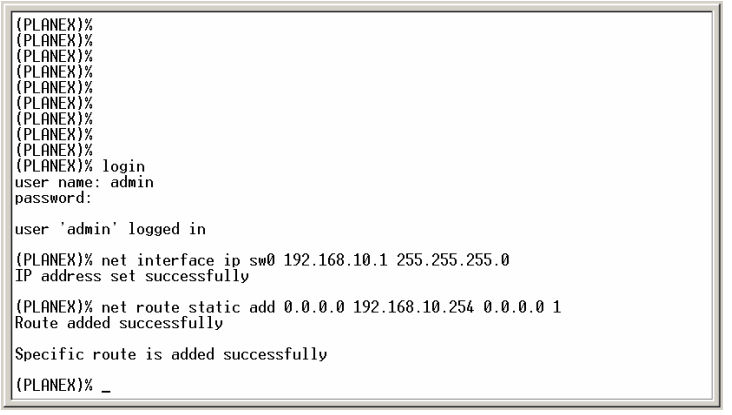

図3.ログインおよびIP設定画面

3.3.2 WEBインタフェースからの設定

コンピュータを当スイッチに適切に接続するには、ネットワークで有効なIPがコンピュータに設定されている必要があります。ネットワーク管理者に問い合わせて、当スイッチ用の有効なIPを入手してください。

当スイッチのIPアドレスをデフォルトから変更する場合は、セクション3.3.1の手順に従ってください。当スイッチはDHCPクライアント機能をサポートしていないので、WEBインタフェースを使用するには、当スイッチ用の有効な静的IPが必要になります。

1. 当スイッチがアクセス可能なネットワークに接続した任意のコンピュータで、WEBブラウザ(Internet Explorer)を開き、以下のURLを「アドレス」ボックスに入力して、Enterキーを押します。

   http://192.168.1.1

   これは当スイッチの工場出荷時のIPアドレスです。図4に示すように、ログイン画面が表示されます。

図4.ログイン画面

   ユーザ名とパスワードを入力して[OK]をクリックし、Configuration Managerを開きます。インタフェースへの初回ログイン時には、以下のデフォルトを使用します。

   デフォルトのユーザ名:admin

   デフォルトのパスワード:password

   注意: パスワードはいつでも変更できます(セクション5.3.1「システムコマンド」を参照)。

2. システム設定を保護するには、「System」カテゴリの「Administration」ページで認証機能を有効にしてください。認証が無効な場合は、ログイン認証は省略されます。

3. 新しいIPアドレスを設定するには、「System」→「IP Setup」と選択します(図8を参照)。IPアドレス、ネットワークマスク、およびデフォルトゲートウェイを入力し、[OK]をクリックします。

4. 新しいアドレスがデフォルトと異なる場合、ブラウザは当スイッチのステータスウィンドウの更新およびページの取得ができません。

   「アドレス」ボックスに正しいIPアドレスを再入力し、Enterキーを押します。WEBリンクが表示されます。

5. WEBアクセスの認証を有効にするには、メニューリストの「Administration」をクリックし、「Enabled」を選択して保護を開始します。

   [OK]をクリックすると、ログインウィンドウが即時に表示されます。次のページの図をご覧ください。

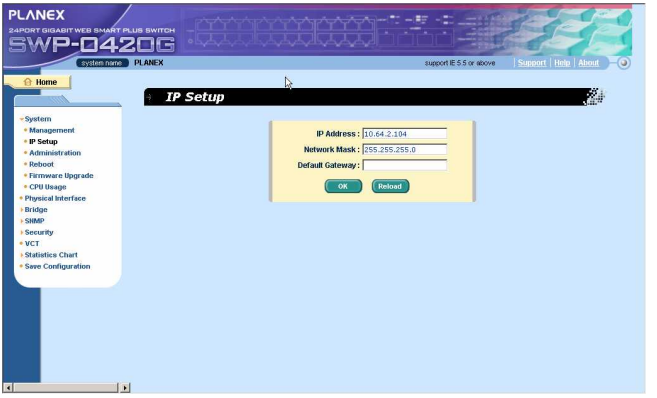

図5.IP Setup

第4章 WEBインタフェースによる管理

当スイッチをインターネットから管理するためのWEBページが用意されています。このプログラムは、Microsoft Internet Explorer 5.5以降のバージョンと最適に連携できるよう設計されています。

注意: Netscape,Firefoxなどはサポートされていません。

4.1 WEBユーザインタフェースへのログイン

1. コンピュータからWEBブラウザを開き、以下のWEBアドレスを「アドレス」ボックスに入力して、Enterキーを押します。

   http://192.168.1.1

   これは当スイッチの工場出荷時のIPアドレスです。図6に示すように、ログイン画面が表示されます。

図6.Configuration Managerのログイン画面

2. ユーザ名とパスワードを入力して[OK]をクリックします。

   プログラムへの初回ログイン時には、以下のデフォルトを使用します。パスワードはCLIインタフェースからいつでも変更できます(37ページのセクション5.3.1を参照)。

   デフォルトのユーザ名:admin

   デフォルトのパスワード:password

   プログラムにログインするたびに、ホームページが表示されます(図11および12を参照)。

図7.ホームページ

4.2 機能レイアウト

標準のWEBページは、3つの異なるフレームで構成されています。図8に示すように、上部フレームにはスイッチのロゴが表示されます。

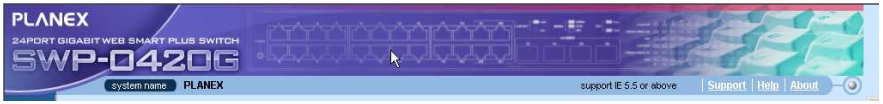

図8.上部フレーム

図9に示すように、左フレームはメニューフレームであり、スイッチ設定に使用できるすべての機能が表示されます。これらの機能は、「System」、「Bridge」など、カテゴリ別にグループ化されています。いずれかの機能をクリックすると、特定の設定ページが表示されます。

図9.展開した状態のメニューリスト

右フレームには、設定ページまたは統計情報の図表が表示されます。

詳細については、セクション4.3を参照してください。

4.2.1 メニュー操作のヒント

- 関連するメニューのグループを展開するには、対応するグループ名をクリックします。展開後、▸記号は▾に変化します。
- 関連するメニューのグループを縮小するには、対応するグループ名をクリックします。グループ名の横に▸記号が表示されます。
- 特定の設定ページを開くには、対象のメニュー項目をクリックします。

4.2.2 一般的に使用されるボタンとアイコン

以下の表では、アプリケーションで使用する個別のボタンとアイコンの機能について説明します。

表5.一般的に使用されるボタンとアイコン

ボタン/アイコン	機能
[OK]	現在のページで行った変更の内容を保存
[Add]	静的MACアドレスやファイアウォールACLルールなど、既存の設定をシステムに追加
[Modify]	既存のエントリを変更
[Edit]	静的ルートやフィルタACLルールなど、システムの既存の設定を変更
[Remove]	静的ルートやフィルタACLルールなど、選択した項目を削除
[Reload]	更新した統計情報や設定で現在のページを再表示

4.3 System

Systemページには、マネージメント、IPセットアップ、アドミニストレーション、再起動、およびファームウエア更新に対応する機能が用意されています。

4.3.1 Management

Managementページには、以下の情報が含まれています。

Model Name：製品名。

MAC Address：スイッチのMACアドレス。

System Name：システムを識別する目的でユーザが割り当てた名前(編集可能)。

System Contact (編集可能)

System Location (編集可能)

変更内容を保存して即時に反映するには、[OK]をクリックします。図10に示すように、設定内容を更新表示するには[Reload]を使用します。

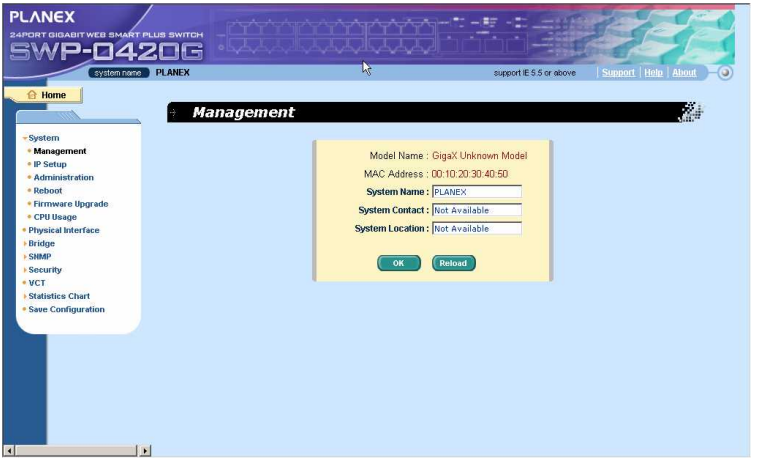

図10.Management

4.3.2 IP Setup

当スイッチは、静的IP割り当てをサポートしています。IP Setupには、以下の編集可能な情報が含まれています。

IP Address：スイッチ管理インタフェースに割り当てる静的IPアドレス。

Network Mask

Default Gateway

変更内容を保存して即時に反映するには、[OK]をクリックします。図12に示すように、設定内容を更新表示するには[Reload]を使用します。

図11.IP Setup

4.3.3 Administration

Administrationページでは、パスワード保護によるWEBユーザの認証を有効または無効にできます。

変更内容を保存して即時に反映するには、[OK]をクリックします。図12に示すように、設定内容を更新表示するには[Reload]を使用します。パスワード保護を有効にすると、即時に再ログインする必要があります。

注意:　　パスワードはCLIインタフェースからいつでも変更できます(セクション5.3.1を参照)。

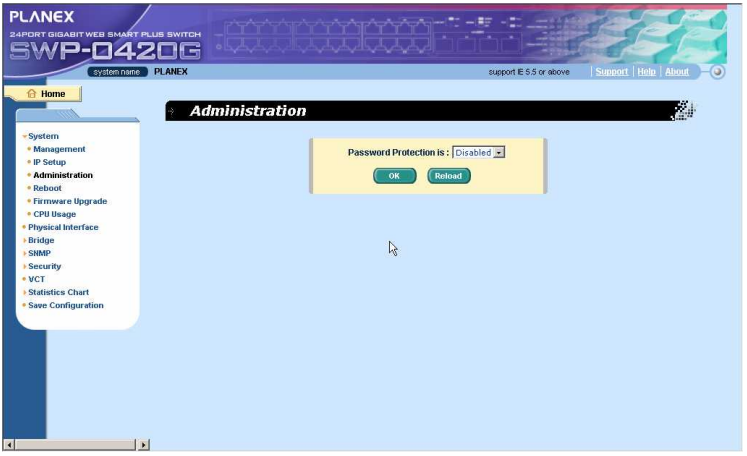

図12.Administration

4.3.4 Reboot

Rebootページには、[Reboot]ボタンが含まれています。このボタンをクリックすると、当スイッチのシステムを再起動します。

警告: 当スイッチのシステムを再起動すると、ネットワークトラフィックが停止し、WEBインタフェース接続が終了します。

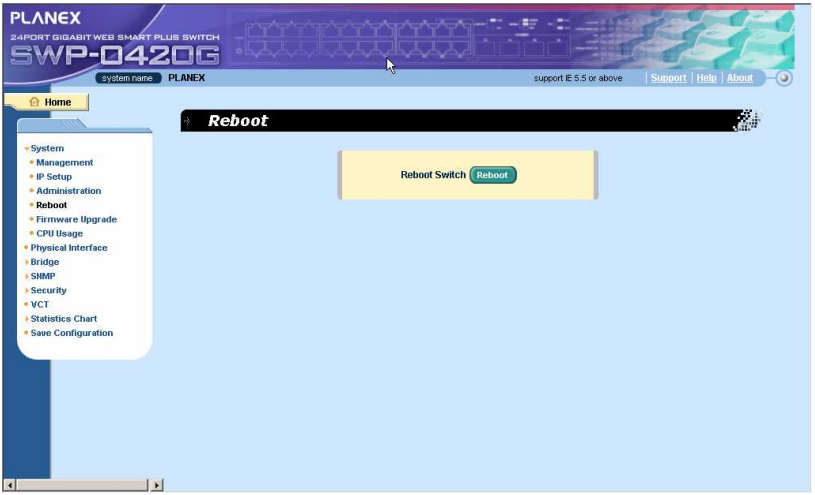

図13. Reboot

4.3.5 Firmware Upgrade

Firmware Upgradeには、以下の情報が含まれています。

Hardware Version：ハードウェアリビジョン番号を表示します。

Boot ROM Version：ブートコードのバージョンを表示します。

Firmware Version：現在動作中のファームウエアバージョンを表示します。この番号は、ファームウエア更新後に更新されます。

ファームウエアの場所をファームウエアのフィールドに直接入力するか、参照をクリックしてプロンプトウィンドウからファームウエアのファイル名を選択します。当スイッチのファームウエアを更新するには、[Upload]をクリックします。詳細については、図14を参照してください。

