



NgWDrking &g0MITIMniCglf0n

マニュアル



8ポートVDSL2 +
2ポートギガビット
TP/SFP 管理スイッチ

>VC-820M



商標

著作権・プラネ・テクノロジー株式会社 2015年コ

ンテンツは予告なく改訂される場合があります。

PLANETはプラネットテクノロジー株式会社の登録商標です。その他すべての商標は、それぞれの所有者に帰属します。

免責事項

PLANETテクノロジーは、ハードウェアがすべての環境およびアプリケーションで正しく動作することを保証するものではなく、特定の目的に対する品質、性能、商品性、または適合性に関して、黙示または表明されたいかなる保証および表明も行いません。

PLANETは、このユーザーズマニュアルが正確であることを保証するためにあらゆる努力をしてきました。

PLANETは、発生した可能性のある不正確さや不作為に対する責任を負いません。

本ユーザーズマニュアルの情報は、dがPLANETの一部に対するコミットメントを表すものではなく、予告なしに変更されることがあります。PLANETは、本ユーザーズマニュアルに含まれる可能性のある不正確さについて一切の責任を負いません。PLANETは、本ユーザーズマニュアルの情報を更新または最新の状態に保つ決意を行わず、予告なしに本ユーザーズマニュアルおよび/または本ユーザーズマニュアルに記載されている製品を改善する権利を否定します。

このマニュアルで、誤った情報、誤解を招く情報、不完全な情報が見つかる場合は、お客様のコメントや提案をお願いいたします。

FCC の警告

この装置はテストされ、FCC規則の第15部に従ってクラスAデジタル装置の限界に従うことを発見された。これらの制限は、機器が商業環境で動作する場合に有害な干渉ceに対して合理的な保護を提供するように設計されています。この装置は、無線周波数エネルギーを生成、使用、および放射することができ、取扱説明書に従って設置および使用されていない場合、無線通信に有害な干渉を引き起こす可能性があります。住宅地でのこの装置の操作は有害な干渉を引き起こす可能性があります。その場合、ユーザーは自費で干渉を行う必要があります。

CE マーク警告

これはクラスAの製品です。国内環境では、電波干渉を引き起こす可能性があります。その場合、ユーザーは適切な措置を講じる必要があります。

開発者の省エネノート

この電源が必要なデバイスはスタンバイモードの動作をサポートしていません。省エネのため、電源ケーブルを取り外して電源回路からデバイスを取り外してください。電源ケーブルを取り外さなくても、デバイスは電源からの電力を消費します。私は、エネルギーを節約し、不要な消費電力を低減するという見解を、この装置がアクティブにすることを意図していない場合は、デバイスから電源接続を取り外すことを強くお勧めします。

WEEE 警告

電気・電子機器に有害物質が存在する結果として、環境や人間の健康に対するポットの影響を避けるために、電気および電子機器のエンドユーザーは、クロスアウトホイールビンシンビポルの意味を理解する必要があります。WEEEを未分類の自治体廃棄物として処分せず、そのようなWEEEを別々に収集する必要があります。

リビジョン

PLANET 8ポートVDSL2 + 2ギガビットTP /SFP管理スイッチユーザーズマ

ニユアルモデル:VC-820M

改訂: 2.0 (2015年9月)

目次

1. はじめに	8
1.1 パッケージ内容	8
1.2 製品説明	9
1.3 このマニュアルの使い方	11
1.4 製品の特徴	12
1.5 製品仕様	14
2. インストール	17
2.1 ハードウェアの説明	17
2.1.1 スイッチフロントパネル	17
2.1.2 LED表示	20
2.2 スイッチの取り付け	21
2.2.1 デスクトップ・インストール	21
2.2.2 ラック取り付け	22
2.2.3 SFP トランシーバの取り付け	24
2.3 VDSL2 ポート用の配線	27
3. スイッチ管理	28
3.1 要件	28
3.2 管理アクセスの概要	29
3.3 ウェブ管理	30
3.4 SNMP ベースのネットワーク管理	31
3.5 管理コンソール	31
3.6 プロトコル	33
3.6.1 仮想端末プロトコル	33
3.6.2 SNMPプロトコル	33
管理アーキテクチャ	33
4. ウェブベースの管理	34
4.1 ウェブベースの管理	34
4.1.1 要件	35
4.1.2 スイッチへのログオン	35
4.1.3 メインWeb ページ	37

4.2 システム	38
4.2.1 システム情報.....	39
4.2.2 IP構成.....	42
4.2.3 コンソール情報.....	44
4.2.4 SNMP設定.....	44
4.2.5 Syslog設定.....	52
4.2.6 システムログ.....	52
4.2.7 SMTP設定.....	53
4.2.8 SNTP設定.....	55
4.2.9 アラーム設定.....	55
4.2.10 スマートファン.....	57
4.2.11 ファームウェアのアップグレード.....	59
4.2.12 構成のバックアップ.....	61
4.2.13 工場出荷時のデフォルト.....	64
4.2.14 システムの再起動.....	64
4.3 ポート構成	65
4.3.1 ポート制御.....	65
4.3.2 レート制御.....	66
4.3.3 ポートステータス.....	67
4.3.4 ポート統計.....	68
4.3.5 ポートスニファァ.....	69
4.3.6 保護ポート.....	71
4.4 VLAN設定	72
4.4.1 VLANの概要.....	72
4.4.2 スタティックVLAN 設定.....	75
4.4.3 ポートベースVLAN.....	76
4.4.4 802.1Q VLAN.....	78
4.4.5 Q-in-Q VLAN.....	84
4.4.6 GVRP VLAN.....	88
4.5 トランキンヅ	91
4.5.1 アヅリヅァタ設定.....	91
4.5.2 アヅリヅァタ情報.....	92
4.5.3 状態アクティビティ.....	96
4.6 転送とフィルタリンヅ	97

4.6.1	ダイナミックMAC表	97
4.6.2	スタティックMAC表	98
4.6.3	MACフィルタリング	99
4.7	IGMPスヌーピング	100
4.7.1	理論.....	100
4.7.2	IGMP設定	104
4.8	スパニングツリー プロトコル	106
4.8.1	理論.....	106
4.8.2	STP.....	109 の図
4.8.3	STPパラメータ	110
4.8.4	STPシステム設定	112
4.8.5	ポート設定.....	115
4.8.6	インスタンス	117
4.8.7	インターフェイス.....	118
4.9	DHCP リレー&オプション 82	119
4.10	LLDP	121
4.10.1	LLDP構成.....	121
4.10.2	パーポート構成.....	122
4.11	アクセスコントロール List.....	123
4.12	セキュリティマネージャ	127
4.13	MACリミット.....	128
4.13.1	MACリミット設定	128
4.13.2	MAC リミットポートステータス	129
4.14	802.1x構成	130
4.14.1	IEEE 802.1xポートベース認証について	130
4.14.2	システム構成	133
4.14.3	802.1xポート設定	135
4.14.4	その他の構成	136
4.15	QoS設定.....	137
4.15.1	QoS.....	137について
4.15.2	QoS設定	138
4.15.3	ToS/DSCP	141
4.16	VDSL設定	144
4.16.1	プロファイル構成.....	144

4.16.2 VDSLポートステータス	148
5. コンソール管理.....	152
5.1 コンソールインターフェイスへのログイン	152
5.2 IP アドレスの構成.....	153
5.3 コマンド・レベル	155
6. コマンドライン インターフェイス	156
6.1 操作に関するお知らせ	156
6.2 システム・コマンド.....	157
6.3 スイッチスタティック設定.....	159
6.3.1 ポート設定とステータスの表示	159
6.4 トランク構成.....	163
6.4.1 トランキングコマンド.....	163
6.4.2 LACPコマンド	164
6.5 VLAN設定	166
6.5.1 仮想LAN.....	166
6.5.2 VLANモード:ポートベース	167
6.5.3 高度な 802.1Q VLAN 設定	168
6.6 その他の構成.....	171
6.7 管理構成.....	172
6.7.1 ユーザー名とパスワードの変更	172
6.7.2 IP構成	173
6.7.3 スイッチの再起動.....	174
6.7.4 デフォルトにリセット.....	174
6.7.5 TFTPアップデートファームウェア	174
6.7.6 構成ファイルの復元	174
6.7.7 バックアップ設定ファイル	175
6.8 MACリミット.....	175
6.9 ポートMの刺激構成	176
6.10 サービスの品質	177
6.10.1 QoS設定	177
6.10.2 ポートあたりの優先順位	178
6.11 MACアドレス設定	179
6.12 STP/MSTPコマンド.....	181
6.13 SNMP	188

6.13.1 システムオプション	188
6.13.2 コミュニティストリング	189
6.13.3 トラップマネージャ	189
6.14 IGMP	190
6.15 802.1xプロトコル	192
6.16 アクセスコントロールリスト	195
6.16.1 IPv4 ACL コマンド	195
6.16.2 非 IPv4 ACL コマンド	197
6.17 バインディング	198
6.17.1 SIP/SMACバインディング・コマンド	198
6.18 DHCP構成.....	200
6.19 VDSL2 Cオマズ.....	201
6.19.1 VDSL2インターフェイスコマンド.....	201
6.19.2 VDSL2プロファイルコマンド	204
7. スイッチ操作	213
7.1 住所表.....	213
7.2 学習	213
7.3 転送とフィルタリング	213
7.4 ストア アンド フォワード	213
7.5 自動ネゴシエーション	213
8. トラブルシューティング	215
付録 A:RJ45 PIN 割り当て	217
A.1 スイッチのRJ45ピン割り当て	217
A.2 10/100Mbps、10/100BASE-TX	217

1. 導入

PLANET 8ポート VDSL2+2ポート ギガビット TP/SFP 管理スイッチ、VC-820Mをご購入いただきありがとうございます。このガイドに記載されている「管理対象スイッチ」とは、VC-820Mを指します。

1.1 パッケージの内容

管理対象スイッチのボックスを開き、慎重に解凍します。ボックスは、次の項目を調べるべきです。

- ◆ 管理対象スイッチ x 1
- ◆ クイック インストール ガイド x 1
- ◆ RS232 から RJ45 ケーブル x 1
- ◆ ラバーフィート x 4
- ◆ 取り付けネジ付きラック取り付けブラケット 2本 x 1セット
- ◆ 電源コード x 1
- ◆ SFP ダストキャップ x 2

これらのいずれかが紛失または破損している場合は、直ちに販売店にお問い合わせください。可能であれば、元の梱包材を含むカートンを保持し、修理のために私たちに返却する必要がある場合に製品を再梱包するために再び使用してください。

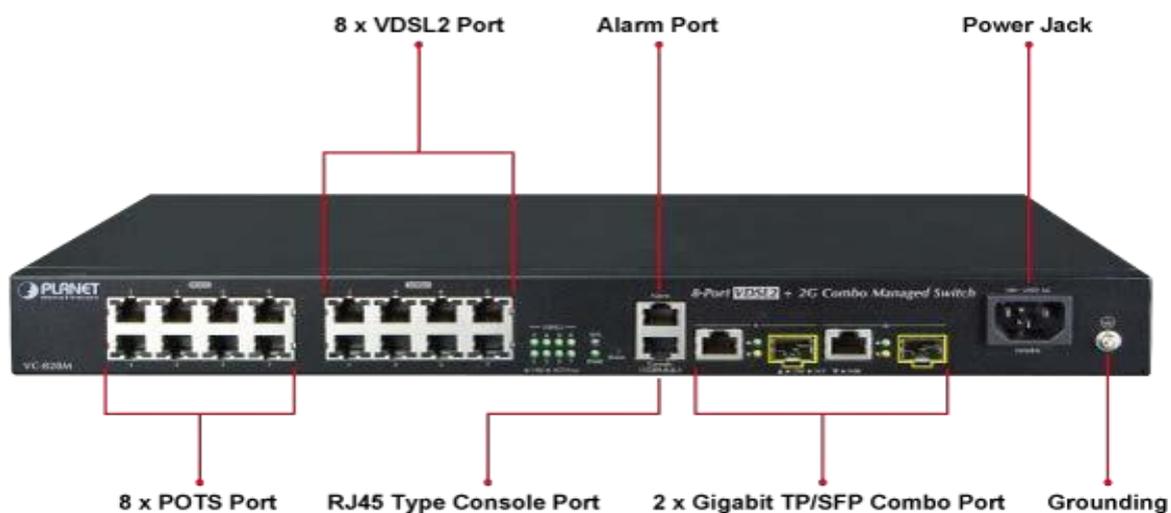
1.2 製品の説明

既存の電話回線での高性能 VDSL2 データ レート

PLANET VC-820M は、2 ギガビット TP/SFP コンボインターフェイスを備えた 8 ポート VDSL2 管理対象 CO(セントラル オフィス)スイッチです。VDSL2 COスイッチは、コミュニティ、ネットワークサービスプロバイダ、SI、IP監視プロバイダなどのネットワーキングアプリケーション向けに完璧に設計されています。イーサネットと VDSL2 (非常に高いデータ レートの Dデジタル加入者回線 2) の 2 つのコア ネットワーキング テクノロジーに基づいています。VDSL2 CPE(顧客宅内 機器)のPLANET VC-23xシリーズで動作し、

VC-820Mは、既存の銅線電話回線を介した絶対に高速なデータ伝送速度を提供し、ラストマイル接続に理想的なソリューションを提供します。

VC-820M の各 VDSL2 インターフェイスは、VDSL2 接続用と POTS(プレーン 旧電話サービス)接続用の 2 つの銅線電話 ポートを提供します。既存の電話回線を POTS と共有するために、VC-820M には POTS sp ゴミが内蔵されており、電 話およびネットワーク データを介した音声を中断することなく同じネットワーク経由で送信できます。



ISP/トリプルプレイデバイス向けに要求の高い接続性を提供

ホーム ブロードバンド接続の需要が高まるにつれて、VDSL2 テクノロジーはホーム サービスの統合をサポートする次のメ ディアであり、現在のケーブル モデムや ADSL テクノロジーよりも高速な伝送速度を提供します。VC-820Mは、 EoVDSL(VDSL 経由のイーサネット)を適用して最大 100 Mbps のダウンロード機能を提供し、ローカル ネットワークで 次のマルチメディア サービスをより効率的にします。

- IPTV/HDTV
- VoD (ビデオオンデマンド)
- ボイスオーバー IP
- ビデオ会議/ビデオ電話
- オンライゲーム
- インターネットラジオ/オンラインミュージック
- 長距離教育

VC-820Mは、ホームエンターテインメントと通信のためのトリプルプレイデバイスの要件を満たすために優れた帯域幅を提供しています。

最高のパフォーマンスを確保するための QoS 機能

VDSL2 スイッチには、ポート ベース、802.1p プライオリティ、IPToS/DSCPなどの堅牢な QoS機能が搭載されており、VoIP およびビデオ ストリーム伝送の最高のパフォーマンスを確保できるため、企業は限られたネットワーク リソースを最大限に活用できます。

サービスの差別化のための選択可能なVDSL2データレート

管理者は、管理インターフェイスを使用して、各 VDSL2 インターフェイスのデータ転送速度を制御できます。テレコムと ISP は、さまざまな要求に応じて帯域幅サービスを即座にリモートでアップグレード/ダウングレードできます。

効率的な管理

現在のネットワークをさらに拡張するために、PLANET VC-820M はコンソールおよびTelnetコマンドライン インターフェイス、および高度な Web および SNMP 管理インターフェイスを提供します。組み込みのWebベースの管理インターフェイスを備えたVDSL2スイッチは、使いやすいプラットフォームに依存しない管理および構成機能を提供します。VDSL2 スイッチは、標準の簡易ネットワーク管理プロトコル(SNMP)をサポートし、標準ベースの管理ソフトウェアを介して監視できます。テキストベースの管理では、VDSL2 スイッチには Telnet とコンソール ポートを通じてアクセスすることもできます。さらに、VDSL2 スイッチは、各セッションでパケット コンテンツを暗号化するセキュア ソケット レイヤ(SSL) 接続をサポートすることにより、セキュアなリモート管理を提供します。上記の機能は、ハードウェアやソフトウェアを使用して余分な安全なシステムを追加する必要がなく、デバイスを管理するための効率的な方法を提供します。

堅牢なレイヤ 2 の機能

Web インターフェイスを介して効率的な管理を行う場合、VC-820M は、port 速度設定、ポートリンク アグリゲーション、IEEE 802.1Q VLAN およびQ-in-Q VLAN、ポート ミラーリング、ラピッド スパニング ツリー、ACL セキュリティなどの基本的なスイッチ管理機能用にプログラムできます。さらに、ファームウェアには、IGMP スヌーピング、QoS(サービス品質)、ブロードキャスト ストーム、帯域幅制御などの高度な機能が含まれており、帯域幅の使用率を向上させます。

上級セキュリティ

VDSL2 スイッチは、不要なトラフィックを除外するための包括的なレイヤ 2、レイヤ 3、およびレイヤ 4 アクセス コントロール リスト(ACL)を提供します。その保護メカニズムは、RADIUS およびポート ベースの 802.1X ユーザおよびデバイス認証で構成されます。さらに、VDSL2スイッチは、エッジにセキュリティポリシーを適用するためのMACフィルタ、スタティック MAC、IP/MAC バインディング、およびポートセキュリティを提供します。管理者は、以前よりもかなり少ない時間と労力で、高度にセキュリティで保護された企業ネットワークを構築できるようになりました。

1.3 このマニュアルの使い方

このユーザーマニュアルの構成は次のとおりです

セクション 2, インストール

このセクションでは、スイッチの機能と、管理対象スイッチを物理的にインストールする方法について説明します。

セクション 3, スイッチ管理

このセクションには、管理対象スイッチのソフトウェア機能に関する情報が含まれています。

セクション 4, WEB 構成

このセクションでは、Web インターフェイスによってマネージ スイッチを管理する方法について説明します。

セクション 5, コンソール管理

このセクションでは、コンソール管理インターフェイスの使用方法について説明します。

セクション 6, コマンドラインインターフェイス

このセクションでは、コマンドライン インターフェイスによって管理対象スイッチを管理する方法について説明します。

セクション 7, 切り替え操作

この章では、管理対象スイッチのスイッチ操作を行う方法について説明します。

セクション 8, トラブルシューティング

この章では、管理対象スイッチのトラブルシューティングを行う方法について説明します。

A ペンディックス A

このセクションには、管理対象スイッチのケーブル接続情報が含まれて

1.4 製品の特徴

VDSL インターフェイス

- VDSL2 接続用の8 x RJ11コネクタ
- POTS 接続用の8 x RJ11コネクタ
- 各 VDSL ポートの内蔵POTS スプリッタ
- VDSL2リンクの自動速度機能(距離とケーブル品質別)

イーサネット インターフェイス

- 2 ギガビット TP および SFP 共有コンポインターフェイス
- ギガビット RJ45ポートでの自動 MDI/MDI-X 検出

VDSL2 の機能

- コスト効率の高いVDSL2リンクと中央管理ソリューション
- ITU-T G.993.2 VDSL2 規格
- DMT (ディスクリットマルチトーン)ラインコーディング VDSL
- 最大100/100Mbps の対称データレート
- 銅配線距離最大1km
- 選択可能なターゲット データ レートとターゲット SNRマージン
- 高エネルギースパイクによるサージダメージに対するサージ保護を内蔵
- 音声通信とデータ通信は、既存の電話回線で同時に共有できます。
- each ポートでダウンストリーム/アップストリーム レート制御をサポート

➤ レイヤ 2の機能

- ストアアンドフォワードアーキテクチャと runt/CRC フィルタリングの高パフォーマンスにより、誤ったパケットを排除してネットワーク帯域幅を最適化
- ブロードキャスト/マルチキャスト/ユニキャスト ストーム制御
- VLAN をサポート
 - IEEE 802.1Qタグベース VLAN
 - ポートベースのVLAN
 - Q-in-Q トンネリング(VLANスタッキング)
 - ダイナミック VLAN管理用 GVRP
 - プライベート VLAN エッジ(PVE/保護ポート)
- リンクアグリゲーション
 - IEEE 802.3ad LACP(リンクアグリゲーション制御プロトコル)
 - シスコイーテル チャンネル(スタティックトランク)
- スパニングツリープロトコル
 - STP、IEEE 802.1D
 - MSTP、IEEE 802.1s
- 特定のポートの着信トラフィックまたは発信トラフィックを監視するポートミラーリング

➤ サービスの品質

- すべてのスイッチポートで 4 つのプライオリティ キュー
- トラフィック分類:
 - IEEE 802.1p CoS
 - IP TOS/DSCP
 - ポートベースの優先順位
- 厳密な優先順位と重み付けラウンドロビン (WRR) CoS ポリシー

➤ マルチキャスト

- IGMP スヌーピング v1 およびv2をサポート
- IGMP クエリア モードのサポート

➤ セキュリティ

- IEEE 802.1X ポートベースのネットワーク アクセス制御プロトコル
- RADIUS ユーザーが認証にアクセスする
- L2/L3/L4 アクセス コントロール リスト(ACL)
- MAC フィルタリングと送信元IP-MAC/ポート バインディング
- 送信元 MAC アドレス エントリフィルタリングのポート セキュリティ

➤ 管理

- スイッチ管理インターフェイス
 - Telnnetコマンド行インターフェース
 - Web スイッチ管理
 - SNMP v1、v2c、v3 スイッチ管理
 - SSL スイッチ管理
- IP アドレス割り当てのDHCP クライアント
- ネットワーク管理を容易にするリンク層検出プロトコル (LLDP)
- DHCP オプション 82 および DHCPリレー
- 組み込みの簡易ファイル転送プロトコル (TFTP)クライアント
- TFTP またはHTTP経由のファームウェア アップグレード
- TFTP またはHTTP経由の設定のアップロード/ダウンロード
- 4つの RMON グループ 1、2、3、9 (履歴、統計、アラーム、およびイベント)
- インターフェイス リンクアップおよびリンク ダウン通知の SNMP トラップ
- システム管理用のリセットボタン
- スイッチの基本管理とセットアップのための RJ45 コンソール インターフェイス

1.5 製品仕様

製品	VC-820M
ハードウェア仕様	
ハードウェアバージョン	2.0
VDSL インターフェイス	8 VDSL2 RJ11 インターフェイス
	8 POTS RJ11 インターフェイス
銅ポート	2 10/100/1000BASE-T RJ45自動MDI/MDI-Xポート
SFP/ミニ GBIC スロット	ポート 9 およびポート 10 と共有される 2 つの 1000BASE-X SFP インターフェイス
コンソール	1 RS232 から RJ45 シリアル ポート(115200、8、N、1)
過渡電圧サプレッサ	IEC 61000-4-2 (ESD): $\pm 15\text{kV}$ (空気), $\pm 8\text{kV}$ (接触) IEC 61000-4 (EFT): 40A (5/50ns) IEC 61000-4-5 (ライトニング): 24A (8/20 μs)
スイッチアーキテクチャ	ストア アンド フォワード
スイッチ・ファブリック	5.6Gbps / ノンブロッキング
スイッチのスループット	4.16Mpps @64 バイト
住所テーブル	8K エントリ
共有データ バッファ	256K バイト
最大フレーム サイズ	9K バイト
フロー制御	半二重の背圧 全二重の IEEE 802.3x 一時停止フレーム
Led	VDSL2, PWR, SYS, LNK/ACT, 1000
リセットボタン	< 5 秒: システムの再起動 > 10 秒: 工場出荷時のデフォルト
寸法(長さ x D x H)	404 x 174 x 44.5 mm、高さ 1U
重量	2.4キロ
電源要件	100~240V AC、50~60 Hz
消費電力/消散	36ワット(最大)/112.8 BTU/時間
VDSL2	
VDSL2 スタンダード	ITU-T G.993.1 および G.993.2 に準拠しています。 VDSL オプションバンド(25K ~ 138K Hz)の使用法のプロビジョニングをサポート
バンドプラン	ポート単位の各 VDSL回線の選択可能なバンド プラン - プロファイル998, G.993.1 の附属 A;対称サービス用に最適化されたバンド プランB: - プロファイル 997, G.993.1の附属 B;非対称サービス用に最適化
プロファイル	G.993.2 で定義された周波数帯域(附属書 A、B、C)の 8a/b/c/d、12a/b、17a、および 30a の選択可能なスペクトル プロファイル
エンコーディング	VDSL-DMT
VDSL2 の機能	選択可能なレート制限制御 選択可能なターゲット SNR(信号対ノイズ比)モード POTS ボイス パススルー
レイヤ 2 機能	
管理インターフェイス	コンソール、Telnet、Web ブラウザ、SSL、SNMP v1、v2c、v3

ギガビット ポートの構成	<p>ポートの無効化/自動ネゴシエーションの有効化</p> <p>10/100/1000Mbps 全二重および半二重モードの選択</p> <p>フロー制御の無効化/有効化</p>
ギガビット ポートの状態	各ポートの速度デュプレックス モード、リンク ステータス、フロー制御ステータスの自動ネゴシエーション ステータス、トランク ステータスを表示する
ポート ミラーリング	<p>TX/RX/両方</p> <p>1 から 1 モニター</p>
帯域幅制御	<p>インGRESS/エGRESS レートリミット制御 ギガビット ポート:</p> <ul style="list-style-type: none"> • 128 Kbpsあたりの構成を許可する <p>VDSL2 ポート:</p> <ul style="list-style-type: none"> • 5Mbpsあたりの構成を許可する
Vlan	<p>IEEE 802.1Q タグ ベース VLAN、最大 256 個の VLAN グループ、4094 VLAN ID ポートベース VLAN</p> <p>GVRP、最大 128 のダイナミック VLAN</p> <p>グループ Q-in-Q トンネリング</p> <p>2 つの保護されたポート グループを持つプライベート VLAN エッジ(PVE/保護ポート)</p>
リンクアグリゲーション	<p>スタティック ポート トランク</p> <p>IEEE 802.3ad LACP(リンクアグリゲーション制御プロトコル) は、トランクあたり 8 ポートの 13 グループをサポート</p>
Qos	<p>4 優先度キュー</p> <p>に基づくトラフィック分類</p> <ul style="list-style-type: none"> - ポートの優先順位 - 802.1p優先度 - アプリケーションプロトコル <p>No による IP パケットVoIP QoSの DSCP/TOS フィールド。</p>
IGMP スヌーピング	IGMP(v1、v2)スヌーピング、最大256のマルチキャストグループ
アクセス制御リスト	<p>IP ベースのレイヤ 3/レイヤ 4</p> <p>ACL 最大 220 ACL ルール エントリ</p>
セキュリティ	<p>ポートセキュリティ(MAC アドレス学習のポートごとに無効にする)スタティック MAC、MAC フィルタ、IP/MAC バインディング</p>
SNMP MIB	<p>RFC 1213 MIB-II</p> <p>RFC 2863 インターフェイス MIB RFC 2665</p> <p>Etherライク MIB RFC 1493ブリッジ MIB</p> <p>RFC 2819 RMON MIB (グループ 1, 2, 3,9)</p>
規格適合	
法令遵守	FCC パート 15 クラス A、CE

標準準拠	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ab 1000BASE-T IEEE 802.3x LACP を使用したフロー制御および背圧ポート トランク IEEE 802.3ad よび背圧ポート トランク IEEE 802.1D スパニングツリー プロトコル IEEE 802.1w ラピッド スパニング ツリー プロトコル IEEE 802.1p ロトコル サービス クラス IEEE 802.1Q VLAN タグ付け IEEE 802.1x ポート認証ネットワーク制御
	ITU-T G.993.1 (VDSL) G.997.1 G.993.2 VDSL2 RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP v1 RFC 2236 IGMP v2
ケーブル	<ul style="list-style-type: none"> • VDSL2: ツイストペアの電話線(AWG24以上)最大1km • 10/100BASE-TX: 2 ペア UTP Cat.5、最大 100m (328 フィート) • 1000BASE-T: 4 ペア UTP Cat.5E、最大 100m • 1000BASE-SX: 50/125μmおよび62.5/125μm光ファイバケーブル、550mまで • 1000BASE-LX: 9/125μm光ファイバケーブル、最大10km 50/125μmおよび62.5/125μm光ファイバケーブル、最大550m
環境	
オペレーティング	温度:-10~50°C 相対湿度:10~90%(結露しない)
ストレージ	温度:-20~70°C 相対湿度:10~90%(結露しない)

A. 2インストール

このセクションでは、デスクトップまたはラックマウントへの管理対象スイッチのハードウェア機能とインストールについて説明します。管理対象スイッチの管理と制御を容易にするために、ディスプレイ インジケータとポートについて理解します。この章のフロントパネルの図は、ユニットLEDインジケータを表示します。ネットワーク デバイスを管理対象スイッチに接続する前に、この章を完全にお読みください。

2.1 ハードウェアの説明

2.1.1 スイッチフロントパネル

ユニットフロントパネルは、スイッチを監視するシンプルなインターフェイスを提供します。図 2-1-1~2-1-2は、管理対象スイッチの前面パネルを示しています。

VC-820Mフロントパネル

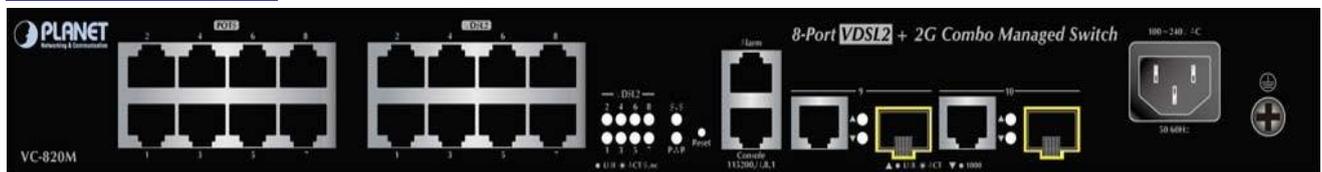


図 2-1-2: VC-820M スイッチの前面パネル

■ VDSL2 および POTSインターフェイス

VC-820Mの前面パネルには8つのPOTSポートwith RJ11電話コネクタがあります。各ポートは、電話の音声とネットワーク アプリケーションのデータを中断することなく同じワイヤで送信するのに役立つ組み込みの POTS スプリッタです。

VDSL2 は、異なる帯域割り当てで動作し、アップストリームとダウンストリームの帯域幅が異なる自動検出トランス ミッション レートをサポートします。異なる電話回線の品質のために、クロストークや延長距離は、実際の達成可能な速度に影響を与える可能性があります。組み込みの管理インターフェイスで individual ポートを設定して、最適化された接続を実現できます。

■ ギガビット TPインターフェイス

10/100/1000BASE-T銅、RJ45ツイストペア:最大100メートル。

■ 100/1000BASE-X SFPスロット

各 SFP(小型フォーム ファクタ プラグ可能)スロットは、デュアルスピード、1000BASE-SX/LX または 100BASE-FX をサポートします。

- 1000BASE-SX/LX SFP トランシーバ モジュールの場合:550 メートル(マルチモード ファイバ)から 10/30/50/70/120 キロメートル(シングルモードファイバ)。
- 100BASE-FX SFP トランスカイバー モジュールの場合:2 キロメートル(マルチモード ファイバ)から 20/40/60 キロメートル(シングルモードファイバ)。

■ コンソールポート

コンソール ポートは RJ45 ポート コネクタです。端末を直接接続するためのインターフェイスです。コンソールを使用するポート、IPアドレス設定、工場出荷時のリセット、ポート管理、リンクステータス、およびシステム設定。

ユーザーは、パッケージ内で接続された **DB9 から RJ45コンソール・ケーブル**を使用して、デバイスのコンソール・ポートに接続できます。接続後、ユーザーは任意の端末エミュレーションプログラム(ハイパーターミナル、プロコムプラス、テリクス、ウィンタームなど)を実行して、デバイスの起動画面に入ることができます。



1. ベイロード レートは、フレーミング オーバーヘッドによるライン レートよりも約 **9%** 小さい値です。
2. **AWG 26(0.4mm)**ケーブルも使用できますが、距離は上の表より**20%**から**40%**短いです。
3. 各終端ブリッジタップは、**VDSLリンク距離を90m短縮**できます。
ケーブルの品質、ケーブルバンドルのサイズ、バンドル内のクロストークも全体的なリーチに影響を与える可能性があります。

■ アラームインターフェイス

アラーム ポートは **RJ45** ポート コネクタです。センサーを直接接続するためのインターフェースです。アラーム機能を有効にするには、**4.2.9章**を参照してください。

■ リセットボタン

フロントパネルの左側にあるリセットボタンは、電源を切ったまま管理スイッチを再起動するように設計されています。リセットボタン機能の概要表を次に示します。

リセットボタンが押され、離された	関数
< 5 秒: システムの再起動	管理対象スイッチを再起動します。
> 5 秒: 工場出荷時のデフォルト	管理対象スイッチを工場出荷時のデフォルト設定にリセットします。次に、管理対象スイッチが再起動し、次に示すようにデフォルト設定がロードされます。 <ul style="list-style-type: none"> ◦ 既定のユーザー名:管理者 ◦ 既定のパスワード:管理者 ◦ デフォルト IP アドレス:192.168.0.100 ◦ サブネットマスク:255.255.255.0 ◦ デフォルト ゲートウェイ:192.168.0.254

AC電源コンセント

世界のほとんどの地域で電気サービスとの互換性を保つために、マネージドスイッチの電源は**100-240V AC**および**50/60 Hz**の範囲のライン電力に自動的に調整される。

電源コードのメス端を管理対象スイッチの**re ar**パネルのコンセントにしっかりと差し込み、電源コードのもう一方の端をコンセントに差し込み、電源が整います。

電源に関する通知:

デバイスは電源が必要なデバイスであるため、電源が入るまで動作しません。ネットワークが常にアクティブである必要がある場合は、**お使いのデバイスにUPS(無停電電源装置)**を使用することを検討してください。これにより、ネットワーク データの損失や時間のダウンタイムを防ぐことができます。

電源に関する通知:

一部の領域では、サージ抑制デバイスを取り付けることで、制御されていないサージや管理対象スイッチへの電流によって管理対象スイッチが損傷を受けないように保護するのにも役立ちます。

2.1.2 LED表示

フロント・パネルのLEDは、ポート・リンク、データ・アクティビティ、およびシステム電源の即時状況を示し、必要に応じてモニターおよびトラブルシューティングに役立ちます。

VC-820M LED表示

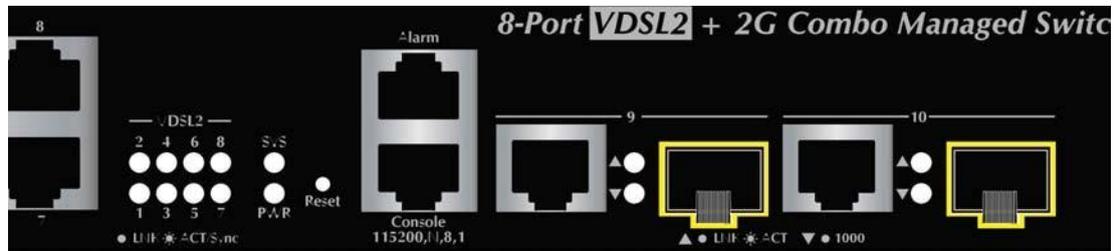


図 2-1-5: VC-820M システムおよびポート LED パネル

■ システム/アラート

Led	色	関数
Pwr	緑	スイッチに電力があることを示すライトが点灯します。
Sys	緑	システムが動作していることを示すライト。 システムが起動中であることを示すには off。
	赤	FAN がダウンしているか、RJ45 アラーム ポートのピンがトリガーされていることを示すライトが点灯します。

■ VDSL2インターフェイス(ポート 1 からポート 8)

Led	色	関数
VDSL2	緑	ライト: そのポートを介したリンクが正常に確立されたことを示します。
		点滅: スイッチがアクティブにデータを送受信しているか、VDSL 同期を介して送信中であることを示すには そのポート。
		オフ: ポートがリンクダウンしていることを示します。

■ TP/SFP コンボインターフェイス(ポート 9 からポート 10)

Led	色	関数
LNK/ACT	緑	ライト: そのポートを介したリンクが正常に確立されたことを示します。
		点滅: スイッチがそのポートを介してアクティブにデータを送受信していることを示します。
1000	オレンジ	ライト: ポートが 1000 Mbps で動作していることを示すには、次の手順を実行します。
		オフ: LNK/ACT LED が点灯している場合は、ポートが 10/100 Mbps で動作していることを示します。 LNK/ACT LED がオフの場合は、ポートがリンクダウンしていることを示します。