注意: 「upload」ボタンをクリックすると、割り当てたファームウエアを当スイッチにロードします。正常にファームウエアが更新されると、当スイッチのシステムは再起動します。WEBインタフェースに再ログインしてください。

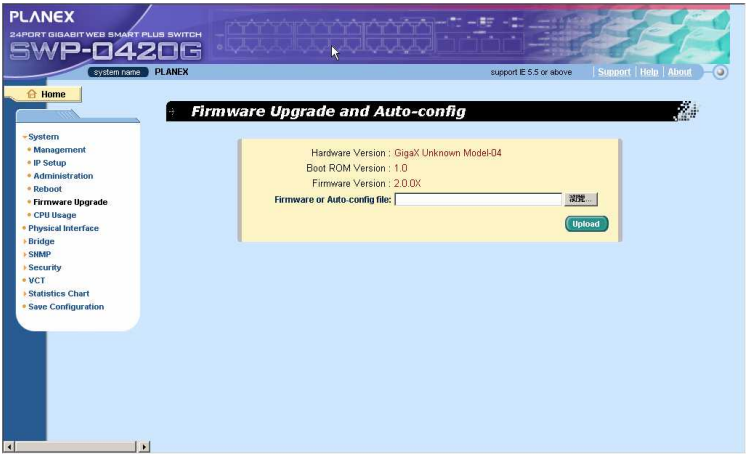

図14.Firmware Upgrade

4.3.6 CPU Usage

このページには、当スイッチのCPU使用率が表示されます。ユーザ側で表示カウントを設定するには、1～10の範囲で有効な数値を入力します。次に、[Query]をクリックすると、CPU使用率が表示されます。たとえば、ユーザが5を入力すると、表示ウィンドウにはCPU使用率が5回表示されます。

図15.CPU Usage

4.4 Physical Interface

Physical Interfaceには、イーサネットポートのステータスがリアルタイムに表示されます。以下のフィールドでポートを設定できます。

Port：設定するポートを選択します。

Admin：ポートを有効/無効にします。

Mode：速度とデュプレクスのモードを設定します。

Flow Control：802.3xフローコントロール機構を有効/無効にします。

Port Status Window：各ポートの以下の情報を表示します。

a) Link status：現在のリンクの速度とデュプレクス、もしくはリンクの停止

b) Admin：ポートを無効化/有効化する設定値

c) Mode：リンク速度とデュプレクスモードの設定値

d) Flow Control：802.3xフローコントロール機構を有効化/無効化する設定値

対応するポート番号を選択してポート設定を構成し、[Modify]ボタンをクリックします。フィールドを変更すると、表示ウィンドウの内容が更新されます。ただし、新しい設定はSave Configurationを実行するまで有効になりません。

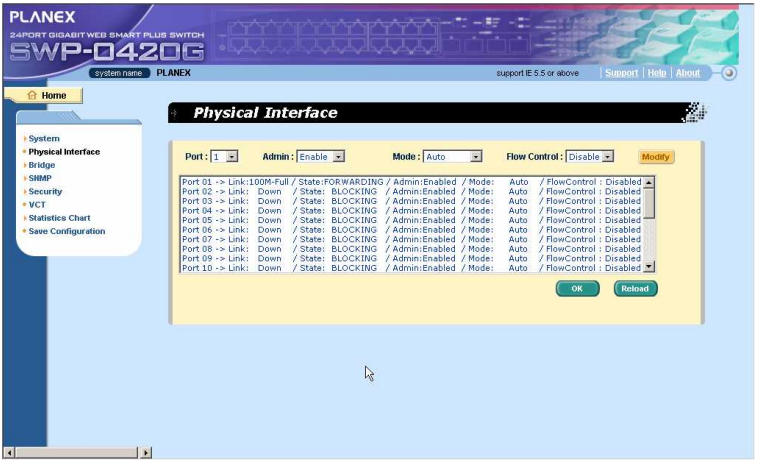

図16.Physical Interface

4.5 Bridge

Bridgeグループには、Link Aggregationなどレイヤ2設定の大半が含まれています。

4.5.1 Link Aggregation

このページは、Link Aggregationグループ(ポートトランキング)を設定します。当スイッチには、7つのLink Aggregationグループを設定できます。

Show Trunk：新しく作成したグループについては、「Add a new Trunk」を選択するか、以下のフィールドおよびポートアイコンで、表示する既存のグループを選択します。

Port Selection Criterion：source and destination MAC hash based (L2)、source and destination IP hash based (L3)、source and destination Port hash based (L4)のいずれかのアルゴリズムを選択します。

Name：グループ名。

Trunk ID：グループ名のほかにトランクグループを識別する番号。

Remove Trunk：選択したトランクを削除します。

Port Icons：これらのポートアイコンは、フロントパネルと同様にリスト化します。グループメンバを選択するには、アイコンをクリックします。グループからポートを削除するには、選択したポートを再クリックします。

スイッチに設定を送信するには、[OK]をクリックします。設定を現行値で更新表示するには、[Reload]をクリックします。設定を有効にするには、Save Configurationページに移動して[Save]をクリックします。

リンク速度とデュプレクスモードをチェックして、トランクが物理的にアクティブであることを確認する必要があります。Physical Interfaceに移動し、トランクポートのランタイムステータスウィンドウでリンクモードをチェックします。すべてのトランクメンバが同じ速度および全二重モードである場合、トランクグループは適切に設定されます。いずれかのメンバが同じ速度または全二重モードに該当しない場合、トランクは適切に設定されません。リンクパートナをチェックし、トランクグループのすべてのメンバに対して同じ速度および全二重モードになるように設定を変更します。

注意: 3つのトランク方式が使用されます。対象はシステム単位であり、ポート単位ではありません。

- Link Aggregationグループ内のすべてのポートは、全二重モードおよび同じ速度で動作する必要があります。
- Link Aggregationグループ内のすべてのポートは、オートネゴシエーションモードまたは全二重モードで構成する必要があります。

  この設定は、全二重リンクを可能にします。全二重フォースモードでポートを設定するには、リンクパートナに同じ設定を構成する必要があります。これに該当しない場合、Link Aggregationの動作に異常が発生する可能性があります。
- Link Aggregationグループ内のすべてのポートに同じVLAN設定を構成する必要があります。

・ Link Aggregationグループ内のすべてのポートは、単一の論理リンクとして取り扱われます。つまり、いずれかのメンバの属性が変更された場合、他のメンバの属性も変更されます。たとえば、トランクグループがポート1とポート2で構成されている場合にポート1のVLANを変更すると、ポート2のVLANもポート1と同様に変更されます。

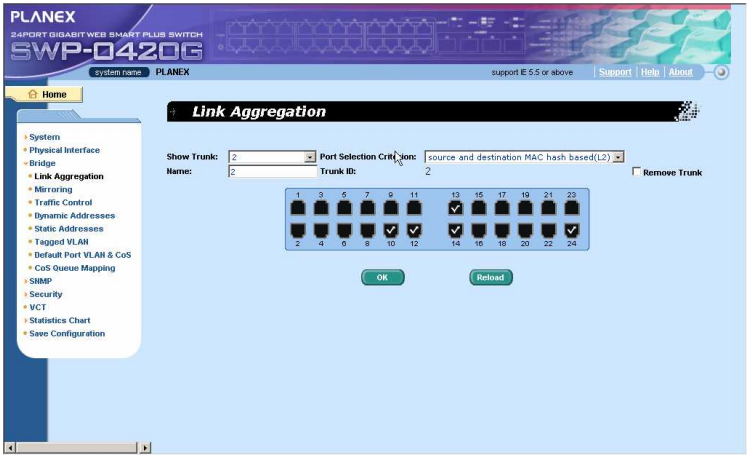

図17.Link Aggregation

4.5.2 Mirroring

ミラーリング機能はネットワークトラフィックアナライザと連携することによって、ユーザによるネットワークトラフィック監視を支援します。発信パケットまたは着信パケットについて、選択したポートの監視が可能です。

Mirror Mode：選択したグループに対するミラー機能を有効/無効にします。

Monitor Port：選択した監視対象ポートの全トラフィックのコピーを受信します。

注意：　モニタポートは、Link Aggregationグループに属することはできません。

モニタポートは、通常のスイッチポートとして動作できません。パケットのスイッチングやアドレス学習は行いません。

ミラー対象の出力ポートとしてサポートされるポート数は4つに限定されます。

スイッチに設定を送信するには、[OK]をクリックします。設定を現行値で更新表示するには、[Reload]をクリックします。

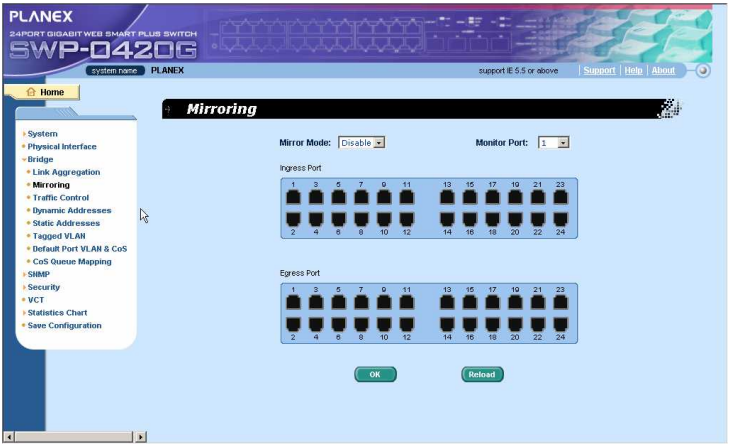

図18.Mirroring

4.5.3 Traffic Control

トラフィックコントロールは、当スイッチの帯域幅で、ブロードキャストパケットやマルチキャストパケットなどを含む、パケットのフラッディング(全ポートへのパケット送出)を防止します。制限値は、選択したタイプのパケットの合計数を制限するしきい値です。たとえば、ブロードキャストおよびマルチキャストが有効な場合、これら2つのタイプの合計トラフィック量は制限値を超過しません。[OK]をクリックし、新しい設定を保存します。設定を有効にするには、Save Configurationに移動して[Save]をクリックします。