2.2 スイッチの取り付け

このセクションでは、管理対象スイッチをインストールして接続する方法について説明します。以下のトピックを読み、記載されている順序で手順を実行してください。

2.2.1 デスクトップインストール

管理スイッチをデスクトップまたはシェルフにインストールするには、次の手順を実行してください。

ステップ 1: マネージドスイッチの底面にある凹部にゴム足を取り付けます。

手順 2: 管理スイッチをデスクトップまたは AC 電源の近くの棚に配置します。

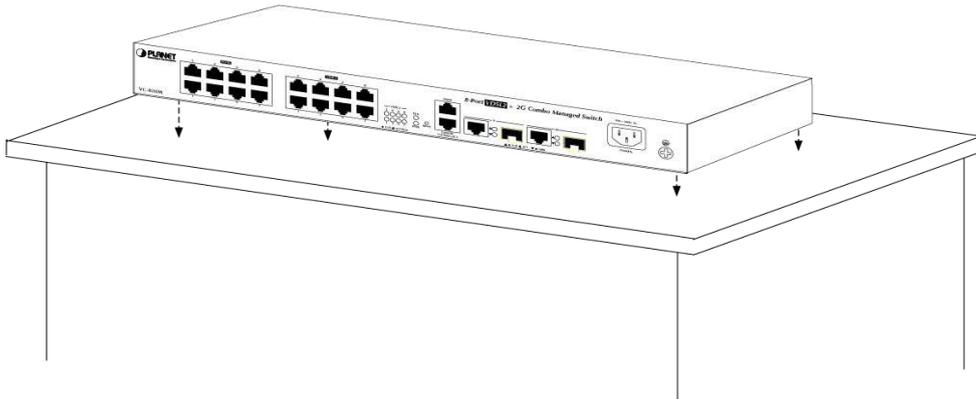


図 2-2-1: デスクトップに管理対象スイッチを配置する

ステップ 3: 管理対象スイッチと周囲のオブジェクトの間に十分な換気スペースを保ちます。



ロカを選択する際には、「仕様」の第1章第4項で説明した環境制限に留意してください。

手順 4: 管理対象スイッチをネットワーク デバイスに接続します。

- A. 標準ネットワーク ケーブルの一方の端を、管理対象スイッチの前面にある 10/100/1000 RJ45 ポートに接続します。
- B. ケーブルのもう一方の端を、プリンタ サーバー、ワークステーション、ルーターなどのネットワーク デバイスに接続します。



管理対象スイッチへの接続には、RJ45チップを備えた UTP カテゴリ 5 ネットワーク ケーブル接続が必要です。詳細については、付録 A のケーブル配線仕様の仕様を参照してください。

ステップ 5: 管理対象スイッチに電源を供給します。

- A. 電源ケーブルの一方の端を管理対象スイッチに接続します。
- B. 電源ケーブルの電源プラグを標準のコンセントに接続します。

管理対象スイッチが電力を受け取ると、電源 LED は緑色のままになります。

2.2.2 ラック取り付け

19インチの標準ラックに管理対象スイッチを取り付けるには、以下の手順に従ってください。

ステップ1:前面パネルを前面に向けて配置したハードフラットサーフェスに管理対象スイッチを配置します。

ステップ 2:パッケージに付属のネジを取り付けたラックマウント ブラケットを管理対象スイッチの両側に取り付けます。

図 2-2-2および図 2-2-3は、管理対象スイッチの片側にブラケットを取り付ける方法を示しています。

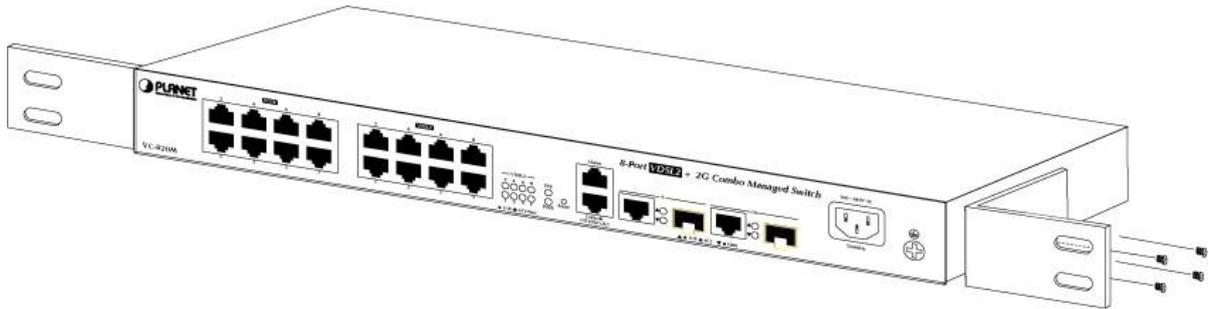


図 2-2-2: ブラケットを VC-820M に取り付ける



取り付けブラケットに付属のネジを使用する必要があります。誤ったネジを使用して部品に損傷を与えると、保証が無効になります。

手順 3: ブラケットをしっかりと固定します。

ステップ 4: 同じ手順に従って、2 番目のブラケットを反対側に取り付けます。

ステップ 5: ブラケットを管理対象スイッチに取り付けた後、図 2-2-3 および図 2-2-4 に示すように、適切なネジを使用してブラケットをラックにしっかりと取り付けます。

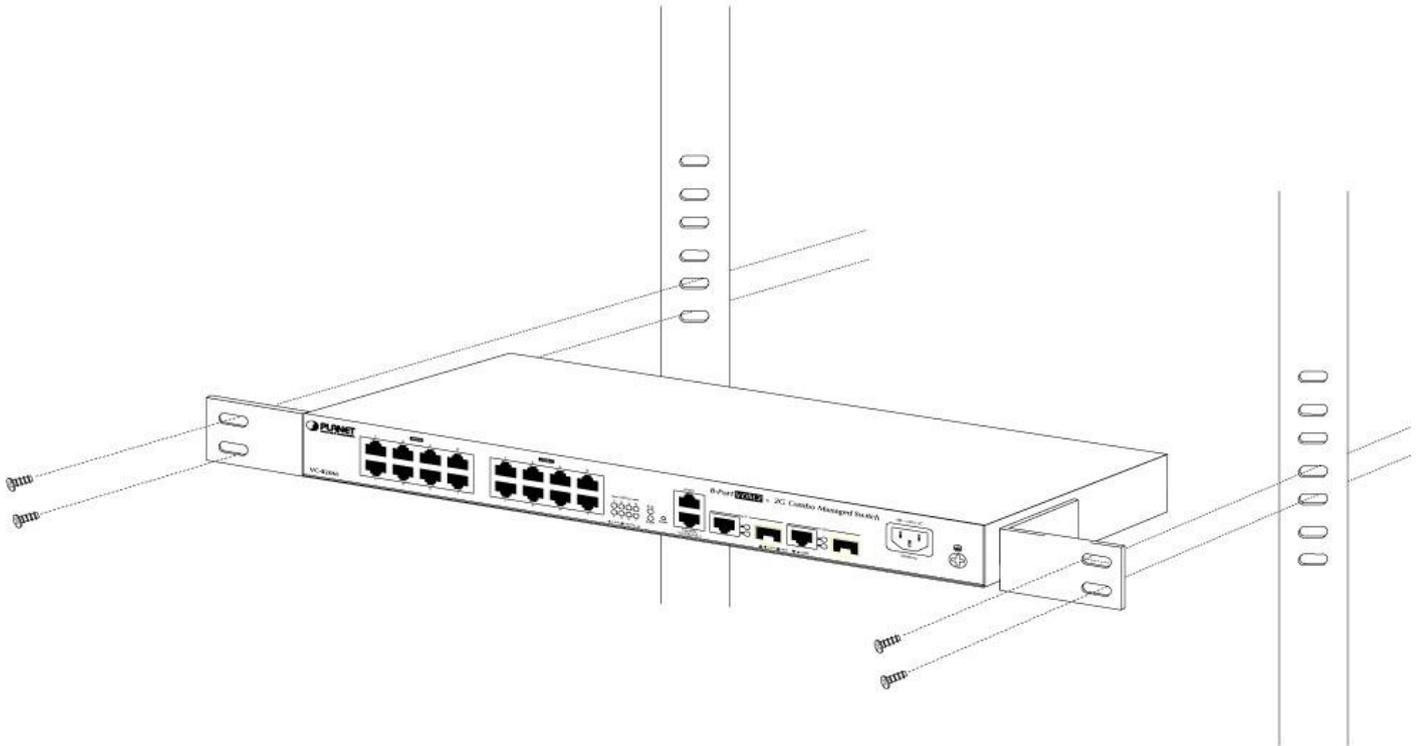


図 2-2-4: ラックへの VC-820M の取り付け

手順 6:セッション 2.2.1 デスクトップ インストールの手順 4 と 5 に進み、ネットワーク ケーブルを接続し、管理対象スイッチに電源を供給します。

2.2.3 SFP トランシーバの取り付け

このセクションでは、SFP トランシーバを SFP スロットに挿入する方法について説明します。SFP トランシーバはホットプラグ可能でホットスワップ可能です。図 2-1-7 に示すように、管理対象スイッチの電源を切ることなく、任意の SFP ポートとの間でトランシーバを接続および接続できます。

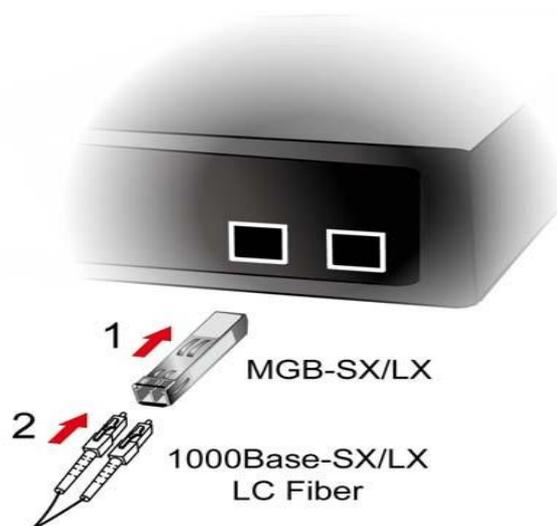


図 2-1-7 SFP トランシーバのプラグ

■ 承認された PLANET SFP トランシーバ

PLANET マネージスイッチは、シングルモードとマルチモード SFP トランシーバの両方をサポートします。次の承認済み PLANET SFP トランシーバのリストは、公開時点で正しいです。

ギガビット SFP トランシーバ モジュール

- **MGB-GT** SFP ポート 1000BASE-T モジュール
- **MGB-SX** SFP ポート 1000BASE-SX ミニ GBIC モジュール
- **MGB-LX** SFP ポート 1000BASE-LX ミニ GBIC モジュール
- **MGB-L50** SFPポート1000BASE-LXミニGBICモジュール - 50km
- **MGB-L70** SFPポート1000BASE-LXミニGBICモジュール - 70km
- **MGB-L120** SFPポート1000BASE-LXミニGBICモジュール - 120km
- **MGB-LA10** SFPポート 1000BASE-LX (WDM,TX:1310nm) - 10km
- **MGB-LA20** SFPポート 1000BASE-LX (WDM,TX:1310nm) - 20km
- **MGB-LB20** SFPポート1000BASE-LX(WDM,TX:1550nm) - 20km
- **MGB-LA40** SFPポート 1000BASE-LX (WDM,TX:1310nm) - 40km
- **MGB-LB40** SFPポート 1000BASE-LX (WDM,TX:1550nm) - 40km



管理対象スイッチで PLANET SFP を使用することをお勧めします。サポートされていない SFP トランシーバを挿入すると、管理対象スイッチはそれを認識しません。



以下のインストール手順では、このマニュアルではギガビットSFPトランシーバを例として使用します。ただし、ファストイーサネット SFP トランシーバの手順は似ています。

1. マネージドスイッチを他のネットワーク デバイスに接続する前に、sFP トランシーバの両側が同じメディアタイプであることを確認する必要があります(たとえば、1000BASE-SX から 1000BASE-SX、1000BASE-LX から 1000BASE-LX を 1000BASE-LX)。
2. 光ファイバ ケーブルタイプが SFP トランシーバ要件と一致するかどうかを確認します。
 - ▶ 1000BASE-SX SFP トランシーバに接続するには、片側がオスデュプレックス LC コネクタ タイプのマルチモードファイバ ケーブルを使用してください。
 - ▶ 1000BASE-LX SFP トランシーバに接続するには、片側がオスデュプレックス LC コネクタタイプのシングルモードファイバ ケーブルを使用してください。

■ ファイバケーブルの接続

1. 両面 LC コネクタを SFPトランシーバに挿入します。
2. ケーブルのもう一方の端を、SFP トランシーバが取り付けられているデバイスに接続します。
3. 管理対象スイッチの前面にある SFPスロットの LNK/ACT LED を確認します。SFPトランシーバが正しく動作していることを確認します。
4. リンクに障害が発生した場合は、SFP ポートのリンク モードを確認します。一部のファイバ NIC またはメディアコンバータを使用して機能するには、ポートリンク モードを"**1000 Force**"に設定する必要があります。

■ トランシーバモジュールの削除

1. ネットワークアクティビティがなくなったことを確認します。
2. 光ファイバケーブルをゆっくりと取り外します。
3. MGBモジュールのレバーを持ち上げ、水平位置に回します。
4. レバーを通してモジュールをゆっくりと引き出します。



図 2-1-8 SFP トランシーバを引き出す方法



Note

モジュールのレバーを持ち上げて水平位置に変えずに、モジュールを引き出すことはありません。モジュールを直接引き出すと、モジュールと SFP モジュール スロットが破損する可能性があります。

管理対象スイッチ。

2.3 VDSL2ポートの配線

VC-820MのVDSL2ポートは、既存の電話回線などの構造化された、または構造化されていないW Iリングを介して、リモートCPE(VC-231、VC-234、VDR-300NUまたは他の互換性のあるCPE)に直接接続することができる8つのRJ11コネクタを使用します。VDS2L CO スイッチ ポートと各 CPE 間のリンクは、プロファイル 30a または最大 5000 フィート(1500 m)の距離で 18/1 Mbps の 1000 フィート(300 m)未満で最大 100/100 Mbps の速度に達できます。管理対象スイッチの電源を切ったり、他のスイッチ ポートを中断したりすることなく、VDSL2 CPEをホット s pp できます。

各 VC-820M VDSL2 管理対象スイッチ シリーズには、同じ電話線を介してVDSL2 トラフィックサービスと電話サービス(音声またはファックスとして suc) の両方を送信する、組み込みのペインオールドテレフォン サービス (POTS)スプリッタがあります。スプリッタは、電話回線および構内交換機 (PBX) スイッチまたは公衆交換電話網 (PSTN)からの VDSL2 データ (高周波) および音声 (低周波) トラフィックをルーティングします。

接続 diaグラムは次のとおりです。

■ VC-820M VDSL2接続

VC-820MのVDSL2ポートは、既存の電話回線を介してリモートCPEに直接接続できる8つのRJ11コネクタを使用します。

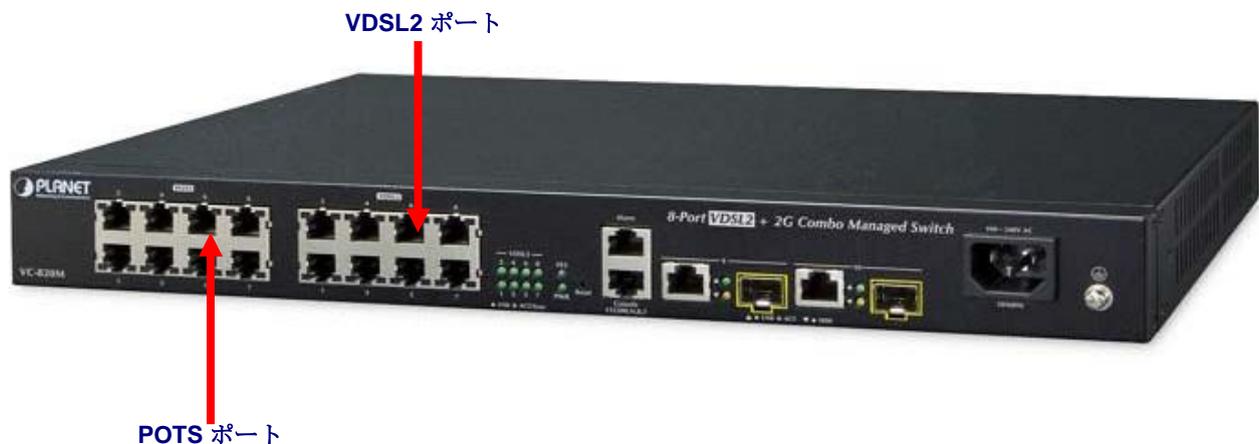


図 2-3-4: VC-820M VDSL2 接続

ポートが接続されていても、関連する LED が暗い場合は、次の項目を確認します。

1. VDSL2スイッチと接続デバイスの電源が入っているか、オンになっているか電源が入っていない。
2. 接続ケーブルは良好で、正しいタイプです。
3. ケーブルは、管理対象スイッチおよび関連デバイスのコネクタにしっかりと取り付けられています。
4. ネットワーク アダプタを含む接続デバイスは、適切にインストールされ、機能しています。
5. CPE(VC-231/VC-234/VDR-300NU)がCPEモードに設定されていることを確認します。背面パネルのDIPスイッチを確認します。
6. CPE(VC-231/VC-234/VDR-300NU)デバイスが干渉なしに動作可能な範囲内で実装されていることを確認します。

3. スイッチ管理

この章では、管理対象 Sw かゆみへの管理アクセスを構成するために使用できる方法について説明します。管理アプリケーションの種類と、管理デバイス (ワークステーションまたはパーソナル コンピュータ) とシステムの間でデータを配信する通信および管理プロトコルについて説明します。また、ポート接続の options に関する情報も含まれています。

この章では、次のトピックについて説明します。

- 要件
- 管理アクセスの概要
- 管理コンソールへのアクセス
- Web 管理アクセス
- SNMPアクセス
- 標準、プロトコル、および関連する読み取り

3.1 要件

- **Windows 98/ME、NT4.0、2000/XP/7/8/10、MAC OS9以降、Linux、UNIX、またはその他のプラット**
フォームを実行しているワークステーションは、**TCP/IP**プロトコルと互換性があります。
- **ワークステーションはイーサネット NIC (ネットワーク インターフェイスカード) と共にインストールされます。**
- **イーサネット ポート接続**
 - ネットワーク ケーブル -RJ45 コネクタで standa rd ネットワーク (UTP) ケーブルを使用します。
- 上記のワークステーションは、**Web ブラウザ**および **JAVA ランタイム環境**プラグインと共にインストールされます。
- **シリアルポート接続**
 - 上記のワークステーションには、COMポート(DB-9 / RS-232)またはUSB-to-RS-232コンバータが付属しています。



管理対象スイッチにアクセスするには、インターネット探索 6.0 以降を使用することをお勧めします。

3.2 管理アクセスの概要

マネージスイッチを使用すると、次の方法のいずれかまたはすべてを使用して、柔軟にアクセスして管理できます。

- Web ブラウザインターフェース
- 外部 SNMP ベースのネットワーク管理アプリケーション
- 管理コンソール

管理コンソールと Web ブラウザ・インターフェースは、管理対象スイッチ・ソフトウェアに組み込まれており、すぐに使用できます。これらの各管理方法は、独自の利点として h.表 3-1 に、3つの管理方法を比較します。

メソッド	利点	欠点
ウェブブラウザ	<ul style="list-style-type: none"> ● スイッチをリモートで構成する場合に最適 ● すべての一般的なブラウザと互換性があります ● 任意の場所からアクセス可能 ● 最も視覚的に魅力的 	<ul style="list-style-type: none"> ● セキュリティが侵害される可能性がある(ハッカーはIP アドレスとサブネット マスクのみを知る必要があります) ● 接続不良でラグ タイムが発生する可能性がある
SNMP エージェント	<ul style="list-style-type: none"> ● MIBレベルでスイッチ機能と通信 ● オープンスタンダードに基づく 	<ul style="list-style-type: none"> ● SNMP マネージャソフトウェアが必要 ● 3つの方法すべてのうち、視覚的に最も魅力的でない ● 一部の設定では計算が必要です ● セキュリティが侵害される可能性がある(ハッカーはコミュニティ名のみを知る必要がある)
コンソール	<ul style="list-style-type: none"> ● IP アドレスやサブネットは不要 ● テキストベース ● Windows 95/98/NT/2000/ME/XP/7/8/10 オペレーティング システムに組み込まれているTelnet機能とハイパーターミナル ● 安全 	<ul style="list-style-type: none"> ● スイッチの近くにあるか、ダイヤルアップ接続を使用する必要があります ● リモートユーザーには不便 ● モデム接続の信頼性が低いか、低速であることが判明する

表 3-1:管理方法の比較

3.3 ウェブ管理

管理スイッチは、ユーザーが Microsoft Internet Explorer などの標準ブラウザを使用して、ネットワーク上のどこからでも管理できる管理機能を提供します。スイッチのIP アドレスを設定した After では、管理対象スイッチの IP アドレスを入力することで、Web ブラウザで管理対象スイッチの Web インターフェイス アプリケーションに直接アクセスできます。

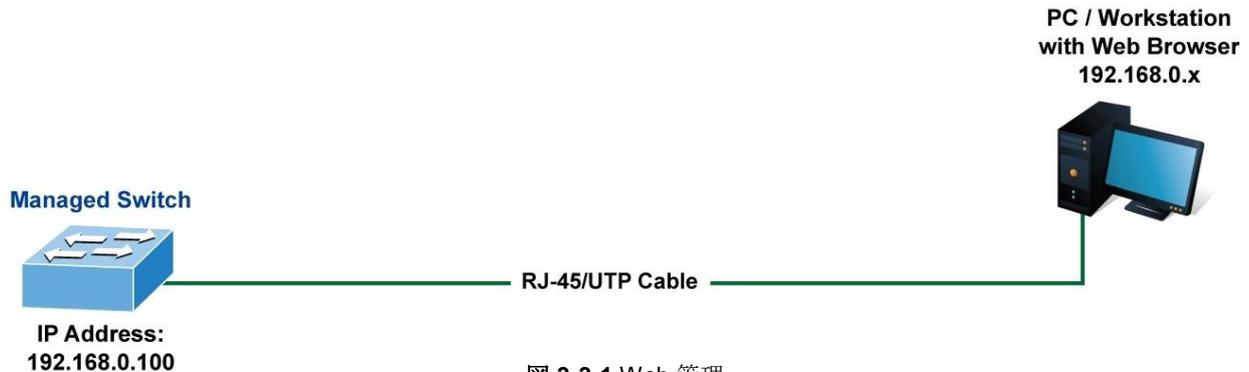


図 3-3-1 Web 管理

その後、Web ブラウザを使用して、管理対象スイッチのコンソール ポートに直接接続している場合と同様に、管理スイッチの構成パラメータを 1 か所から一覧表示および管理できます。ウェブ管理には、マイクロソフトのインターネ



ットエクスプローラ 6.0 以降、Safari または Mozilla Firefox 2.0 以降が必要です。

図 3-3-2 管理対象スイッチの Web メイン画面

3.4 SNMP ベースのネットワーク管理

外部 SNMP ベースのアプリケーションを使用して、SNMPCネットワーク マネージャ、HP オープンビューネットワーク ノード管理(NNM)、Whatsup Gold などの管理対象スイッチを設定および管理できます。この管理方法では、スイッチの SNMP エージェントと SNMP ネットワーク管理ステーションが同じコミュニティ ストリングを使用する必要があります。この管理方法では、実際には、**get** コミュニティ ストリングと **set** コミュニティ ストリングの2つの **community** 文字列が使用されます。SNMP Net-work 管理ステーションが設定されたコミュニティ ストリングのみを認識している場合は、MIB の読み取りと書き込みを行うことができます。ただし、**get** コミュニティ ストリングのみを認識している場合は、MIB のみを読み取ることができます。

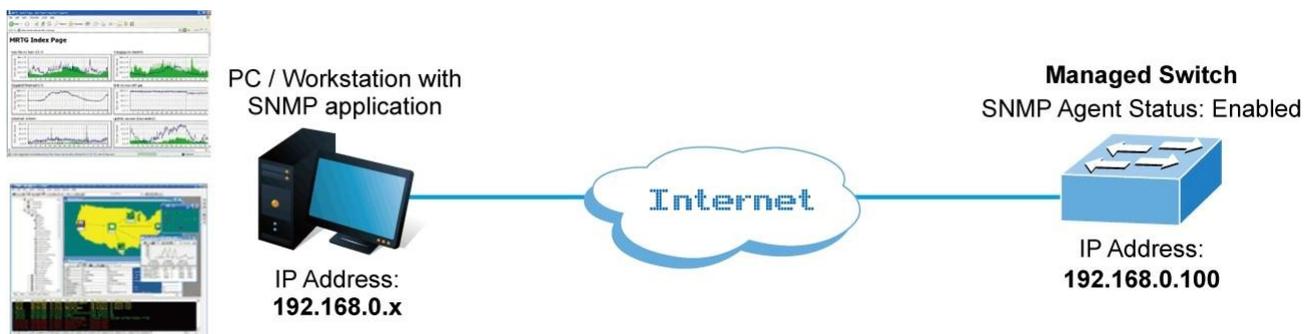


図 3-4-1 SNMP 管理

3.5 管理コンソール

管理コンソールは、統計の表示やオプション設定の変更などのシステム管理を実行するための、内部、文字指向、およびコマンド行のユーザー・インターフェースです。この方法を使用すると、スイッチのコンソール(シリアル)ポートに接続されている端末、パーソナルコンピュータ、Apple Macintosh、またはワークステーションから管理コンソールを表示できます。この管理方法を使用するには、直接アクセスまたはモデムポートアクセスの2つの方法があります。次のセクションでは、これらのメソッドについて説明します。コンソールの使用方法の詳細については、「第5章 コンソール管理」を参照してください。

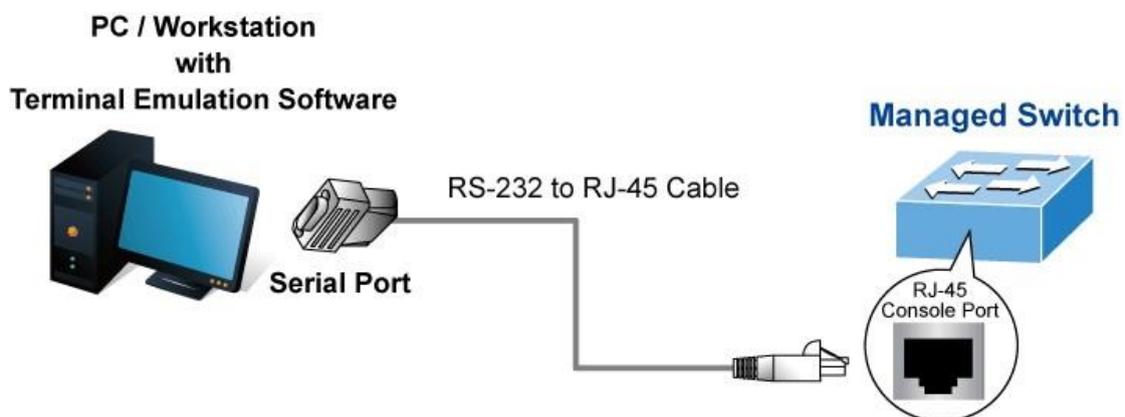


図 3-5-1 コンソール管理

直接アクセス

管理コンソールへの直接アクセスは、端末または端末エミュレーション・プログラム (ハイパーターミナルなど) を備えた PC を管理対象スイッチ・コンソール (シリアル) ポートに直接接続することによって実現されます。この管理方法を使用する場合、スイッチをPCに接続するには**DB9 RS-232ストレートケーブル**が必要です。この接続を行った後、以下のパラメーターを使用するように端末エミュレーション・プログラムを構成します。

既定のパラメーターは次のとおりです。

- 115200 bps
- 8 データビット
- パリティなし
- 1 ストップビット

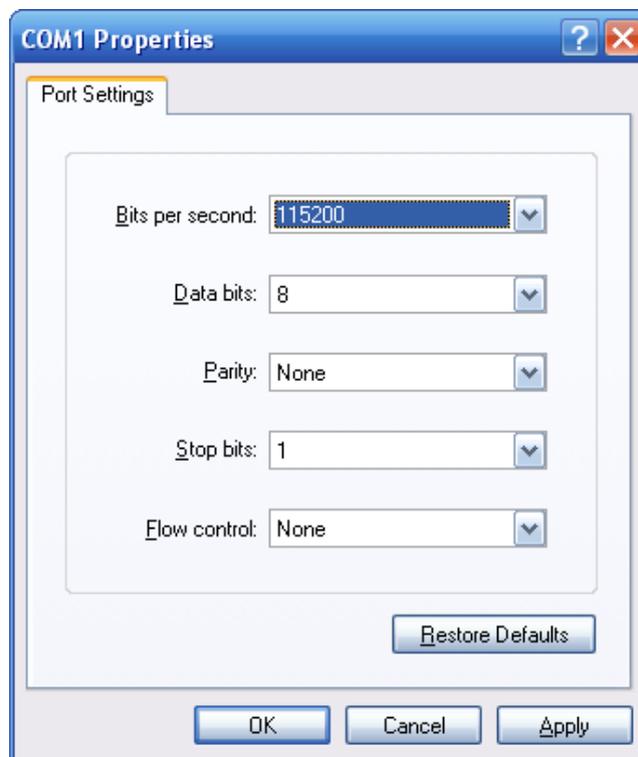


図 3-5-2 端子パラメータの設定

これらの設定は、必要に応じてログオン後に変更できます。この管理方法は、システムの再起動中も接続したままシステムを監視できるため、多くの場合、推奨されます。また、関連付けられたアクションが開始された e インターフェイスに関係なく、特定のエラーメッセージがシリアルポートに送信されます。Macintosh または PC 接続は、端末シリアル・ポートに接続するための任意の端末エミュレーション・プログラムを使用できます。UNIX の下のワークステーション接続は、TIP などのエミュレーターを使用できます。

3.6 プロトコル

管理対象スイッチは、次のプロトコルをサポートします。

- Telnetなどの仮想端末プロトコル
- 簡易ネットワーク管理プロトコル (SNMP)

3.6.1 仮想端末プロトコル

仮想端末プロトコルは Telnetなどのソフトウェア・プログラムであり、Macintosh、PC、または UNIX ワークステーションから管理セッションを確立できます。Telnet は TCP/IP 経由で実行されるため、仮想端末プロトコルを使用してアクセスを確立するには、Man agedt スイッチで少なくとも 1 つの IP アドレスが設定されている必要があります。



端末エミュレーションは、端末をコンソール(シリアル)ポートに直接接続する必要があるという点で、仮想端末プロトコルとは異なります。

Telnet セッションを介して管理対象スイッチにアクセスするには、次の手順に従います。

1. 管理対象スイッチが IP アドレスで設定され、管理対象スイッチが PC から到達可能であることを確認します。
2. PCで Telnet プログラムを起動し、管理対象スイッチに接続します。管

理インターフェイスはRS232コンソール管理とまったく同じです。

3.6.2 SNMPプロトコル

簡易ネットワーク管理プロトコル (SNMP) は、マルチベンダー IP ネットワークの標準管理プロトコルです。SNMPは、プロトコルがメッセージをフォーマットし、レポートデバイスとデータ収集プログラム間で情報を送信できるようにするトランザクションベースのクエリをサポートします。SNMP はユーザー データグラム プロトコル (UDP) の上で実行され、コネクションレス モードのサービスを提供します。

管理アーキテクチャ

すべての管理アプリケーション モジュールは、同じメッセージング アプリケーション プログラミング インターフェイス (MAPI) を使用します。単一の MAPI で管理メソッドを統合することにより、1 つのメソッド (コンソール ポートなど) を使用する構成パラメータは、他の管理方法 (Web ブラウザーの SNMP エージェントなど) によってすぐに表示されます。スイッチの管理アーキテクチャは、IEEE オープン標準に準拠しています。このコンプライアンスにより、管理対象スイッチと互換性があり、同じオープンスタンダードに準拠する他のソリューションと相互運用できます。

4. ウェブベースの管理

このセクションでは、Web ベースの管理の構成と機能について説明します。

4.1 Web ベースの管理について

管理スイッチは、ユーザーが Microsoft Internet Explorer などの標準ブラウザを使用して、ネットワーク上のどこからでも管理できる管理機能を提供します。Web ベースの管理では、Internet Explorer 6.0 がサポートされています。これは、ネットワーク帯域幅の消費を削減し、アクセス速度を向上させ、簡単な表示画面を提示することを目的としたJavaアプレットに基づいています。

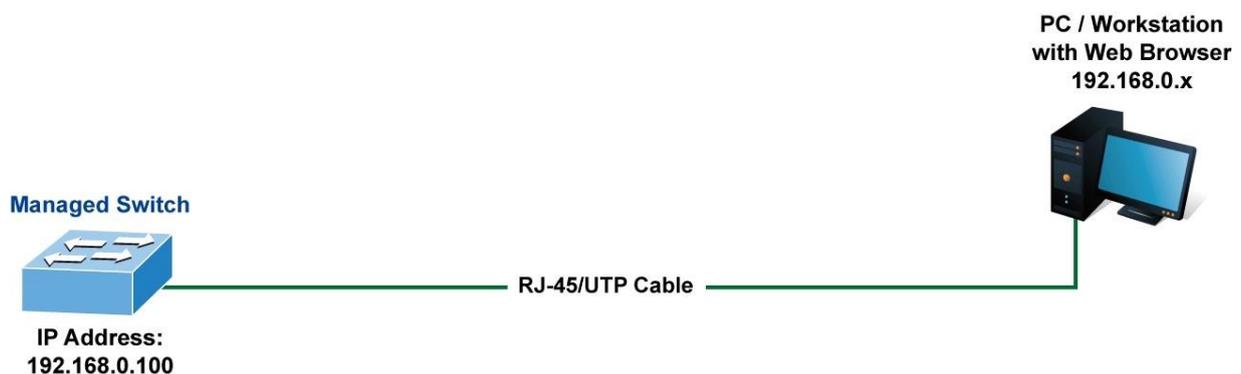


デフォルトでは、IE6.0 以降のバージョンでは、Java アプレットはソケットを開く必要はありません。ユーザーは、Java アプレットがネットワーク・ポートを使用できるように、ブラウザのエッチングを明示的に変更する必要があります。

管理対象スイッチはイーサネット接続を介して設定できるため、マネージャ PC は管理対象スイッチと同じ IP サブネットアドレスに設定する必要があります。

たとえば、管理対象スイッチのデフォルト IP アドレスは **192.168.0.100** で、マネージャ PC は **192.168.0.x** (x は 1 ~ 254 の数値で、100 を除く) で、デフォルトのサブネットマスクは 255.255.255.0 です。

コンソール経由でサブネットマスク 255.255.255.0 を使用して管理対象スイッチのデフォルト IP アドレスを 192.168.1.1 に変更した場合、マネージャ PC を 192.168.1.x (x は 2 ~ 254 の数値) に設定して、Manager PC で相対構成を実行する必要があります。



4.1.1 レクイエメント

- Windows 98/ME、NT4.0、2000/2003/XP/7/8/10、MAC OS9 以降を実行しているワークステーションは、Linux、UNIX、またはその他のプラットフォームを実行し、TCP/IP プロトコルと互換性があります。
- ワークステーションはイーサネット NIC (ネットワークカード)と共にインストールされます。
- **イーサネット ポート接続**
 - ネットワーク ケーブル – RJ45 コネクタで標準ネットワーク (UTP) ケーブルを使用します。
 - 上記のワークステーションは、Web ブラウザおよびJAVA ランタイム環境プラグインと共にインストールされます。



VC-820Mにアクセスするには、インターネット探索6.0以上を使用することをお勧めします

4.1.2 スイッチへのログオン

1. インターネットエクスプローラ 6.0 以上の Web ブラウザを使用します。Web インターフェイスにアクセスするための工場出荷時の既定の IP アドレスを入力します。工場出荷時のデフォルト IP アドレスは次のとおりです

http://192.168.0.100

2. 以下のログイン画面が表示されたら、デフォルトのユーザー名「**admin**」にパスワード"admin"(またはコンソールで変更したユーザー名/パスワード)を入力して、メイン画面にログインしてください。マネージスイッチの。図4-1-1のログイン画面が表示されます。



図 4-1-1: ログイン画面

Default User name: **admin**

Default Password: **admin**

1. ユーザー名とパスワードを入力すると、メイン画面が図 4-1-2と表示されます。



図 4-1-2: Web メイン ページ

2. Web ページの左側にある [切り替えメニュー] を使用すると、スイッチが提供するすべてのコマンドと統計情報にアクセスできます。

これで、Web 管理インターフェイスを使用してスイッチ管理を続行したり、Web インターフェイスによる管理対象スイッチを管理したりできるようになりました。 Web ページの左側にあるスイッチメニューを使用すると、管理対象スイッチが提供するすべてのコマンドと統計情報にアクセスできます。