図19.Traffic Control

4.5.4 Dynamic Addresses

このページには、ポート、VLAN ID、または特定のMACアドレスによる動的MACアドレス検出の結果が表示されます。動的アドレスはスイッチによって学習されたMACアドレスであり、該当するアドレスが所定の経過時間(エージタイム)内に再び学習されなかった場合、アドレステーブルから削除(エージアウト)されます。ユーザ側でエージタイムを設定するには、10～600の範囲で有効な数値(秒単位)を入力します。[OK]をクリックし、新しいエージタイムの値を保存します。設定を有効にするには、Save Configurationに移動して[Save]をクリックします。

MACアドレスを検出するには、Port、VLAN ID、or/and MAC addressをチェックして[Query]をクリックします。アドレスウィンドウにクエリ結果が表示されます。

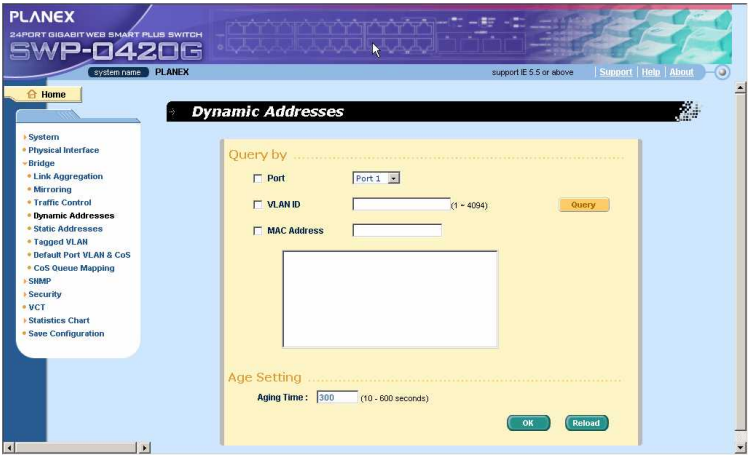

図20.Dynamic Address

4.5.5 Static Addresses

当スイッチのアドレステーブルにはMACアドレスを追加できます。この方法で追加したMACアドレスは、アドレステーブルから削除(エージアウト)されません。これに該当するアドレスを静的アドレスと呼びます。

MAC Address:MACアドレスを入力します。

VLAN ID:MACが属するVLAN IDを入力します。

Port Selection:MACが属するポートを選択します。

Discard:MACアドレスが、宛先アドレス、ソースアドレス、またはこの両方としてパケットに現れた場合に、パケットフィルタリングを実行します。

上記の情報に基づいて新しい静的MACアドレスを作成した場合は、[Add]をクリックします。

新しく追加したエントリは、アドレスウィンドウに表示されます。既存のアドレスを削除するには、対象のエントリをマウスで選択して[Remove]をクリックします。[Modify]ボタンは、既存のMACアドレスエントリを更新します。設定を保存して有効にするには、[OK]をクリックします。設定を現行値で更新表示するには、[Reload]をクリックします。設定を有効にするには、[Save Configuration]に移動して[Save]をクリックします。

図21.Static Address

4.5.6 Tagged VLAN

このページでは、最大256系統のVLANグループを設定して表示できます。当スイッチにはデフォルトVLANが用意されています。デフォルトVLANは変更できません。この機能により、当スイッチの誤動作を防止します。デフォルトVLANを除いて、既存のVLANを削除できます。

ポートをタグ付きポートまたはタグ無しポートに割り当てるには、ポートのボタンで切り替えます。以下の3種類のボタンが表示されます。

「U」タイプ：送信パケットからVLANタグを削除するタグ無しポート。

「T」タイプ：このポートから送信されるすべてのパケットに対するタグ付け。

「blank (空白)」タイプ：VLANグループのメンバに該当しないポート。

単一のタグ無しポートが同時に複数のVLANグループに属している場合、スイッチの処理が混乱し、トラフィックが停滞してしまいます。この現象を回避するため、当スイッチでは単一のタグ無しポートは同時に単一のVLANにのみ属するように許可を行います。具体的には、タグ無しポートは「PVID」と呼ばれるVLANグループに属し、「Default Port VLAN & CoS (デフォルトポートVLAN & CoS)」ページで設定されます。あるVLANから別のVLANにタグ無しポートを割り当てるには、最初に対象のポートを元のVLANから削除するか、元のVLANでタグ付きに変更する必要があります。

Show VLAN ：既存のVLANを選択して表示するか、「Add a new VLAN」を選択して新しいVLANグループを作成します。

Name：VLAN名。

VLAN ID：新しいVLANの作成時にユーザ側がVLAN IDを入力する必要のあるフィールド。

Remove VLAN：既存のVLANを削除します。

［OK］をクリックし、設定を保存します。設定を有効にするには、Save Configurationに移動して［Save］をクリックします。

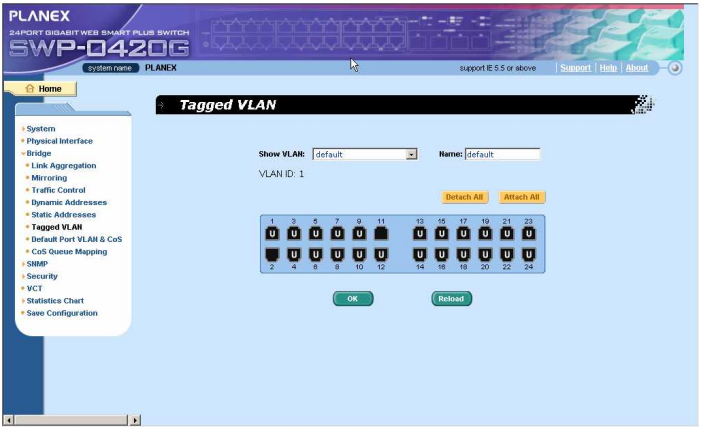

図22.Tagged VLAN

4.5.7 Default Port VLAN & CoS

このページには、各ポートのいくつかのVLANタグ関連フィールド設定が含まれています。具体的には、以下のものです。

Port：設定するポートを選択します。

PVID：ポートベースのVLAN ID。対象のポートから受信された各タグ無しパケットは、このVLANグループIDでタグ付けされます。

CoS (Class of Service) value：対象のポートから受信された各タグ無しパケットは、タグ付きVLANでこのCoSに割り当てられます。4つの内部トラフィッククラスが8つの優先度に対応しているので、CoS Queue Mappingに従って、CoS値0、2、5、7のみが有効になります。

ポートリストウィンドウの内容を変更するには、［Modify］をクリックします。［OK］をクリックし、設定を保存します。設定を有効にするには、Save Configurationページに移動して［Save］をクリックします。

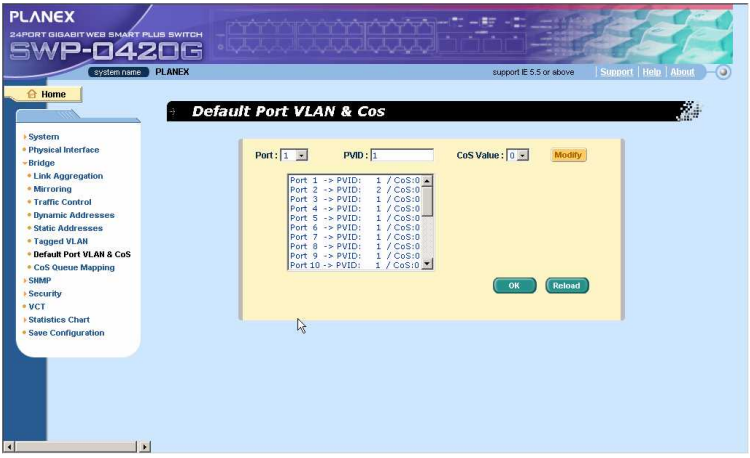

図23.Default Port VLAN & CoS

4.5.8 CoS Queue Mapping

当スイッチは、厳密な優先度スケジューラによりポート単位に4つの発信キューをサポートしています。すなわち、各CoS値は4つのキューのいずれかにマッピングすることができます。キュー4には、パケット送信の最も高い優先度が設定されています。[OK]をクリックし、設定を保存します。設定を有効にするには、Save Configurationページに移動して[Save]をクリックします。

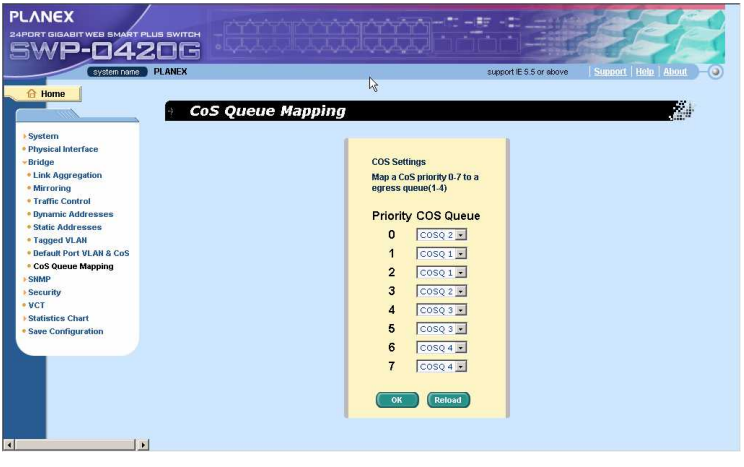

図24.CoS Queue Mapping

4.6 SNMP

このグループは、Community Table、Host Table、およびTrap Settingを含むSNMP設定を提供します。これにより、さらにセキュアな管理およびアクセス制御が実現します。

4.6.1 Community Table

別のコミュニティ名を入力し、当該コミュニティにアクションの設定権限(書き込みアクセス)を与えるかどうか指定するには、このチェックボックスをオンにします。[OK]をクリックして設定を確定して保存するか、[Reload]をクリックしてページの表示を更新します。

図25.Community Table

4.6.2 Host Table

このページでは、Community Tableページで入力したコミュニティ名にホストIPアドレスをリンクします。IPアドレスを入力し、ドロップダウンリストからコミュニティ名を選択します。[OK]をクリックして設定を確定して保存するか、[Reload]をクリックしてページの表示を更新します。

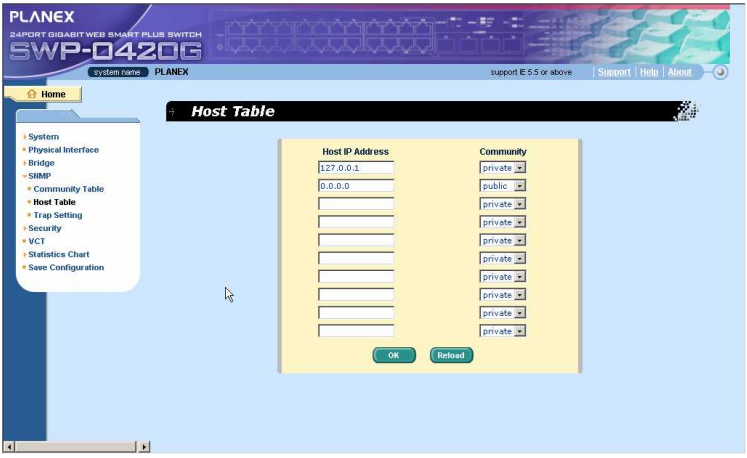

図26.Host Table

4.6.3 Trap Setting

SNMPトラップ機能を有効にし、別バージョン(v1またはv2c)でトラップパケットの送信を可能にするには、トラップ対象の宛先IPアドレスとコミュニティ名を設定します。[OK]をクリックして設定を確定して保存するか、[Reload]をクリックしてページの表示を更新します。

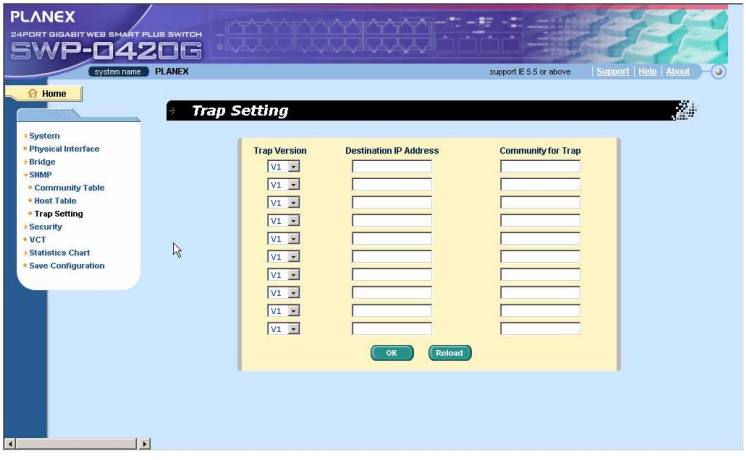

図27.Trap Setting

4.7 Security

当スイッチは、802.1Xポートベースのセキュリティ機能を備えています。当スイッチのポートにアクセスできるのは、許可済みのホストのみに限定されます。認証に失敗したホストに対しては、トラフィックはブロックされます。認証サービスは、RADIUSサーバまたは当スイッチ内のローカルデータベースによって提供されます。

この機能を有効にする前に、ユーザ/ポートのVLAN情報を認証サーバで適切に設定する必要があります。

4.7.1 Port Access Control

Port Access Controは、さまざまな802.1Xパラメータを構成する目的で使用します。802.1Xでは、RADIUSサーバまたはローカルデータベースを使用してポートユーザを認証します。

最初の部分は、次のグローバル設定を含むBridge Settingです。

- Reauthentication：有効にすると、再認証時間が経過した時点で、当スイッチがポートユーザを再認証します。
- Reauthentication Time：Reauthenticationを有効にした場合、当スイッチが認証要求をポートユーザに再送信する際に参照する時間間隔を表します(上記を参照)。
- Authentication Method：ポートユーザの認証に、RADIUSまたはローカルデータベースの使用が可能です。
- Quiet Period：RADIUSまたはローカルデータベースからの認証に失敗した場合、当スイッチはポートユーザに別の認証要求を送信する前に、この期間が経過するまで待機します。
- Retransmission Time：ポートユーザが当スイッチからの認証要求に応答できなかった場合、当スイッチはこの期間が経過するまで待機してから、ポートユーザに別の認証要求を送信します。
- Max Reauthentication Attempts：ポートユーザが当スイッチからの認証要求に応答できなかった場合のリトライ回数。

  2番目の部分は、Port settingです。変更が終了したら、[Modify]をクリックします。
- Port：設定するポートを指定します。
- Multi-host：有効にした場合、選択したポートに接続しているすべてのホストに対して、そのいずれかが認証に成功していることを条件にポートの使用を許可します。無効にした場合、認証に成功したホストの中から単一のホストに限定してポートの使用を許可します。
- Authentication Control：force_authorizedを選択した場合、選択されたポートは強制的に許可されます。具体的には、すべてのホストからのトラフィックが通過を許可されます。これに対して、[force_unauthorized」を選択した場合、選択されたポートはブロックされ、トラフィックの通過は許可されません。[Auto」を選択した場合、選択されたポートの動作は802.1Xプロトコルによって制御されます。通常の状況では、すべてのポートを[Auto」に設定することをおすすめします。

[OK]をクリックし、設定を確定します。設定を現行値で更新表示するには、[Reload]をクリックします。

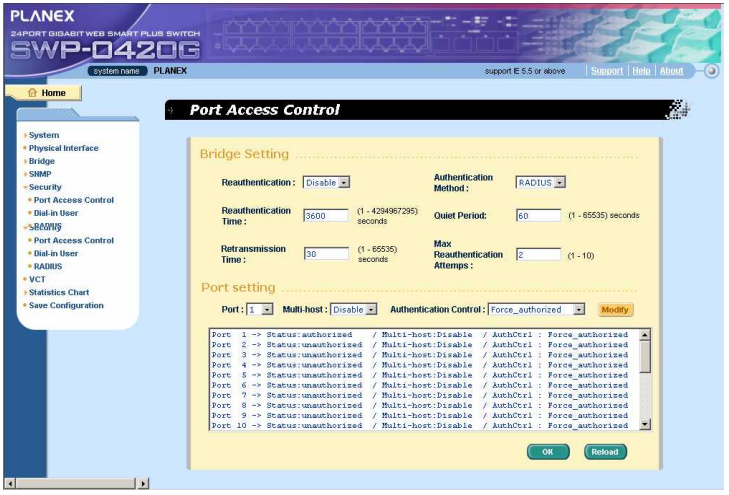

図28.Port Access Control

4.7.2 Dial-In User

Dial-In Userは、当スイッチのローカルデータベースにユーザを定義する目的で使用します。

- User Name：新しいユーザ名。
- Password：新しいユーザのパスワード。
- Confirm Password：上記のパスワードを再入力します。

[Add]をクリックし、新しいユーザを追加します。変更が終了したら、[Modify]をクリックします。選択したユーザを削除するには、[Remove]をクリックします。[OK]をクリックし、設定を確定します。設定を現行値で更新表示するには、[Reload]をクリックします。

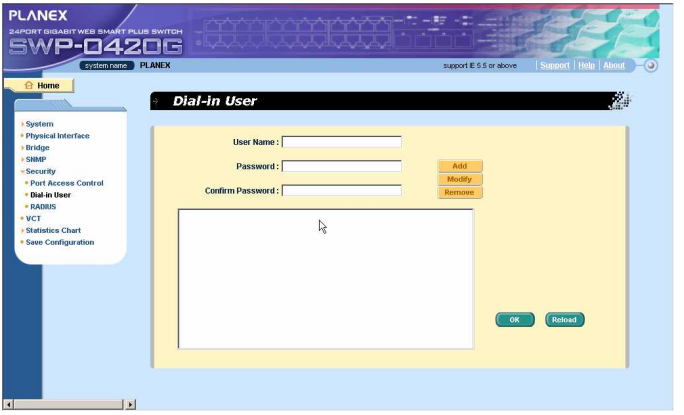

図29.Dial-In User

4.7.3 RADIUS

外部RADIUSサーバを使用するには、以下のパラメータを設定する必要があります。

- Authentication Server IP：RADIUSサーバのIPアドレス。
- Authentication Server Port：RADIUSサーバが受信待機(リスニング)中のポート番号。
- Authentication Server Key：SWP-0412/0420GとRADIUSサーバとの間の通信に使用するキー。
- Confirm Authentication Key：上記のキーを再入力します。

注意：　当スイッチに接続したRADIUSサーバのVLANは、システム管理インタフェースのVLANと同じである必要があります。

[OK]をクリックし、設定を確定します。設定を現行値で更新表示するには、[Reload]をクリックします。

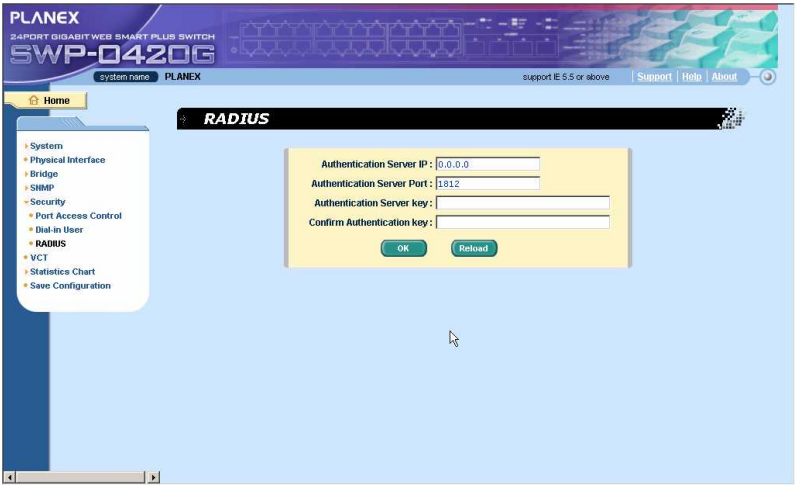

図30.RADIUS

4.8 VCT

VCTは、Virtual Cable Testerの頭字語です。VCTの主な機能は、ケーブルの障害(切断や短絡)を検出し、障害があると推定される箇所を報告することです。

さらに、VCTはノーマルケーブルの推定ケーブル長だけでなく、PHYタイプ(100M、1000M、10000M)の検出も可能です。ケーブル長の試算は、Giga (ギガ)速度モードのみをサポートしています。

ポート番号を選択し、[GO]をクリックします。選択に応じてテスト結果が表示されます。

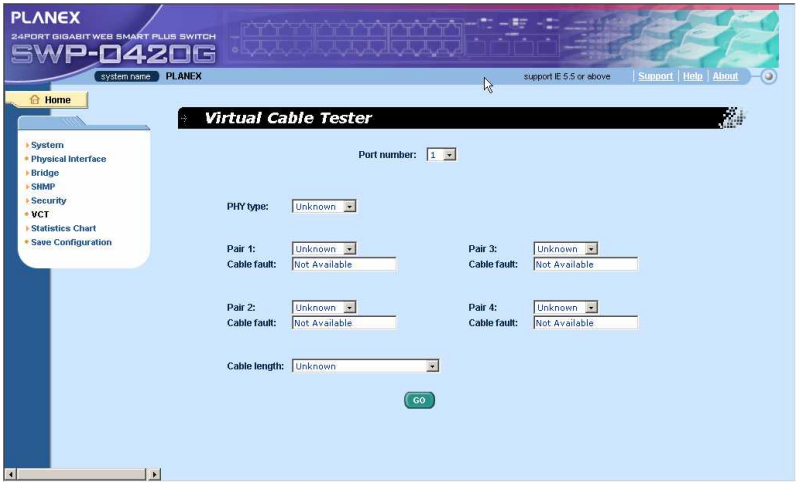

図31.VCT

4.9 Statistics Chart

Statistics Chartページは、さまざまなグラフ形式でネットワークフローを表示します。グラフを更新表示する時間間隔を指定できます。各ページのさまざまなグラフ表示で、ネットワークトラフィック量を監視できます。

新しいデータをスイッチから取得する間隔を設定するには、Refresh Rateをクリックします。

統計やポートの表示を区別するには、Colorを選択します。最後にDrawをクリックし、ブラウザでグラフを描画します。Drawをクリックするたびに、統計表示はリセットされます。