1. 管理対象スイッチにアクセスするには、インターネット探索 6.0 以降を使用することをお勧めします。

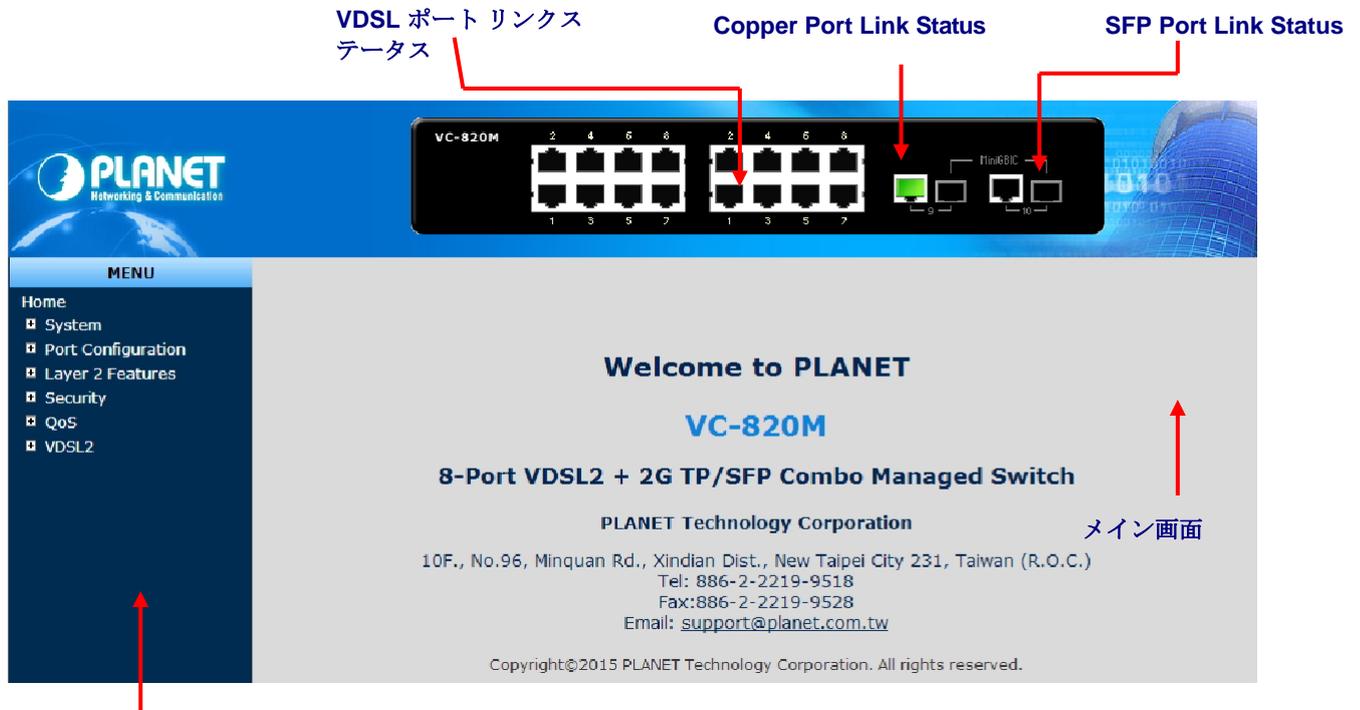
2. 変更されたIP アドレスは、[適用]ボタンをクリックした直後に有効になります。

Web インターフェイスにアクセスするには、新しい IP アドレスを使用する必要があります。

3. セキュリティ上の理由から、この最初のセットアップ後に新しいパスワードを変更して暗記してください。

4.1.3 メイン Web ページ

管理対象スイッチは、Web-ba sed ブラウザ インターフェイスを提供し、Web-ba sed ブラウザ インターフェイスを提供して構成および管理します。このインターフェイスを使用すると、任意の Web ブラウザを使用して管理対象スイッチにアクセスできます。この章では、マネージスイッチの Web ブラウザ インターフェイスを使用して、管理する方法について説明します。



主な機能メニュー

図 4-1-3:メイン ページ

パネル表示

Web エージェントは、管理対象スイッチのポートのイメージを表示します。モードは、リンクアップやリンクダウンなど、ポートに関する異なる情報を表示するように設定できます。ポートのイメージをクリックすると、[ポート統計] ページが開きます。

ポート status は次のように示されています。

状態	無効	ダウン	リンク
RJ45 ポート			
SFP ポート			

メインメニュー

オンボードWebエージェントを使用すると、システム・パラメータの定義、管理対象スイッチとそのすべてのポートの管理と制御、またはネットワーク状態のモニターを行うことができます。管理者は、Web 管理を使用して、主機能にリストされている機能を選択して管理対象スイッチを設定できます。図 4-1-4 の画面が表示されます。



図 4-1-4: VC-820M マネージ スイッチの主な機能メニュー

4.2 システム

[システム] メニュー項目を使用して、管理対象スイッチの基本的な管理詳細を表示および構成します。システムの下では、システム情報を構成および表示するために、次のトピックが提供されます。このセクションには、次の項目があります。

- システム情報 連絡先情報を含む基本的なシステムの説明を提供します。
- IP構成 管理アクセスの IP アドレスを設定します。
- コンソール情報 管理対象スイッチに必要なコンソール設定を表示します。
- SNMP構成 SNMP エージェントと SNMP トラップを設定します。
- Syslogの設定 メッセージのログインを構成し、リモート Syslog サーバーの IP アドレスを割り当てます。
- システムログ システム ログ情報を表示します。
- SMTP設定 SMTP 機能を構成します。
- SNTP設定 SNTP 機能を構成します。
- アラーム設定 RJ45 アラーム ポート機能を設定します。
- スマートファン スマートファン制御機能を構成
- ファームウェアのアップ
グレード TFTP サーバまたは Web ブラウザのファイル転送を介してファームウェアをアップグレードします。
- 構成のバックアップ 管理対象スイッチ構成をリモート・ホストに保存/表示します。
。リモート ホストからスイッチ設定をアップロードします。
- 工場出荷時のデフォルト 管理対象スイッチの設定をリセットします。
- システムの再起動 管理対象スイッチを再起動します。

4.2.1 システム情報

システム情報では、設定には**[基本設定]**と**[その他の設定]**の2つの部分があります。設定の詳細については、次のように説明します。

4.2.1.1 基本的な

[基本システム情報] ページには、現在のデバイス情報に関する情報が表示されます。[基本システム情報] ページでは、スイッチ管理者がモデル名、ファームウェア/ハードウェアのバージョン、MAC アドレスを識別できます。

System Information	
Basic	Misc Config
Model Name	VC-820M
Description	8-Port VDSL2 + 2G TP/SFP Combo Managed Switch
MAC Address	00:30:4F:00:00:06
Firmware Version	2.0b150820
Hardware Version	V2

図 4-2-1-1:基本システム情報 S クリーンショット

このページには、次のフィールドが含まれています。

オブジェクト	説明
モデル名:	管理対象スイッチのシステム名が表示されます。
説明:	マネージ スイッチについて説明します。
MAC アドレス:	製造元によって割り当てられた一意のハードウェア アドレスを表示します (既定)。
ファームウェアのバージョン:	管理対象スイッチのファームウェアバージョンを表示します。
ハードウェアのバージョン:	管理対象スイッチのハードウェアバージョンを表示します。
ファームウェアの構築日:	ファームウェアの日付情報を表示します。

4.2.1.2 その他の構成

管理対象スイッチのシステム情報から[その他の設定]を選択します。

System Information

Basic **Misc Config**

MAC Table Address Entry
Age-Out Time: seconds (6~1572858,must multiple of 6,default is 300s)

Turn On Port Interval: seconds (0~3600 seconds, interval time between turning off and turning on port for flooding CPU port, 0:disable)

Broadcast Storm Filter Mode: OFF ▾

Broadcast Storm Filter Packet select

Broadcast Packets

IP Multicast

Control Packets

Flooded Unicast/Multicast Packets

Collisions Retry Forever : Disable ▾

Hash Algorithm : CRC-Hash ▾

IP/MAC Binding : Disable ▾

802.1x Protocol : Disable ▾

Apply Default Help

図 4-2-1-2:スイッチの設定のスクリーンショット

このページには、次のフィールドが含まれています。

オブジェクト	説明
MAC アドレス経過時間	非アクティブな MAC アドレスがスイッチのアドレス テーブルに残っている秒数を入力します。値は 6 の倍数です。 デフォルトは 300 秒です。
ブロードキャスト ストーム フィルタ	ブロードキャストストーム制御を構成するには、それを有効にし、上限しきい値を設定します

	<p>個々のポートをモードします。しきい値は、ブロードキャスト トラフィックで使用されるポートの合計帯域幅の割合です。ポートのブロードキャスト トラフィックが設定したしきい値を超えると、ブロードキャスト ストーム制御がアクティブになります。</p> <p>有効なしきい値は、 1/2、 1/4、 1/8、 1/16、 および OFFです。</p> <p>既定値は "OFF" です。</p>
ブロードキャスト ストーム フィルタ パケットの選択	<p>ブロードキャスト ストーム フィルタ パケット タイプを選択します。選択したパケットタイプがない場合、meanはパケットをフィルタリングできません。</p> <p>ブロードキャスト ストーム フィルタ モードは OFF と表示されます。選択可能な項目を以下に示します。</p> <ul style="list-style-type: none"> • ブロードキャストパケット • IPマルチキャスト • パケットの制御 • フラッディング ユニキャスト/マルチキャストパケット
衝突再試行は永久に	<p>マネージ スイッチで [衝突再試行の永久] 機能 "無効" または 16、 32、 48 の衝突番号を提供します。この機能が無効になっている場合、パケットが衝突を満たすと、管理対象スイッチはパケットを破棄する前に 6 回再試行します。それ以外の場合、管理対象スイッチはパケットが正常に送信されるまで再試行します。</p> <p>既定値は 16です。</p>
ハッシュアルゴリズム	<p>管理対象スイッチで MAC アドレス テーブルのハッシュ設定を指定します。使用可能なオプションは、CRC ハッシュとダイレクトマップです。</p> <p>既定のモードはCRC ハッシュです。</p>
IP/MAC バインディング	<p>IP MAC バインド機能を有効/無効にします。</p>
802.1x プロトコル	<p>802.1x プロトコルを有効/無効にします。</p>
ボタンの適用	<p>ボタンを押して構成を完了します。</p>

4.2.2 IP構成

管理対象スイッチは、ネットワーク上で識別される IP アドレスを割り当てる必要があるネットワーク デバイスです。

ユーザーは、管理対象スイッチに IP アドレスを割り当てる方法を決定する必要があります。

IP アドレスの概要

IP アドレスとは

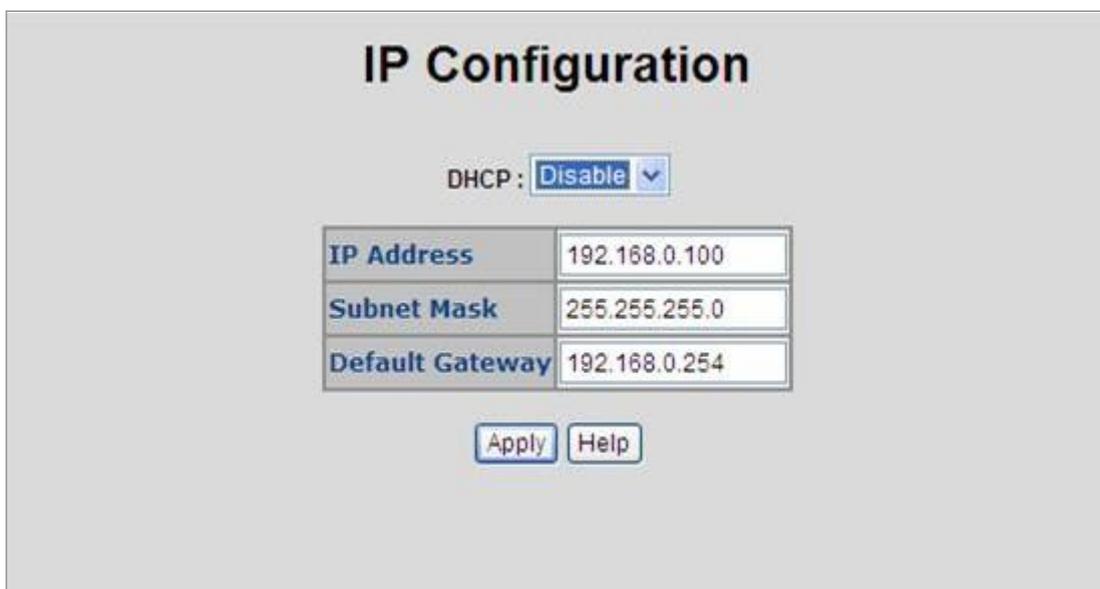
IP ネットワークに参加する各デバイス (コンピュータなど) には、ネットワーク上で一意の"アドレス" が必要です。これは、米国のメールアドレスを持っているのと似ていますので、他の人はあなたにメッセージを送信する知っている方法を持っています。 IP アドレスは 4 バイトの数値で、通常は "ドット表記" で書き込まれ、各バイトの 10 進値は数値として書き込まれ、数値は "ドット" (別名ピリオド) で区切られます。例: 199.25.123.1

この箱の入手方法を教えてください。

最新のコラクタ ネットの IP アドレスは、"ネットワーク管理者" または "Sys" と呼ばれる従業員によって割り当てられます。「管理者」。このユーザーは IP アドレスを割り当て、IP アドレスが重複していないことを確認する必要があります - これが発生した場合、重複する追加のレスを持つ一方または両方のマシンが動作を停止します。もう 1 つの可能性は、DHCP プロトコルを介してネット経由で自動的にアドレスを割り当てることです。DHCP 機能を有効にし、マシンをリセットします。ネットワークがこのサービス用に設定されている場合は、ネットワークに IP アドレスが割り当てられます。約 30 秒以内にアドレスが取得されない場合は、DHCP がいない可能性があります。

■ IP 構成

IP 構成には、IP アドレス、サブネット マスク、およびゲートウェイが含まれます。[構成済み] 列は、IP 構成を表示または変更するために使用されます。デバイスの IP アドレス、サブネット マスク、およびゲートウェイを入力します。図4-2-4の画面が表示されます。



The screenshot shows a web-based configuration page titled "IP Configuration". At the top, there is a "DHCP:" label followed by a dropdown menu currently set to "Disable". Below this are three input fields arranged in a table-like structure:

IP Address	192.168.0.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.254

At the bottom of the form, there are two buttons: "Apply" and "Help".

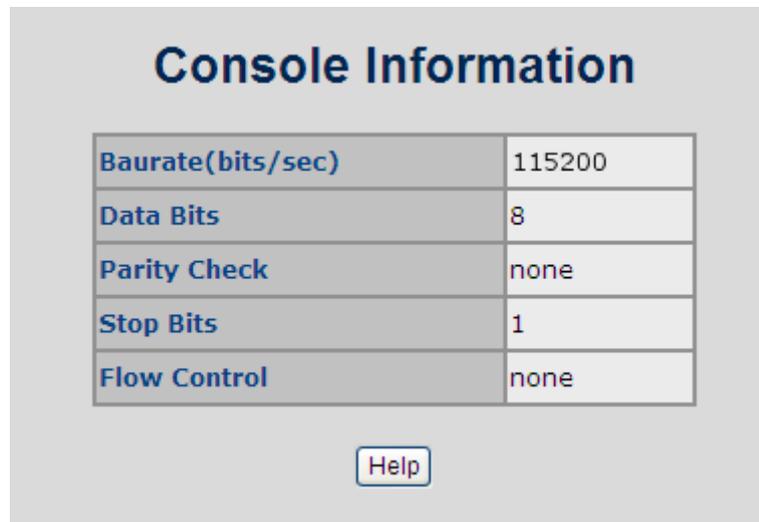
図4-2-2-1: IP 設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
Dhcp	<p>DHCP クライアント機能を有効または無効にします。</p> <p>DHCP 機能を有効にすると、管理対象スイッチにはネットワーク DHCP サーバからの IP アドレスが割り当てられます。既定の IP アドレスは、DHCP サーバで割り当てられた IP アドレスに置き換えられます。ユーザーが [適用] をクリックすると、DHCP クライアントが有効になると、ポップアップ ダイアログが表示され、</p> <p>現在の IP は失われ、ユーザーは DHCP サーバで新しい IP を見つける必要があります。</p>
IP アドレス	<p>ネットワークが使用している IP アドレスを割り当てます。</p> <p>DHCP クライアント機能が有効になっている場合、このスイッチはDHCP クライアントとして設定されます。ネットワーク DHCP サーバはスイッチに IP アドレスを割り当て、この列に表示します。</p> <p>デフォルトの IP は192.168.0.100であるか、DHCP クライアントが無効になっている場合、ユーザーはIP アドレスを手動で割り当てる必要があります。</p>
サブネット マスク	<p>サブネット マスクを IP アドレスに割り当てます。</p> <p>DHCP クライアント機能が無効になっている場合、ユーザーはこの列フィールドにサブネット マスクを割り当てる必要があります。</p>
ゲートウェイ	<p>スイッチのネットワーク ゲートウェイを割り当てます。</p> <p>DHCP クライアント機能が無効になっている場合、ユーザーはこの列フィールドにゲートウェイを割り当てる必要があります。</p> <p>デフォルト ゲートウェイは192.168.0.254です。</p>

4.2.3 コンソール情報

コンソールは、シリアルポートと通信するための標準的な UART インターフェイスです。Windows ハイパーターミナルプログラムを使用して、マネージスイッチをリンクできます。このページには、管理対象スイッチで必要なコンソール設定が表示されます。



Console Information	
Baurate(bits/sec)	115200
Data Bits	8
Parity Check	none
Stop Bits	1
Flow Control	none

Help

図 4-2-3-1:コンソール情報インターフェース

4.2.4 SNMP構成

4.2.4.1 SNMPの概要

簡易ネットワーク管理プロトコル (SNMP)は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。これは、伝送制御プロトコル/インターネットプロトコル (TCP/IP) プロトコルスイートの一部です。SNMP を使用すると、ネットワーク管理者は、network のパフォーマンスを管理し、ネットワークの問題を見つけて解決し、ネットワークの拡張を計画できます。

SNMP で管理されるネットワークは、ネットワーク管理ステーション (NMS)、SNMP エージェント、管理情報ベース (MIB)、およびネットワーク管理プロトコルの 3 つの主要コンポーネントで構成されます。

- **Netwオーク管理ステーション (NMS):**コンソールと呼ばれることがあるこれらのデバイスは、管理を実行します。ネットワーク要素を監視および制御するアプリケーション。物理的には、NMS は通常、高速 CPU、メガピクセル カラー ディスプレイ、実質的なメモリ、および豊富なディスク領域を備えたワークステーションキャリアコンピュータをエンジニアリングしています。各 mアジンド環境には、少なくとも 1 つの NMS が存在する必要があります。
- **エージェント:**エージェントは、ネットワーク要素に存在するソフトウェアモジュールです。管理を収集して保管する。ネットワーク要素が受信したエラー パケットの数などの情報。
- **管理情報ベース (MIB):**MIB は、仮想インフォメーション ストアに存在する管理対象オブジェクトの集合です。関連する管理対象オブジェクトのコレクションは、特定の MIB モジュールで定義されます。
- **ネットワーク管理プロトコル:**管理プロトコルは、エージェントとNMS間で管理情報を伝達するために使用されます。

SNMP 操作

SNMP 自体は単純な要求/応答プロトコルです。NMS は、応答を受信せずに複数の要求を送信できます。

- **Get --** NMS がエージェントからオブジェクトインスタンスを取得できるようにします。
- **Set --** NMS がエージェント内のオブジェクトインスタンスの値を設定できるようにします。
- **トラップ--** 何らかのイベントを NMS に非同期的に通知するためにエージェントによって使用されます。

SNMPv2 トラップ・メッセージは、SNMPv1 トラップ・メッセージを置き換えるように設計されています。

SNMP コミュニティ

SNMP コミュニティは、SNMP を実行しているデバイスおよび管理ステーションが属するグループです。これは、情報の送信先を定義するのに役立ちます。コミュニティ名は、グループを識別するために使用されます。SNMP デバイスまたはエージェントは、複数の SNMP コミュニティに属している場合があります。コミュニティの1つに属さない管理ステーションからの要求に応答しません。通常の SNMP デフォルト コミュニティは、設定時に次のとおりです。

- 書き込み =プライベート
- 読み取り =パブリック

4.2.4.2 システムオプション

このページを使用して、管理ステーションを定義します。 マネージドスイッチの名前、場所、連絡先を定義することもできます。 .

The image shows a web-based configuration interface titled "SNMP Configuration" with a sub-section "System Options". It contains a form with four rows: "Name:" with the value "VC-820M", "Location:" with "No Location", "Contact:" with "No Contact", and "SNMP Status:" with a dropdown menu set to "Enable". Below the form are two buttons: "Apply" and "Help".

図 4-2-4-1: SNMP 設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
システム名	この管理対象ノードに管理的に割り当てられた名前。慣例により、これはノードの完全修飾ドメイン名です。ドメイン名は、アルファベット (A-Za-z)、数字 (0 から 9)、マイナス記号 (-) から描画されるテキスト文字列です。名前の一部としてパーミ文字は使用できません。最初の文字はアルファベットでなければなりません。また、最初または最後の文字はマイナス記号で指定できません。指定できる文字列の長さは 0 ~ 255 です。
システムの場所	このノードの物理的な位置(例えば、電話クローゼット、3階)。

システムコンタクト	この管理対象ノードの連絡担当者のテキスト ID この人への連絡方法に関する情報を提供します。
SNMP ステータス	SNMP モード操作を示します。可能なモードは次のとおりです。 <ul style="list-style-type: none"> 有効: SNMP モード操作を有効にします。 無効: SNMP モード操作を無効にします。

4.2.4.3 コミュニティストリング

コミュニティストリングはパスワードとして機能し、次のいずれかとして入力できます。



図 4-2-4-2: コミュニティストリング インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
コミュニティストリング:	ここでは、新しいコミュニティストリングセットを定義し、不要なコミュニティストリングを削除できます。 <ul style="list-style-type: none"> ■ 文字列: 名前の文字列を入力します。 ■ RO: 読み取り専用です。このコミュニティストリングを伴う要求を有効にして、MIB オブジェクト情報を表示します。 ■ RW: 読み取り/書き込み。このコミュニティストリングを伴う request を有効にします。 MIB オブジェクト情報を表示し、MIB オブジェクトを設定します。
追加 ボタン	ボタンを押して、管理 SNMP コミュニティストリングを管理対象スイッチ。
削除 ボタン	ボタンを押して、管理 SNMP コミュニティストリングを削除します。管理対象スイッチで以前に定義されています。

4.2.4.4 トラップマネージャ

トラップ・マネージャは、スイッチによって生成されたトラップ・メッセージを受信する管理ステーションです。トラップ・マネージャが定義されていない場合、トラップは発行されません。管理ステーションをトラップマネージャとして定義するには、IPアドレスを割り当て、SNMPコミュニティストリングを入力して、SNMPトラップバージョンを選択します。

図 4-2-4-3: トラップマネージャ インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
IP アドレス:	トラップマネージャの IP アドレスを入力します。
コミュニティ:	トラップステーションのコミュニティストリングを入力します。

4.2.4.5 SNMPv3グループ

このページで SNMPv3 グループテーブルを設定します。エントリ インデックス キーは、セキュリティモデルとセキュリティ名です。

図 4-2-4-4: SNMP 設定インターフェイス

このページには次のフィールドが含まれます:

オブジェクト	説明
グループ名:	このエントリが属するグループ名を識別する文字列。 指定できる文字列の長さは 1 ~ 15 です。
V1 V2c Usm	このエントリが属する必要があるセキュリティ モデルを示します。可能なセキュリティ モデルは次のとおりです。 <ul style="list-style-type: none"> • v1 : SNMPv1 用に予約済みです。 • v2c : SNMPv2c 用に予約済みです。 • usm: ユーザーベースのセキュリティ モデル (USM)。
セキュリティ名:	このエントリ should が属するセキュリティ名を識別する文字列。 指定できる文字列の長さは 1 ~ 15 です。
削除	エントリを削除する場合にオンにします。次回の保存時に削除されます。

4.2.4.6 SNMPv3ビュー

このページで SNMPv3 ビュー テーブルを設定します。エントリ インデックス キーは、ビュー名と OID サブツリーです。

図 4-2-4-5: SNMP 設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
ビュー名:	このエントリが属するビュー名を識別する文字列。 指定できる文字列の長さは 1 ~ 15 です。
含まれるもの 除外:	このエントリが属するビュータイプを示します。可能なビュータイプは次のとおりです。 <ul style="list-style-type: none"> • included : このビューサブツリーを含める必要があることを示すオプションのフラグ。

- **ExcludeD:** このビュー サブツリーが次の値であることを示すオプションのフラグ

除外。

サブツリーの表示	名前付きビューに追加するサブツリーのルートを定義する OID。許可された OID の長さは 1 ~ 128 です。許可される文字列の内容は、デジタル番号またはアスタリスク(*)です。
マスクの表示 (16 進数):	ビューマスクは、きめ細かいアクセス制御が必要な場合に必要な設定情報の量を減らすために定義されます(例えば、アクセス制御 オブジェクト インスタンス レベル)

4.2.4.7 SNMPv3アクセス

このページの「SNMPv3 アクセステーブルの設定」を参照してください。エン트리 インデックス キーは、グループ名、セキュリティ モデル、およびセキュリティ レベルです。

図 4-2-4-6: SNMP 設定インターフェイス この

ページには、次のフィールドが含まれています。

オブジェクト	説明
グループ名:	このエントリが属するグループ名を識別する文字列。 指定できる文字列の長さは 1 ~ 15 です。
V1 V2c Usm :	このエントリが属する必要があるセキュリティ モデルを示します。可能なセキュリティ モデルは次のとおりです。 <ul style="list-style-type: none"> • v1 : SNMPv1 用に予約済みです。 • v2c : SNMPv2c 用に予約済みです。 • usm: ユーザーベースのセキュリティ モデル (USM)
SNMP アクセス:	このエントリが属する必要があるセキュリティ モデルを示します。可能なセキュリティ モデルは次のとおりです。 <ul style="list-style-type: none"> • NoAuth: 認証なし、プライバシーなし。 • 認証: 認証とプライバシーなし。

- 認証:認証とプライバシー。

読み取りビュー:

この要求が現行値を要求する MIB オブジェクトを定義する MIB ビューの名前。
指定できる文字列の長さは 1 ~ 16 です。

書き込みビュー:

この要求が新しい値を設定する可能性がある MIB オブジェクトを定義する MIB ビューの名前。
指定できる文字列の長さは 1 ~ 16 です。

通知ビュー:

通知ビューを設定します。

追加

ボタン

ボタンを押して、管理 SNMP コミュニティ スtring を
管理対象スイッチ。

削除

ボタン

選択したエントリを削除する場合にオンにします。次回の保存時に削除されます。

4.2.4.8 SNMP V3 usm-user

このページで SNMPv3 ユーザー・テーブルを構成します。エントリ インデックス キーは、[エンジン ID] と [ユーザー名] です。

図 4-2-4-7: SNMP 設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
SNMPユーザー名:	このエントリが属する必要があるユーザー名を識別する文字列。許可された文字列の長さは 1 ~ 15 です。

このエントリが属する必要がある認証プロトコルを示します。可能な認証プロトコルは次のとおりです。

認証の種類:

- **なし:** 認証プロトコルなし。
- **MD5:** このユーザーが MD5 認証プロトコルを使用していることを示すオプションのフラグ。

エントリが既に存在する場合は、セキュリティ レベルの値を変更できません。ということは

最初に値が正しく設定されていることを確認する必要があります。

認証キー(8~32):

認証パス フレーズを識別する文字列。

MD5 認証プロトコルの場合、許可される文字列の長さは 8 ~ 32 です。

秘密鍵(8~32):

プライバシー パス フレーズを識別する文字列。

指定できる文字列の長さは 8 ~ 32 です。

追加
ボタン

ボタンを押して、管理 SNMP コミュニティ スtring を管理対象スイッチ。

削除
ボタン

選択したエントリを削除する場合にオンにします。次回の保存時に削除されます。

4.2.5 Syslogの設定

[Syslog の設定] ページでは、リモート syslog サーバーまたはその他の管理ステーションに送信されるメッセージのログ記録を構成できます。また、送信されるイベントメッセージを、指定したレベルより下のメッセージのみに制限することもできます。

図 4-2-5-1: Syslog の Web インターフェイスの設定

このページには、次のフィールドが含まれています。

オブジェクト	説明
Syslog サーバー IP	syslog サーバーの IP アドレス。
ログ レベル	<ul style="list-style-type: none"> なし: syslog メッセージを syslog サーバに送信せず、ルートブリッジの Max Age パラメータは、設定方法に関係なく送信されません。 メジャー: メジャー syslog のみを syslog サーバに送信します(リンクアップ/ダウン、システムウォーム/コールドスタートなど) すべて: すべての syslog メッセージを syslog サーバに送信します。

4.2.6 システムログ

[システム ログ] ページでは、syslog 機能を有効または無効にできます。

図 4-2-6-1: システム ログ Web インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
システム ログ モード	システム ログ サービスを有効または無効にする
ログ レベル	<ul style="list-style-type: none"> メジャー: メジャー syslogのみをsyslogサーバに送信します(リンクアップ/ダウン、システムウォーム/コールドスタートなど) すべて: すべての syslog メッセージを syslog サーバに送信します。

4.2.7 SMTP設定

SMTP アラームを使用すると、ユーザーは電子メールアカウントと受信者アカウントを設定できます。イベントが発生した場合、システムは電子メールでエラーメッセージを送信します。

図 4-2-7-1: システム ログのスクリーンショット

このページには、次のフィールドが含まれています。

オブジェクト	説明
SMTP 電子メール アラーム	ユーザーが SMTP アラーム機能を有効または無効にできるようにします。
SMTP サーバーの IP アドレス	SMTP サーバーの IP アドレスを入力する場合
SMTP ポート	SMTP ポート番号を入力する場合、既定値は 25 です。
SMTP 認証	<p>ユーザーが SMTP 認証を有効にできるようにします。SMTP サーバーが拒否するため</p> <p>メールを別のドメインに中継する場合、ユーザーは中継に有効なアカウントを設定する必要があります</p>

メール。メールが同じドメインに送信するだけの場合は、SMTP 認証
は必要ない可能性があります。ネットワーク管理者にご相談ください

(メール・ユーザー)	メールアドレスではなく、メールアカウント名を入力します。
パスワード	メールアカウントのパスワードを入力します。
送信者の電子メール アドレス	管理者からの電子メール アドレスの入力。
メール先	アラームが通知されるメール アドレスをユーザーが入力できるようにします。

最初にアタ

4.2.8 SNTP設定

簡易ネットワーク タイム プロトコル (SNTP) を使用すると、ユーザーは、IP アドレスを介して特定のタイム サーバー (クライアント モード) に時刻同期要求を送信するように管理対象スイッチを構成できます。

The screenshot shows the 'SNTP Setting' web interface. It contains the following fields and controls:

- SNTP**: A dropdown menu currently set to 'Disable'.
- SNTP server IP**: An empty text input field.
- UTC Type**: A dropdown menu currently set to 'Before-UTC'.
- Time Range (0~24)**: A text input field containing the number '0'.
- Time**: An empty text input field.
- At the bottom, there are two buttons: 'Apply' and 'Help'.

図 4-2-8-1: SNTP 設定 Web インターフェイス

このページには、fo llowing フィールドが含まれています。

オブジェクト	説明
Sntp	SNTP 機能を有効または無効にします。
SNTP サーバー IP	ここで SNTP サーバ IP アドレスを割り当てることができます。
UTC タイプ	ユーザーがタイム ゾーンを選択できるようにします。たとえば、お住まいの地域が台北 (UTC+08) の場合は、[UTC から UTC 後]を選択する必要があります。 お住まいの地域がサンフランシスコにある場合 (UTC-08) を選択する必要があります。
時間範囲 (0~24)	ユーザー入力の時間範囲を許可します。たとえば、タイム ゾーンが UTC+08 の場合は 8 を入力し、次の場合は タイム ゾーンは UTC-05、入力 5 です。
時間	NTP サーバーに接続した後の現在の時刻を表示します。

4.2.9 アラーム設定

このページでは、アラーム設定を設定できます。

Alarm Configuration

Configure Alarm Information

Alarm Item	Admin	Security	Title
Alarm1 ▲			
Alarm2 ■	Disable ▼	Critical ▼	
Alarm3 ▼			

Alarm Information

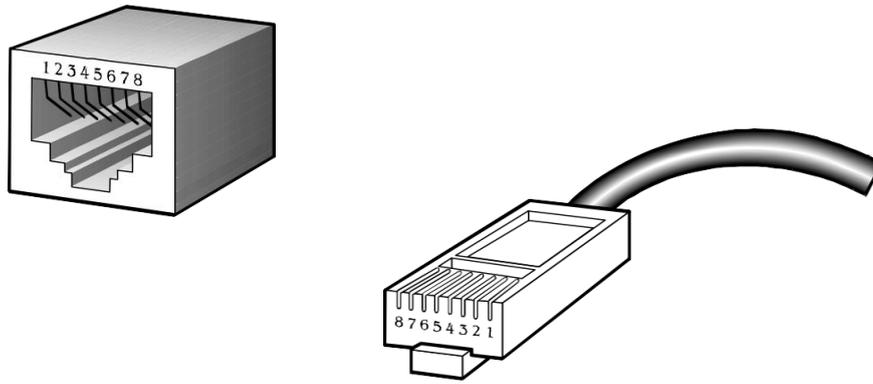
Alarm Item	Admin	Security	Title	Status
Alarm1	Disable	Critical		
Alarm2	Disable	Critical		
Alarm3	Disable	Critical		
Alarm4	Disable	Critical		

図 4-2-9-1:アラーム設定

オブジェクト	説明
アラーム項目	アラーム グループを選択します。
管理者	アラーム グループを有効または無効にします。
セキュリティ	アラーム出力のセキュリティ優先順位を定義できます。その機能はメモ用です だけ。
タイトル	アラーム出力の説明を定義できます。この機能はメモ専用です。
ステータス	アラーム グループの状態を表示する

アラーム グループのステータスとアラーム RJ45 ピン定義:

RJ45ピン	グループ	短絡(10秒以上)	オープンサーキット
1, 2	アラーム1	SYS LED: 赤 アラーム 1 ステータス: 発生	SYS LED: 緑のアラーム 1 ステータス: クリア
3, 4	アラーム2	SYS LED: 赤 アラーム 2 ステータス: 発生	SYS LED: 緑のアラーム 2 ステータス: クリア
5, 6	アラーム3	SYS LED: 赤 アラーム 3 ステータス: 発生	SYS LED: 緑のアラーム 3 ステータス: クリア
7, 8	アラーム4	SYS LED: 赤 アラーム 4 ステータス: 発生	SYS LED: 緑のアラーム 4 ステータス: クリア



4.2.10 スマートファン

このページでは、ユーザーがスマートファン構成を構成できます。

Smart Fan

Enable Disable

Low Speed: 0 °C-- 50 °C
 Medium Speed: 50 °C-- 70 °C
 High Speed: 70 °C-- °C

Set

Temperature and Fan Information

Temperature Local	44 °C
Temperature Remote 1	53 °C
Temperature Remote 2	43 °C
Fan1 Status	Medium Speed(4000 RPM)
Fan2 Status	Medium Speed(4000 RPM)
Fan3 Status	Medium Speed(4000 RPM)

図 4-2-10-1:スマートファンの構成

このページには、次のフィールドが含まれています。

オブジェクト	説明
有効	スマートファン機能を有効にします。
無効	スマートファン機能を無効にします。
低速	低速ファンで温度ゾーンを定義できます。
中速	中速ファンで温度ゾーンを定義できます。
高速	高速ファンで温度ゾーンを定義できます。



温度ゾーンをデフォルト値なしで変更すると、特に過酷な環境でスイッチが破損する可能性があります。

4.2.11 ファームウェアのアップグレード

これは、ユーザーが簡易ファイル転送プロトコル(TFTP)を介してスイッチファームウェアを更新することを可能にする機能を提供します

サーバー。更新する前に、TFTP サーバの準備が整い、ファームウェア イメージが TFTP サーバ上にあることを確認します。

4.2.11.1 TFTP ファームウェアのアップグレード

[ファームウェア のアップグレード] ページには、ユーザがネットワーク内のTFTP サーバから管理対象スイッチファームウェアを更新できるようにする機能が用意されています。更新する前に、TFTP サーバの準備が整い、ファームウェア イメージが TFTP サーバ上に配置されていることを確認してください。図 4-2-11-1のスクリーンが表示されます。

このメニューを使用して、指定したTFTP サーバから管理対象スイッチにファイルをダウンロードします。

図 4-2-11-1:ファームウェア アップグレードインターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
TFTP サーバの IP アドレス:	TFTP サーバの IP を入力します。
ファームウェア ファイル名:	更新するファームウェア イメージ ファイルの名前を入力します。

4.2.11.2 HTTP ファームウェアのアップグレード

[HTTPファームウェアのアップグレード] ページには、ローカル ファイル ブラウザからデバイスにシステム イメージ ファイルをダウンロードするためのフィールドが含まれています。図 4-2-11-2の Web ファームウェア アップグレード画面が表示されます。



図 4-2-11-2: HTTP ファームウェア アップグレード インターフェイス

ファームウェアのアップグレード画面を開くには、次の手順に従います。

1. [システム]->[Web ファームウェアのアップグレード]をクリックします。
2. ファームウェアのアップグレード画面は、図4-2-11-3のように表示されます。
3. メインページの「参照」ボタンをクリックすると、システムがファイル選択メニューをポップアップ表示して、firmwareを選択します。

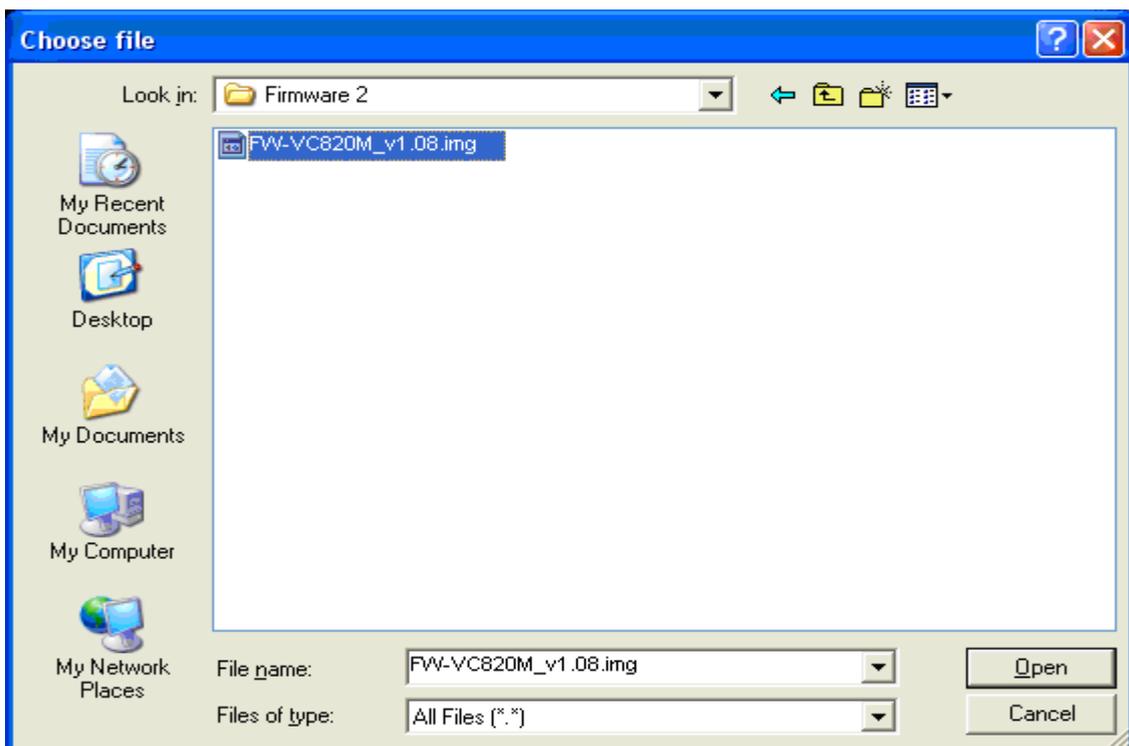


図 4-2-11-3: HTTP ファームウェア アップグレードの選択ウィンドウ

4. ファームウェアを選択し、[送信] をクリックすると、ソフトウェアアップロードの進行状況がアップロードステータスと表示されます。



ファームウェアのアップグレードには数分かかります。しばらく待ってから、Web ページを手動で更新してください。

4.2.12 構成のバックアップ

4.2.12.1 TFTP 復元設定

TFTP サーバから以前のバックアップ設定を復元して、設定をリカバリできます。その前に、まずTFTP サーバ上のイメージファイルを見つける必要があり、管理対象スイッチはフラッシュ イメージをダウンロードし直します。

図4-2-12-1: TFTP Configuration 復元インターフェイ

ス	何をする	おと
	TFTP サーバの IP アドレス	TFTP サーバ IP を入力します。
	復元ファイル名:	復元する正しいファイル名を入力してください。

4.2.12.2 HTTP 構成ファイルの復元

Microsoftインターネット探索や Mozilla Firefox などのインターネットブラウザを使用して、現在のワークステーションから以前のバックアップ設定を復元して設定を復元することもできます。その前に、まずローカル管理ステーションでイメージファイルを見つける必要があり、管理対象スイッチはフラッシュ イメージをダウンロードし直します。

図4-2-12-2: HTTP設定復元インターフェイス

4.2.12.3 TFTP バックアップ設定

後で設定を回復するために、フラッシュ ROM から TFTP サーバ r に現在の設定をバックアップできます。構成をバックアップすることで、設定の構成に時間を無駄にしないようにするのに役立ちます。

図4-2-12-3:TFTP 設定バックアップ インターフェイス

このページには、次のフィールドがあります。

何をする	説明
TFTP サーバの IP アドレス :	TFTP サーバ IP を入力します。
バックアップ ファイル名:	TFTP サーバでバックアップするファイル名を入力します。

4.2.12.4 HTTP 構成ファイルのバックアップ

この機能により、管理対象スイッチの現在の設定をローカル管理ステーションにバックアップできます。図4-2-12-4および図4-2-12-5の画面が表示されます。

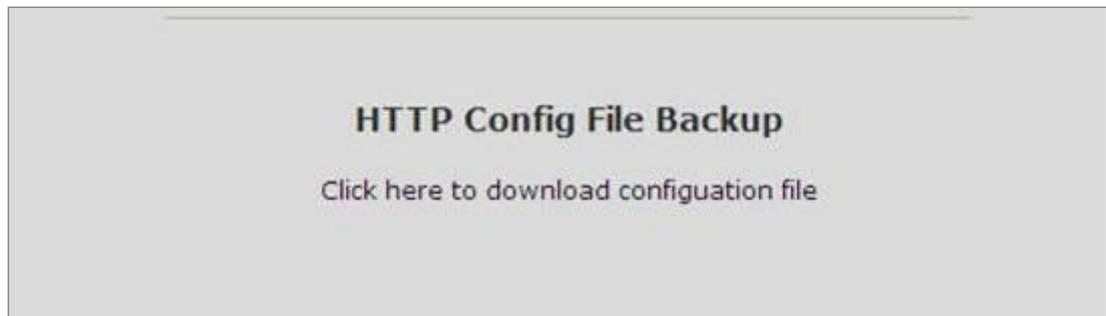


図 4-2-12-4: HTTP 設定ファイルのバックアップ インターフェイス

カーソルを [構成ファイルをダウンロードするにはここをクリックしてください] に移動し、クリックします。バックアップ構成ファイルは、既定で "config.tar" ファイルとしてパッケージ化されます。

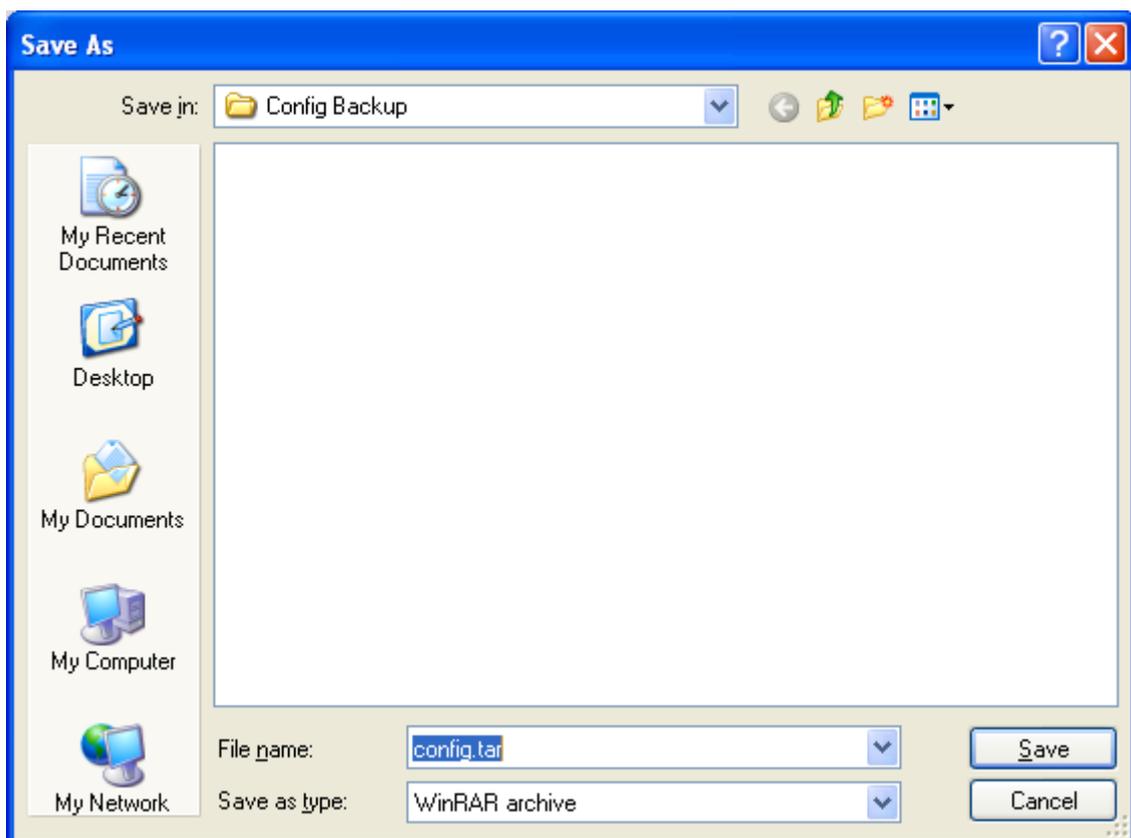


図 4-2-12-5: HTTP 構成のバックアップ ウィンドウ

4.2.13 工場出荷時のデフォルト

スイッチを既定の構成にリセットします。[reset](#) すべての構成を既定値にリセットする場合にクリックします。



図 4-2-13-1:工場出荷時のデフォルト インターフェイス

4.2.14 システムの再起動

ソフトウェアでスイッチを再起動する [リセット](#)。 [クリック](#) をクリックしてシステムを再起動します。



図 4-2-14-1:システムリブートインタフェース

この項目は、管理対象スイッチの**ギガビット・ポート**専用です。

二重：

[ネゴシエーション] 列が [強制] に設定されている場合に選択できます。[ネゴシエーション] 列が [自動] に設定されている場合、この列は読み取り専用です。

フロー制御：

受信側ノードが送信側ノードにフィードバックを送信するかどうかは、この item によって決まります。有効にすると、デバイスが別のデバイスの入力データレートを超えると、受信側デバイスは、指定された期間、送信側の送信を停止するPAUSEフレームを送信します。無効にすると、

処理する量が多すぎると、受信側のデバイスはパケットをドロップします。

セキュリティ：

セキュリティ モードのポートは、アドレス学習の許可なしに "ロック" されます。アドレス テーブルに既に存在する SMAC を持つ着信パケットのみを正常に転送できます。

ユーザはポートが新しい MAC アドレスを学習しないように無効にしてから、スタティック MAC アドレス画面を使用して、セキュア ポートを使用できる MAC アドレスのリストを定義できます。設定を入力し、[適用] ボタンをクリックして変更します。

ページ。

Bsf：

ユーザは、ポートによってポートブロードキャストストームフィルタリングオプションを無効または有効にできます。

フィルタ モードとフィルタ パケットタイプは、[スイッチ設定] > [\[その他の設定\]](#) ページで選択できます。

ジャンボフレーム：

ユーザはポートごとにポートジャンボフレームオプションを無効/有効にすることができます。ポートジャンボフレームの場合

が有効になっている場合は、ポートフォワードジャンボ フレーム パケット。



Note

管理対象スイッチは、最大**9K** バイトのジャンボ フレーム転送をサポートします。

4.3.2 レート制御

レート制御により、ユーザは特定のポートに対してレート制限速度を実行できます。

Port	Ingress	Egress
Port9 Port10	0 *128 (kbps)	0 *128 (kbps)

Apply

Port Ingress Egress

図 4-3-2: レート制御インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
レート制御:(単位:128KBbps)	<p>ポート 9 ~ ポート 10 は、ポートによる入り口と出力レート制御をサポートします。</p> <p>たとえば、ポート 1 が 10 Mbps で、ユーザは有効出力レートを 1 Mbps に設定し、入力レートを 500 Kbps に設定できます。</p>
ポート	<p>速度を制限するポートをユーザーが選択できるようにします。</p>
インGRESS	<p>ポートの有効入力レートを入力します。</p> <p>有効な範囲は0 ~ 8000です。単位は128K。0:レート制御を無効にします。</p> <p>1 ~ 8000: 有効なレート値</p>
出口	<p>ポートの有効出力レートを入力します。</p> <p>有効な範囲は0 ~ 8000です。単位は128K。0:レート制御を無効にします。</p> <p>1 ~8000: 有効なレート値。</p>

4.3.3 ポートの状態

このページには、現在のポート構成と動作状態が表示されます。概要テーブルを使用すると、ポートリンクアップ/リンクダウンステータス、ネゴシエーション、リンク Speed、レート制御、デュプレックスモード、フロー制御など、各ポートのステータスを一目でわかりやすく確認できます。

Port Status											
The following information provides a view of the current status of the unit.											
Port	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit:128Kbps)		Security	BSF	Jumbo Frame
							Ingress	Egress			
Port9	On	Down	---	---	---	---	Off	Off	Off	On	On
Port10	On	Up	Auto	1000	Full	On	Off	Off	Off	On	On

図 4-3-3:ポート ステータス インターフェイス

4.3.4 ポート統計

The following chart provides the current statistic information which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

Port Statistics									
The following information provides a view of the current status of the unit.									
Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
Port9	On	Down	0	0	0	0	0	0	0
Port10	On	Up	9824	0	8690	0	0	0	3

図 4-3-4:ポート統計インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
ポート:	ポート番号。
状態:	ポートコントロールによって設定されます。状態が無効になっている場合、ポートは送信しないか、任意のパケットを受信します。
リンク:	リンクの状態— 'アップ' または 'ダウン'。
Tx グッド パケット:	このポートを介して良好なパケットを送信するカウント。
Tx 不良パケット:	不良パケットを送信する数(小さいサイズ(64オクテット未満)を含む、このポートを介して、CRC 位置合わせエラー、フラグメント、ジャバ— パケット)。
Rx 良いパケット:	このポートを介して正常なパケットを受信する数。
Rx 不良パケット:	良好なパケットを受信する数(小さいサイズ(64オクテット未満)を含む、このポートを介して、大きすぎる、CRCエラー、フラグメントとジャバ—)。
Tx 中止パケット:	送信中に中止されたパケット。
パケットの衝突:	衝突パケットの数。
パケットドロップ:	ドロップされたパケットの数。

4.3.5 ポートスニファア

ポートスニファ(ミラーリング)は、スイッチドネットワークのトラフィックを監視する方法です。ポートを通過するトラフィックは、1つの特定のポートで監視できます。つまり、監視対象のポートに出入りするトラフィックは、スニファポートに複製されます。

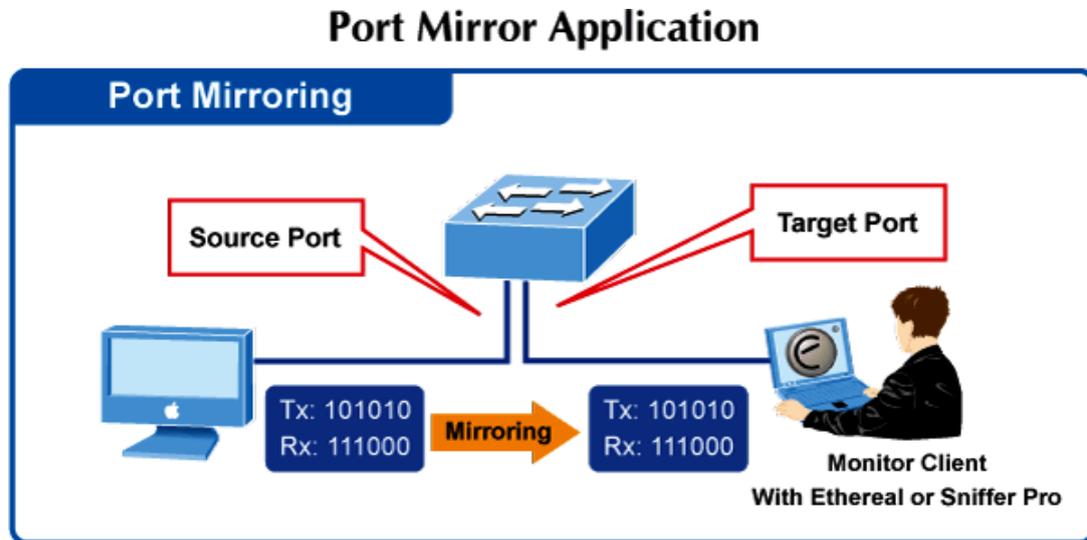


図 4-3-5:ポート ミラー アプリケーション

Configuring the port mirroring by assigning a source port from which to copy all packets and a destination port where those packets will be sent.

Port Sniffer

Sniffer Type: BOTH <input type="button" value="v"/>	
Analysis Port: Port1 <input type="button" value="v"/>	
Port	Monitor
Port1	<input type="radio"/>
Port2	<input checked="" type="radio"/>
Port3	<input type="radio"/>
Port4	<input type="radio"/>
Port5	<input type="radio"/>
Port6	<input type="radio"/>
Port7	<input type="radio"/>
Port8	<input type="radio"/>
Port9	<input type="radio"/>
Port10	<input type="radio"/>
<input type="button" value="Apply"/> <input type="button" value="Default"/> <input type="button" value="Help"/>	

図 4-3-6:ポート スニファ インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
スニファータイプ:	<p>スニファ モードを選択します。</p> <ul style="list-style-type: none"> • 無効 • Rx • Tt • 両方とも
分析 (監視) ポート:	<p>これは、分析ポートを使用して、必要な別のポートのトラフィックを確認できることを意味します。</p> <p>モニター。分析ポートは、LAN アナライザまたはnetxrayに接続できます。</p>
監視対象ポート:	<p>監視するポート。モニタ ポート トラフィックは分析ポートにコピーされます。</p> <p>スイッチ内のモニタ ポートを 1 つ選択できます。ユーザーは、監視するポートを 1 つのスニファの種類でのみ選択できます。</p>



- 1 ミラー モードが**RX** または **TX**に設定され、分析ポートが選択されている場合、分析ポートとの間のパケットは送信されません。分析ポートは、**モニタ対象ポート**からコピーされたパケットのみを受け入れます。
- 2 この機能を無効にする場合は、モニタ ポートを[なし] に選択する必要があります。

4.3.6 保護ポート

保護されたポートグループは2 つあります。異なるグループ内のポートは通信できません。同じグループ内では、保護されたポートは相互に通信できませんが、保護されていないポートと通信できます。保護されていないポートは、保護ポートを含む任意のポートと通信できます。

Portected Port Setting

Port ID	Protected	Group1	Group2
Port1	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port2	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port3	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port4	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port5	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port6	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port7	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port8	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port9	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port10	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>

図 4-3-7:保護されたポート設定 Web インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
ポート ID	管理対象スイッチ インターフェイスを識別します。
保護	選択したポートで Protected 機能を有効にします。 チェック ボックスが  として表示されない場合、このポートは保護されていないポートであり、保護されたポートを含む任意のポートと通信できます。
グループ1	保護されたポートをグループ 1 メンバーに設定します。
グループ2	保護ポートをグループ 2 メンバーに設定します。



通常、アップリンク ポートまたはポートがコア スイッチまたはルータに接続されている
保護されていないポート:

4.4 VLAN設定

4.4.1 VLANの概要

仮想ローカルエリア ネットワーク (VLAN)は、物理レイアウトではなく論理スキームに従って構成されたネットワークトポロジです。VLAN を使用すると、LAN セグメントの任意のコレクションを、単一の LAN として表示される自律ユーザ グループに結合できます。また、VLAN は、パケットが VLAN 内の **between** ポートのみを転送するように、ネットワークを異なるブロードキャスト ドメインに論理的にセグメント化します。通常、VLANは特定のサブネットに対応しますが、必ずしも対応しているわけではありません。

VLAN は、帯域幅を節約することでパフォーマンスを向上させ、トラフィックを特定のドメインに制限することでセキュリティを向上させることができます。

VLAN は、物理的な場所ではなくロジック別にグループ化されたエンド ノードのコレクションです。ネットワーク上の物理的な場所に関係なく、同じ VLAN に割り当てられた相互に頻繁に通信するエンド ノード。ブロードキャスト パケットはブロードキャストが開始された VLAN のメンバーにのみ転送されるため、論理的には、VLAN をブロードキャスト ドメインに同一視できます。



1. エンド ノードを一意に識別し、これらのノードに VLAN メンバーシップを割り当てるために使用される基準に関係なく、パケットは VLAN 間のルーティング機能を実行するネットワーク デバイスなしでは VLAN を通過できません。
2. 管理対象スイッチはIEEE 802.1Q VLAN をサポートします。ポートアンタグ付け機能を使用すると、パケットヘッダーから 802.1 タグを削除し、タグを認識し。

管理対象スイッチは、Web 管理ページで**IEEE 802.1Q(タグ付きベース)**および**ポートベースの VLAN** 設定をサポートします。デフォルト設定では、VLAN サポートは「**802.1Q**」です。

■ ポートベースのVLAN

ポート ベースの VLAN 制限トラフィックは、スイッチ ポートとの間で流れ込みます。したがって、ポートに接続されているすべてのデバイスは、スイッチに直接接続されている単一のコンピュータがあるかどうか、または部門全体に接続されている場合でも、ポートが属する VLAN のメンバーです。

ポート ベースed VLAN では、NIC はパケット ヘッダー内の 802.1Q タグを識別できる必要はありません。NIC は通常のイーサネット パケットを送受信します。パケットの宛先が同じセグメントにある場合、通信は通常のイーサネット プロトコルを使用して行われます。thは常にそうですが、パケットの宛先が別のスイッチ ポートにある場合、VLAN に関する考慮事項は、パケットがスイッチによってドロップされるか、配信されるかを決定するために行われます。

■ IEEE 802.1Q VLAN

IEEE 802.1Q(タグ付き)VLAN は Switch. 802.1Q VLAN に実装されており、ネットワーク全体にまたがることできません(ネットワーク上のすべてのスイッチが IEEE 802.1Q 準拠であると仮定します)。

VLAN を使用すると、ブロードキャスト ドメインのサイズを小さくするためにネットワークをセグメント化できます。

VLAN に入るすべてのパケットは、その VLAN のメンバーであるステーション(IEEE 802.1Q 対応スイッチ経由)にのみ転送され、これには不明な送信元からのブロードキャスト、マルチキャスト、およびユニキャスト パケットが含まれます。

VLAN は、ネットワークにレベルのセキュリティを提供することもできます。IEEE 802.1Q VLAN は、VLAN のメンバーであるステーション間でのみパケットを配信します。任意のポートをタグギングまたはタグ解除として設定できます。IEEE 802.1Q VLAN のタグなし機能により、VLAN はパケットヘッダー内の VLAN タグを認識しないレガシースイッチを使用できます。タグ付け機能を使用すると、VLAN は単一の物理方式を介して複数の 802.1Q 準拠スイッチにまたがるのが可能になり、スパンニングツリーをすべてのポートでイネーブルにして正常に動作させることができます。

任意のポートをタグ付けまたはタグ解除として設定できます。IEEE 802.1Q VLAN のタグなし機能により、VLAN は packet ヘッダー内の VLAN タグを認識しないレガシースイッチを使用できます。タグ付け機能を使用すると、VLAN は単一の物理接続を介して複数の 802.1Q 準拠スイッチにまたがるのが可能になり、スパンニングツリーをすべてのポートでイネーブルにして正常に動作させることができます。

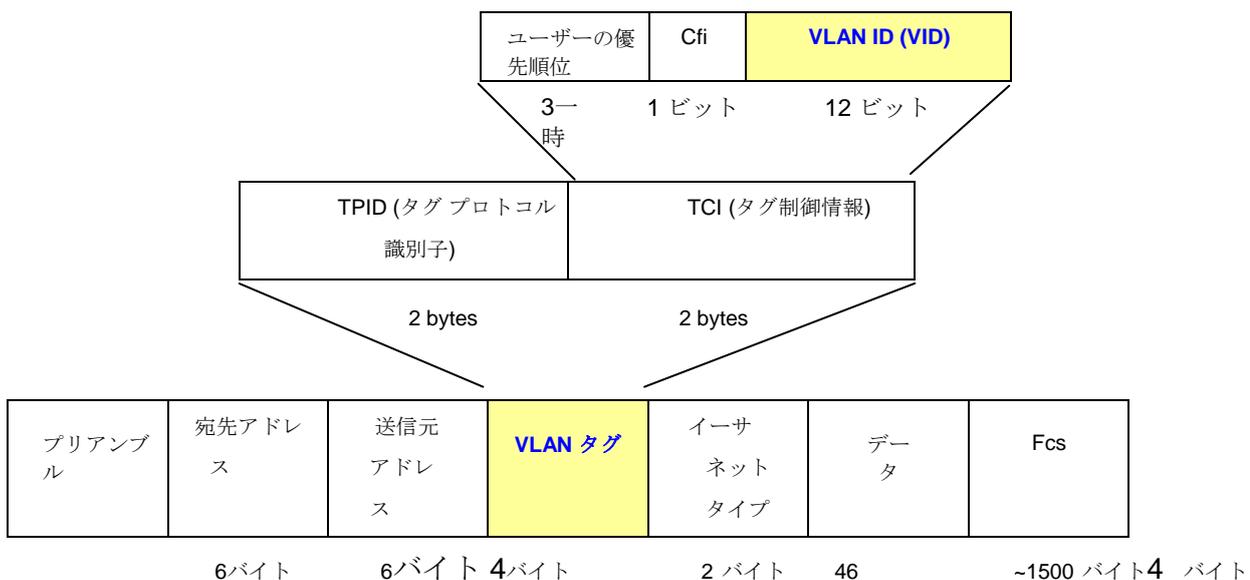
関連する用語:

- タグ付け - 802.1Q VLAN 情報をパケットのヘッダーに入れる動作。
- タグ付け解除 - パケットヘッダーから 802.1Q VLAN 情報を取り除く行為。

■ 802.1Q VLAN タグ

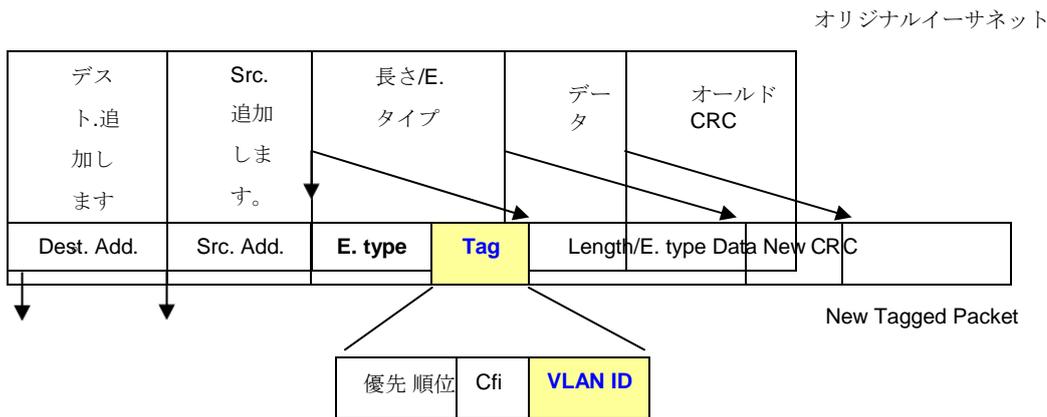
次の図は、802.1Q VLAN タグを示しています。ソースMAC広告ドレスの後に挿入された4つの追加のオクテットがあります。これらの存在は、[エーテルタイプ]フィールドの値 0x8100 で示されます。パケットのエーテルタイプフィールドが 0x8100 に等しい場合、パケットは IEEE 802.1Q/802.1p タグを伝送します。このタグは、次の 2 つのオクテットに含まれ、3 ビットのユーザプライオリティ、1 ビットのユーザプライオリティ識別子(CFI - イーサネットバックボーンを介して伝送できるようにトークンリングパケットをカプセル化するために使用)、および 12 ビットの VLAN ID(VID)で構成されます。ユーザー優先順位の 3 ビットは 802.1p によって使用されます。VID は VLAN アイデンティファイアで、802.1Q 規格で使用されています。VID の長さは 12 ビットであるため、4094 個の一意の VLAN を識別できます。タグはパケットヘッダーに挿入され、パケット全体が 4 オクテット長くなります。パケットに最初に含まれていたすべての情報は保持されます。

802.1Q タグ



エーテルタイプと VLAN ID は、MAC 送信元アドレスの後、元のエーテルタイプ/長さまたは論理リンクコントロールの前に挿入されます。パケットは元のパケットよりも少し長くなったため、巡回冗長検査 (CRC) を再計算する必要があります。

IEEE802.1Q タグの追加



■ Port VLAN ID

タグ付けされたパケット(802.1Q VID 情報を伝送している)は、VLAN 情報をそのまま使用して、1つの802.1Q 準拠ネットワーク デバイスから別のネットワーク デバイスに送信できます。これにより、802.1Q VLAN はネットワーク デバイス(および実際にはネットワーク全体)にまたがる可能性があります(すべてのネットワーク デバイスが802.1Q 準拠の場合)。

スイッチ上のすべての物理ポートには PVID があります。802.1Q ポートには、スイッチ内で使用するために PVID も割り当てられます。スイッチに VLAN が定義されていない場合、すべてのポートは PVID が 1 のデフォルト VLAN に割り当てられます。タグなしパケットには、受信したポートの PVID が割り当てられます。転送の決定は、VLAN に関する限り、この PVID に基づいています。タグ付きパケットは、タグに含まれる VID に従って転送されます。タグ付きパケットにも PVID が割り当てられますが、PVID はパケット転送の決定には使用されません。

タグ対応スイッチは、スイッチ内の PVID をネットワーク上の VID に関連付けるテーブルを保持する必要があります。スイッチは、パケットを送信するポートの VID に送信されるパケットの VID を比較します。2つの VID が異なる場合、スイッチはパケットを drop します。タグなしパケット用の PVID とタグ付きパケットの VID が存在するため、タグ対応ネットワーク デバイスとタグ非対応ネットワーク デバイスを同じネットワーク上に共存させることができます。

スイッチ ポートは PVID を 1 つだけ持つことができますが、switch が VLAN テーブルにメモリを持っているのと同じ数の VID を持つことができます。

ネットワーク上の一部のデバイスはタグに認識されない可能性があるため、パケットが送信される前にタグ対応デバイスの各ポートで決定を下す必要があります。トランスミット ポートがタグ非対応デバイスに接続されている場合、パケットはタグ付け解除する必要があります。送信ポートがタグ対応デバイスに接続されている場合は、パケットにタグを付ける必要があります。

■ デフォルトVLAN

スイッチは最初に、1つの VLAN VID = 1 を設定します。工場出荷時のデフォルト設定では、スイッチのすべてのポートが「デフォルト」に割り当てられます。新しい VLAN がポートベース モードで設定されると、それぞれのメンバー ポートは「デフォルト」から削除されます。

■ VLAN およびリンク アグリゲーショングループ

VLAN segmentati をポート リンク アグリゲーション グループと組み合わせて使用するには、最初にポート リンク アグリゲーション グループを設定してから、VLAN 設定を設定します。ポート リンク集約のグループ化を変更する場合 VLAN が既に設定されている場合は、ポート リンク アグリゲーション グループの設定を変更した後に VLAN 設定を再設定する必要はありません。VLAN 設定は、ポート リンク アグリゲーション グループ設定の変更に伴って自動的に変更されます。

4.4.2 スタティック VLAN設定

仮想 LAN (VLAN) は、ブロードキャスト ドメインを制限する論理ネットワーク グループです。これにより、VLAN のメンバーのみが同じ VLAN メンバーからトラフィックを受信できるように、ネットワーク トラフィックを分離できます。基本的に、スイッチから VLAN を作成することは、ネットワークデバイスのグループを別のレイヤ 2スイッチに再接続することと論理的に同じです。ただし、すべてのネットワークデバイスは、物理的に同じスイッチに接続されます。

管理対象スイッチは、Web 管理ページでポートベースおよび 802.1Q(タグ付きベース)VLANをサポートします。デフォルトの設定では、VLAN サポートは "802.1Q" です。

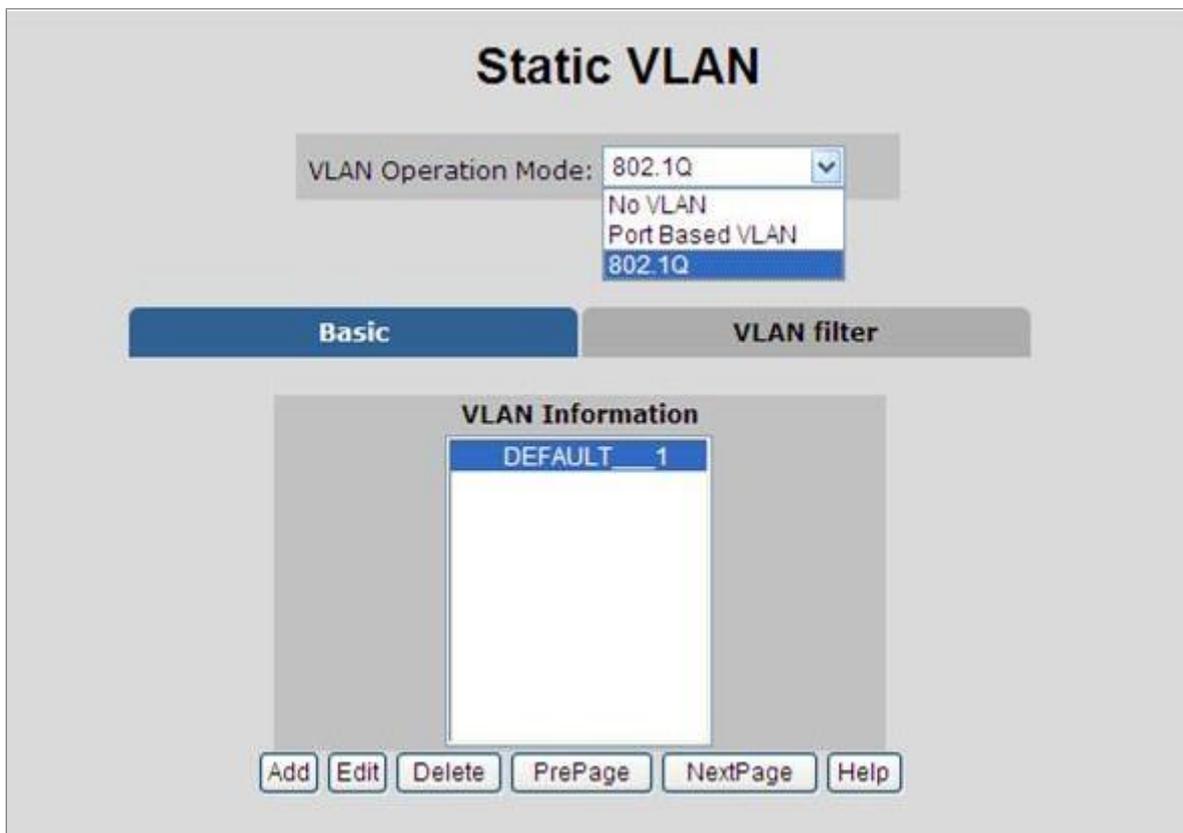


図 4-4-2-1:スタティック VLAN インターフェイス



Note

- 1 エンド ノードを一意に識別し、これらのノードに VLAN メンバーシップを割り当てるために使用される基準に関係なく、パケットはVLAN 間のルーティング機能を実行するネットワークデバイスなしでは VLAN を通過できません。
- 2 スイッチはポート ベース VLAN およびIEEE 802.1Q VLANをサポートします。ポートタグ解除機能を使用すると、パケット ヘッダーから 802.1 タグを削除して、タグを認識しないデバイスとの互換性を維持できます。

4.4.3 ポートベースのVLAN

パケットは、同じ VLAN グループのメンバー間でのみ送信できます。選択されていないすべてのポートは、別の単一の VLAN に属するものとして扱われます。ポートベースの VLAN が有効になっている場合、VLAN タグ付けは無視されます。

エンドステーションが異なる VLAN にパケットを送信するには、エンドステーション自体が VLAN タグを使用して送信するパケットにタグを付けることができるか、デフォルト PVID だけでなく、プロトコルなどのパケットに関するその他の情報に基づいて、異なる VLAN ID でパケットを分類およびタグ付けできる VLAN 対応ブリッジに接続できる必要があります。

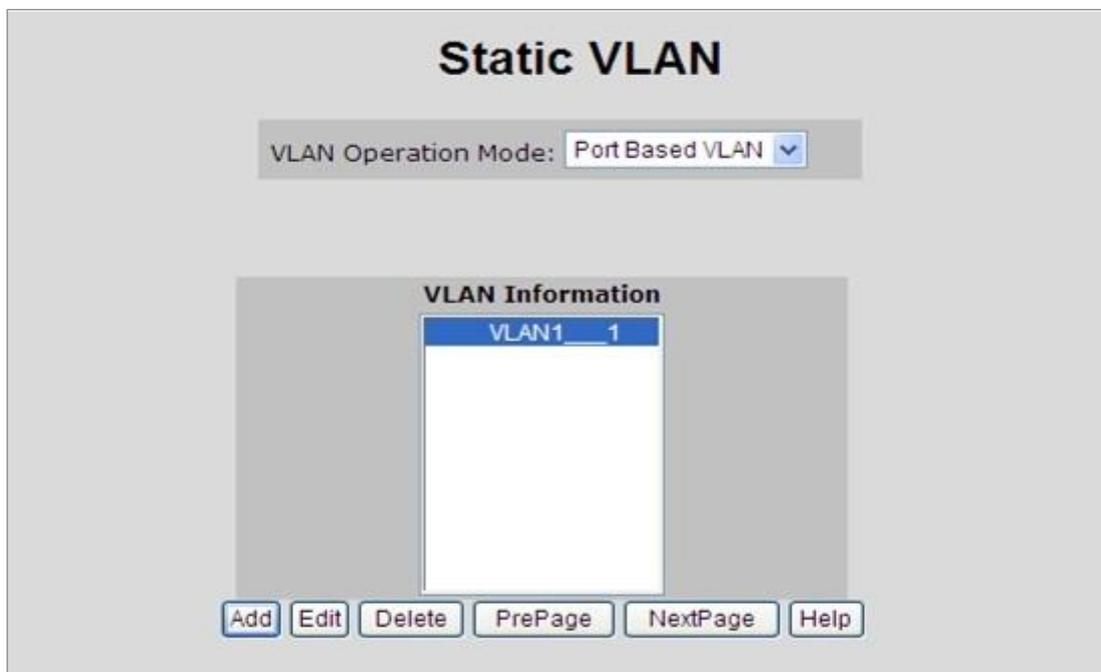


図 4-4-3-1:ポートベースの VLAN インターフェイス

■ VLAN を作成し、それにメンバー ポートを追加する

1. ハイパーリンク "VLAN" "静的 VLAN" をクリックして、VLAN コンフィギュレーションインターフェイスに入ります。
2. ポートベースの VLAN 機能を有効にするには、VLAN 操作モードで [ポートベース VLAN] を選択します。
3. Click "Add" to create a new VLAN group. Then the following Figure 4-4-3 appears.
4. 新しい VLAN の名前とグループ ID を入力します。
5. [使用可能なポート] ボックスから、管理対象スイッチに追加するポートを選択し、[追加] をクリックします。
6. [適用] をクリックします。
7. VLAN グループが表示されます。
8. ポートベース VLAN グループリストを 1 ページに分けてください。「次のページ」をクリックすると、他の VLAN グループが別のページに表示されます。
9. Use the [Delete] button to delete the unwanted port-based VLAN groups
10. Use the [Edit] button to modify the existing port-based VLAN groups.