4.9.1 Traffic Comparison Chart

このページは、1項目に対して1グラフの形式で、すべてのポートを対象とする統計項目を表示します。表示する統計項目を選択してDrawをクリックすると、ブラウザで更新データが

表示され、グラフが定期的に更新表示されます。

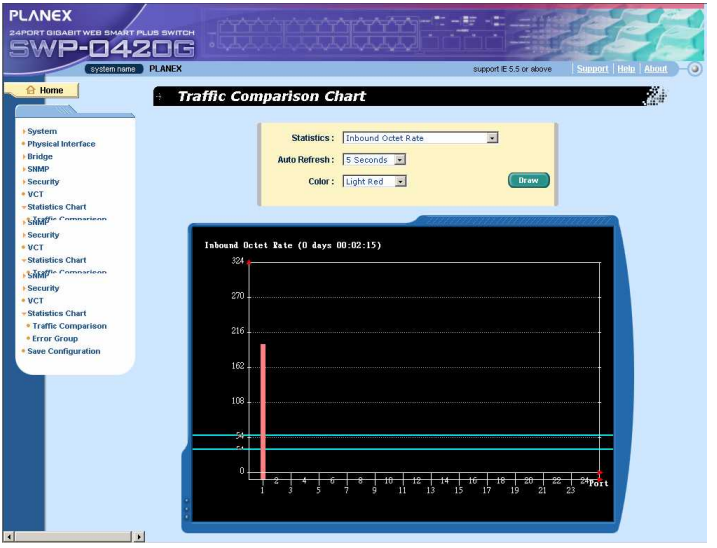

図32.Traffic Comparison Chart

4.9.2 Error Group Chart

Portを選択してColorを表示し、Drawをクリックすると、指定したポートの全破棄数または全エラーカウントが統計ウィンドウに表示されます。このデータは、定期的に更新されます。

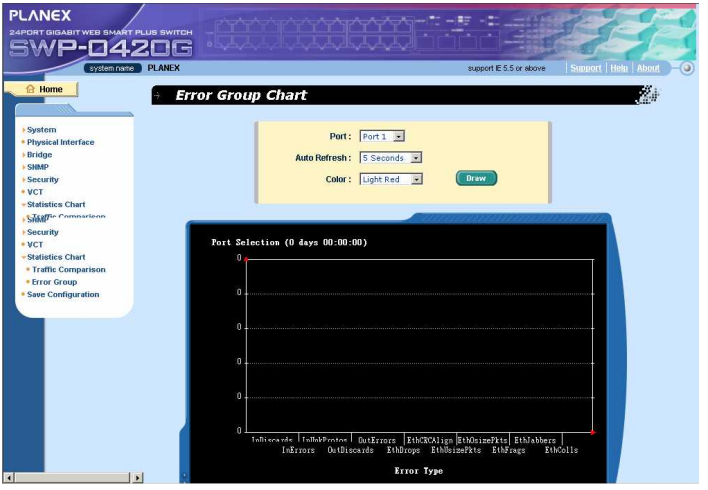

図33.Error Group Chart

4.10 Save Configuration

設定を確定して保存するには、[Save]をクリックします。保存が正常に行われると、設定も有効になります。

当スイッチの設定をリセットする必要がある場合は、[Restore]をクリックして、設定ファイルを工場出荷時の状態にリセットします。この復元処理には、当スイッチのシステムの再起動を必ず伴います。

注意:工場出荷時の設定への復元を選択すると、現在の設定はすべて失われます。

図34.Save Configuration

第5章 コンソールインタフェース

本章では、コンソールインタフェースを使用して当スイッチを設定する方法について説明します。

当スイッチには、コンピュータに接続するためのRS232Cコネクタが用意されています。コンピュータからハイパーターミナルなどの端末エミュレータとコマンドライン インタプリタを使用して、当スイッチを設定します。ボーレート9600、8ビットデータ、パリティなし、1ストップビット、フロー制御なしという指定で、端末エミュレータを設定する必要があります。

CLIモードに移動して「?」と入力すると、使用可能なコマンドのヘルプメッセージが表示されます。この機能は、CLIコマンドを使い慣れていない場合に便利です。CLIモードは、アイドル状態で10分間経過するとタイムアウトになります。タイムアウト後は、再度ログインしてCLIモードに移動する必要があります。

すべてのCLIコマンドは大文字小文字を区別します。便宜上、フルコマンドを入力することによって別のカテゴリに移動できます。これにより、移動先のカテゴリが作業カテゴリになります。移動後は、どのサブコマンドの前にも「sys」を入力する必要はなくなります。たとえば、「sys」は多くのサブコマンドを含むコマンドカテゴリです。「sys」と入力して作業カテゴリを「sys」に変更した場合、サブコマンドで「sys」を入力する必要はありません。作業カテゴリが「sys」の場合、プロンプトの表示は「(system name)sys%」になります。

5.1 電源オン自己診断テスト(POST)

POSTはシステムの起動時に実行されます。スイッチボード上のシステムメモリ、LED、およびハードウェアチップのテストが行われます。システムテストおよび初期化の結果として、システム情報が表示されます。プロンプト「(Planex)%」よりも前に表示された情報は無視しても構いません(図35を参照)。

```
scanFlash: b10  used = 0 dirty = 0 bad = 0
scanFlash: b11  used = 0 dirty = 0 bad = 0
scanFlash: b12  used = 0 dirty = 0 bad = 0
scanFlash: b13  used = 0 dirty = 0 bad = 0
scanFlash: b14  used = 0 dirty = 0 bad = 0
scanFlash: b15  used = 0 dirty = 0 bad = 0

System Log Restoring ............................. [ DONE ]
Network Library Initialization ................... [ DONE ]
Thread System Initialization ..................... [ DONE ]
SSHd Host Key Initialization...................... [ DONE ]
CLI Initialization ............................... [ DONE ]

>>>>>> ASUS OS Initialization Start(Phase 2)

System Parameters Reloading ...................... [ DONE ]
CLI Command Tree Initialization .................. [ DONE ]
In-ROM File System Initialization ................ [ DONE ]
FTPd Initialization .............................. [ DONE ]
Telnetd Initialization ........................... [ DONE ]
HTTPd Initialization ............................. [ DONE ]
SNMPd Initialization ............................. [ DONE ]
Login is required!
(GigaX)% _
```

図35.CLIインタフェース

5.1.1 Boot ROM Command Mode

図36に示すように、POST処理中にEnterキーを押すとBoot ROM Command Modeに移動できます。

注意: Boot ROMコマンドモードにて、Boot ROMコマンドは使用しないで下さい。Boot ROMコマンドを使用された場合の不具合はサポート対象外とさせて頂く場合がございますので、ご注意ください。

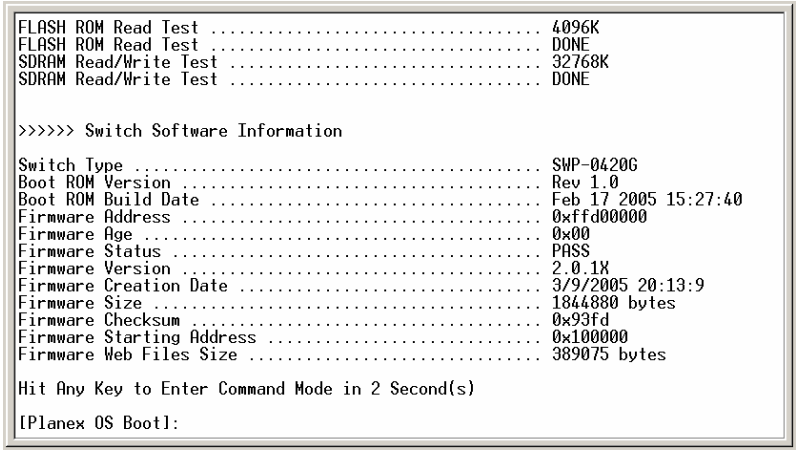

図36.Boot ROM Command Mode

5.2 ログインとログアウト

CLIモードに移動するには「login」と入力し、有効なユーザ名とパスワードを入力する必要があります。初めてログインする際には、ユーザ名として「admin」と入力し、パスワードの入力は省略できます。セキュリティ上の理由から、ログイン後にユーザ名とパスワードを変更してください。

CLIモードを安全に終了するには、「logout」と入力します。この操作により、CLIモードの保護が可能になります。次回の再ログイン時に、ユーザは認証済みのユーザ名とパスワードを入力する必要があります。

5.3 CLIコマンド

当スイッチには、管理機能全般に対応するCLIコマンドが用意されています。使用コマンドは、WEB管理インタフェースと同様にカテゴリ別にリストされます。これにより、WEBインタフェースを使用して当スイッチを設定する場合と同じくらい簡単に、指示に従って当スイッチ

を正しく設定できます。saveコマンドは、設定をフラッシュメモリに保存する目的で使用します。いくつかのCLIコマンドは、saveコマンドの実行後にのみ有効になります。

注意: 使用可能なコマンドのリストやヘルプを表示するには、「?」と入力します。

root (ルート)ディレクトリに戻るには、「/」と入力します。

コマンドのヘルプを表示するには、コマンドのみを入力します。

5.3.1 システムコマンド

Sytem Name
当スイッチに設定された名前を表示します。これはシステムグループに含まれるRFC-1213定義のMIBオブジェクトに該当し、管理対象ノードに関する管理情報を提供します。

CLIコマンド：sys name

当スイッチのsystem nameは、system nameフィールドに入力した新しいsystem nameに変更されます。

System Contact
当スイッチに関する連絡先の詳細情報を表示します。これはシステムグループに含まれるRFC-1213定義のMIBオブジェクトに該当し、管理対象ノードに関する連絡先情報を提供します。

CLIコマンド：sys contact

当スイッチのcontactは、system contactフィールドに入力した新しいcontactに変更されます。

System Location
当スイッチのsystem locationを表示します。これはシステムグループに含まれるRFC-1213定義のMIBオブジェクトに該当し、管理対象ノードに関するsystem locationを提供します。

CLIコマンド：sys location

当スイッチのsystem locationを変更するには、新しいlocationをsystem locationフィールドに入力します。

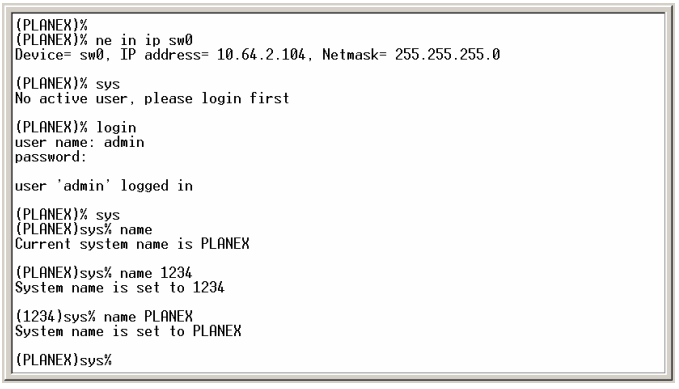

図37.SYSコマンド

[IPアドレス/ネットワークマスク]
当スイッチの静的IPアドレスを表示します。このIPアドレスは、管理目的で使用されます。httpサーバ、SNMPサーバ、telnetサーバなど、当スイッチのネットワークアプリケーションはすべて、このIPアドレスを使用します。