VLAN にポートを追加することで、1 つのポートベース VLAN グループが完全に作成されました。

Static VLAN

VLAN Operation Mode: Port Based VLAN ▼

VLAN Name:	<input type="text" value="VLAN-1"/>	
Group ID:	<input type="text" value="1"/>	
<div style="border: 1px solid gray; padding: 5px;"> Port5 Port6 Port7 Port8 Port9 Port10 </div>	<input type="button" value="Add >>"/> <input type="button" value="<< Remove"/>	<div style="border: 1px solid gray; padding: 5px;"> Port1 Port2 Port3 Port4 </div>
<input type="checkbox"/> CPU Port		
<input type="button" value="Apply"/> <input type="button" value="Help"/>		

図 4-4-3-2:スタティック VLAN インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
VLAN 名	このオプションフィールドを使用して、VLAN の名前を指定します。ブランクを含め、最大 16 文字の英数字を指定できます。
グループ ID	このアイテムによって VLAN の ID 番号を設定できます。このフィールドは、VLAN を一度に 1 つずつ追加するために使用されます。VLAN グループ ID と使用可能な範囲は 2 ~ 4094 です。
ポート	ポート 1 からポート 10 を示します。
メンバー	追加 インターフェイスを VLAN のポート ベース メンバとして定義します。
	削除 禁止ポートは VLAN に含まれません。



Note

選択されていないすべてのポートは、別の単一の VLAN に属するものとして扱われます。ポート ベースの VLAN が有効になっている場合、VLAN タグ付けは無視されます。

802.1Q VLAN

タグ付きベースの VLAN は IEEE 802.1Q 仕様標準です。したがって、異なるスイッチベンダーのデバイス間で VLAN を作成できます。IEEE 802.1Q VLAN は、イーサネットフレームに「タグ」を挿入する手法を使用します。タグには、VLAN 番号を示す VLAN 識別 r(VID)が含まれています。

タグベース VLANを作成および削除できます。設定する VLAN グループは 256 個あります。802.1Q VLAN をイネーブルにし、スイッチ上のすべてのポートがデフォルト VLAN に属します。VIDは1です。デフォルト VLAN は削除できません。

スイッチの用語を理解する

■ IEEE 802.1Qタグ付けおよびタグなし

802.1Q 準拠スイッチのすべてのポートは、タグ付きまたはタグなしとして設定できます。

- **付き** タグ付けが有効になっているポートは、VID番号、プライオリティ、およびその他のVLAN情報を、それらのポートに流れるすべてのパケットのヘッダーに配置します。パケットが以前にタグ付けされている場合、ポートはパケットを変更しないため、VLAN情報はそのまま維持されます。タグ内のVLAN情報は、他の802.1Q 準拠デバイス on ネットワークで使用して、パケット転送の決定。
- **タグ** タグなしが有効になっているポートは、それらのポートに流れるすべてのパケットから802.1Q タグを削除します。パケットに802.1Q VLAN タグがない場合、ポートはパケットを変更しません。したがって、タグ付けされていないポートによって送受信されるすべてのパケットは、802.1Q VLAN 情報を提供しません。(PVID はスイッチ内でのみ内部的に使用されます)。タグ付け解除は、802.1Q 準拠のネットワーク デバイスから非準拠ネットワークにパケットを送信するために使用されます。デバイス。

フレーム収入 フレーム休暇	収入フレームにタグが付けられている	収入フレームにタグが付けがつい
ポートにタグが付いたまま	フレームはタグ付けされたまま	タグが挿入されました
ポートにタグを付けずにする	タグが削除されました	フレームにタグなしのまま

4.4.3.1 VLAN グループの設定

■ VLAN グループの設定

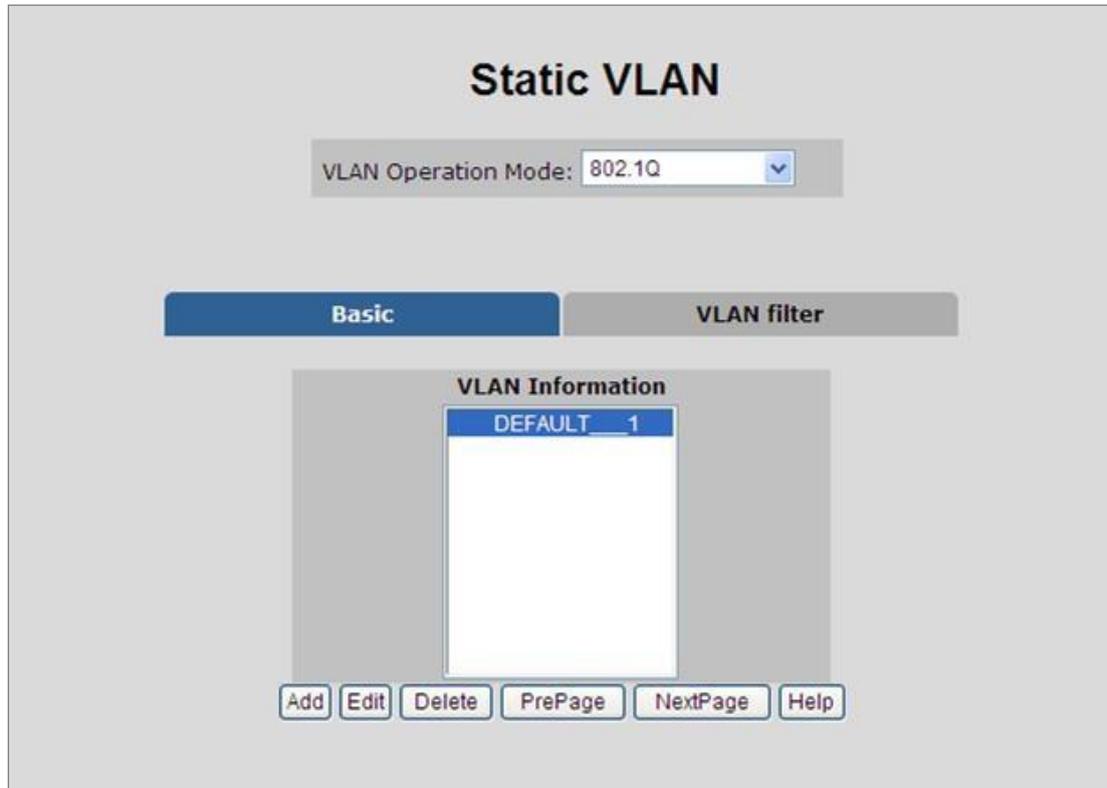


図 4-4-4-1: VLAN グループ設定インターフェイス

1. ハイパーリンク "VLAN" "静的 VLAN" をクリックして、VLAN 設定インターフェイスに入ります。
2. VLAN 動作モードで [802.1Q] を選択して、802.1Q VLAN 機能を有効にします。
3. [追加] をクリックして新しい VLAN グループを作成するか、既存の VLAN グループに [編集] をクリックします。次に、[VLAN グループ] 列が表示されます。
4. VLAN グループ ID を入力し、使用可能な範囲は2 ~ 4094です。

Static VLAN

VLAN Operation Mode: 802.1Q

VLAN Group
VLAN Filter

VLAN Name:	<input style="width: 90%;" type="text"/>
VID:	<input style="width: 90%;" type="text" value="1"/>
<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10 </div>	<input type="button" value="Add >>"/> <input type="button" value="<< Remove"/>
<input type="checkbox"/> CPU Port	

図 4-4-4-2: VLAN グループ設定インターフェイス

5. メンバーポートとして特定のポートを選択すると、図4-4-4-3の画面が表示されます。
6. セットアップが完了したら、**[適用]**ボタンを押して有効にしてください。
7. 図 4-33 の画面に示すように、VLAN設定画面に戻るには**[戻る]**を押して別のVLAN グループを追加してください。
8. 1 ページの制限を超えるグループが多数ある場合は、**[次へ]** をクリックして他の VLAN グループを表示できます。
9. 不要なVLANを削除するには、**[削除]**ボタンを使用します。
10. **[編集]**ボタンを使用して、existing VLANグループを変更します。

Static VLAN

VLAN Operation Mode:

VLAN Name: DEFAULT			
VLAN ID: 1			
UnTag Member			
Port1	Untag ▼	Port2	Untag ▼
Port3	Untag ▼	Port4	Untag ▼
Port5	Untag ▼	Port6	Untag ▼
Port7	Untag ▼	Port8	Untag ▼
Port9	Untag ▼	Port10	Untag ▼

図 4-4-4-3: 802.1Q VLAN 設定 Web ページ画面

このページには、次のフィールドが含まれています。

オブジェクト	説明
VLAN 名	このオプションフィールドを使用して、VLAN の名前を指定します。16まで可能英数字の長さ (ブランクを含む)。
VLAN ID	このアイテムによって VLAN の ID 番号を設定できます。このフィールドは、VLAN を一度に 1 つずつ追加するために使用されます。 VLAN グループ ID と使用可能な範囲は 2 ~ 4094 です。
ポート	ポート 1 からポート 10 を示します。
メンバーのタグを解除する	<p>タグ解除 インターフェイスによって転送されるパケットはタグ付け解除されます。</p> <p>タグ インターフェイスを VLAN のタグ付きメンバーとして定義します。インターフェイスによって転送されるすべてのパケットにタグが付けられます。パケットに VLAN が含まれている</p> <p style="text-align: right;">情報。</p>



Note

802.1Q VLAN をイネーブルにし、スイッチ上のすべてのポートがデフォルト VLAN に属します。VIDは1です。デフォルト VLAN は削除できません。

4.4.3.2 VLANフィルタ

■ 802.1Q VLAN ポート設定

このページは、スイッチポートVLAN の設定に使用されます。[ポートごとの VLAN 設定]ページには、VLAN の一部であるポートを管理するためのフィールドが含まれています。ポートのデフォルト VLAN ID(PVID)は、[VLAN ポート設定]ページで設定します。デバイスに到着するすべてのタグなしパケットは、ポート PVID によってタグ付けされます。

この section は、スイッチからの各ポートの 802.1Q イングレス フィルタを提供します。

The screenshot shows the 'Static VLAN' configuration page. At the top, 'VLAN Operation Mode' is set to '802.1Q'. Below this, there are two tabs: 'Basic' and 'VLAN filters'. The 'VLAN filters' tab is active, showing two ingress filtering rules: 'Ingress Filtering Rule 1 (Forward only packets with VID matching this port's configured VID)' and 'Ingress Filtering Rule 2 (Drop Untagged Frame)'. A table below these rules shows the configuration for Port2, with PVID set to 1, Ingress Filtering 1 set to 'Enable', and Ingress Filtering 2 set to 'Disable'. At the bottom, a summary table shows the configuration for Port2: PVID 1, Ingress Filtering 1 ENABLE, and Ingress Filtering 2 DISABLE.

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port2	1	Enable	Disable

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port2	1	ENABLE	DISABLE

図 4-4-4-4: 802.1Q イングレス フィルタ インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
いいえ	ポート 1 からポート 10 を示します。
Pvid	特定のポートのタグなしトラフィックに割り当てるポート VLAN ID を設定します。この機能は、VLAN に参加したいがタグ付けをサポートしていないデバイスに対応する場合に便利です。 各ポートでは、1つの VLAN ID を設定できます。範囲 is 1 ~255。デフォルト VLAN ID

1 です。

VLAN ID は、ポートが VLAN グループに属する VLAN ID と同じである必要があります。

インGRESS フィルタリング
1

Ingress フィルタリングを使用すると、ポートがその VLAN に属している場合に、特定の VLAN に属するフレームを転送できます。

Enable: このポートの設定された VID に一致する VID を持つパケットのみを転送します。

無効: 入力フィルター機能を無効にします。

タグなしフレームをドロップします。

インGRESS フィルタリング
2

無効: すべてのパケットが受け入れられます。

イネーブル: 一致する VLAN ID を持つパケットのみがポートを通過することを許可できます。

[適用] ボタン

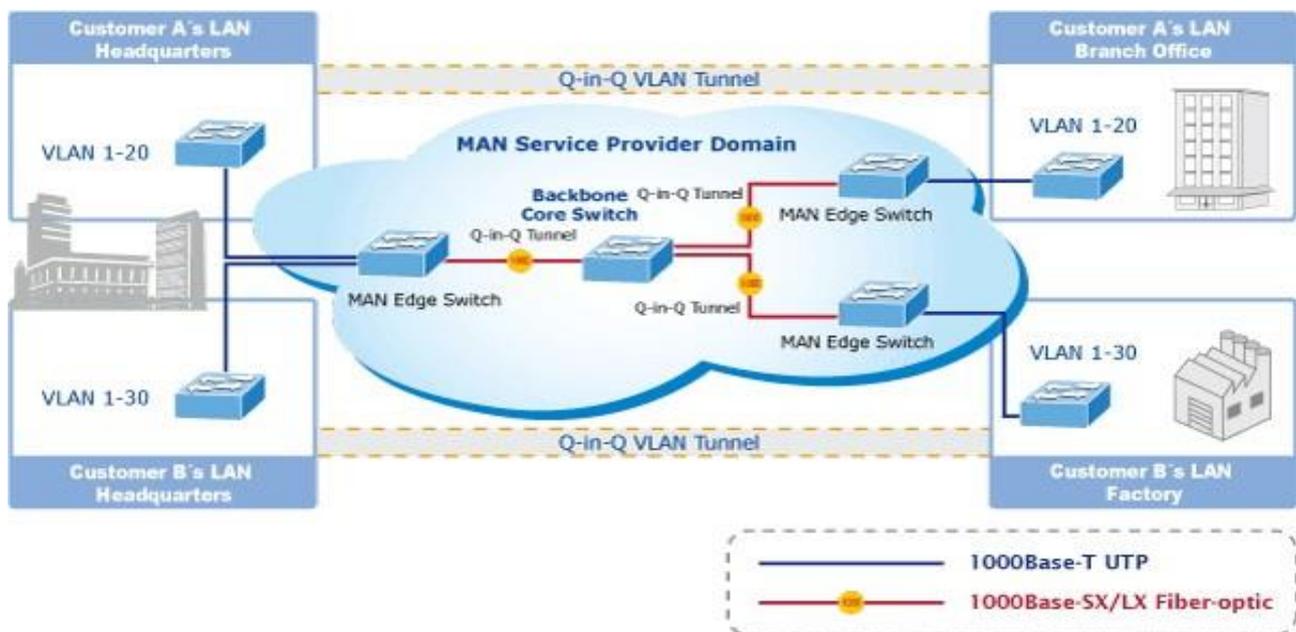
ボタンを押して構成を保存します。

4.4.4 Q-in-Q VLAN

■ IEEE 802.1Q トンネリング(Q-in-Q)

IEEE 802.1Q トンネリング(Q-in-Q)は、ネットワークを介して複数の顧客のトラフィックを伝送するサービス プロバイダ 一向けに設計されています。Q-in-Q トンネリングは、異なるお客様が同じ内部 VLAN ID を使用する場合でも、お客様固有の VLAN およびレイヤ 2 プロトコル設定を維持するために使用されます。これは、**サービス プロバイダー VLAN (SPVLAN)** タグをサービス プロバイダーのネットワークに入ったときに顧客のフレームに挿入し、フレームがネットワークから出るときにタグを取り除くことによって実現されます。

サービスプロバイダーのお客様は、内部VLAN ID とサポートされるVLANの数に関する特定の要件を持つ場合があります。同じサービス プロバイダー ネットワーク内の異なる顧客が必要とする VLAN 範囲は、簡単に重複し、インフラストラクチャを通過するトラフィックが混在する可能性があります。各顧客に一意の VLAN ID の範囲を割り当てると、顧客 c のオンフィギュレーションが制限され、VLAN マッピング テーブルの集中的な処理が必要になり、VLAN の最大制限である



4096 を簡単に超える可能性があります。

管理対象スイッチは複数の VLAN タグをサポートしているため、MAN アプリケーションでプロバイダーブリッジとして使用できるため、多数の独立した顧客 LAN からMAN(メトロ アクセス ネットワーク)スペースへのトラフィックを集約できます。プロバイダ bridgeの目的の1つは、MAN 空間内のVLANを顧客の VLAN から独立して使用できるように、VLAN タグを認識して使用することです。これは、MAN に入るフレームに MAN 関連の VID を含む VLAN タグを追加することで実現されます。MAN を離れると、タグが削除され、顧客関連の VID を含む元の VLAN タグが再び使用可能になります。

これにより、VLAN タグを妨げることなく、共通の MAN 空間を介してリモート スカーサー VLAN を接続するためのトンネリング メカニズムが提供されます。すべてのタグは Ether Type 0x8100 または 0x88A8 を使用し、顧客タグには 0x8100 が使用され、0x88A8 はサービス プロバイダー タグに使用されます。

特定のサービス VLAN にスイッチに 2 つのメンバー ポートしかない場合、特定のVLANに対して学習を無効にできるため、2 つのポート間の転送メカニズムとしてフラッドングに依存できます。これにより、MAC テーブルの要件が減少します。

4.4.4.1 Q-in-Q ポート設定

図 4-4-5-1の Q-in-Q VLAN\Q-in-Q ポート設定画面が表示されます。

QinQ		
QinQ Enable		
QinQ Tpid 8100		
Port	QinQ	QinQ Uplink
Port1	<input type="checkbox"/>	<input type="checkbox"/>
Port2	<input type="checkbox"/>	<input type="checkbox"/>
Port3	<input type="checkbox"/>	<input type="checkbox"/>
Port4	<input type="checkbox"/>	<input type="checkbox"/>
Port5	<input type="checkbox"/>	<input type="checkbox"/>
Port6	<input type="checkbox"/>	<input type="checkbox"/>
Port7	<input type="checkbox"/>	<input type="checkbox"/>
Port8	<input type="checkbox"/>	<input type="checkbox"/>
Port9	<input type="checkbox"/>	<input type="checkbox"/>
Port10	<input type="checkbox"/>	<input type="checkbox"/>

図 4-4-5-1: Q-in-Q ポート設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
Q-in-Q	<p>有効: 管理対象スイッチをQ-in-Qモードに設定し、Q-in-Q トンネル ポートを許可します。</p> <p>を構成します。</p> <p>無効: 管理対象スイッチは通常の VLAN モードで動作します。</p> <p>デフォルトでは、マネージスイッチが無効モードで機能します。</p>
Q-in-Q TPID	<p>タグ プロトコル識別子(TPID)は、トンネルアクセス ポート上の着信パケットのエタヘタイプを指定します。</p> <ul style="list-style-type: none"> • 802.1Qタグ: 8100 • vMANタグ: 88A8 <p>デフォルト: 802.1Q タグ。</p>
ポート Q-in-Q	<p>チェック: ポートをQ-in-Qモードに設定します。または、ポートは通常の VLAN モードで動作します。デフォルト: チェックを解除します。</p>

Q-in-Q アップリンク	チェック :	サービス プロバイダ ネットワーク内の別のデバイスへのアップリンク ポートの IEEE 802.1Q トンネリング(Q-in-Q)を設定します。
	キャンセル:	クライアント アクセス ポート用の IEEE 802.1Q トンネリング(Q-in-Q)を設定して、サービスを横断する traffic 用の顧客 VLAN ID を分離および保持します。 プロバイダ ネットワーク。

4.4.4.2 Q-in-Q トンネル設定

多くの場合、サービスプロバイダーのビジネス顧客には、VLAN IDに関する特定の要件と、サポートするVLANの数があります。同じサービスプロバイダーネットワーク内の異なる顧客が必要とするVLAN範囲が重複する可能性があります。インフラストラクチャのトラフィックが混在する可能性があります。各顧客に一意のVLAN IDを割り当てると、お客様の設定が制限され、IEEE 802.1Q仕様のVLAN制限(4096)を簡単に超える可能性があります。

Q-in-Q機能を使用すると、サービスプロバイダーは単一のVLANを使用して、複数のVLANを持つお客様をサポートできます。顧客VLAN IDは保持され、異なる顧客からのトラフィックは、同じVLAN内にあるように見えても、サービスプロバイダーネットワーク内で分離されます。Q-in-Qを使用すると、VLAN内階層を使用し、タグ付きパケットのタグ付けを変更することで、VLAN空間が拡張されます。Q-in-Qをサポートするように設定されたポートは、Q-in-Qユーザー・ポートと呼ばれます。Q-in-Qアップリンクをサポートするように設定されたポートは、Q-in-Qアップリンクポートと呼ばれます。

QinQ VLAN		
QinQ Port Setting		QinQ Tunnel Setting
Tunnel ID	Tunnel1	<< Get
Tunnel VID	0	
	<< Add <<	Port1
	Remove >>	Port2
		Port3
		Port4
		Port5
		Port6
		Port7
		Port8
		Port9
<input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Help"/>		

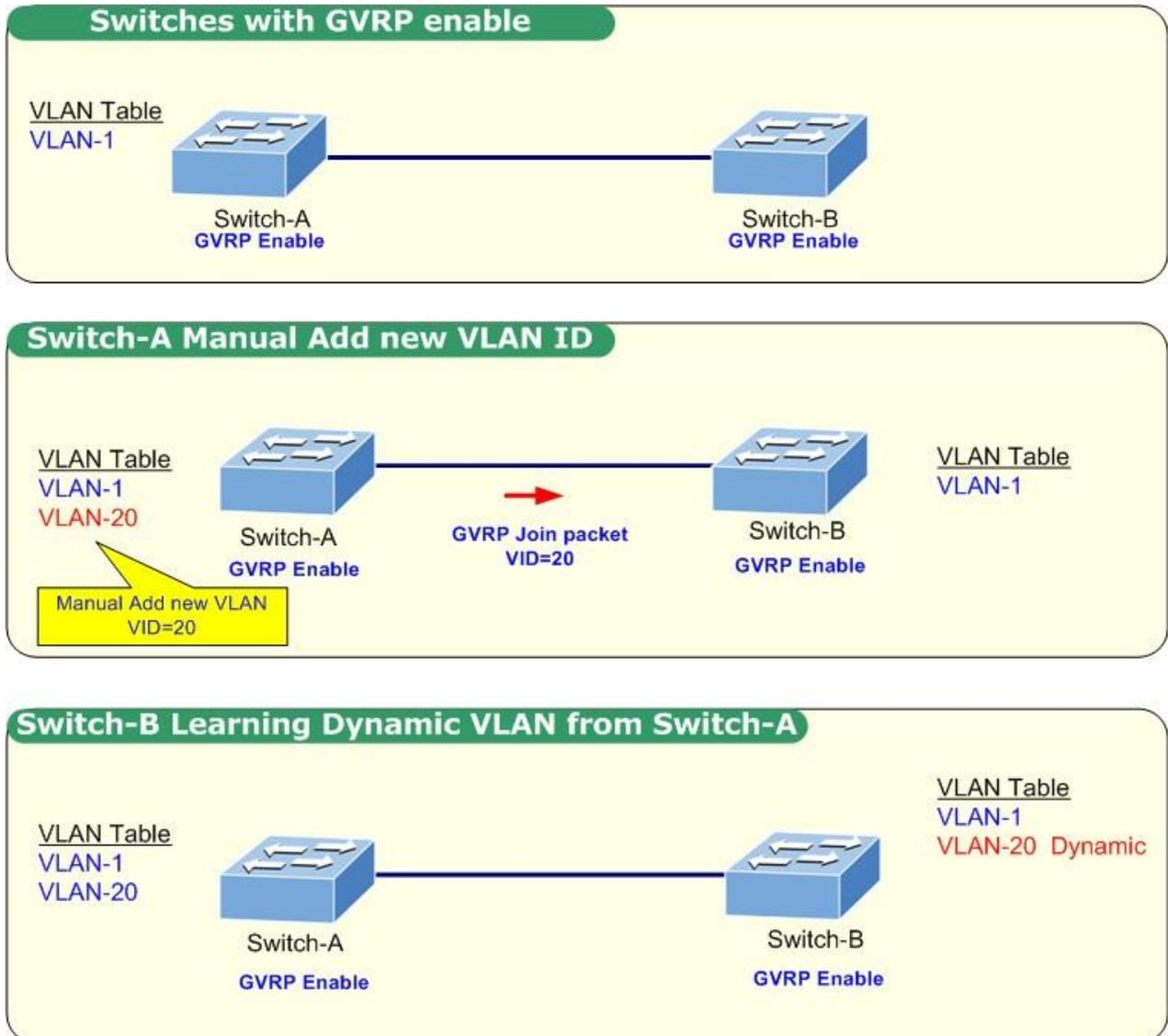
図 4-4-5-2: Q-in-Q トンネル Sエッティング インターフェイス

■ Q-in-Q ポートを設定するには

1. グローバル Q-in-Q 機能を有効にするには、**Q-in-Q**を選択し、「有効にする」を有効にします。
2. Q-in-Q Tpidに記入してください。
3. ポート Q-in-Q 機能を使用可能にするには、特殊ポートの **Q-in-Q** チェックボックスを選択します。
4. ポート Q-in-Q アップリンク機能を使用可能にするには、特殊ポートの **Q-in-Q** アップリンク チェックボックスを選択します。

4.4.5 GVRP VLAN

GVRP(GARP VLAN 登録プロトコルまたは汎用 VLAN 登録プロトコル)は、大規模なネットワーク内の仮想ローカルエリア ネットワーク(VLAN)の制御を容易にするプロトコルです。GVRP は IEEE 802.1Q 仕様に準拠しており、VLAN 設定データを使用してフレームにタグを付ける方法を定義します。これにより、ネットワーク デバイスは VLAN 設定情報を他のデバイスと動的に交換できます。



4.4.5.1 GVRP設定

GVRP を設定するには

グローバル GVRP 機能を有効にするには、[GVRP] を選択して [有効にする] を選択します。

ポート GVRP 機能を有効にするには、特殊ポートの GVRP チェックボックスを選択します。

GVRP	
Port	GVRP
Port1	<input type="checkbox"/>
Port2	<input type="checkbox"/>
Port3	<input type="checkbox"/>
Port4	<input type="checkbox"/>
Port5	<input type="checkbox"/>
Port6	<input type="checkbox"/>
Port7	<input type="checkbox"/>
Port8	<input type="checkbox"/>
Port9	<input type="checkbox"/>
Port10	<input type="checkbox"/>

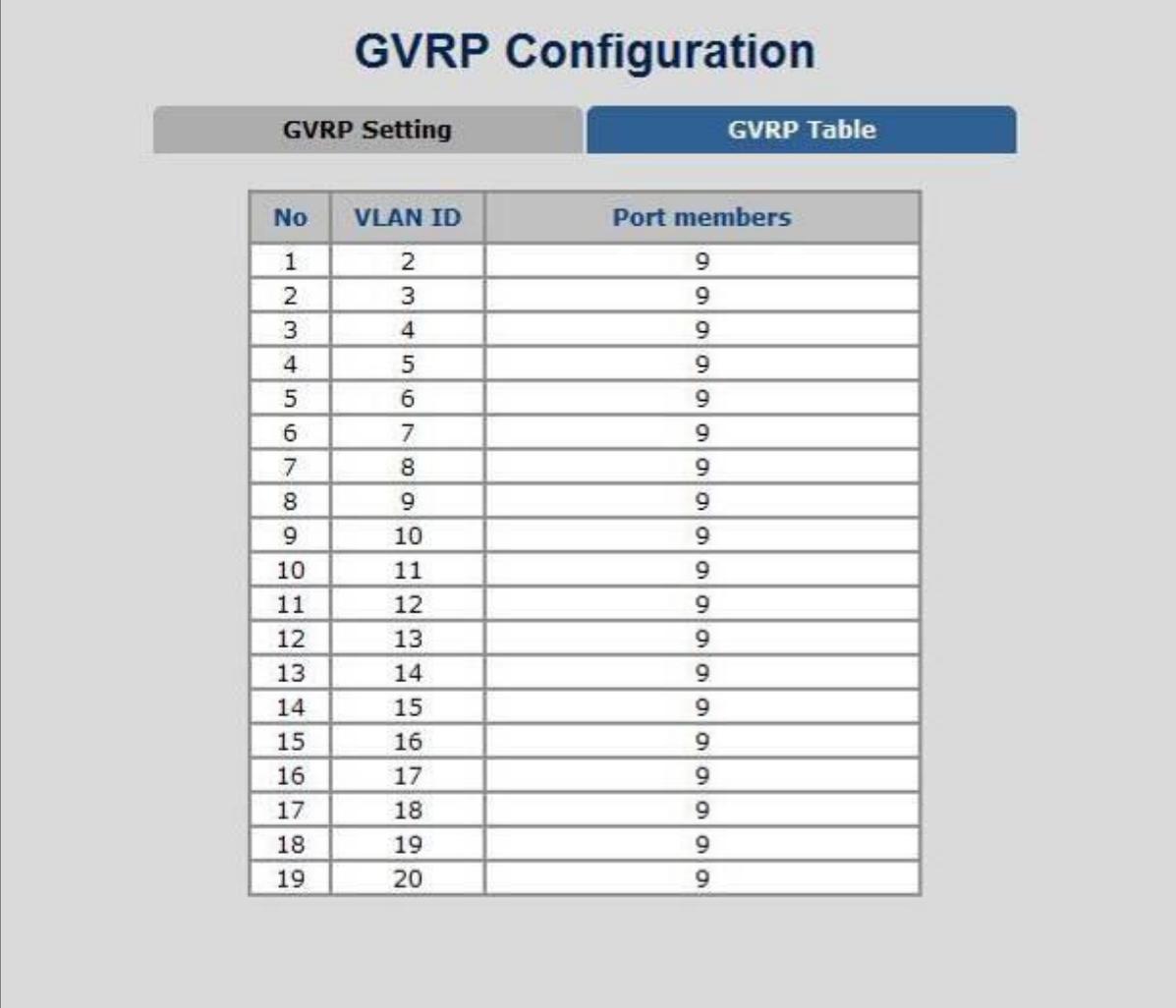
図 4-4-6-1: GVRP 設定 Web インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
Gvrp	グローバル GVRP 機能を有効にする
ポート	ポート 1 からポート 10 を示します。
ポート GVRP	選択したポート GVRP 機能を有効にする

4.4.5.2 GVRPテーブル

GVRP テーブルを使用して、GVRP を介して学習されたダイナミック VLAN を表示できます。



GVRP Configuration		
GVRP Setting		GVRP Table
No	VLAN ID	Port members
1	2	9
2	3	9
3	4	9
4	5	9
5	6	9
6	7	9
7	8	9
8	9	9
9	10	9
10	11	9
11	12	9
12	13	9
13	14	9
14	15	9
15	16	9
16	17	9
17	18	9
18	19	9
19	20	9

図 4-4-6-2: GVRP テーブル Web インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
VLAN ID	GVRP 対応ポートで GVRP プロトコルを介して学習した VLAN を表示します。 管理対象スイッチでは、最大 128 個のダイナミック VLAN エントリを表示できます。
ポートメンバー	ダイナミック VLAN を学習する GVRP 対応ポートを特定します。

4.5 トランキング

ポートトランキング(「リンク アグリゲーション」とも呼ばれる)は、複数のポートまたはネットワーク ケーブルを組み合わせて、1 つのポートまたはネットワークケーブルの制限を超えて接続速度を拡張します。管理対象スイッチは、次の 2 種類のポート トランクテクノロジーをサポートします。

- スタティックトランク
- LACP

リンクアグリゲーション制御プロトコル(LACP)は、リンク上のパートナー システム間で情報を交換するための標準化された手段を提供し、リンクアグリゲーション 制御インスタンスがリンクアグリゲーション グループの ID で合意に達し、リンクが属するリンク アグリゲーショングループへのリンクを移動し、 整然とした方法で送受信機能を有効にします。リンクアグリゲーションを使用すると、最大 8 つの連続するポートを 1 つの専用接続にグループ化できます。この機能により、ネットワーク上のデバイスに帯域幅を拡張できます。LACP 動作には全二重モードが必要です。詳細については、IEEE 802.3adを参照してください。

4.5.1 アグリゲータの設定

このセクションでは、管理対象スイッチからの各ポートのポート トランク アグリゲータ設定について説明します。

Trunking

Aggregator Setting
Aggregator Information
State Activity

LACP	System Priority
<input checked="" type="checkbox"/>	32768

Group ID	1 <input type="text"/>	<input type="button" value=" << Get"/>
LACP	Enable <input type="text"/>	
Work Ports	2 <input type="text"/>	
<div style="border: 1px solid gray; padding: 2px;">Port9 Port10</div>	<input type="button" value=" << Add <<"/> <input type="button" value=" Remove >>"/>	<div style="border: 1px solid gray; padding: 2px;">Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8</div>

図 4-5-1-1:ポート トランク:アグリゲータ設定インターフェイス(LACP がイネーブルの場合、2 つのポートが左側のフィールドに追加されます)

このページには、次のフィールドが含まれています。

オブジェクト	説明
システムの優先順位:	アクティブな LACP を識別するために使用される値。値が最も小さい管理対象スイッチは最も高い優先順位を持ち、アクティブ LACP ピアとして選択されます。トランクグループ。
グループ ID:	選択するトランク グループは 13 個あります。"グループID"をトランク グループに割り当てます。
Lacp :	<ul style="list-style-type: none"> ■ 有効-- トランク グループは LACPを使用します。LACP トランク グループに参加するポートは、最初にそのメンバー ポートとアグリーメントを行う必要があります。 ■ 無効-- トランク グループはスタティック トランク グループです。LACP を無効にする利点は、ポートがメンバー ポートとのハンドシェイクなしでトランク グループに参加することですが、メンバポートはロジック トランク グループを形成するには、一緒に集約する必要があります。
作業ポート:	この列フィールドを使用すると、ユーザーはアクティブなポートの合計数を最大 4 つまで入力できます。LACP スタティック トランク グループでは、ワーク ポート列フィールドが 2 に設定されているトランク グループのメンバーとして 4 つのポートを割り当てます。スタティックトランクグループ(非LACP)の場合、作業ポートの数はグループ メンバー ポートの総数と同じである必要があります。



2つのスイッチ間で分割されたメンバー ポートを含むトランク グループは、2つのスイッチの LACP 機能をイネーブルにする必要があることに注意してください。

4.5.2 アグリゲータ情報

LACP アグリゲータを設定すると、関連情報がここに表示されます。

■ LACPが無効

LACP を無効にしてアグリゲータ設定を設定すると、

アグリゲータ情報:

Trunking

Aggregator Setting
Aggregator Information
State Activity

LACP	<input type="checkbox"/>
System Priority	<input type="text" value="32768"/>

Group ID	<input type="text" value="1"/> ▼	<input type="button" value=" << Get"/>
LACP	<input type="text" value="Disable"/> ▼	
Work Ports	<input type="text" value="2"/>	
<div style="border: 1px solid gray; padding: 2px;">Port9 Port10</div>	<input type="button" value=" << Add <<"/> <input type="button" value=" Remove >>"/>	<div style="border: 1px solid gray; padding: 2px;">Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8</div>

図 4-5-2-1: LACP を無効にしたトランク グループへの 2 つのポートの割り当て

Trunking

Aggregator Setting
Aggregator Information
State Activity

The following information provides a view of LACP current status.

Static Trunking Group	
Group Key	1
Port_No	9 10

図 4-5-2-2: スタティック トランキング グループ 情報

このページには、次のフィールドが含まれています。

オブジェクト	説明
グループ キー:	これは、トランク グループ ID を表示する読み取り専用の列フィールドです。
ポート メンバー:	これは、この静的トランクのメンバーを表示する読み取り専用の列フィールドです。 グループ。

■ LACPが有効

LACP を有効にしてアグリゲータ設定を設定すると、[アグリゲータ情報]のタブに2つのスイッチ間のトランキンググループ情報が表示されます。

■ スイッチ 1の構成

1. トランク グループのシステムプライオリティを設定します。デフォルトは **32768**です。
2. ドロップダウン メニュー バーをプルして、**trunk グループ ID**を選択します。
3. LACP を有効にします。
4. ポート番号と列フィールドを選択した後、[追加]ボタンをクリックしてメンバポートを含めます。ワーク ポートは自動的に変更されます。

Trunking

Aggregator Setting **Aggregator Information** **State Activity**

LACP	System Priority
<input checked="" type="checkbox"/>	32768

Group ID	1 ▼	<< Get
LACP	Enable ▼	
Work Ports	2	
Port1 Port2	<< Add << Remove >>	Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10

Apply Delete Help

図 4-5-2-3:スイッチ 1 の集約情報

5. 2つのスイッチの設定後に上の図に示すように、**アグリゲータ情報**のタブをクリックしてトランク グループ情報を確認します。

■ スイッチ 2の構成

6. トランク グループのシステムプライオリティを設定します。たとえば、1。
7. ドロップダウン メニュー バーをプルして、**トランク グループ ID**を選択します。
8. LACP を有効にします。

9. ポート番号と列フィールドを選択した後、[追加]ボタンをクリックしてメンバポートを含めます。
ワークポートは自動的に変更されます。

Trunking

Aggregator Setting
Aggregator Information
State Activity

LACP	System Priority
<input checked="" type="checkbox"/>	1

Group ID	1	<< Get
LACP	Enable	
Work Ports	2	
<div style="border: 1px solid gray; padding: 2px;"> Port1 Port2 </div>	<div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"><< Add <<</div> <div style="border: 1px solid gray; padding: 2px;">Remove >></div>	<div style="border: 1px solid gray; padding: 2px;"> Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10 </div>

Apply
Delete
Help

図 4-5-2-4:スイッチ 2 の設定インターフェイス

10. 2つのスイッチの設定後に上の図に示すように、**アグリゲータ情報**のタブをクリックしてトランクグループ情報を確認します。

Trunking

Aggregator Setting
Aggregator Information
State Activity

The following information provides a view of LACP current status.

Group1						
Actor				Partner		
Priority	32768			1		
MAC	00304f000000			00304f112233		
PortNo	Key	Priority	Active	PortNo	Key	Priority
PORT1	258	32768	selected	PORT1	258	1
PORT2	258	32768	selected	PORT2	258	1

図 4-5-2-5:スイッチ 1 アグリゲータ情報

4.5.3 状態アクティビティ

アグリゲータ設定のタブで LACP アグリゲータを設定したら、LACPトランクグループのメンバーの状態アクティビティを設定できます。状態ラベルの横にあるチェックボックスをオンまたはオフにできます。の目盛りを削除すると、

ポートそして **使用ク** の場合、ポートの状態アクティビティは次の値に変わります。 **パッシブ**。

Trunking

Aggregator Setting
Aggregator Information
State Activity

Port	LACP State Activity	Port	LACP State Activity
1	<input checked="" type="checkbox"/> Active	2	<input checked="" type="checkbox"/> Active
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A

Apply Help

図 4-5-3-1:スイッチ 1 の状態アクティビティ

このページには、次のフィールドが含まれています。

オブジェクト	説明
アクティブ:	ポートは LACP プロトコル パケットを自動的に送信します。
パッシブ:	ポートは LACP プロトコル パケットを自動的に送信せず、反対側のデバイスから LACP プロトコル パケットを受信した場合にのみ応答します。



Note

2つのパッシブ LACP ノードを持つリンクは、両方のポートが反対側のデバイスからの LACP プロトコル パケットを待機しているため、ダイナミック LACP トランクを実行しません。

4.6 転送とフィルタリング

イーサネットパケットのフレームには、フレームを送信する機器の MAC アドレスを示す MAC アドレス(SMAC アドレス)が含まれています。SMAC アドレスは、これらのダイナミック MAC アドレスを使用して MAC テーブルを自動的に更新するためにスイッチによって使用されます。設定可能な経過時間の後に、対応する SMAC アドレスを持つフレームが見られない場合、動的 entries は MAC テーブルから削除されます。

4.6.1 ダイナミック MAC テーブル

MAC テーブルのエントリは、このページに表示されます。ダイナミック MAC テーブルには最大8192エントリが含まれ、最初に VLAN ID で並べ替えられ、次に MAC アドレスで並べ替えられます。リストされたポートで学習したすべてのダイナミック MAC アドレスを表示できます。

Forwarding and Filtering

Dynamic MAC Table Static MAC Table MAC Filtering

Click "Clear" will clear Dynamic addresses from the switch .

Dynamic addresses currently learned on the switch are listed below.

NO	MAC	PORT	VID	TYPE
1	00:08:B6:00:06:90	1	1	Dynamic
2	00:03:6D:F7:80:7F	2	1	Dynamic

There are total 2 Mac Adresses.

図 4-6-1:ダイナミック MAC アドレス インターフェイス

MAC テーブル列

オブジェクト	説明
• いいえ	MAC アドレス インデックス エントリ。
• Mac	エントリの MAC アドレス。
• ポート	エントリのメンバーであるポート。
• Vid	エントリの VLAN ID。
• 型	エントリが静的エントリか動的エントリかを示します。

[クリア] をクリックして、画面に表示されている現在のポートの動的 MAC アドレス情報をクリアします。

4.6.2 スタティック MAC テーブル

デバイスがスイッチに物理的に接続されているかどうかに関係なく、スイッチのアドレス テーブルに残るスタティック MAC アドレスを追加できます。これにより、切断または電源オフの de vice がネットワーク上で再びアクティブになったときに、スイッチがデバイスの MAC アドレスを再学習する必要がなくなります。このインターフェイスを使用して、静的 MAC アドレスを追加/削除できます。

■ スタティック MAC アドレスの追加

ここでスイッチ MAC テーブルにスタティック MAC アドレスを追加できます。

Forwarding and Filtering

Dynamic MAC Table **Static MAC Table** MAC Filtering

Dynamic addresses currently defined on the switch are listed below.
Click Add to add a new static entry to the address table.

MAC Address	PORT	VID
00:30:4F:11:22:33	1	1

MAC Address: 00:30:4F:22:33:44

Port num: Port 2

VLAN ID: 1

Add Delete Help

図 4-6-2:スタティック MAC アドレス インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
MAC アドレス:	デバイスのネットワーク アクティビティに関係なく、トラフィックを永続的に転送するポートの MAC アドレスを入力します。
ポート番号:	選択メニューをプルダウンして、ポート番号を選択します。
VLAN ID:	エントリの VLAN ID。

4.6.3 MACフィルタリング

MAC アドレスをフィルタリングすることで、スイッチは事前設定された MAC アドレスを簡単にフィルタリングし、安全性を低下させることができます。フィルタリング MAC アドレスを追加および削除できます。

NO	MAC	SOURCE	VID	TYPE
1	00:30:4F:55:66:77	Filter	1	Static
2	00:30:4F:77:2B:FC	Filter	1	Static

図 4-6-3: MAC フィルタリング インターフェイス

このページには、次のフィールドが含まれています。

オ・ビェクト	説明
MAC アドレス:	フィルタリングする MAC アドレスを入力します。
VLAN ID:	エントリの VLAN ID。

4.7 IGMPスヌーピング

4.7.1 理論

インターネットグループ管理プロトコル (IGMP) を使用すると、ホストとルーターはマルチキャストグループメンバーシップに関する情報を共有できます。IGMP スヌーピングは、IGMP メッセージの交換を監視し、機能処理のためにCPU にコピーするスイッチ機能です。IGMP スヌーピングの全体的な目的は、マルチキャストフレームの転送をマルチキャストグループのメンバーであるポートのみに制限することです。

インターネットグループ管理プロトコル (IGMP) スヌーピングについて

マルチキャスト転送を受信するコンピュータとネットワーク デバイスは、近くのルーターにマルチキャストグループのメンバーになることを通知する必要があります。インターネットグループ管理プロトコル (IGMP) は、この情報を伝達するために使用されます。IGMP は、アクティブでなくなったメンバーのマルチキャストグループを定期的にチェックするためにも使用されます。サブネットワーク上に複数のマルチキャストルーターがある場合、1 台のルーターが「照会済み」として選択されます。このルーターは、アクティブなメンバーを持つマルチキャストグループのメンバーシップを追跡します。次に、IGMP から受信した情報を使用して、マルチキャストパケットを特定のサブネットワークに転送する必要があるかどうかを判断します。ルータは IGMP を使用して、特定のサブネットワーク作業にマルチキャストグループのメンバーが少なくとも1つ存在するかどうかを確認できます。サブネットワークにメンバーがない場合、パケットはそのサブネットワークに対してワードされません。

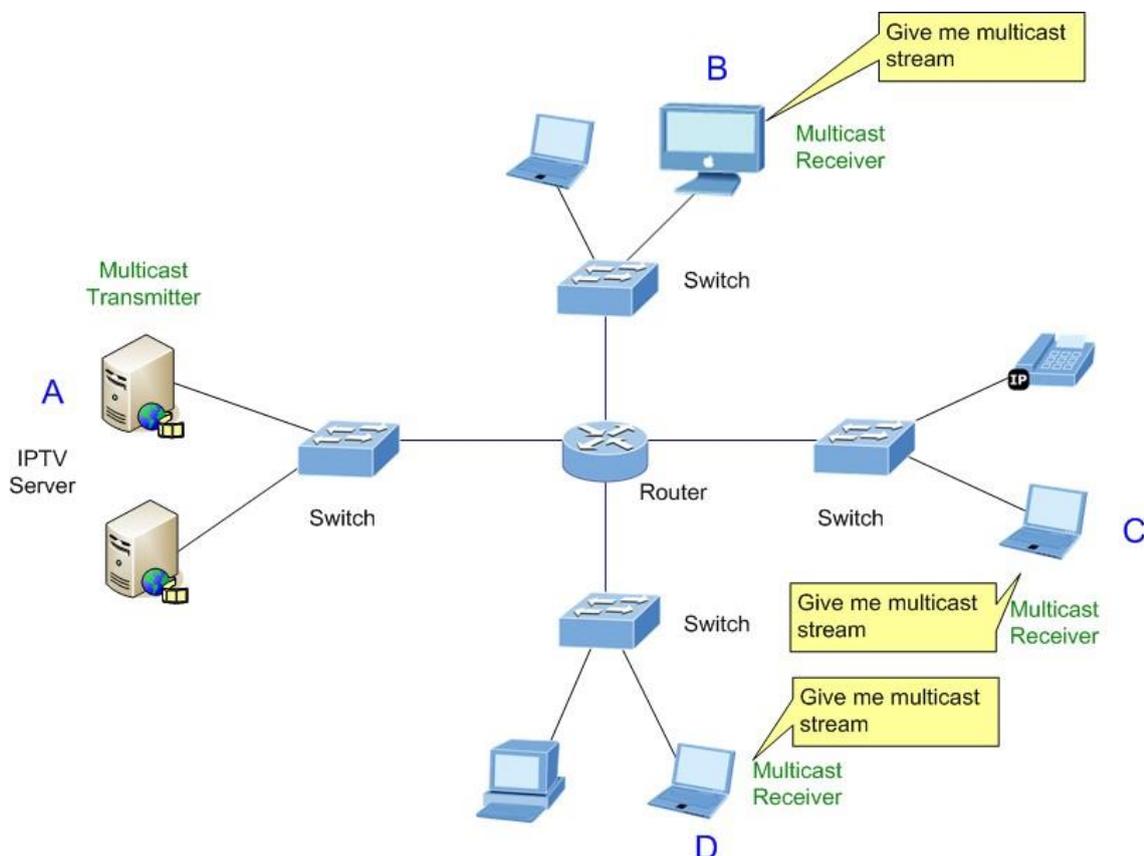


図 4-7-1-1:マルチキャスト サービス

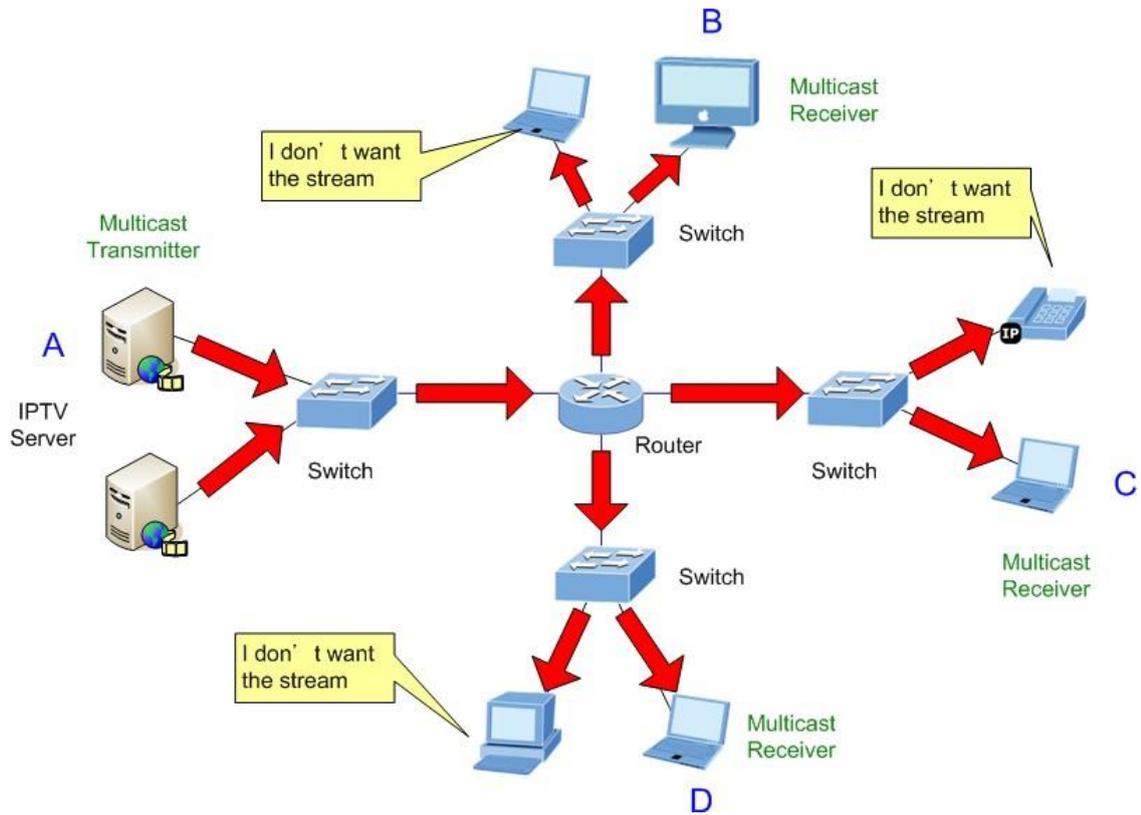


図 4-7-1-2:マルチキャスト フラッディング

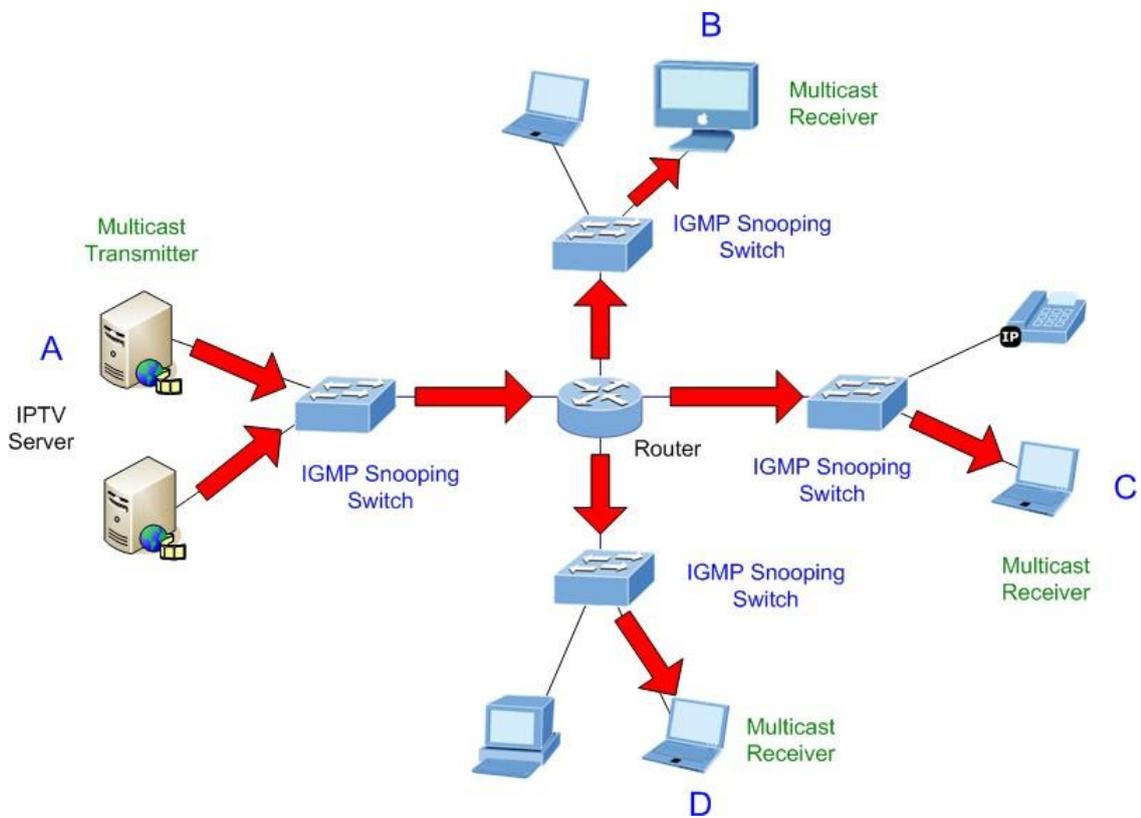


図 4-7-1-3: IGMP スヌーピング マルチキャスト ストリーム制御

IGMPバージョン1および2

マルチキャストグループを使用すると、メンバーはいつでも参加または退出できます。IGMPは、メンバーとマルチキャストルーターがマルチキャストグループに参加または離脱するときに通信する方法を提供します。IGMPバージョン1はRFC 1112で定義されています。パケットサイズが固定されており、オプションのデータはありません。

IGMPパケットの形式を次に示します。

IGMPメッセージ形式

オクテット

0	8	16	31
型	応答時間	チェックサム	
グループアドレス (クエリの場合はすべてゼロ)。			

IGMPタイプコードを次に示します。

型	意味
0x11	メンバーシップクエリ (グループアドレスが0.0.0.0の場合)。
0x11	特定のグループメンバーシップクエリ (グループアドレスが存在する場合)。
0x16	メンバーシップレポート (バージョン2)。
0x17	グループを終了する (バージョン2)。
0x12	メンバーシップレポート (バージョン1)。

IGMPパケットを使用すると、マルチキャストルータは、それぞれのサブネットワーク上のマルチキャストグループのメンバーシップを追跡できます。次に、IGMPを使用してマルチキャストルータとマルチキャストグループメンバー間で通信される内容の概要を示します。

ホストは、グループに参加するためにIGMP "レポート"を送信します。

ホストは、グループを離れたときにレポートを送信しません (バージョン1の場合)。

ホストは、グループを離れるときに「脱退」レポートを送信します (バージョン2の場合)。

マルチキャストルータはIGMPクエリを送信し(すべてのホストグループにress: 224.0.0.1を追加します)、サブネットワークにグループメンバーが存在するかどうかを確認します。特定のグループからの応答がない場合、ルータはネットワーク上にグループメンバーがいないと見なします。

クエリが他のサブネットワークに転送されないように、クエリ メッセージの存続時間 (TTL) フィールドを 1 に設定します。

IGMP バージョン 2 では、各 LAN に対して照会されたマルチキャストを選択する方法など、いくつかの機能強化が導入されています。

メッセージを残し、特定のグループに固有のメッセージを照会します。

次に示すように、コンピュータがマルチキャストグループに参加または脱退する状態。

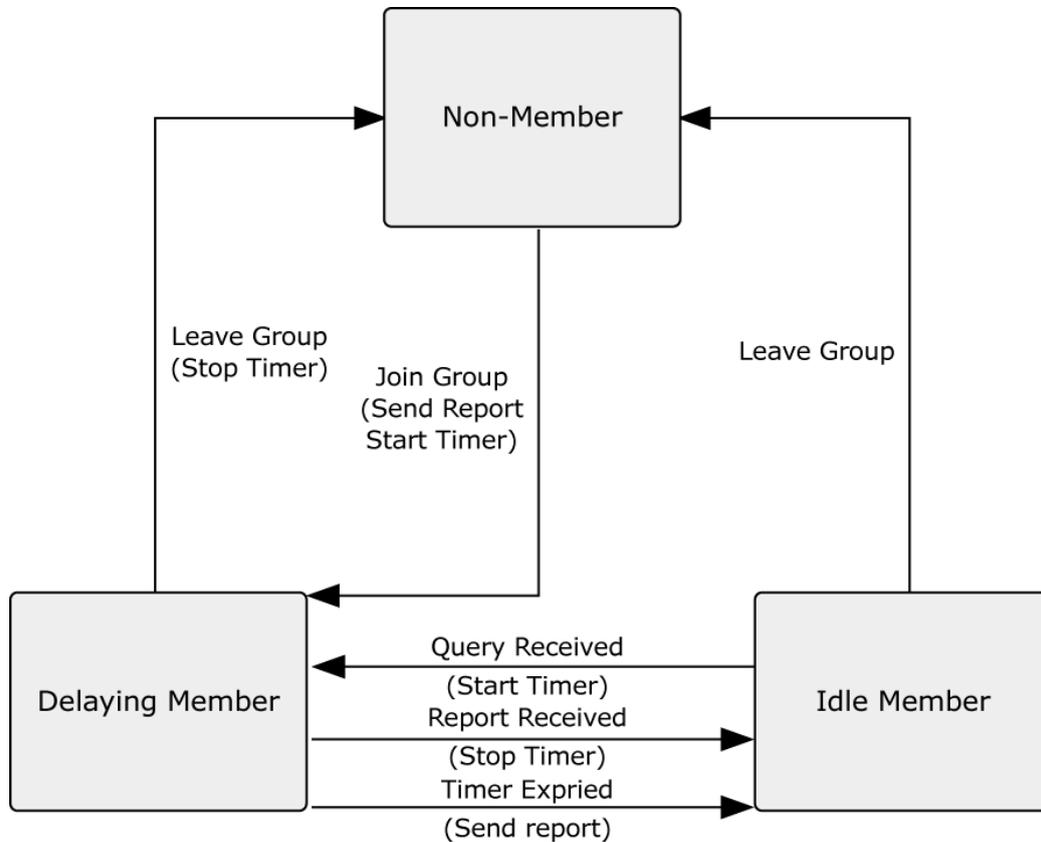


図 4-7-1-4: IGMP 状態遷移

■ IGMPクエリア

ルーターまたはマルチキャスト対応スイッチは、マルチキャストトラフィックを受信するかどうかをホストに定期的に問い合わせることができます。IP マルチキャストを実行している LAN に複数のルーター/スイッチがある場合、これらのデバイスの1つが"クエリア"と選択され、グループメンバに対して LAN を照会する役割を担います。次に、サービス要求をアップストリームマルチキャストスイッチ/ルータに伝播し、マルチキャストサービスを引き続き受信できるようにします。



Note

マルチキャストルーターは、この情報と DVMRP や PIM などのマルチキャストルーティングプロトコルを使用して、インターネット経由の IP マルチキャストをサポートします。

4.7.2 IGMP設定

スイッチは IP マルチキャストをサポートしており、Web 管理のスイッチ設定の詳細ページで IGMP プロトコルを有効にできます。その後、IGMP スヌーピング情報が表示されます。IP マルチキャスト アドレスの範囲は**224.0.0.0 ~ 239.255.255.255**です。

図 4-7-2-1: IGMP 設定インターフェイスのスクリーンショット

このページには、次のフィールドが含まれています。

オブジェクト	説明
IGMP プロトコル:	IGMP プロトコルを有効または無効にします。
IGMPファストリーブ:	ポートで高速脱退を有効または無効にします。
IGMP クェリア:	IGMP クェリ機能を有効または無効にします。IGMP クェリ情報は次の値になります。 IGMP ステータス セクションに表示されます。



断食:

管理対象スイッチは、そのポートで脱退パケットを受信し、親 VLAN に対して高速脱退機能が有効になっている場合に、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するように設定できます。これにより、管理対象スイッチは、最初にIGMP グループ固有のクエリをそのインターフェイスに送信しなくても、マルチキャスト転送テーブルからポートを削除できます。

4.8 スパニングツリープロトコル

4.8.1 理論

スパニングツリープロトコルを使用すると、ネットワークループを検出して無効にしたり、スイッチ、ブリッジ、またはルータ間のバックアップリンクを提供したりできます。これにより、スイッチはネットワーク内の他のブリッジングデバイスと対話して、ネットワーク上の任意の2つのステーション間に1つのルートのみが存在することを確認し、プライマリリンクがダウンしたときに自動的に引き継ぐバックアップリンクを提供できます。この管理対象スイッチでサポートされるスパニングツリーアルゴリズムには、次のバージョンがあります。

- **STP** – スパニングツリープロトコル(IEEE 802.1D)
- **MSTP** – 複数のスパニングツリープロトコル(IEEE 802.1s)

STP - スパニングツリープロトコル(STP)は、スイッチングネットワークのループを回避するための標準化された方法(IEEE 802.1D)です。STPを有効にして、ネットワーク上の任意の2つのデス間で一度に1つのパスのみがアクティブになるようにします。

MSTP - マルチスパニングツリープロトコル(MSTP)は、ターコネクテッドブリッジ(各動作MSTP、STP、またはRSTP)で任意に構成されるブリッジドローカルエリアネットワーク全体で、特定のVLANに割り当てられたフレームにシンプルで完全な接続を提供するための標準化された方法(IEEE 802.1S)です。MSTPを使用すると、LANまたはMSTブリッジで構成されるマルチスパニングツリー(MST)リージョン内の独立したマルチスパニングツリーインスタンス(MSTI)に基づいて、異なるVLANに割り当てられたフレームが個別のパスをたどることができます。これらのリージョンと他のブリッジおよびLANは、単一の共通スパニングツリー(CST)に接続されます。

IEEE 802.1D スパニングツリープロトコルおよび**IEEE 802.1s** マルチスパニングツリープロトコルを使用すると、ネットワーク内のループを形成するswかゆみ間のリンクをブロックできます。スイッチ間の複数のリンクが検出されると、プライマリリンクが確立されます。重複したリンクは使用をブロックされ、スタンバイリンクになります。このプロトコルを使用すると、プライマリリンクに障害が発生した場合に重複リンクを使用できます。スパニングツリープロトコルを設定してイネーブルにすると、プライマリリンクが確立され、重複したリンクが自動的にブロックされます。ブロックされたリンクの再アクティブ化(1次リンク障害時)は、オペレーターの介入なしに自動的に実行されます。

この自動ネットワーク再構成により、ネットワーク・ユーザーに最大の稼働時間が提供されます。ただし、スパニングツリーアルゴリズムとプロトコルの概念は複雑で複雑なテーマであり、十分に調査および理解する必要があります。スパニングツリーが正しく設定されていないと、ネットワークのパフォーマンスが著しく低下する可能性があります。デフォルト値から変更を加える前に、以下をお読みください。

スイッチSTPは次の機能を実行します。

- スwitchング要素またはブリッジ要素の任意の組み合わせから単一のスパニングツリーを作成します。
- ユーザー指定のグループ内の単一スイッチに含まれるポートの任意の組み合わせから、複数のスパニングツリーを作成します。

- スパニング ツリーを自動的に再構成して、ツリー内の要素の障害、追加、または削除を補正します。
- Reconfiは、オペレーターの介入なしにスパニング・ツリーをギュリングします。

ブリッジプロトコルデータ ユニット

STP が安定したネットワーク トポロジに到達するには、次の情報が使用されます。

- 一意のスイッチ識別子
- 各スイッチポートに関連付けられたルートへのパス コスト
- ポート識別子

STP は、ブリッジプロトコルデータユニット(BPDU)を使用してネットワーク上のスイッチ間で通信します。

各 BPDU には、次の情報が含まれています。

- 送信スイッチが現在考えているスイッチの一意の識別子がルート スイッチです。
- 送信ポートからルートへのパス コスト。
- 送信ポートのポート識別子。

スイッチは BPDU を送信して、スパニングツリー トポロジを通信および構築します。パケットが送信される LAN に接続されているすべてのスイッチは BPDU を受信します。BPDU はスイッチによって直接転送されませんが、受信側スイッチはフレーム内のインフォメーションを使用して BPDU を計算し、トポロジが変更されると BPDU 伝送を開始します。

BPDU を介したスイッチ間の通信は、次のようになります。

- 1つのスイッチがルートスイッチとして選択されます。
- ルート sw かゆみまでの最短距離は、スイッチごとに計算されます。
- 指定されたスイッチが選択されます。これは、パケットがルートに転送されるルート スイッチに最も近いスイッチです。
- 各スイッチのポートが選択されます。これは、swかゆみからルートスイッチへの最適なパスを提供するポートです。
- STP に含まれるポートが選択されます。

安定した STP トポロジの作成

ルート ポートを最速のリンクにします。すべてのスイッチで STP がデフォルト設定でイネーブルになっている場合、ネットワーク内で最も低い MAC アドレスを持つスイッチがルート スイッチになります。最適な switch の優先度を上げる(優先度番号を下げる)ことで、STP はルート スイッチとして最適なスイッチを選択することを余儀なくされます。

デフォルト・パラメーターを使用して STP を使用可能にした場合、スイッチド・ネットワーク内のソース・ステーションと宛先ステーション間のパスは理想的ではない場合があります。たとえば、現在のルート ポートよりも大きい番号のポートに高速リンクを接続すると、ルート ポートが変更される可能性があります。

STP ポートの状態

BPDUは、ネットワークを通過するのに時間がかかります。この伝播遅延により、mをブロッキングステートから転送状態に直接移行したポートが一時データ ループを作成するトポロジの変更が発生する可能性があります。ポートは、パケットの転送を開始する前に、新しいネットワーク トポロジ情報がネットワーク全体に伝達されるのを待つ必要があります。また、古いトポロジに基づいて転送された f パケットまたは BPDU パケットが期限切れになるまで、パケットの有効

期間が切れるのを待つ必要があります。転送遅延タイマーは、トポロジの変更後にネットワークトポロジを安定させるために使用されます。さらに、STPは、トポロジの変更後に安定したネットワークトポロジが作成されるように、ポートが遷移する必要がある一連の状態を指定します。

STP が存在するスイッチの各ポートは、次の 5 つの状態のいずれかになります。

- **ブロッキング** – ポートはフロウm 転送または受信パケットをブロックされます。
- **リスン**: ポートは、ポートがブロッキング ステートに戻るようにポートに指示する BPDU パケットの受信を待機しています。
- **ラーニング** – ポートは転送データベースにアドレスを追加していますが、まだパケットを転送していません。
- **フォーワー・ディング** – ポートはパケットを転送しています。
- **Disabled** – ポートはネットワーク管理メッセージにのみ応答し、最初にブロッキング状態に戻る必要があります。

ポートは、次のようにある状態から別の状態に遷移します。

- 初期化(スイッチブート)からブロッキングへ。
- ブロッキングからリスニング、または無効にします。
- リスニングから学習、障害者まで。
- 学習から転送、または無効へ。
- 転送から無効へ。
- 無効からブロッキングへ。

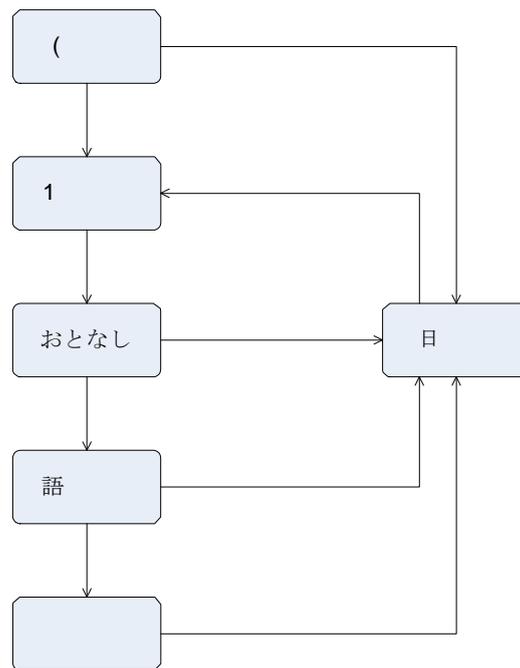


図 4-8-1: STP ポート状態の遷移

管理ソフトウェアを使用して、各ポートの状態を変更できます。STP をイネーブルにすると、ネットワーク内のすべてのスイッチのすべてのポートがブロッキングステートを通過し、電源投入時にリスンと学習の状態を遷移します。適切に設定されている場合、each ポートはフォーワーディングステートまたはブロッキングステートに安定します。パケット (BPDU を除く) は、そのポートのフォーワーディング ステートが有効になるまで、STP 対応ポートから転送または受信されません。

4.8.2 STPの図

ループ内で接続された3つのスイッチの簡単な図を次の図に示します。この例では、STP アシスタンスが適用されない場合に、いくつかの主要なネットワークの問題を予測できます。

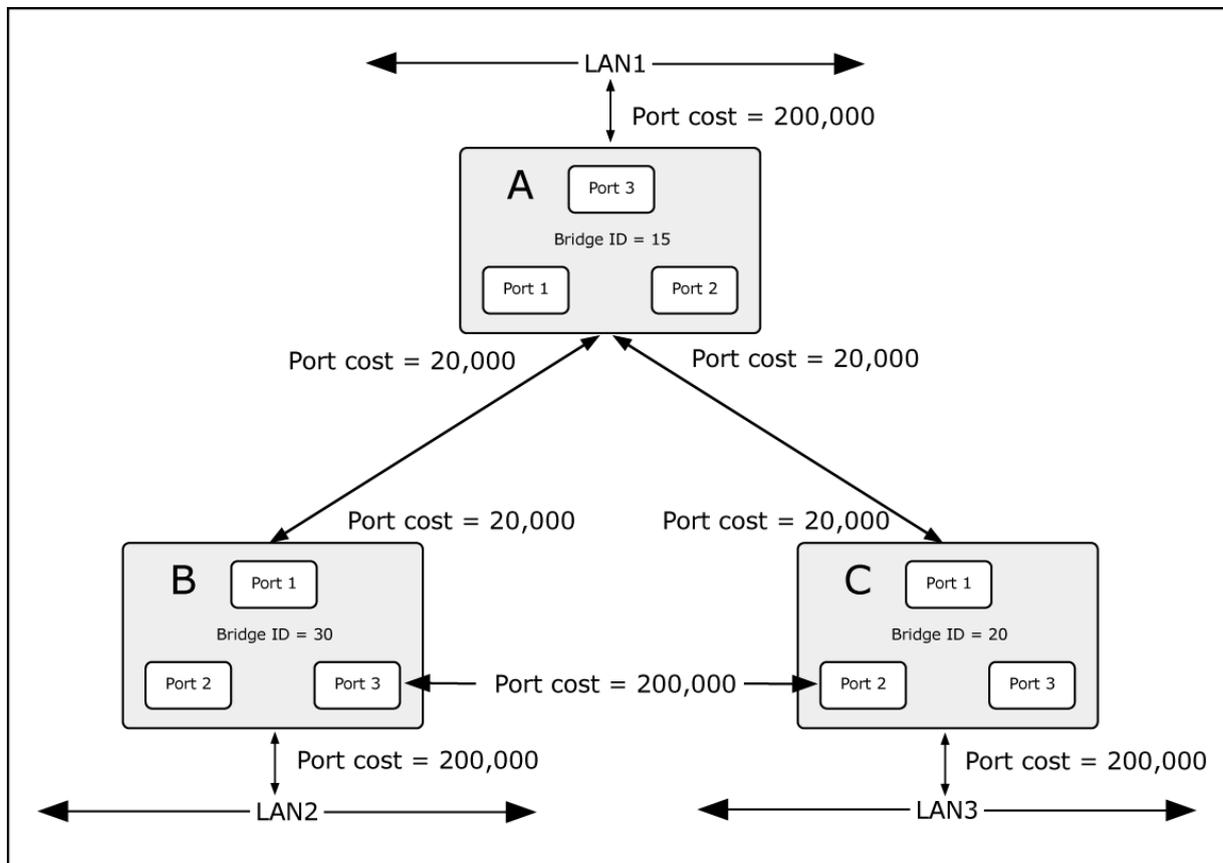


図 4-8-2: STA ルールを適用する前に

スイッチ A がスイッチ B にパケットをブロードキャストする場合、スイッチ B はそれをスイッチ C にブロードキャストし、スイッチ C はそれをブロードキャストしてスイッチ A などに戻します。ブロードキャスト パケットはループ内で無期限に渡され、ネットワーク障害が発生する可能性があります。この例では、STP はスイッチ B と C の間の接続をブロックしてループを解除します。特定の接続をブロックする決定は、最新のブリッジおよびポート設定の STP 計算に基づきます。

スイッチ A がスイッチ C にパケットをキャストする場合、スイッチ C はポート 2 でパケットをドロップし、ブロードキャストはそこで終了します。デフォルト以外の値を使用した STP のセットアップは複雑になる可能性があります。したがって、デフォルトの工場出荷時の設定を維持し、STP はルートブリッジ/ポートとブロックループ接続を自動的に割り当てます。ただし、プライオリティ設定を使用してルートブリッジとして特定のスイッチを選択する STP に影響を与えたり、ポートプライオリティとポートコスト設定を使用してブロックする特定のポートを選択するように STP に影響を与えたりすることは、比較的簡単です。

この例では、デフォルトの STP 値のみが使用されます。

ブリッジ ID が最も低いスイッチ(スイッチ C)がルートブリッジに選択され、スイッチ B と C の間に高いポートコスト

を与えるためにポートが選択されました。スイッチ A の 2 つの(オプション)ギガビット ポート(デフォルト ポート コスト = 20,000)は、スイッチ B と C の両方の 1 つの(オプション)ギガビット ポートに接続されます。スイッチ B と C 間の冗長リンクは、100 Mbps ファスト イーサネット リンクとして意図的に選択されます(デフォルトのポート コスト = 200,000)。ギガビット ポートを使用できますが、スイッチ B とスイッチ C の間のリンクがブロックされたリンクになるように、ポート コストをデフォルトから増やす必要があります。