CLIコマンド:net interface ip sw0 〈IPアドレス〉〈ネットマスク〉

[デフォルトゲートウェイ]
デフォルトゲートウェイのIPアドレスを表示します。このフィールドは、スイッチネットワークに1台以上のルータが含まれている場合に必須です。

CLIコマンド:net route static add 〈宛先サブネット/IP〉〈ゲートウェイ〉〈ネットマスク〉〈メトリック〉

[パスワード保護] [有効/無効]
パスワード保護が有効な場合、ユーザがブラウザを介して当スイッチにアクセスすると、WEBインタフェースはユーザ名とパスワードによる認証を要求します。

CLIコマンド:sys weblogin set 〈enable/disable〉

[パスワードの新規作成/変更]
デフォルトのユーザ名は「admin」です。デフォルトのパスワードは「password」です。以下のパラメータでパスワードを設定できます。

CLIコマンド:sys users modify 〈ユーザ名、デフォルトは「admin」〉

user name (old user name, 'admin' by default (古いユーザ名、デフォルトは「admin」)):〈新しいユーザ名〉

password (old password, 'password' by default (古いパスワード、デフォルトは「password」)):〈新しいパスワード〉

privilege level (Only 3 is supported (3のみサポート)):(Enterキー)

[再起動]
当スイッチを再起動するには、rebootコマンドを発行します。

CLIコマンド：sys reboot

[アップロード]
この機能に対応するCLIコマンドはありません。この機能については、Boot ROMコマンドに関する記述を参照してください。

5.3.2 物理インタフェースコマンド

[Admin] [Enable/Disable]
ポートの管理ステータスを表示し、ポートのオン/オフを切り替えます。

CLIコマンド：l2 port admin <ポート番号> <enable/disable>

[モード] [自動/10M半二重/10M全二重/100M半二重/100M全二重/1G全二重]
ポートの現在の速度とデュプレクスモードを表示します。ポートに対してオートネゴシエーションを有効にすると、速度とデュプレクスモードを自動的に検出できます。

CLIコマンド：l2 port autoneg <ポート番号> <enable/disable>

CLIコマンド：l2 port speed <ポート番号> <10/100/1000>

CLIコマンド：l2 port duplex <ポート番号> <full /half >

[フローコントロール] [有効/無効]
ポートのIEEE802.3xフローコントロール設定を表示します。このフローコントロールは、全二重モードでのみ動作することに注意してください。

CLIコマンド：l2 port flow <ポート番号> <enable/disable>

[リロード]
以前のポート設定を設定ファイルから復元します。

CLIコマンド：l2 port retrieve

5.3.3ブリッジコマンド

5.3.3.1トランク

[トランクの表示]
特定のトランクグループの設定を表示します。新しいトランクグループを作成するには、一意なトランクID、トランク名、ポート選択条件(rtag)、トランクグループのメンバポートを指定します。

CLIコマンド：l2 trunk show <トランクID>

[rtag]
トラフィック配信アルゴリズム(1～3)を設定します。「rtag」はトランクグループのパケット配信

アルゴリズムです。

CLIコマンド：l2 trunk rtag <1|2|3>

rtagの値と対応する意味：

1：ソースXOR宛先MAC (L2)

2：ソースXOR宛先IP (L3)

3：ソースXOR宛先ポート(L4)

[トランクの作成]
トランクID、rtag、名前、およびポート番号を指定し、新しいトランクグループを作成します。

「rtag」はトランクグループのパケット配信アルゴリズムです。

CLIコマンド：l2 trunk create <トランクID> <トランク名> <ポートリスト>

[トランクの追加/削除]
トランクグループのポートメンバは、既存のトランクグループから追加または削除できます。

CLIコマンド：l2 trunk add <トランクID> <ポートリスト>

CLIコマンド：l2 trunk remove <トランクID> <ポートリスト>

[リロード]
以前に保存したトランク設定を設定ファイルから復元します。

CLIコマンド：l2 trunk retrieve

5.3.3.2 ミラー

[ミラーモードの作成/削除]
当スイッチのミラーリング設定を表示します。

CLIコマンド：l2 mirror create <モニタポート番号> <enable/disable>

CLIコマンド：l2 mirror ingress <ポートリスト>

CLIコマンド：l2 mirror egress <ポートリスト>

CLIコマンド：l2 mirror remove <ingress /egress > <ポートリスト>

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：l2 mirror retrieve

[速度制限の表示]
当スイッチの現在の速度制限値を表示します。

CLIコマンド：l2 rate show

5.3.3.3 Rate Limit

[ブロードキャストの速度制限]

[ブロードキャストとマルチキャストの速度制限]
ブロードキャスト、マルチキャストのトラフィックに速度制限を設定するには、トラフィックコントロールをオンにします。

[Limit Rate]
この値を変更するには、新しい制限値を指定します。この値は、上記のトラフィックコントロールすべてに対して適用されます。対象はシステム全体であり、ポート単位ではありません。

CLIコマンド：l2 rate set <1：broadcast /2：broadcast and multicast > <enable /disable ><limit rate>

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：l2 rate retrieve

5.3.3.4 ARL (アドレス解決ロジック)

[エージング期間]
ARL (アドレス解決ロジック)エントリのエージング期間を設定するには、エージング期間値を設定します。

CLIコマンド：l2 arl age [エージング値]

[ポートによるクエリ]
ARLテーブル内に存在するARLエントリは、ポート番号によるクエリに対応しています。

CLIコマンド：l2 arl port <ポート番号>

[VLAN IDによるクエリ]
ARLテーブル内に存在するARLエントリは、VLAN IDによるクエリに対応しています。

CLIコマンド：l2 arl vlan <VLAN ID>

[MACアドレスによるクエリ]
ARLテーブル内に存在するARLエントリは、MACアドレスによるクエリに対応しています。

CLIコマンド：l2 arl mac <MACアドレス> [VLAN ID]

[MACアドレス]

[VLAN ID]

[ポート選択]

[破棄] [なし/ソース/宛先/ソースおよび宛先]

静的ARLエントリを追加または変更するには、MACアドレス、VLAN ID、ポート番号、トランクID、および破棄条件を指定します。

CLIコマンド：l2 arl static <MACアドレス> <VLAN ID> <ポート番号> <トランクID> <破棄：0～3>

[削除]
静的ARLエントリを削除するには、MACアドレスとVLAN IDを指定します。これら2つのフィールドの組み合わせは、ARLテーブル内で一意なエントリを表します。

CLIコマンド：l2 arl delete <MACアドレス> <VLAN ID>

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：l2 arl retrieve

5.3.3.5 VLAN

[VLAN表示]
当スイッチの既存のVLAN情報を表示します。

CLIコマンド：l2 vlan show <VLAN ID>

[VLANの作成]
VLAN設定を設定します。新しいVLANを作成するには、一意なVLAN ID、VLAN記述名、およびポートメンバ一覧を指定します。この場合、ポートメンバはタグ付きポートメンバとして指定します。VLANポートメンバをタグ無しポートとして指定するには、CLIコマンドutportaddを使用します。ポートメンバをVLANに追加する場合や、既存のポートメンバをVLANから除外する場合には、CLIコマンドaddまたはremoveを使用します。

CLIコマンド：l2 vlan create <VLAN ID> <VLAN名> <ポートリスト>

[VLANからのポートの追加/削除]
CLIコマンド：l2 vlan add <VLAN ID> <ポートリスト>

CLIコマンド：l2 vlan remove <VLAN ID> <ポートリスト>

[タグ無しポートの設定]
CLIコマンド：l2 vlan utportadd <VLAN ID> <タグ無しポートリスト>

[VLANの削除]
既存のVLANを完全に削除します。

CLIコマンド：l2 vlan delete <VLAN ID>

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：l2 vlan retrieve

5.3.3.6 ポート

[ポートの表示]
ポート設定を表示します。

CLIコマンド：l2 port show 〈ポートIDまたは *すべてのポート〉

[PVID]
ポートのデフォルトVLANを設定するには、VLAN IDと関連するポートメンバー一覧を指定します。

CLIコマンド：l2 port vlan 〈VLAN ID、4095はポートベースのVLANを無効化〉 〈ポートリスト〉

[CoS値]
ポートのクラスオブサービスを設定するには、タグ無しパケットの優先度の条件値(0～7の範囲)を割り当てます。4つの内部トラフィッククラスが8つの優先度に対応しているので、「CoS Queue Mapping (CoSキュー割り当て)」に従って、4つのCoS値(キュー割り当てのデフォルトでは、0、2、5、7)のみが有効になります。

CLIコマンド：l2 port priority 〈CoS〉 〈ポートリスト〉

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：l2 port retrieve

5.3.3.7 QoS

[Cos] [割り当て]
バッファキュー(キューID 1～4の合計4つ)に対するCoS優先度(0～7の範囲)を割り当てます。

CLIコマンド：l2 cos map 〈キューID (1～4)〉 〈CoS (0～7)〉

[Cos] [スケジュール]
厳密優先度ベースまたは加重優先度ベースでスケジューリングを設定します。

CLIコマンド：l2 cos sched 〈モード(1：strict)〉 〈Q1加重〉 〈Q2加重〉 〈Q3加重〉 〈Q4加重〉

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：l2 cos retrieve

5.3.4 SNMP

5.3.4.1 コミュニティ

[コミュニティ名の追加/設定/削除]
コミュニティエントリは、コミュニティを説明する文字列と一連の権限で構成されています。取得権限(Get Privilege)はデフォルトではオンになっており、新しいエントリの作成時に設定権限(Set Privilege)を付与するかどうかを指定できます。

[追加]
CLIコマンド：snmp community add

New community string：<新しいコミュニティ文字列>

Get privileges ：[y, always turn on by default (y、デフォルトでは常にオン)]

Set privileges? (y/n)：[n] <権限を設定、「はい」の場合y、「いいえ」の場合n>

[設定]
CLIコマンド：snmp community set

テーブル内のコミュニティエントリを変更するには、コミュニティ文字列と権限を再割り当てします。

Community entry (table index)：<設定するエントリID>

Community string (old community string)：<新しいコミュニティ文字列>

この操作により、すべてのホストのコミュニティ文字列を「古いコミュニティ文字列」から「新しいコミュニティ文字列」に変更します。

Are you sure? (y/n) ：[y] <「はい」の場合y、「いいえ」の場合n>

Get privileges：[y, always turn on by default (y、デフォルトでは常にオン)]

Set privileges? (y/n)：[n] <権限を設定、「はい」の場合y、「いいえ」の場合n>

[削除]

CLIコマンド：snmp community delete

コミュニティテーブルからコミュニティエントリを削除します。

Community entry (table index) ：<削除するエントリID>

この操作により、「delete community」のコミュニティ文字列に該当するすべてのホストを削除します。

Are you sure? (y/n) ：[y] <「はい」の場合y、「いいえ」の場合n>

[リロード]

以前に保存した設定を設定ファイルから復元します。

CLIコマンド：snmp community retrieve

5.3.4.2 SNMPホスト

[SNMPホストの追加]
ホストエントリは、ホストIPアドレス、ネットワークマスク、特定のコミュニティ文字列で構成されています。

CLIコマンド：snmp host add

Host IP/Subnet ：<IPアドレス>

Netmask ：<ネットマスク>

Community ：<コミュニティ文字列>

[SNMPホストの設定]