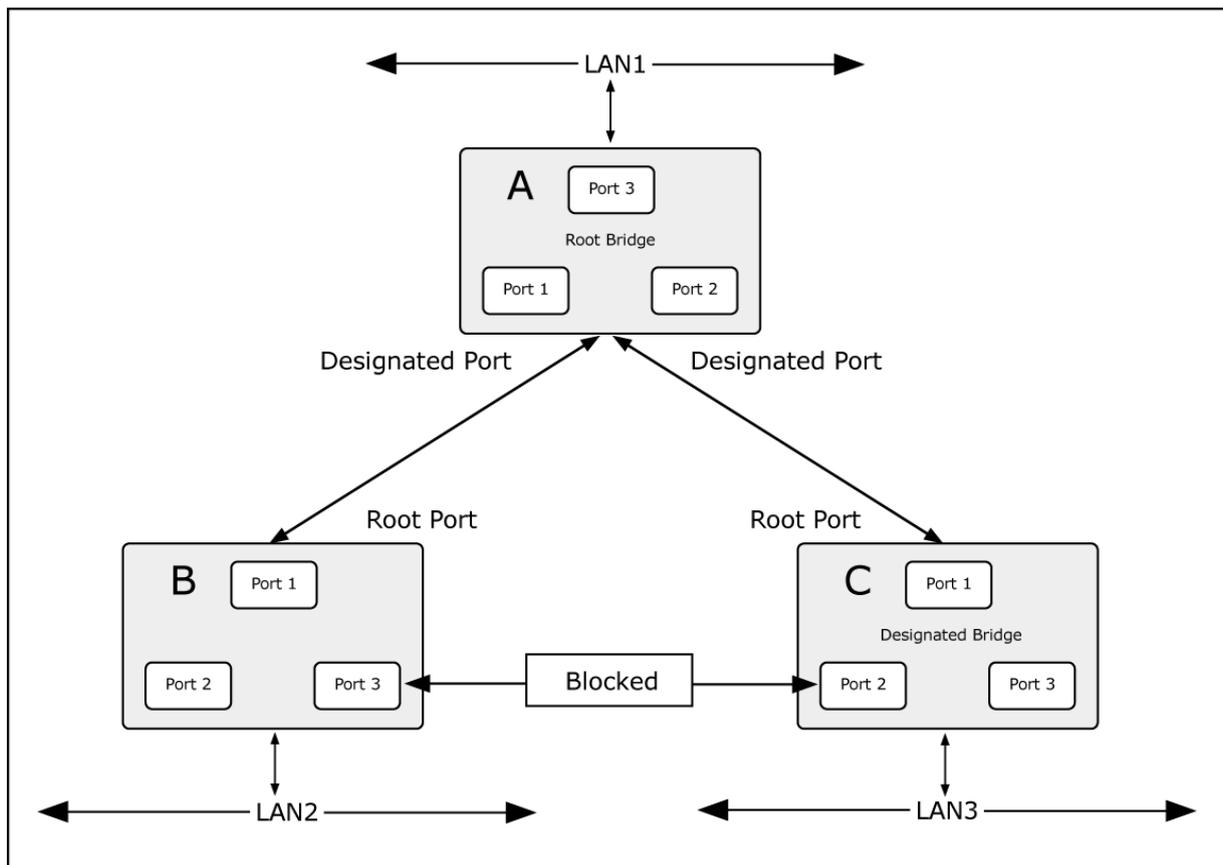


図 4-8-3: STA ルールの適用後

4.8.3 STPパラメータ

STP 操作レベル

スイッチでは、スイッチ レベルとポート レベルの 2 つの動作レベルが可能です。スイッチ レベルは、1 つ以上のスイッチ間のリンクで構成されるスパニング ツリーを形成します。ポート レベルは、1 つ以上のポートのグループで構成されるスパニング ツリーを構築します。STP は、両方のレベルでほとんど同じ方法で動作します。



Note

スイッチ レベルでは、STP は各スイッチのブリッジ識別子を計算し、ルート橋と指定橋。ポート レベルでは、STP はルート ポートと指定ポートを設定します。

スイッチ レベルのユーザ設定可能な STP パラメータを次に示します。

パラメーター	説明	既定値
ブリッジ識別子 (ユーザが構成できません) 以下の優先度を設定する場合を除く)	ユーザ設定の優先順位とスイッチの MAC アドレスの組み合わせ。 ブリッジ識別子は、16 ビットプライオリティと 48 ビットイーサネット MAC の 2	32768 + MAC

	つの部分で構成されます。 アドレス 32768 + MAC。	
--	-----------------------------------	--

優先順位	各スイッチの相対的な優先順位 – 数値が小さいほど、優先順位が高くなり、特定のスイッチが次のように選択される可能性が高くなります。 ルートブリッジ。	32768
こんにちは時間	のブロードキャスト間の時間の長さ スイッチによる hello メッセージ。	2秒
最大経過時間タイマー	ポートの受信 BPDU の経過時間を測定し、その経過時間が 最大年齢タイマー。	20秒
転送遅延タイマー	ポートを ブロッキング状態。	15秒

ポートまたはポート グループ レベルのユーザ設定可能な STP パラメータを次に示します。

変数	説明	既定値
ポートの優先順位	それぞれの相対的な優先順位 port –数値が小さいほど、優先順位が高くなり、特定のポートがルートポートとして選択される可能性が高くなります。	128
ポートコスト	パスを評価するために STP が使用する値 – STP はパス コストを計算し、最小コストのパスをアクティブパスとして選択します。 パス。	200,000-100Mbps 高速イーサネット ポート 20,000 -1000Mbps ギガビットイーサネット ポート 0 - 自動

デフォルト スパニングツリー設定

機能	既定値
状態を有効にする	すべてのポートに対して STP が無効
ポートの優先順位	128
ポートコスト	0
ブリッジの優先順位	32,768



こんにちは時間は、最大よりも長くすることはできません。年齢。それ以外の場合は、構成エラーが発生します。



Observe the following formulas when setting the above parameters:

Max. Age _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

4.8.4 STP システム設定

このセクションでは、図 4-7-4の画面に従って、管理対象スイッチからの STP システム設定について説明します。

- ユーザはルートのスパニングツリー情報を表示できます。橋。
- ユーザーはSTP状態を変更できます。変更後、をク **使用** します。

図 4-8-4: STP システム設定インターフェイス

のページには、次のフィールドが含まれています。

何をする	おと
STP 以下:	●おとなしい、おとなしいお尻を分かって、おとな、sTPを取り込み、おとなとくおと
> 内のバージョン	スパニング ツリー プロトコル、元のスパニング ツリー プロトコル(STP、802.1d)、またはマルチ スパニング ツリー プロトコル(MSTP、802.1s)を指定するために使用される値。
優先度 (0 ~ 61440):	値が最も小さいスイッチの優先順位が最も高く、ルートとして選択されます。値が変更された場合、ユーザーはスイッチを再起動する必要があります。
最大年齢(6-40):	値は、プロトコル標準規則に従って 4096 の倍数である必要があります。スイッチがスパニングツリー プロトコル設定メッセージを受信せずに待機してから、再設定を試行する秒数。
こんにちは時間(1-10):	6 ~ 40 の値を入力します。STP の現在のステータスをチェックするために BPDU パケットを送信するスイッチを制御する時間。

転送遅延時間(4-30):

ポートがラピッド スパニングツリー プロトコルの学習とリッスン状態からフォワーディング ステートに変更するまでに待機する秒数。

4 ~ 30 の値を入力します。



Note

次に示すルールに従って、[最大経過時間]、[Hello Time]、および [転送遅延時間] を構成します。

$2 \times (\text{前方遅延時間値} - 1) > = \text{最大経過時間値} > = 2 \times (\text{Hello Time 値} + 1)$ 。



Note

スパニングツリー内の各スイッチは、設定方法に関係なく、ルートブリッジのHello Time、Forward Delay Time、および Max Age パラメータを採用します。

■ ルートブリッジ情報

このページでは、すべての STP ブリッジインスタンスのステータスの概要を示します。

表示されるテーブルには、各 STP ブリッジ インスタンスの行が含まれ、列には次の情報が表示されます。

Priority	32768
MAC Address	00:30:4F:26:20:D1
Root Path Cost	0
Root Port	PORT140
Maximum Age	20
Hello Time	2
Forward Delay	15

図 4-8-5: STP ブリッジステータスのスクリーンショット

このページには、次のフィールドが含まれています。

オブジェクト	説明
優先順位	ルートブリッジのブリッジ識別子。それは橋の優先順位から成り立っていて、ブリッジのベース MAC アドレス。
MAC アドレス	ルートブリッジのブリッジ識別子。それは橋の優先順位から成り立っていて、ブリッジのベース MAC アドレス。
ルート パスコスト	ルートブリッジの場合、これはゼロです。他のすべてのブリッジの場合は、ポートの合計です。 ルートブリッジへの最小コストパスのパス コスト。
ルート ポート	スイッチ ポートは現在ルートポートの役割を割り当てられています。
最大年齢	ルートブリッジの指定ルートへのパス コスト。
こんにちは時間	設定 BPDU の送信間隔の最小時間。
転送遅延	ルート ポートブリッジ転送遅延パラメータの派生値。

4.8.5 ポートの構成

この Web ページは、STP のポート設定インターフェイスを提供します。各ポートに高い優先順位または低い優先順位を割り当てることができます。スパニングツリー プロトコルは、フォワーディング ステートで優先度の高いポートを持ち、LAN にループがないことを確認するために他のポートをブロックします。

Spanning Tree

System Configuration	PerPort Configuration	Instance	Interface			
Configure Spanning Tree Port Parameters						
Port Number Port1 ▲ Port2 ▲ Port3 ▲ Port4 ▲ Port5 ▼	Path Cost (1-200000000) <input type="text" value="200000"/>	Priority (0 - 240; Default 128) <input type="text" value="128"/>	Admin Edge (Default NO) <input type="text" value="NO"/> ▼			
			Admin Non-STP (Default NO) <input type="text" value="NO"/> ▼			
			Admin P2P (Default AUTO) <input type="text" value="AUTO"/> ▼			
<input type="button" value="Apply"/> <input type="button" value="Help"/>						
STP Port Status						
PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P
Port1	200000	128	Disabled	NO	NO	NO
Port2	200000	128	Disabled	NO	NO	NO
Port3	200000	128	Disabled	NO	NO	NO
Port4	200000	128	Disabled	NO	NO	NO
Port5	200000	128	Disabled	NO	NO	NO
Port6	200000	128	Disabled	NO	NO	NO
Port7	200000	128	Disabled	NO	NO	NO
Port8	200000	128	Disabled	NO	NO	NO
Port9	20000	128	Forwarding	NO	NO	YES
Port10	2000000	128	Disabled	NO	NO	NO

図 4-8-6: STP ポート設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
パスコスト:	指定したポートで、この送信ブリッジから他のブリッジへのパスのコスト。 1 ~ 200,000,000 の数値を入力します。
優先順位:	優先度を最も低いものに設定して、ブロックするポートを決定します。 0 ~ 240 の数値を入力します。 優先順位の値は 16 の倍数でなければなりません。

管理者 P2P:

STP 内で可能な高速状態遷移は、関係するポートが正確に別のブリッジにのみ接続できるかどうか (つまり、ポイントツーポイント LAN セグメントによって提供される)、または 2 つ以上のブリッジに接続できるかどうか (つまり、共有メディア LANセグメントによって提供される) かに依存します。この機能を使用すると、リンクの P2P ステータスを管理上操作できます。

- **YES**は、ポートがポイントツーポイント リンクと見なされていることを意味します。
- **NO**は、ポートが共有リンクと見なされていることを意味します。
- **AUTO**は、リンク・タイプが 2 つのピア間の自動ネゴシエーションによって決定することを意味します。

管理エッジ:

エンドステーションに直接接続されているポートは、ネットワークにブリッジンググループを作成しません。ポートをエッジポートとして構成するには、ポートを"YES"状態に設定します。

管理者非 STP:

ポートには、STP の数学計算が含まれています。

- **YES**は STP 数学的計算を含みませんでした。
- **NO**には、STP マセマティック計算が含まれます。



Note

パス コスト "0" は、自動構成モードを示すために使用されます。短いパスコスト法を選択し、IEEE 8021w規格で推奨されるデフォルトのパスコストが65,535を超える場合、デフォルトは65,535に。

デフォルトでは、システムは各ポートで使用される速度とデュプレックス モードを自動的に検出し、次に示す値に従ってパス コストを設定します。

ポートの種類	IEEE 802.1D-1998	IEEE 802.1w-2001
イーサネット	50-60 200,000-20,000,000	00
ファストイーサネット	10-60 20,000-2,000,000	
ギガビットイーサネット	3-10 2,000-200,000	

表 4-8-1:推奨される STP パス コスト範囲

ポートの種類	リンクの種類	IEEE 802.1D-1998	IEEE 802.1w-2001
イーサネット	半二重全二	100	2,000,000
	重	95	1,999,999
	トランク	90	1,000,000
ファストイーサネット	半二重全二	19	200,000
	重	18	100,000
	トランク	15	50,000

ギガビットイーサネット	全二重	4	10,000
	トランク	3	5,000

表 4-8-2:推奨される STP パス コスト

4.8.6 インスタンス

このページでは、MST インスタンス構成を構成できます。

Spanning Tree

System Configuration
PerPort Configuration
Instance
Interface

Configure Spanning Tree Instance

Instance	Bridge Priority (0-61440)	Status	VLAN Range
Instance0	32768	Enable ▼	
Instance1			
Instance2			
Instance3			
Instance4			

STP Instance

Instance	Bridge Priority	Status	VLAN Range
Instance0	32768	Enable	1-4094
Instance1	32768	Disable	
Instance2	32768	Disable	
Instance3	32768	Disable	
Instance4	32768	Disable	
Instance5	32768	Disable	
Instance6	32768	Disable	
Instance7	32768	Disable	
Instance8	32768	Disable	
Instance9	32768	Disable	
Instance10	32768	Disable	
Instance11	32768	Disable	
Instance12	32768	Disable	
Instance13	32768	Disable	
Instance14	32768	Disable	
Instance15	32768	Disable	

図 4-8-6: STP ポート設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
インスタンス :	MSTI ID の割り当てを許可します。
ブリッジプライオリティ (0~61440):	MSTI ID の範囲は 1 ~ 15 です。 ブリッジの優先順位をコントロールします。数値が小さいと優先順位が高くなります。
ステータス :	MSTI ID の有効化または無効化を許可する

VLAN 範囲:	VLAN リストを特別な MSTI ID に割り当てることを許可します。
	VLAN リストの範囲は 1 ~ 4094 です。

4.8.7 インターフェイス

このページでは、MSTP ポートの優先順位とパス コストの構成を構成できます。

図 4-8-7: STP ポート設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
インスタンス :	[MSTI ID] を選択します。 MSTI ID の範囲は 1 ~ 15 です。
ポート番号:	[MSTI ID] を選択します。 ポート番号の範囲はポート 1 ポート 10 です。
ポートプライオリティ (0~240):	ポートの優先順位を制御します。これは、同じポート コストを持つポートの優先順位を制御するために使用できます。 有効な値の範囲は 0 ~ 240 です。 ポートによって発生するパス コストを制御します。
パスコスト(1~200000000):	[自動] 設定では、802.1D の推奨値を使用して、物理リンク速度によって必要に応じてパス コストが設定されます。特定の設定を使用して、ユーザー定義値を入力できます。 パス コストは、ネットワークのアクティブ なトポロジを確立するために wh を使用します。低いパス コスト ポートは、より高いパス コスト ポートを優先してフォワーディング ポートとして選択されます。 有効な値の範囲は 1 ~ 200000000 です。

4.9 DHCP リレーとオプション82

リレー エージェント情報オプション (Option82) は、クライアントが発信した DHCP パケットを DHCP サーバー (RFC 3046) に転送するときに、DHCP リレーエージェントによって挿入されます。[リレー エージェント情報] オプションを認識するサーバーは、この情報を使用して IP 追加の **ress** またはその他のパラメータ割り当てポリシーを実装できます。

DHCP リレーは、DHCP ブロードキャスト パケットを別のサブネット (RFC 1542) の DHCP サーバーに転送できます。したがって、DHCP サーバーは、すべてのサブネットに DHCP を展開する代わりに、複数のサブネットにまたがるクライアントに IP アドレスを提供できます。

DHCP リレーとオプション 82 の設定

DHCP オプション 82 を構成するには

1. グローバルオプション82機能を有効にする:DHCPオプション82を有効にする「有効」を選択します。
2. ポートオプション82機能を有効にする:特別なポートのOption82チェックボックスを選択します。
3. [DHCP ルーター ポート] を選択します。
4. [適用] をクリックします。

DHCP リレーを構成するには

5. グローバルリレー機能を有効にする:DHCPリレー有効「有効」を選択します。
6. ポートリレー機能を有効にする:DHCP「リレーIP」のIPアドレスを入力します。
7. DHCP サーバーは、サブネットがリレー IP と同じスコープの **list** からクライアントに IP アドレスを提供します。
8. [DHCP ルーター ポート] を選択します。
9. [適用] をクリックします。

DHCP Relay & Option 82

DHCP Option 82 Disable ▼		
DHCP Relay Disable ▼		
DHCP Option 82 Router Port		Port1 ▼
DHCP Opt.82 Port	Option	Relay IP
Port1	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port2	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port3	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port4	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port5	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port6	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port7	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port8	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port9	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>
Port10	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>

Apply Default Help

図 4-9-1: DHCP リレーとオプション 82

The page includes the following fields:

オブジェクト	説明
DHCP オプション 82	グローバル オプション 82 機能を有効にする
DHCP リレー	グローバル リレー機能を有効にする
DHCP オプション 82 ルーター ポート	DHCP サーバーへの接続に使用するルーター ポートを選択します。 ドメイン
DCHP Opt.82 ポート オプション	ポート 1 からポート 10 への接続を識別して DHCP オプション 82 を 設定する 選択したポートでポート オプション 82 機能を有効にします。
リレー IP	DHCP "リレー IP" の IP アドレスを入力します。

4.10 Lldp

リンク層探索プロトコル (LLDP) は、ローカルブロードキャストドメイン上の近隣デバイスに関する基本情報を検出するために使用されます。LLDP は、定期的なブロードキャストを使用して送信デバイスに関する情報をアドバタイズするレイヤ 2 プロトコルです。アドバタイズされた information は、IEEE 802.1ab 標準に従ってタイプ長の値 (TLV) 形式で表され、デバイスの識別、機能、構成設定などの詳細を含めることができます。LLDP は、検出した近隣ネットワークノードに関して収集された情報を格納および管理する方法も定義します。

4.10.1 LLDPの構成

このページを使用して LLDP パラメータを変更します。

図 4-10-1: LLDP 設定

このページには、次のフィールドが含まれています。

オブジェクト	説明
LLDP ステータス	LLDP を有効または無効にします。
LLDP こんにちは時間	LLDP こんにちはは時間の値を変更できます。伝送 LLDP 情報パケット間の時間間隔。値の範囲は 5 ~ 32768 です。 デフォルト値は 30 です。
LLDP ホールドタイム	LLDP 保留時間の値を変更できます。(ホールドタイム * hello time) は LLDP 情報パケットの TTL 時間です。値の範囲は 2 ~ 10 です。 デフォルト値は 4 です。

4.10.2 PerPortの構成

This page allows the user to inspect and configure the current LLDP port settings.

LLDP Configuration

LLDP Configuration
PerPort Configuration

Configure Port Status

Port Number	Port Status
<div style="border: 1px solid #ccc; padding: 2px;"> Port1 ▲ Port2 ≡ Port3 Port4 Port5 ▼ </div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> Tx_only ▼ </div>

Port Status

PortNum	Status
Port1	Tx_and_Rx
Port2	Tx_and_Rx
Port3	Tx_and_Rx
Port4	Tx_and_Rx

図 4-10-2:ポート設定ごとの LLDP

このページには、次のフィールドが含まれています。

オブジェクト	説明
LLDP ステータス	LLDP を有効または無効にします。
LLDP こんにちは時間	LLDP こんにちは時間の値を変更できます。伝送 LLDP 情報パケット間の時間間隔。値の範囲は 5 ~ 32768 です。 デフォルト値は 30 です。
LLDP ホールドタイム	LLDP 保留時間の値を変更できます。(ホールドタイム * hello time) は TTL 時間 in LLDP 情報パケットです。値の範囲は 2 から 10 に変更します。デフォルト値は 4 です。
ポートの状態	LLDP ポートの状態をTx_only/Rx_only/Tx_and_Rx/無効に変更できます。 Tx_only: LLDP はポートのパケットのみを送信します。 Rx_only: LLDP はポートのパケットのみを受信します。Tx_and_Rx: LLDP はポートのパケットを送受信します。 無効: LLDP はポートのパケットを送受信しません。

4.11 アクセス制御リスト

アクセス制御リスト (ACL) は、特権の分離を強制するために使用されるコンピュータ セキュリティの概念です。これは、要求を行うプロセスの特定の側面 (主にプロセスのユーザー identifier) に応じて、特定のオブジェクトに対する適切なアクセス権を決定する手段です。アクセス制御リスト (ACL) は、リソースへのアクセスを許可または拒否されるシステム エンティティの ID を一覧表示することによって、システムリソースのアクセス制御を実装するメカニズムです。次の画面が表示されます。

パケットは、IPv4 または非 IPv4 を含む ACL ルールによって転送またはドロップできます。管理対象スイッチは、送信元と宛先の IP アドレス、プロトコルなどによってインデックス付けされたパケット フラグメントのテーブルを維持することで、パケットをブロックするために使用できます。

※パケットタイプ/バインディングは、IPv4 または非IPv4のACLにセレクトドすることができます。

Access Control List					
Group Id	<input type="text" value=""/> (1~220)				
Action	Permit <input type="checkbox"/> QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage)				
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> VID <input type="text" value="1"/> (1~4094; Any means Vid=0 if uses binding)				
Packet Type / Binding	<input checked="" type="radio"/> IPv4		<input type="radio"/> Non-IPv4		<input type="radio"/> Binding
Src IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/> Mask <input type="text" value="255.255.255.255"/>	Ether Type	<input type="text" value="Any"/> Type# <input type="text" value=""/>	MAC Address	<input type="text" value="00:11:22:33:44:55"/>
Dst IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/> Mask <input type="text" value="255.255.255.255"/>	IP Address	<input type="text" value="0.0.0.0"/>		
IP Fragment	<input type="checkbox"/> Uncheck			Port Id	<input type="text" value="1"/> (1~10)
L4 Protocol	<input checked="" type="radio"/> Any <input type="radio"/> TCP <input type="radio"/> UDP	Protocol#:	Priority#	<input type="text" value="7"/>	
	Port#:		PortID#	<input type="text" value="0"/>	Value (Hex, 0~1F)
	Port#:		Protocol#	<input type="text" value="0"/>	Mask (Hex, 0~FF)
	Port#:		Source Port#	<input type="text" value="0"/>	Mask (Hex, 0~FFFF)
			Destination Port#	<input type="text" value="0"/>	Mask (Hex, 0~FFFF)
Port Id	<input type="text" value="0"/> (1~10, 0: don't care)				
Current List	<input type="text"/>				

図 4-11-1: アクセス制御リスト (ACL) Web ページ画面

このページには、次のフィールドが含まれています。

■ IPv4 ACL

オブジェクト	説明	デフォルト・ヴァ ォーレ
グループ ID	1 ~ 220 (最大 220 ACL グループ)。	
アクション	許可/拒否。 <ul style="list-style-type: none"> ■ 許可: パケットクロススイッチを許可します。 ■ 拒否: パケットをドロップします。 	許可
Vlan	任意/VID。 <ul style="list-style-type: none"> ■ 任意: 任意の VLAN ID。 ■ VID: 1~4094.特定の VLAN ID。 	任意
パケットの種類	IPv4/非 IPv4/バインディング <ul style="list-style-type: none"> ■ IPv4: IPv4 パケット フィールドを設定します。 ■ 非 IPv4: 非 IPv4 パケット フィールドを設定します。 ■ バインド: バインドエントリを設定します。 	IPv4
Src IP アドレス	パケット・タイプが IPv4 の場合は、このフィールドを設定します。Any/IP とマスク <ul style="list-style-type: none"> ■ 任意: 任意の IPアドレス。 ■ IP:特定の IP アドレス 。マスク: ****.*.*.*.* * は 0 ~ 9 の数字を表し、 は 0 ~ 255 の範囲です。 注: これはサブネット マスクではありません。	任意
Dst IP アドレス	パケット・タイプが IPv4 の場合は、このフィールドを設定します。Any/IP とマスク <ul style="list-style-type: none"> ■ 任意: 任意の IPアドレス。 ■ IP:特定の IP アドレス 。マスク: ****.*.*.*.* * は 0 ~ 9 の数字を表し、 は 0 ~ 255 の範囲です。	任意
IP フラグメント	パケット・タイプが IPv4 の場合は、このフィールドを設定します。チェックの解除/チェック <ul style="list-style-type: none"> ■ オフ: IP フラグメントフィールドをチェックしません。 ■ チェック: IP フラグメント フィールドを確認します。 	オフ
L4 プロトコル	パケット・タイプが IPv4 の場合は、このフィールドを設定します。 Any/ICMP(1)/IGMP(2)/TCP(6)/UDP(17)	任意

プロトコル

パケット・タイプが IPv4 の場合は、このフィールドを

設定します。0~255。

[L4 プロトコル] フィールドでプロトコルが見つからない場合は、直接
数。

Tcp	パケット・タイプが IPv4 の場合は、このフィールドを設定します。 Any/FTP(21)/HTTP(80)	任意
ポート	パケット・タイプが IPv4 の場合は、このフィールドを設定します。0~65535 TCP ポートが TCP フィールドで見つからない場合は、番号を直接割り当てることができます。	
Udp	パケット・タイプが IPv4 の場合は、このフィールドを設定します。 Any/DHCP(67)/TFTP(69)/ネットバイオス(137)	任意
ポート	パケット・タイプが IPv4 の場合は、このフィールドを設定します。0~65535 UDP ポートがUDP フィールドで見つからない場合は、直接数。	
ポート ID	送信元ポート ID は、1 ~ 10 から 0 で、気にし 0 ません。	
現在のリスト	ACL およびバインディング グループを作成します。	

■ 非 IPv4 ACL

※パケットタイプ/バインドボックスでは※非IPv4を選択してください

オブジェクト	説明	デフォルト・ヴァー
グループ ID	1 ~ 220 (最大 220ACL グループ)	
アクション	許可/拒否。 <ul style="list-style-type: none"> ■ 許可: パケットクロススイッチを許可します。 ■ 拒否: パケットをドロップします。 	許可
Vlan	任意/VID。 <ul style="list-style-type: none"> ■ 任意: 任意の VLAN ID。 ■ VID: 1~4094,特定の VLAN ID。 	任意
パケットの種類	IPv4/非 IPv4/バインディング <ul style="list-style-type: none"> ■ IPv4: IPv4 パケット フィールドを設定します。 ■ 非 IPv4: 非 IPv4 パケット フィールドを設定します。 ■ バインド: バインドエントリを設定します。 	IPv4
エーテルタイプ	パケット・タイプが非 IPv4 の場合は、このフィールドを設定します。 任意の/ARP(0x0806)/IPX(0x8137)	任意

型	パケット・タイプが非 IPv4 の場合は、このフィールドを設定します。0~0xFFFF エーテルタイプが[エーテルタイプ]フィールドに見つからない場合は、 割り当てられた番号。
現在のリスト	ACL およびバインディング グループを作成します。

■ バインディング

特定の IP アドレスと MAC アドレスを持つデバイスがネットワークを使用できるようにします。特定の IP アドレス、MAC アドレス、VLAN ID、ポート ID をバインドするように設定し、すべての条件が一致する場合はデバイスがスイッチを越えることができます。

バインド関数を使用します。最初に次のページで有効にする必要

があります。インテ※[パケットの種類/バインド] ボックスを選択

何をする	おと	(設定)・レ
グループ番号	1 ~ 220 (220 ACL グループ)	
お付け	場合は、必要に日を与) <ul style="list-style-type: none"> ■ : 時間一時を起き込む。 ■ 以下:. 	一時は一時
Vlan	おとなしい/VID... <ul style="list-style-type: none"> ■ おとな: VLANid。 ■ VID:1~4094。特定の VLAN ID。 	任意
パケットの種類	IPv4/非 IPv4 / バインディング <ul style="list-style-type: none"> ■ IPv4: IPv4 パケット フィールドを設定します。 ■ 非 IPv4: 非 IPv4 パケット フィールドを設定します。 ■ バインド: バインドエントリを設定します。 	IPv4
MAC アドレス	**.***.***.***.*** <p>*は0~9およびA~Fからの数字を表し、 は 0 ~ FF の範囲です。</p>	00:11:22:33:44:55
IP アドレス	***.***.***.*** <p>* は 0 ~ 9 の数字を表し、 は 0 ~ 255 の範囲です。</p>	0.0.0.0
ポート ID	送信元ポート ID(1~ 10)。 1	

4.12 セキュリティマネージャ

この Web ページには、スイッチ管理アクセス レベルのユーザ設定が表示されます。



図 4-12-1: ユーザー構成インターフェイスのスクリーンショット

このページには、次のフィールドが含まれています。

オブジェクト	説明
名 :	管理対象スイッチのユーザ名を表示します。
アクセス レベル:	管理対象スイッチのアクセス レベルを表示します。
編集 :	現在の特定のユーザー設定の編集を指定します。
新しいユーザーの追加:	管理対象スイッチの新しいユーザー設定の追加を提供する



図 4-12-2: 新しいユーザー構成インターフェイスのスクリーンシ

ョットの追加 このページには、次のフィールドが含まれています。

オブジェクト	説明
ユーザー名:	管理対象スイッチのユーザ名を割り当てます。
アクセス レベル:	管理対象スイッチのアクセス レベルを割り当てます。使用可能なオプションは次のとおりです。 "管理者"、"オペレータ"、および "ビューア"。既定値は "管理者" です。
パスワードの割り当て/変更:	管理対象スイッチのパスワードを割り当てます。
パスワードの再確認:	設定を確認するためにもう一度パスワードを入力します。
適用 :	を使用して を使用します。

4.13 MACリミット

MAC 制限を使用すると、ユーザーは MAC アドレス テーブルに格納する MAC アドレスの最大数を設定できます。

MAC アドレス テーブルに格納するように選択された MAC アドレスは、先入れ先保存ポリシーの結果です。MAC アドレスが MAC アドレス テーブルに格納されると、タイムアウトになるまで残ります。「開口部」が使用可能な場合、スイッチはその開口部に表示される最初の新しい MAC アドレスを保存します。MAC アドレス テーブルにない MAC アドレスからのパケットはすべてブロックする必要があります。

4.13.1 MAC リミット設定

レイヤ 2 MAC 制限機能は、セキュリティ管理のためにポート単位で設定できます。ポートが MAC 制限モードの場合、ポートはアドレス学習の許可なしに「ロック」されます。アドレス テーブルに存在する送信元 MAC already を持つ着信パケットのみを通常どおり転送できます。ユーザーは、新しい MAC アドレスの学習からポートを無効にできます。

The screenshot shows a web-based configuration page for 'MAC Limit'. The main heading is 'MAC Limit' and the sub-heading is 'Configure MAC Limit'. A table-like interface contains the following elements:

- A checkbox labeled 'MAC Limit' which is checked.
- A section labeled 'Port Number' with a list of ports: Port1, Port2, Port3, Port4, Port5. Port1 is selected.
- A text input field next to the port list containing the number '15'. Above this field is the label 'Limit (1-64, 0 to turn off MAC limit)'.
- At the bottom of the form are two buttons: 'Apply' and 'Help'.

図 4-13-1: MAC リミット - MAC リミットの設定

このページには、次のフィールドが含まれています。

オブジェクト	説明
MAC リミット	管理対象スイッチの MAC 制限機能を有効または無効にします。
ポート番号	ポート 1 からポート 8 を示します。
制限	学習するポートごとの MAC アドレスの最大数(1 ~64、0 ~ このポートの MAC 制限機能を無効にします)。



MAC リミットは、VC-820M のポート 1 からポート 8 への高速イーサネット ポートでのみ機能します。

4.13.2 MAC リミット ポートステータス

次の表に、各ポートの現在の MAC 制限ステータスを示します。

MAC Limit Port Status	
Port Number	Limit
Port1	off
Port2	off
Port3	off
Port4	off
Port5	off
Port6	off
Port7	off
Port8	off

図 4-13-2: MAC リミット – MAC リミット ポートステータス

このページには、次のフィールドが含まれています。

オブジェクト	説明
ポート番号	ポート 1 からポート 8 を示します。
制限	各ポートの現在の MAC リミット設定とステータスを表示します。

4.14 802.1x構成

802.1x は IEEE 認証仕様で、認証サーバによって検証されるユーザ名やパスワード(RADIUS サーバなど)などの権限が提供されるまで、クライアントがワイヤレス アクセス ポイントまたは有線スイッチにアクセスできないようにします。

4.14.1 IEEE 802.1x ポートベース認証について

IEEE 802.1x 標準では、クライアント サーバ ーベースのアクセス制御および認証プロトコルが定義されており、承認されていないクライアントがパブリックにアクセス可能なポートを介して LAN に接続できないように制限します。起テナレーションサーバは、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチ ポートに接続されている各クライアントを認証します。

クライアントが認証されるまで、802.1x アクセス制御では、クライアントが接続されているポートを介した LAN (EAPOL) トラフィックを介した拡張認証プロトコルのみが許可されます。認証が成功すると、通常のトラフィックはポートを通過できます。

ここでは、次の概念について説明します。

- デバイスの役割
- 認証の開始とメッセージ交換
- 承認済みおよび承認されていない状態のポート

■ デバイスの役割

802.1x ポートベース認証では、ネットワーク内のデバイスは次に示すように特定の役割を持ちます。

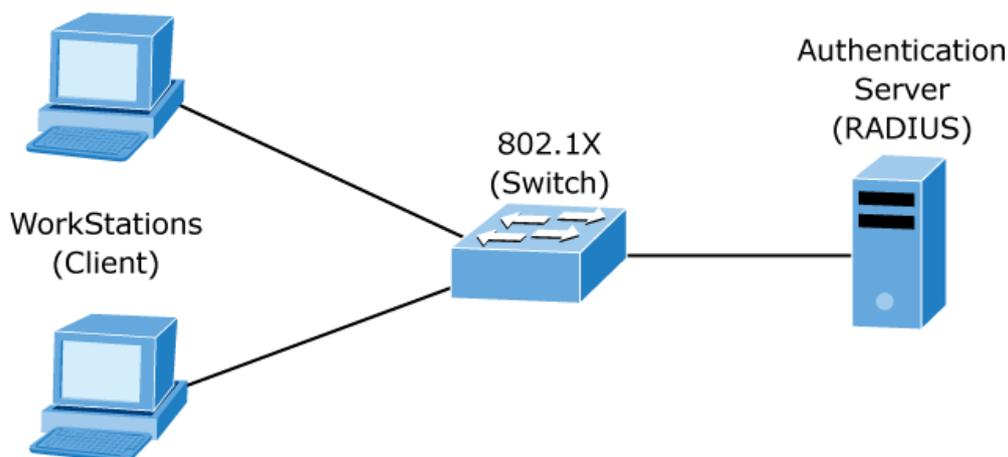


図 4-14-1: 802.1x デバイスの役割

クライアント:LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス(ワークステーション)。ワークステーションは、Microsoft Windows XP オペレーティング システムで提供されているような 802.1x 準拠のクライアントソフトウェアを実行している必要があります。(クライアントは IEEE 802.1x のサブリカントです。仕様)

- **Authentication server**—performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with **Extensible Authentication**

プロトコル(EAP)拡張機能は、サポートされている唯一の認証サーバであり、Cisco セキュア アクセス コントロールサーババージョン 3.0で使用できます。RADIUSは、RADIUS サーバーと 1 つ以上の RADIUS クライアントの間でセキュリティで保護された認証情報が交換されるクライアント/サーバーモデルで動作します。

- **Switch (802.1x device)**—controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

■ 認証の開始とメッセージ交換

スイッチまたはクライアントは認証を開始できます。**dot1x ポート制御自動**インターフェイス コンフィギュレーション コマンドを使用してポートで認証を有効にする場合、スイッチはポート リンク状態がダウンからアップに遷移することを判断したときに認証を開始する必要があります。次に、EAP 要求/ID フレームをクライアントに送信してID をリクエストします(通常、スイッチは初期 ID/要求フレームを送信し、その後に認証情報の要求を1つ以上送信します)。フレームを受信すると、クライアントは EAP 応答/ID フレームで応答します。

ただし、ブートアップ中にクライアントがスイッチから EAP 要求/ID フレームを受信しない場合、クライアントは EAPOL 開始フレームを送信して認証を開始できます。



802.1x がネットワーク アクセス デバイスで有効になっていないかサポートされていない場合、クライアントからの EAPOL フレームはすべてドロップされます。クライアントが認証を 3 回 試行しても EAP 要求/ID フレームを受信しない場合、クライアントはポートが許可された状態であるかのようにフレームを送信します。のポート 承認された状態は、クライアントが正常に認証されたことを効果的に意味します。

クライアントが ID を提供すると、スイッチは仲介者としての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバの間で EAP フレームを渡します。認証が成功すると、スイッチ ポートは承認されます。