CLIコマンド：snmp host set

テーブル内のホストエントリを変更するには、許容IPアドレス、ネットワークマスク、およびコミュニティ文字列を再割り当てします。

Host table entry (table index) ：<設定するエントリID>

Host IP/Subnet (old IP address) ：<新しいIPアドレス>

Netmask (old netmask) ：<新しいネットマスク>

Community (old community string) ：<新しいコミュニティ文字列>

[SNMPホストの削除]

CLIコマンド：snmp host delete

ホストテーブルからホストエントリを削除します。

Entry id (table index) ：<削除するエントリID>

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：snmp host retrieve

5.3.4.3 トラップ

[トラップの追加/設定/削除]
トラップエントリは、SNMPバージョン(現在、バージョン1とバージョン2cをサポート)、宛先IPアドレス、およびリモートコミュニティ文字列で構成されています。

[追加]

CLIコマンド：snmp trap add

SNMP version? (1/2c) :[1, by default (1、デフォルト)] <SNMPバージョン>

Destination IP :<IPアドレス>

Community :<コミュニティ文字列>

[設定]

CLIコマンド：snmp trap set

テーブル内のトラップエントリを変更するには、SNMPバージョン、宛先IPアドレス、およびコミュニティ文字列を再割り当てします。

Trap table entry (table index) :<設定するエントリID>

SNMP version? (1/2c) :[old snmp version (古いSNMPバージョン)] <新しいSNMPバージョン>

Destination IP (old IP address) :<新しいIPアドレス>

Community (old community string) :<新しいコミュニティ文字列>

[削除]

CLIコマンド：snmp trap delete

トラップテーブルからトラップエントリを削除します。

Trap table entry (table index) :<削除するエントリID>

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：snmp trap retrieve

5.3.5 セキュリティコマンド

5.3.5.1 dot1x

[Reauthentication]
定期的な再認証を有効または無効にします。

CLIコマンド：security dot1x bridge reauth <enable /disable >

[Reauthentication Time]
再認証期間を設定します。

CLIコマンド：security dot1x bridge reauthtime <reauthentication time(1～4294967295秒)>

[Reauthentication Method]
再認証方法(RADIUSまたはローカルデータベース)を設定します。

CLIコマンド：security dot1x bridge authmeth <type(1：ローカル、2：RADIUS)>

[Quiet Period]
沈黙期間を設定します。

CLIコマンド：security dot1x bridge quietperiod <quiet Period(1～65535秒)>

[Retransmission Time]
再送信期間を設定します。

CLIコマンド：security dot1x bridge retxtime <retransmission time(1～65535秒)>

[Max Reauthentication Attempts]
再認証の最大試行回数を設定します。

CLIコマンド：security dot1x bridge reauthmax <max reauthentication attempts(1～10)>

[マルチホスト]
特定のポートに対してマルチホストを有効または無効にします。

CLIコマンド：security dot1x port multihost <enable /disable ><ポートリスト/*>

[認証制御]
特定のポートの認証制御を設定します。

CLIコマンド：security dot1x port authctrl <type(1：force_authorized 、2：force_unauthorized 、3：auto ><ポートリスト/*>

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：security dot1x retrieve

5.3.5.2 ダイヤルユーザ

[ダイヤルユーザの作成/変更/削除]
802.1x認証用に当スイッチのローカルデータベース内にユーザを作成します。ユーザエントリは、ユーザ名、パスワード、および動的VLANで構成されています。

CLIコマンド：security dialinuser create

User Name：〈ユーザ名の文字列〉

Password：〈パスワードの文字列〉

Confirm Password：〈確認パスワードの文字列〉

CLIコマンド：security dialinuser remove 〈ユーザ名/*〉

ローカルデータベースからユーザエントリを削除します。

CLIコマンド：security dialinuser modify 〈ユーザ名/*〉

ローカルデータベースのユーザエントリを変更します。このエントリは、ユーザ名、パスワードで構成されています。

User Name：〈新しいユーザ名の文字列〉

Password：〈新しいパスワードの文字列〉

Confirm Password：〈新しい確認パスワードの文字列〉

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：security dialinuser retrieve

5.3.5.3 RADIUS

[RADIUSユーザの設定]
RADIUSサーバIP、サーバポート、およびサーバキーを設定します。

CLIコマンド：security radius set

authentication server ip 〈ip/none〉：(old server ip (古いサーバIP))〈新しいサーバIP〉

authentication server port 〈port/default〉：(old server port (古いサーバポート))〈新しいサーバポート〉

authentication server key 〈key/none〉：〈サーバキー〉

confirm authentication key 〈key/none〉：〈確認サーバキー〉

[リロード]
以前に保存した設定を設定ファイルから復元します。

CLIコマンド：security radius retrieve

5.4 その他のコマンド

sys uptime ：システムのブートから経過した時間を表示します。

sys date ：現在の日付と時刻を表示します。

sys settime ：現在の時刻を設定します。

net ping ：リモートホストに対してpingを実行します。

net route show ：ルーティングテーブル内のエントリを表示します。

第6章 IPアドレス、ネットワークマスク、サブネット

6.1 IPアドレス

注意: このセクションでは、IPv4 (インターネットプロトコルのバージョン4)対応のIPアドレスのみを取り上げます。IPv6アドレスについては取り上げません。

このセクションでは、2進数、ビット、バイトなどの基本的な知識が読者にあることを前提としています。このテーマの詳細については、付録6をご覧ください。

IPアドレスは電話番号のインターネット版のようなものであり、インターネット上の個々のノード(コンピュータまたはデバイス)を識別する目的で使用します。各IPアドレスは、ドット(ピリオド)で区切られた0～255の範囲の数字4つ(例:20.56.0.211)で構成されています。各数字は、左から右の順でフィールド1、フィールド2、フィールド3、フィールド4と呼ばれます。

このようにドット区切りの10進数でIPアドレスを記述するスタイルは、ドット10進表記と呼ばれます。IPアドレス20.56.0.211は、「20ドット56ドット0ドット211」と読みます。

6.1.1 IPアドレスの構造

IPアドレスは、電話番号と同様の階層型の設計です。

たとえば、7桁の電話番号は電話回線のグループを識別する先頭3桁のプレフィックス(局番)と、グループ内の特定の回線を識別する末尾4桁で構成されています。

同様に、IPアドレスは以下の2種類の情報で構成されています。

ネットワークID
インターネットまたはイントラネット内の特定のネットワークを識別します。

ホストID
ネットワーク上の特定のコンピュータまたはデバイスを識別します。

各IPアドレスの最初の部分はネットワークIDに該当し、アドレスの残りの部分はホストIDに該当します。ネットワークIDの長さは、ネットワークのクラス(以下のセクションを参照)に応じて異なります。表7に、IPアドレスの構造を示します。

表7.IPアドレスの構造

	フィールド1	フィールド2	フィールド3	フィールド4
クラスA	ネットワークID	ホストID		
クラスB	ネットワークID		ホストID	
クラスC	ネットワークID			ホストID

有効なIPアドレスの例を以下に示します。

クラスA:10.30.6.125 (ネットワーク = 10、ホスト = 30.6.125)

クラスB：129.88.16.49（ネットワーク = 129.88、ホスト = 16.49）

クラスC：192.60.201.11（ネットワーク = 192.60.201、ホスト = 11）

6.1.2 ネットワーククラス

一般的に使用される3つのネットワーククラスは、A、B、Cです(クラスDも存在しますが、用途は特殊なのでここでは取り上げません)。これらのクラスはそれぞれ用途や特徴が異なります。

クラスAネットワークはインターネットの最大規模のネットワークであり、ネットワーク単位に収容可能なホスト数は1,600万を超えます。このクラスのネットワークは最大126系統存在し、合計20億台を超えるホストに対応します。規模の大きさから、これらのネットワークはISPなど、インターネットのインフラストラクチャレベルでWANや組織ネットワーク向けに使用されます。

クラスBネットワークはクラスAネットワークと比較すると規模は小さくなりますが、それでも規模は大きなものであり、ネットワーク単位に収容可能なホスト数は65,000を超えます。最大16,384系統のクラスBネットワークが存在します。クラスBネットワークは、企業や政府機関などの大規模な組織に適していると考えられます。

クラスCネットワークは規模としては最小であり、収容可能なホスト数は最大254に限定されます。ただし、クラスCネットワークの総数は200万を超えます(正確には2,097,152)。インターネットに接続しているLANは通常、クラスCネットワークに該当します。

IPアドレス関連の重要な注意事項：

クラスはフィールド1から識別可能：

フィールド1 = 1～126：クラスA
フィールド1 = 128～191：クラスB
フィールド1 = 192～223：クラスC

（上記以外のフィールド1の値は特殊な用途用に予約済み）

ホストIDには、任意の値を指定できます。ただし、すべてのフィールドが0または255である値は特殊な用途用に予約されているので、ホストIDには指定できません。

6.2 サブネットマスク

定義：　マスクは通常のIPアドレスのように見えますが、IPアドレスのどの部分がネットワークIDおよびホストIDに該当するのかを表すビットパターンが含まれています(1に設定されたビットは「このビットはネットワークIDの部分」、0に設定されたビットは「このビットはホストIDの部分」を意味します)。

サブネットマスクは、サブネット(ネットワークを細かく分割した単位)を定義する目的で使用します。サブネットのネットワークIDは、アドレスのホストID部分から1つ以上のビットを転用する形で作成されます。サブネットマスクは、これらのホストIDビットを識別します。

たとえば、クラスCネットワーク192.168.1の場合、このネットワークを2つのサブネットに分割するには、サブネットマスクを使用します。

以下のように、2進数で記述すると処理がわかりやすくなるでしょう。

11111111. 11111111. 11111111.10000000

クラスCアドレスと同様に、フィールド1からフィールド3のビットはすべてネットワークID部分に該当しますが、マスクによってフィールド4の先頭ビットも識別処理の対象に含まれることに注意してください。この追加ビットには2つの値(0および1)のみが設定され、2つのサブネットが存在することを意味します。各サブネットは、フィールド4の残りの7ビット(0～127の範囲。クラスCアドレスで通常の0～255の範囲とは異なる)をホストIDとして使用します。

同様に、クラスCネットワークを4つのサブネットに分割する場合、マスクは以下のようになります。

255.255.255.192 または 11111111. 11111111. 11111111.11000000

フィールド4に含まれる2つの追加ビットには4種類の値(00、01、10、11)が設定され、4つのサブネットが存在することを意味します。各サブネットは、フィールド4の残りの6ビット(0～63の範囲)をホストIDとして使用します。

注意: サブネットマスクでネットワークIDの追加ビットを指定していない場合もあります。この場合、サブネットは存在しません。このようなマスクは、デフォルトサブネットマスクと呼ばれます。該当するマスクは以下のようになります。

クラスA:255.0.0.0

クラスB:255.255.0.0

クラスC:255.255.255.0

これらのマスクは、サブネットが存在しない、ネットワークの初期設定時に使用されるので、デフォルト(初期設定)と呼ばれます。

第7章 トラブルシューティング

本セクションでは、いくつかのIPユーティリティを使用して問題を診断する方法について説明します。発生する可能性のある問題と、推奨される対応の一覧も記載しています。

既知のバグについては、リリースノートにすべて記載しています。当スイッチの設定を始める前に、リリースノートをご覧ください。推奨される対応で問題が解決しない場合は、弊社のサポート窓口までお問い合わせください。

7.1 IPユーティリティを使用して問題を診断

7.1.1 ping

pingは、ネットワークおよびインターネット上の他のコンピュータをコンピュータが認識できるかどうかチェックするためのコマンドです。pingコマンドは、ユーザの指定したコンピュータにメッセージを送信します。対象のコンピュータはメッセージを受信すると、応答のメッセージを返します。pingを使用するには、通信先のコンピュータのIPアドレスが必要になります。

Windowsベースのコンピュータでは、「スタート」メニューからpingコマンドを実行できます。「スタート」ボタンをクリックし、「ファイル名を指定して実行」をクリックします。「名前」テキストボックスに、以下のような命令を入力します。

ping 192.168.1.1

[OK]をクリックします。LAN上のプライベートIPアドレスや実際のインターネットサイトのIPアドレスを指定できます。

対象のコンピュータがメッセージを受信すると、図38に示すように、「コマンドプロンプト」ウィンドウが表示されます。

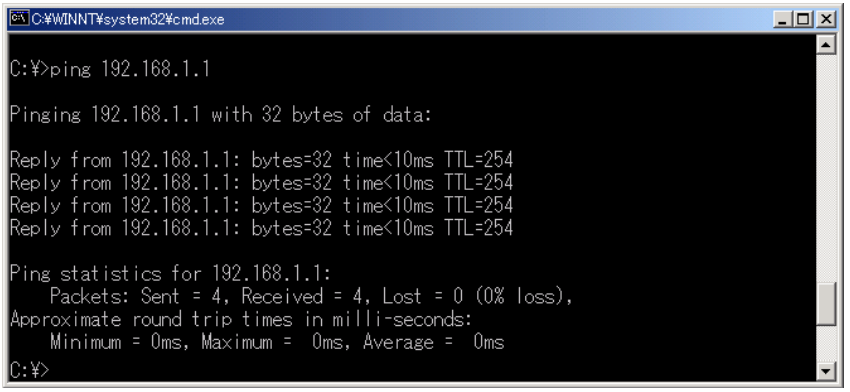

図38.pingユーティリティの使用

対象のコンピュータを特定できない場合、「Request timed out (要求がタイムアウトしました)」というメッセージが表示されます。

pingコマンドを使用すると、当スイッチ(事前に設定されているデフォルトのLAN IPアドレス192.168.1.1を使用)やユーザの割り当てた別のアドレスへの経路が正常かどうかをテストできます。

www.yahoo.com (216.115.108.243)などの外部アドレスを入力すると、インターネットへのアクセスが正常かどうかもテストできます。特定のインターネットロケーションのIPアドレスがわからない場合は、以下のセクションで説明するようにnslookupコマンドで調べることができます。

他のIP対応のオペレーティングシステムでも、ほとんどの場合、コマンドプロンプトやシステム管理ユーティリティを介して同様のコマンドを実行できます。

7.1.2 nslookup

インターネットサイト名に関連付けられているIPアドレスを調べるには、nslookupコマンドを使用します。nslookupコマンドは、ユーザの指定したサイトの通称に該当する名前をDNSサーバ(通常、ISPによって設置される)上で検索します。該当する名前がISPのDNSテーブルにエントリとして含まれていない場合、対象のエントリが検出されるまで、この要求は上位レベルの別のサーバを順番に参照します。対象のエントリが検出された時点で、関連付けられているIPアドレスがサーバから返されます。

Windowsベースのコンピュータでは、「スタート」メニューからnslookupコマンドを実行できます。「スタート」ボタンをクリックし、「ファイル名を指定して実行」をクリックします。「名前」テキストボックスに、以下のように入力します。

nslookup

[OK]をクリックします。プロンプト(>)の状態で、「コマンドプロンプト」ウィンドウが表示されます。プロンプトで、www.absnews.comなど、調べたいインターネットアドレスの名前を入力します。

判明した場合、関連付けられているIPアドレスがウィンドウに表示されます。図39を参照してください。

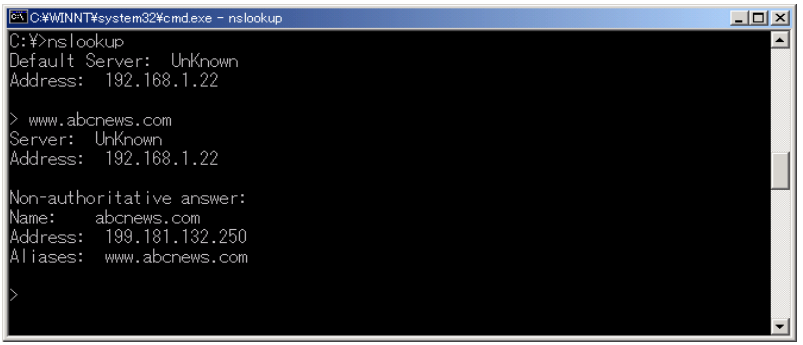

図39.nslookupユーティリティの使用

インターネットサイト名には複数のアドレスが関連付けられている場合があります。この構成は大量のトラフィックを受信するWEBサイトでは一般的であり、同じ情報を提供する目的で複数の冗長サーバが使用されます。

nslookupユーティリティを終了するには、コマンドプロンプトで「exit」と入力しEnterキーを押します。

7.2 応急処置

以下の表に、当スイッチの導入時や使用時に発生する可能性のある一般的な問題と、問題を解決するために推奨される対応を示します。

表8.トラブルシューティング

問題	推奨される対応
LED	
当スイッチの電源をオンにしているのに、SYSTEM LEDが点灯しない	・ 電源ケーブルが当スイッチおよび壁面のコンセント/電源タップにしっかりと接続されているか確認します。
イーサネットケーブルを接続しているのに、Fast Ethernet Link LEDが点灯しない	・ イーサネットケーブルがLANスイッチ/ハブ/コンピュータおよび当スイッチにしっかりと接続されているか確認します。コンピュータおよびハブ/スイッチの電源がオンになっていることを確認します。 ・ ケーブルがネットワーク要件を満たしているかどうか確認します。100Mbpsネットワーク(100BaseTx) では、Cat 5(カテゴリ5)相当のケーブルを使用する必要があります。10Mbit/secケーブルには、低品質のケーブルが使用されている場合があります。

問題	推奨される対応
ネットワークアクセス	
コンピュータが同じネットワーク内の別のホストにアクセスできない	•イーサネットケーブルの配線が適切で、LEDが緑色に点灯してることを確認します。 •ポートLEDが橙色に点灯している場合は、ポートが無効になっているかどうかを確認します。
コンピュータがWEB設定ページを表示できない	• 当スイッチの電源がオンであり、接続ポートが有効な状態であることを確認します。当スイッチの工場出荷時のIPアドレスは192.168.1.1です。 • コンピュータのネットワーク設定で上記の情報を確認します。コンピュータが有効なルートで当スイッチにアクセスできない場合は、当スイッチのIPをコンピュータからアクセスできる適切なIPに変更します。 • コンピュータから「当スイッチのIP」にpingを実行します。これでも失敗する場合は、ステップ2を繰り返します。 • pingが成功してもWEB設定を行えない場合は、RS232Cコンソールポートを介してコンピュータを接続し、いずれかのフィルタルールまたは静的MACアドレスでWEBトラフィックをブロックするように設定しているかどうか確認します。
WEB設定インタフェース	
一部のページが適切に表示されない	• Internet Explorer v5.5以降を使用していることを確認します。Netscapeはサポートされていません。Javascriptのサポートをブラウザで有効にする必要があります。Javaのサポートも必要になります。 • 当スイッチのIPアドレスにpingを実行し、リンクが安定しているかどうか確認します。pingパケットの一部が失われた場合は、ネットワーク設定が有効であるか確認します。
コンソールインタフェース	
端末エミュレータでテキストを表示できない	• 工場出荷時の設定(ボーレート9600、フロー制御なし、8ビットデータ、パリティチェックなし、1ストップビット)であることを確認します。 • ケーブルに問題がないことを確認します。 • 付属のシリアルケーブルをご利用下さい。

ユーザ登録について

この度は弊社製品をお買い上げいただき誠にありがとうございます。

弊社では製品をお買い上げいただいたお客様にユーザ登録をお願いしております。ユーザ登録を行っていただいたお客様には新製品情報、バージョンアップ情報、キャンペーン情報等さまざまな情報を提供させていただきます。また、製品の故障等でユーザサポートをお受けになるにはお客様のユーザ登録が必要となります。

ユーザ登録の際は、ホームページ掲載の「個人情報保護方針について」をご確認後、ユーザ登録を行ってくださいますようお願いいたします。

ユーザ登録は下記弊社インターネットホームページ上で受け付けております。

http://www.planex.co.jp/user/

弊社へのお問い合わせ

■弊社製品の追加購入
弊社製品のご購入は、販売店様またはPLANEX DIRECTまで。

ケーブル1本からレイヤ3スイッチまで、お客様が探しているものが見つかります。

〈PLANEX DIRECT〉
http://direct.planex.co.jp/

■製品に関するお問い合わせ
製品購入前のご相談や、ご質問は弊社専任アドバイザーにお任せください。

ネットワーク導入やシステム構築・拡張など、お客様のお手伝いをいたします。

〈ご質問/お見積もりフォーム〉
http://www.planex.co.jp/lan.shtml

■技術的なお問い合わせ・修理に関するお問い合わせ
製品購入後のご質問は、弊社サポートセンターまでお問い合わせください。

豊富な知識をもったサポート技術者が、お客様の問題を解決いたします。

〈お問い合わせフォーム〉
http://www.planex.co.jp/support/techform/
受付:24時間
〈電話〉
フリーダイヤル:0120-415977
受付:月～金曜日、10～12時、13～17時
＊祝祭日および弊社指定の休業日を除く
〈FAX〉
ファクス番号:03-5766-1615
受付:24時間

◇お問い合わせ前のお願い

サポートを円滑に行うため、お問い合わせ前に以下のものをご用意ください。

お客様のご協力お願いいたします。

- 弊社製品の製品型番とシリアルナンバー
- ご利用のコンピュータの型番とオペレーティングシステム名(Windows XP/Meなど)
- ご利用のネットワークの環境(回線の種類やインターネットサービスプロバイダ名など)
- ご質問内容(現在の状態、症状など。エラーメッセージが表示されている場合はその詳細を書きとめてください)

■その他
その他のお問い合わせ先は、弊社ホームページからお確かめください。

プラネックスコミュニケーションズ

http://www.planex.co.jp/

注)上記内容は2005年12月現在の情報です。内容は予告なく変更または削除される場合があります。ご了承ください。

質問表

技術的なご質問は、この2ページをプリントアウトして必要事項をご記入の上、下記FAX番号へお送りください。

プラネックスコミュニケーションズ テクニカルサポート担当 行

FAX:03-5766-1615

送信日: 年 月 日

会社名		部署名	
名前			
電話		FAX	
E-MAIL			

製品名 Product name	ギガビット WEBスマートプラススイッチ
型番 Product No.	**SWP-0412/0420G**
製造番号 Serial No.	

① ご使用のコンピュータについて

メーカー	
型番	

② OS

OS	SP

③ 質問内容

プラネックスコミュニケーションズ株式会社