EAP フレームの具体的な交換は、使用する認証方法によって異なります。次の図は、RADIUS サーバーでワンタイム パスワード (OTP) 認証方法を使用してクライアントによって開始されたメッセージ交換を示しています。

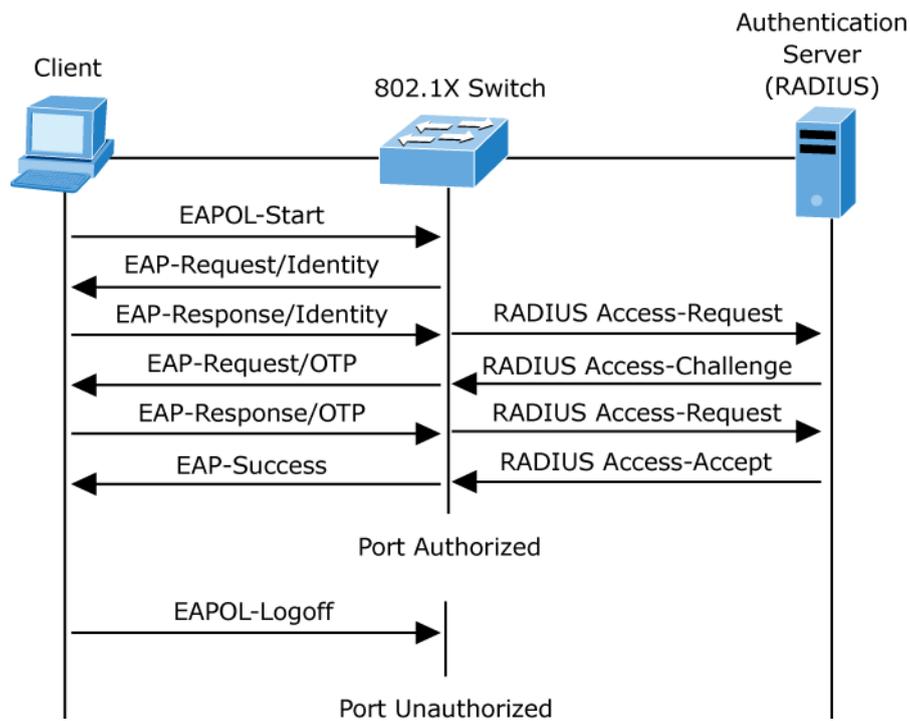


図 4-14-2: EAP メッセージ交換

■ 承認済みおよび承認されていない状態のポート

スイッチ ポートの状態によって、クライアントにネットワークへのアクセスが許可されるかどうかが決まります。ポートは許可されていない状態で開始されます。この状態では、ポートは 802.1x プロトコル パケットを除くすべての入り口および出力トラフィックを許可します。クライアントが正常に認証されると、ポートは承認済み状態に移行し、クライアントのすべてのトラフィックが正常に流れるようになります。

802.1x をサポートしないクライアントが許可されていない 802.1x ポートに接続されている場合、スイッチはクライアントの IDENTITY を要求します。この状況では、クライアントは要求に応答せず、ポートは承認されていない状態のままになり、クライアントはネットワークへのアクセスを許可されません。

これに対し、802.1x 対応クライアントが 802.1x プロトコルを実行していないポートに接続すると、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答が受信されない場合、クライアントは一定の回数だけ要求を送信します。応答が受信されないため、クライアントはポートが許可された状態であるかのようにフレームの送信を開始します。

クライアントが正常に認証された場合 (認証サーバーから Accept フレームを受信した場合)、ポート状態は許可され、認証されたクライアントからのすべてのフレームがポートを介して許可されます。認証に失敗した場合、ポートは許可されていない状態のままですが、認証は再試行できます。認証サーバーに到達できない場合、switch は要求を再送信できます。指定した回数の試行後にサーバーから応答を受信しなかった場合、認証は失敗し、ネットワーク アクセスは許可されません。

クライアントがログオフすると、EAPOL-logoff メッセージが送信され、スイッチ ポートが不正な状態に移行します。

ポートのリンク状態が最大からダウンに遷移する場合、または EAPOL ログオフ フレームを受信した場合、ポートは許可されていない状態に戻ります。

4.14.2 システム構成

802.1x は IEEE802 LAN inf rastructures の物理アクセス特性を利用して、ポイントツーポイント接続特性を持つ LAN ポートに接続されているデバイスを認証および承認する手段を提供し、認証および認可プロセスが失敗した場合にそのポートへのアクセスを防止します。

To enable 802.1x, from **System \ System Information \ Misc Config** then you still to fill in the authentication server information :

図 4-14-3:システム情報\その他の構成\802.1x プロトコル

IEEE 802.1x 機能を有効にした後、この関数のパラメータを設定できます。

Configure 802.1x Parameters	
Radius Server IP:	192.168.0.99
Server Port:	1812
Accounting Port:	1813
Shared Key:	
NAS,Identifier:	NAS_L2_SWITCH

図 4-14-4: 802.1x システム設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
IEEE 802.1x プロトコル:	802.1x プロトコルを有効または無効にします。
RADIUS サーバー IP:	RADIUS サーバーの IP アドレスを割り当てます。
サーバー ポート:	認証要求の UDP 宛先ポートを指定された RADIUS に設定するサーバー。
アカウンティング ポート:	アカウンティング要求の UDP 宛先ポートを指定された RADIUS に設定するサーバー。
共有キー:	指定した RADIUS サーバーでの認証セッション中に使用する暗号化キーを設定します。このキーは RADIUS で使用される暗号化キーと一致する必要があります。 サーバー。
NAS、識別子:	RADIUS クライアントの識別子を設定します。

4.14.3 802.1xポート設定

このページでは、特定のポートを選択し、承認状態を構成できます。この状態は、承認なし、承認の強制、承認の強制、および承認を提供します。

802.1X Configuration

System Configuration **PerPort Configuration** Misc Configuration

Configure 802.1X Per Port State

Port Number	Port State
Port1 ▲ Port2 ▢ Port3 ▢ Port4 ▢ Port5 ▼	Au ▼

Apply Help

Port Status

PortNum	State
Port1	No
Port2	No
Port3	No
Port4	No

図 4-14-5:ポート設定インターフェイスあたり 802.1x

このページには、次のフィールドが含まれています。

オブジェクト	説明
Fu (強制無許可)	指定されたポートは、許可されていない状態で保持される必要があります。
Fa (強制承認済み)	指定されたポートは、許可された状態で保持される必要があります。
オー (承認)	指定されたポートは、サブリカントと認証サーバー。
いいえ	指定されたポートは、802.1x プロトコルに準拠せずに動作します。

4.14.4 その他の構成

このページでは、802.1x 標準の既定の構成を変更できます。

802.1x Configuration

System Configuration PerPort Configuration **Misc Configuration**

Configure 802.1x misc configuration

Quiet period:	60
Tx period:	15
Supplicant timeout:	30
Server timeout:	30
Max requests:	2
Reauth period:	3600

Apply Help

図 4-14-6: 802.1x その他の設定インターフェイス

このページには、次のフィールドが含まれています。

オブジェクト	説明
静かな期間:	サブリカントの取得を試みない期間を定義するために使用します。 デフォルトの時間は 60 秒です。
TX 期間:	認証セッション中にポートが次の EAPOL PDU の再送信を待機する期間を設定します。 デフォルト値は 30 秒です。
サブリカント タイムアウト:	スイッチがEAP 要求に対するサブリカント応答を待機する期間を設定します。 デフォルト値は 30 秒です。
サーバーのタイムアウト:	スイッチが認証要求に対するサーバ応答を待機する時間を設定します。 デフォルト値は 30 秒です。
最大要求数:	認証が失敗して認証セッションが終了するまでにタイムアウトする必要がある認証の数を設定します。 デフォルト値は 2 回です。
認証期間:	接続されているクライアントを再認証する必要がある期間を設定します。 デフォルト値は 3600 秒です。

4.15 QoS構成

4.15.1 QoSについて

サービスの品質 (QoS)は、ネットワーク トラフィックの制御を確立できる高度なトラフィックの優先順位付け機能です。QoS を使用すると、マルチメディア、ビデオ、プロトコル固有、タイムクリティカル、ファイルバックアップ トラフィックなど、さまざまな種類のトラフィックにさまざまなレベルのネットワーク サービスを割り当てることができます。

QoS は帯域幅の制限、遅延、損失、ジッタを削減します。また、データの配信に対する信頼性が向上し、ネットワーク全体で特定のアプリケーションに優先順位を付けることができます。選択したアプリケーションとトラフィックの種類を処理するためにスイッチを使用する方法を正確に定義できます。

システムで QoS を使用すると、次のことができます。

- 次の方法で、さまざまなネットワーク トラフィックを制御します。
- パケット属性に基づいてトラフィックを分類する。
- トラフィックに優先順位を割り当てる (たとえば、より高い優先順位をタイムクリティカルなアプリケーションやビジネスクリティカルなアプリケーションに設定する場合など)。
- トラフィック フィルタリングによるセキュリティ ポリシーの適用。
- 遅延とジッタを最小限に抑えることで、ビデオ会議やボイス オーバー IP などのマルチメディア アプリケーションに予測可能なスループットを提供します。
- 特定のタイプのトラフィックのパフォーマンスを向上させ、トラフィック量の増加に伴ってパフォーマンスを維持します。
- 常にネットワークに帯域幅を追加するには、need を減らします。
- ネットワークの輻輳を管理します。

スイッチのQoSページには、CoSモード、ToSモード、ポートベースモードの3種類のQoSモードを選択できます。3つのモードはどちらも、packet内の事前定義フィールドを使用して出力待ち行列を判別します。

- **CoS/ 802.1pタグプライオリティモード** - 出力キューの割り当ては、IEEE 802.1p VLAN プライオリティタグによって決定されます。
- **ToS/DSCPモード** - 出力キューの割り当ては、IPパケットのToS または DSCP フィールドによって決定されます。
- **Portベースのプライオリティモード** - 指定された高優先度ポートから受信したパケットは、優先度の高いパケットとして扱われます。

4.15.2 QoS構成

QoS 設定を使用すると、遅延の問題の影響を受ける可能性のあるデータ トラフィックの配信を容易にするために、パケット優先順位をカスタマイズできます。 CoS/802.1p タグプライオリティが適用されると、スイッチは 802.1Q VLAN タグパケットを認識し、ユーザプライオリティ値を持つVLAN tagged パケットを抽出します。

802.1Q タグおよび 802.1p プライオリティ

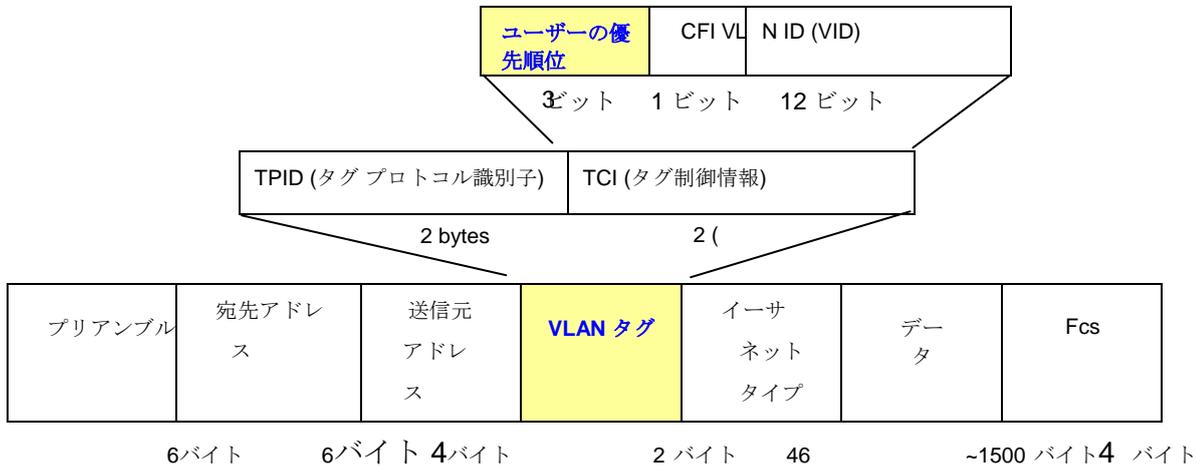


図 4-15-1: 802.1p タグの優先順位

COS 優先順位レベルを設定します。上記の [優先度の種類] のドロップダウン選択項目が最初に COS のみ/COS として選択されると、この制御項目を使用して各ポートのキューイング ポリシーを設定できるようになります。

4.15.2.1 プライオリティ キュー サービスの設定

QoS 設定を使用すると、遅延の問題の影響を受ける可能性のあるデータ トラフィックの配信を容易にするために、パケット優先順位をカスタマイズできます。 IEEE 802.1p プライオリティ仕様では、8 つの優先度レベルを使用してデータ パケットを分類します。 802.1p 準拠の devices では、パケット ヘッダーに挿入されたタグを使用して、データ パケットの優先順位を識別します。

スイッチは、スタティック ポートインセレスプライオリティと 4 つのキューをサポートします。

QoS Configuration

QoS Configuration
PerPort Configuration

Priority Queue Service:

QoS Mode

First Come First Service

All High before Low

WRR

Highest	SecHigh	SecLow	Lowest
8	4	2	1

802.1p priority [0-7]

Lowest	Lowest	SecLow	SecLow	SecHigh	SecHigh	Highest	Highest
--------	--------	--------	--------	---------	---------	---------	---------

Apply
Default
Help

図 4-15-2: QoS 設定 – 802.1Priority

このテーブルには、次のフィールドが含まれます。

オブジェクト	説明
先着順	送信されるパケットの順序は、到着順によって異なります。
低の前にすべて高	優先度の低いパケットの前に送信される優先度の高いパケット。 スイッチの優先度の高いキュー内のパケットに与えられるプリファレンスを選択します。これらのオプションは、優先度の低いパケットが送信される前に送信される優先度の高いパケットの数を表します。
加重ラウンドロビン	たとえば、8最高：4 SecHigh：2 SecLow：1 最低：1 最低は、スイッチが4秒の高優先度パケットを送信する前に、2秒の優先順位の低いパケットを送信する前に、1つの最も低い優先順位を送信する前に、8つの最も高い優先順位のパケットを送信することを意味します。 パケット。
802.1p 優先度 [0-7]	CoS 優先度レベル 0~7 を 設定します。



802.1p プライオリティ:スイッチ転送パケットのプライオリティ分類子。CoS の範囲は 0 ~ 7 です。7はハイクラスです。ゼロは低クラスです。ユーザーは、次の間のマッピングを構成できます。

CoSおよびトラフィック分類子。

4.15.2.2 QoSパーポート構成

各ポートの優先度レベルを設定します。上記の [優先度の種類] のドロップダウン選択項目が [ポート ベース] として選択されている場合、このコントロール項目を使用して各ポートのキュー イング ポリシーを設定できます。

The screenshot shows the 'QoS Configuration' interface with the 'PerPort Configuration' tab selected. Under 'Configure Port Priority', there is a list of ports (Port1 to Port5) and a dropdown menu for 'Port Priority' currently set to 'Disable'. Below this is a table with columns 'PortNum' and 'Port Priority' showing 'Disable' for Port1 through Port6.

PortNum	Port Priority
Port1	Disable
Port2	Disable
Port3	Disable
Port4	Disable
Port5	Disable
Port6	Disable

図 4-15-3: QoS 設定 – ポートベースの優先順位

このテーブルには、次のフィールドが含まれています。

オブジェクト	説明
ポート番号:	ポート 1 からポート 10 を示します。
ポートの優先順位:	各ポートには 8 つの優先度レベル(0-7 または [無効]) が選択されます。 7 が最も高い優先順位です。

4.15.3 ToS/DSCP

ToS/DSCP 優先順位は、6 ビットサービスの種類 (ToS) または差別化サービス コード ポイント (DSCP) から 3 ビットの優先順位マッピングを通じて取得されます。

IPv4 ヘッダーのサービスの種類 (ToS) オクテットは、3 つの部分に分かれています。優先順位 (3 ビット)、ToS (4 ビット)、および MBZ (1 ビット)。優先順位ビットはパケットの重要性を示し、ToS ビットはネットワークがスルーポイント、遅延、信頼性、およびコスト (RFC 1394 で定義) の間でどのようにトレードオフを行う方法を示します。MBZ ビット ("は 0 である必要があります") は現在使用されず、0 に設定されているか、単に無視されます。

0	1	2	3	4	5	6	7
優先 順位			ToS				MBZ

サービス オクテットの IPv4 パケット ヘッダー タイプ

4 つのToSビットは15の異なる優先順位値を提供しますが、定義された意味を持つ値は5つだけです。

DiffServコード ポイント (DSCP) - 特定のアプリケーションによってエンコードされる IP ヘッダー内のトラフィック優先順位付けビットです。

パケットがネットワーク経路で必要とするサービスのレベルを示すデバイス。DSCP は、トラフィックを異なるサービスクラスに分類するために RFC2597 で定義されています。管理対象スイッチは、IPv4 パケットから DS フィールドのコードポイント値を抽出し、設定されたプライオリティに基づいて着信 IP パケットの前の y を識別します。

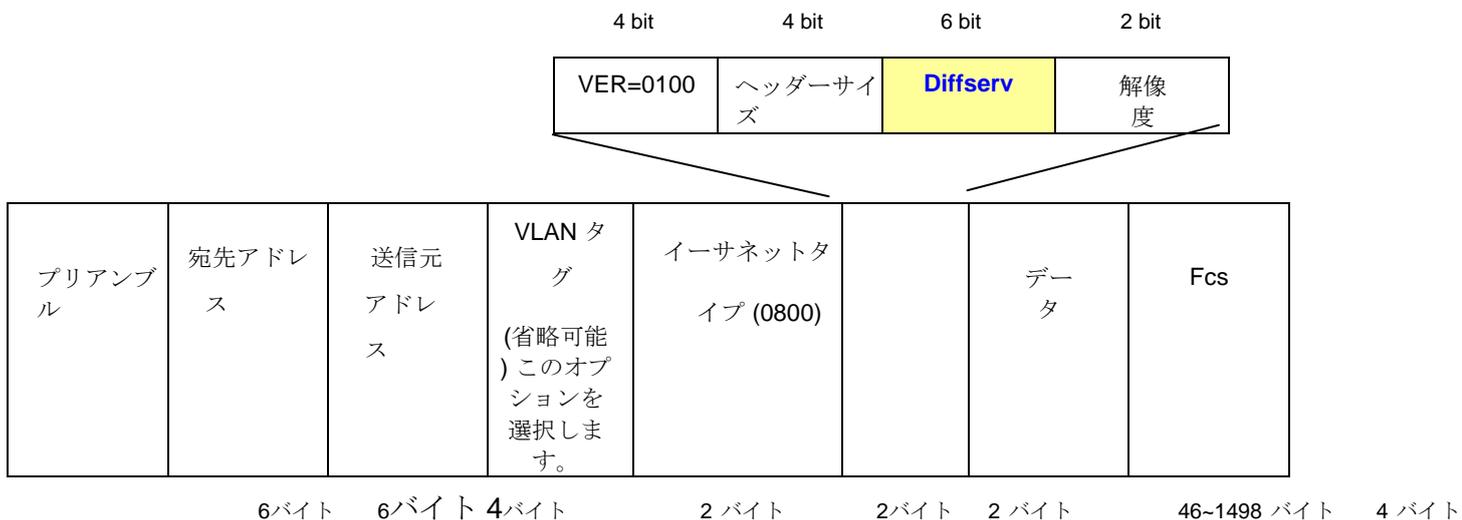


図 4-15-4: IPv4 フレーム形式

DSCP の幅は6 ビットで、最大 64 の異なる転送動作のコーディングが可能です。DSCP は 3 つの優先順位ビットとの下位互換性を維持するため、非 DSCP 準拠のToS対応デバイスが DSCP マッピングと競合しないようにします。nのネットワークポリシーに基づいて、さまざまな種類のトラフィックをさまざまな種類の転送用にマークできます。

4.15.3.1 ToS/DSCP 構成

ToS/DSCP ページには、特定の DSCP フィールドに出力待ち行列を定義するためのフィールドが用意されています。

TCP/IP の ToS/DSCP モードが適用されると、管理対象スイッチは RFC2474 で定義されている DS フィールドから TCP/IP 差別化サービス コードポイント (DSCP) の優先順位情報を認識します。

トラフィック分類に ToS/DSCP を有効にし、DSCP から優先順位へのマッピング列を設定できます。

DSCP	Priority
DSCP1	0
DSCP2	0
DSCP3	0
DSCP4	0
DSCP5	0
DSCP6	0
DSCP7	0
DSCP8	0
DSCP9	0
DSCP10	0

図 4-15-5: QoS 設定 – ToS プライオリティ

このページには、次のフィールドが含まれています。

オブジェクト	説明
ToS/DSCP	内部トラフィック クラス(0~7)を有効/無効にして、対応する IP DSCP をマップする 値。
Dscp	着信パケット内の IP DSCP ヘッダー フィールドの値。 0~63。
優先 順位	対応する IP DSCP をマップする 802.1p プライオリティを指定します。 値は 0 ~ 7 です。

4.15.3.2 ToS/DSCP ポート設定

IPv4 パケットを受信するときに IP ToS /DSCP マッピングを 802.1p プライオリティに設定し、管理対象スイッチはポートで QoS ステータスを設定できるようにします。この ToS/DSCP ポート構成ページでは、ポートで IP ToS/DSCP マッピングを構成し、現在の port ステータスを表示します。

Port Number	TOS/DSCP Status
Port1	Disable
Port2	
Port3	
Port4	
Port5	

PortNum	TOS/DSCP Port Status
Port1	Enable
Port2	Enable
Port3	Enable
Port4	Enable
Port5	Disable
Port6	Disable

図 4-15-6: QoS 設定 – ToS/DSCP ポートステータス このテ

ーブルには、次のフィールドが含まれています。

オブジェクト	説明
ポート番号	ポート 1 からポート 10 を示します。
ToS/DSCP ステータス	ポートの指定時に ToS/DSCP マップを 802.1p 優先順位に有効または無効にします。

4.16 VDSL構成

VDSL2(非常に高ビットレートデジタル加入者線2)、G.993.2は、xDSLブロードバンド線通信の最新かつ最先端の規格です。音声、データ、高精細テレビ(HDTV)、インタラクティブゲームなどのトリプルプレイサービスの広範な導入をサポートするように設計されたVDSL2は、オペラのトーラとキャリアを徐々に柔軟に、そしてコスト効率よくアップグレードし、既存のxDSL-インフラストラクチャをアップグレードすることができます。

VDSL2 は、既存のアクセス テクノロジーの欠点に対処するために、記録的な時間で開発および標準化されました。これは、ラストマイルのボトルネックを排除し、事前のトリプルプレイサービスのグローバルな大量展開を可能にするための理想的なxDSL技術としてサーバーを提供します。 **DMT(離散マルチトーン)**または**QAM(直交振幅変調)**技術のいずれかを選択することができたその前身とは異なり、VDSL2はDMTラインコードのみを使用します。

DMTは、使用可能な周波数範囲が複数の小さな周波数帯域(トーン)に分離されるようにDSL信号を分離する方法です。それは4 kHzまたは8 kHz間隔の4096までのトーンを使用する。各トーンは、ダウンストリームまたはアップストリームのいずれかに使用できます。

PLANET VDSL2 管理対象スイッチは、最大 100 Mbps のダウンストリームとアップストリームの両方で、リモート CPE への非常に高いパフォーマンスのアクセスを提供できます。VDSL2 管理対象スイッチは ITU-T G993.2 標準に準拠し、CO 動作モードをサポートします。WEB UIとユーザーによるCOは、既存の銅線を介して複数のネットワーク間のデータ伝送、ポイントツーマルチポイントアプリケーションのための複数のCPEに接続することができます。

4.16.1 プロファイルの構成

このオプションを使用すると、VDSL 構成プロファイルを設定できます。[VDSL 構成] メニューの[VDSL 構成プロファイル]をクリックしてください。次のページが表示されます。

Profile Setting

Status : Load OK

Configuration
Profile Table

User profile name default ▼

New profile Name (Max 64 bytes)

system profile name AnnexA_R_POTS_D-32_EU-32_30a ▼

CARRIER A43 ▼

SNR Ds: 6dB ▼ Us: 6dB ▼

Rate limit Ds Us Ds: 101 Mb/s ▼ Us: 101 Mb/s ▼

INP 30a Ds: 2 symbol ▼ Us: 2 symbol ▼

INP no 30a Ds: 2 symbol ▼ Us: 2 symbol ▼

MaxDelay Ds: 8ms ▼ Us: 8ms ▼

Port

Add

<< Remove

Port1 ▲
 Port2
 Port3
 Port4
 Port5
 Port6
 Port7
 Port8 ▼

New

Set

Delete

図 4-16-1: VDSL2 プロファイル設定インターフェイ

ス このページには、次のフィールドが含まれています。

オブジェクト	説明
ユーザー プロファイル名	このフィールドには、プロファイルのインデックス名が表示されます。ドロップダウンリストをクリックし、作成または構成するインデックス プロファイル名を選択します。
新しいプロファイル名	新しいプロファイルを作成するときに、プロファイル名を入力します。使用できる文字は、0 から 9、A から Z、a から z、"_"、"-" です。最大 64 バイト。

VDSL2 管理対象スイッチは、ユーザに最も一般的な VDSL2 プロファイルを提供します。それは30a、17a、12a、12b、8a、8b、8cおよび8dを支う。実際の環境に適したプロファイルを選択できます。プロファイルが異なると、データレートの接続状態が異なります。

システム プロファイル名

ドロップダウン リストをクリックし、使用する VDSL バンドプランを選択します。VDSL2 管理対象スイッチは、以下のプロファイルをサポートします。

1. [AnnexA_R_POTS_D-64_EU-64_30a](#)
 2. [AnnexA_R_POTS_D-32_EU-32_17a](#)
 3. [AnnexA_R_POTS_D-32_EU-32_12b](#)
 4. [AnnexA_R_POTS_D-32_EU-32_12a](#)
 5. [AnnexA_R_POTS_D-32_EU32_8a](#)
-

-
6. AnnexA_R_POTS_D-32_EU-32_8b
 7. AnnexA_R_POTS_D-32_EU-32_8c
 8. AnnexA_R_POTS_D-32_EU-32_8d
 9. AnnexA_R_POTS_D-64_EU64_30a_NUS0
 10. AnnexA_R_POTS_D-64_EU-64_17
AnnexB_B7-1_997-M1c-A-7
 12. AnnexB_B7-2_997-M1x-M-8
 13. AnnexB_B7-3_997_M1x-M
 14. AnnexB_B7-4_997_M2x-M-
8
 15. AnnexB_B7-5_997_M2x-A
 16. AnnexB_B7-6_997_M2x-M
 17. AnnexB_B7-9_997E17-M2x-
A
 18. AnnexB_B7-10_997E30-M2x-NUS0
 19. AnnexB_B8-1_998-M1x-A
 20. AnnexB_B8-2_998-M1x-B
 21. AnnexB_B8-4_998-M2x-A
 22. AnnexB_B8-5_998-M2x-M
 23. AnnexB_B8-6_998-M2x-B
 24. AnnexB_B8-8_998E17-M2x-NUS0
 25. AnnexB_B8-9_998E17-M2x-NUS0-M
 26. AnnexB_B8-10_998ADE17-M2x-NUS0-M
 27. AnnexB_B8-11_998ADE17-M2x-A
 28. AnnexB_B8-12_998ADE17-M2x-B
 29. AnnexB_B8-13_998E30-M2x-
NUS0
 30. AnnexB_B8-14_998E30-M2x-NUS0-M
 31. AnnexB_B8-15_998ADE30-M2x-NUS0-M
 32. AnnexB_B8-16_998ADE30-M2x-NUS0-A
 33. AnnexC_POTS_25-138_b
 34. AnnexC_POTS_25-276_b
 35. AnnexC_TCM-ISDN
-

VDSL ポートのG.ハンドシェイクトーンを設定します。

ド롭ダウン リストをクリックし、使用する VDSL キャリア プランを選択し
ます。VDSL2 管理対象スイッチは、以下のプロファイルをサポートします。

キャリア

1. 自動
 2. A43
 3. B43
 4. V43
-

Snr

回線品質は**SNR(信号対ノイズ比)**を使用して決定され、VDSL 回線接続にのみ適用されます。SNRは、特定の時点におけるノイズ信号の振幅に対する実際の信号の振幅の比です。SNRが高いほど、ラインの品質が向上します。パフォーマンスを向上させるか、ラインを新しいラインに置き換えるために、ラインの品質と距離に応じて手動でSNRマージンを広告してください。

ドロップダウン リストをクリックし、使用する SNR を選択します。ダウンストリームまたはアップストリームの SNR マージンを設定します。

SNR マージン値: 6 dB ~ 24 dB

デフォルト値: **6 dB**

レート制限 DS 米国

- **DS:** 最大ダウンストリームの送信レートを設定します。VDSL2 CO マネージドからのダウンストリームトラフィック制限 (Mbps) の値
CPE に切り替えます。1 Mbps および 5 Mbps のステップでポートごと。

デフォルト: **101Mbps/s** (ビット/秒)

1Mbps ~ 101Mbps の範囲

- **US:** 最大アップストリームの送信レートを設定します。VDSL2 CPE から CO へのアップストリームトラフィック制限の値(Mbps 単位)
管理対象スイッチ。1 Mbps および 5 Mbps のステップでポートごと。

デフォルト: **101Mbps/s** (ビット/秒)

1Mbps ~ 101Mbps の範囲

INP 30a

ポートプロビジョニングの最小保護値を設定するには、アップストリームまたはダウンストリームを指定して INP を設定します。ドロップダウンリストをクリックし、使用する**INP(インパルス ノイズ保護)**を選択します。

1 (または 30a の場合は 0.5) から 16 シンボルまたは**保護なし**の範囲

デフォルト値: **2 シンボル**

最大遅延

VDSL 回線タイプは、**最大インターリーブ遅延**を選択して設定できます。

ダウンストリームまたはアップストリーム方向の。基本的には、3つのタイプがあります

- 制限なし
- 高速モード
- インターリーブ

インターリーブプロセスは、デジタル信号をアナログ信号に変調する前にデータエラーを修正するために使用されます。インターリーブは、拡張修正によるエラーを防ぎますが、パケットが収集されるため、送信レートが遅くなる可能性があります。

インターリーブモードは、250未満の持続時間を持つインパルスノイズに対するインパルスノイズ保護を提供します。インターリーブ最大遅延を設定することにより、収集された待機データによる送信遅延を防ぐことができます。

インターリーブプロセスをスキップするには、「遅延なし」を選択して高速モードで動作します。

高速モードでは、最小エンドツーエンドの待機時間が 1 ミリ秒未満で保証されます。

ドリップダウン リストをクリックし、使用するMaxDelayを選択します

。ダウンストリームまたはアップストリームを指定してインターリーブ遅延を設定します。単位はミリ秒です。0ms ~ 63ms の範囲

デフォルト値: 8ms

ポート

VDSL2 管理対象スイッチでは、すべての VDSL ポートが 1つのプロファイルに含まれています。メンバポートを他のプロファイルに変更するには、最初に [ユーザー プロファイル名] を選択する必要があります。

追加: 指定したポートにプロファイルを適用します。

削除: 指定したポートのプロファイルを無効にします。



1. VDSL ポートのデフォルト プロファイルは"30a"
2. SNR マージンが大きすぎると、送信レートが遅くなり、通信は安定します。
3. "MaxDelay"が "遅延なし" (高速モード) に構成されている場合、エラー訂正はダウンしません。
一方、データの送信速度は速くなります。



(下):

AnnexA: 上流の方向の別館 A 環境では 6 ~ 32 トーンを使用します。**附属編B:** 上流の方向に別館B環境で32~64トーンを使用します。

4.16.2 VDSL ポートの状態

ネットワークマネージャは、この VDSL ポートステータスWebページで VDSL 回線のステータスを確認できます。これには、回線ステータス、アップストリーム/ダウンストリーム日付レート、SNR および VDSL2 ファームウェアバージョンが含まれます。

Port	Status	Upstream Rate (Unit:Kb/s)	Downstream Rate (Unit:Kb/s)	SNR Margin (US) (Unit:0.1db)	SNR Margin (DS) (Unit:0.1db)	Firmware Version	Detail
Port1	Showtime	100992	100992	78	249	10201	Advance
Port2	Showtime	100992	100992	63	234	10201	Advance
Port3	Idle	0	0	NA	NA	10201	Advance
Port4	Idle	0	0	NA	NA	10201	Advance
Port5	Idle	0	0	NA	NA	10201	Advance
Port6	Idle	0	0	NA	NA	10201	Advance
Port7	Idle	0	0	NA	NA	10201	Advance
Port8	Idle	0	0	NA	NA	10201	Advance

図 4-16-2: VDSL2 ポート ステータス インターフェイス

[進む] ボタンをクリックすると、ウィンドウ ポップアップに指定したポートの詳細な VDSL アップストリーム/ダウンストリーム情報が表示されます。

Up Stream		Down Stream	
Delay	5 ms	Delay	5 ms
INP	20 0.1 symbols	INP	20 0.1 symbols
CRC 15M	0	CRC 15M	0
CRC 1Day	0	CRC 1Day	0
CRC Total	0	CRC Total	0
Error Correction 15M	0	Error Correction 15M	0
Error Correction 1Day	1195	Error Correction 1Day	0
Error Correction Total	9808	Error Correction Total	456
xdsl2ChStatusPrevDataRate	0 Kbps	xdsl2ChStatusPrevDataRate	0 Kbps
xdsl2LineStatusAttainableRate	105448 Kbps	xdsl2LineStatusAttainableRate	168634 Kbps
xdsl2LineStatusElectricalLength	11 0.1 dB	xdsl2LineStatusElectricalLength	11 0.1 dB
xdsl2LineBandStatusSnrMargin	NA (US0) 0.1dB	xdsl2LineBandStatusSnrMargin	-- (--) 0.1dB
xdsl2LineBandStatusSnrMargin	79 (US1) 0.1dB	xdsl2LineBandStatusSnrMargin	248 (DS1) 0.1dB
xdsl2LineBandStatusSnrMargin	79 (US2) 0.1dB	xdsl2LineBandStatusSnrMargin	248 (DS2) 0.1dB
xdsl2LineBandStatusSnrMargin	77 (US3) 0.1dB	xdsl2LineBandStatusSnrMargin	249 (DS3) 0.1dB
xdsl2LineBandStatusSnrMargin	NA (US4) 0.1dB	xdsl2LineBandStatusSnrMargin	NA (DS4) 0.1dB
xdsl2PMLCurr15MTimeElapsed	733 secs	xdsl2PMLCurr15MTimeElapsed	29 secs
xdsl2PMLCurr15MFecs	0	xdsl2PMLCurr15MFecs	0
xdsl2PMLCurr15MEs	0	xdsl2PMLCurr15MEs	0
xdsl2PMLCurr15MSes	0	xdsl2PMLCurr15MSes	0
xdsl2PMLCurr15MLoss	0	xdsl2PMLCurr15MLoss	0
xdsl2PMLCurr15MUas	0	xdsl2PMLCurr15MUas	0
xdsl2PMLCurr1DayTimeElapsed	60133 secs	xdsl2PMLCurr1DayTimeElapsed	60329 secs
xdsl2PMLCurr1DayFecs	7	xdsl2PMLCurr1DayFecs	0
xdsl2PMLCurr1DayEs	0	xdsl2PMLCurr1DayEs	0
xdsl2PMLCurr1DaySes	0	xdsl2PMLCurr1DaySes	0
xdsl2PMLCurr1DayLoss	0	xdsl2PMLCurr1DayLoss	0
xdsl2PMLCurr1DayUas	0	xdsl2PMLCurr1DayUas	0
xdsl2PMLCurrTotalFecs	0	xdsl2PMLCurrTotalFecs	0
xdsl2PMLCurrTotalEs	0	xdsl2PMLCurrTotalEs	0

このページには、次のフィールドが含まれています。

オブジェクト	説明
遅延	選択した VDSL 回線の現在のインターリーブ遅延を表示します。 下流または上流の方向
Inp	VDSL 回線で設定された INP を表示します。
CRC 15M	過去 15 分間の CRC エラーの数を表示します。

	現時点でエラーの時刻を最初から確認するために使用できます。 前の15分の誤差の15分と時間の。
CRC 1Day	前日の CRC エラーの数を表示します。 これは、今日の開始から現在のエラーの時間、昨日のエラーの時間を確認するために使用することができます。
CRC 合計	ブートからすべてのエラーの収集されたデータを表示します。
エラー訂正 15M	過去 15 分間のエラー修正の数を表示します。
エラー訂正 1日	前日のエラー訂正の数を表示します。
エラー訂正合計	ブートからすべてのエラー訂正の収集されたデータを表示します。
xdsI2Ch ステータスプレブ データレート	ベアラ チャンネルが最新のレート変更イベントの直前に動作していた以前の正味データ レート。これは、完全または短い初期化、高速再トレーニング、DRA、または電源管理の遷移で、遷移 between L0 状態と L1 または L2 状態を除く場合があります。データレートは次のコードでコーディングされています。 ビット/s。
xdsI2ラインステータス達成可能	アップストリームの最大達成可能なデータ レート。 VTU-R送信機とVTU-C受信機で現在達成可能な最大アップストリームネットデータレート(ビット/sでコード化)。
xdsI2ラインステータス電氣的長さ	このパラメータには、1 MHz、kI0 で dB で表される推定電気長が含まれます。これは、電気長がによって強制されなかった場合に VTU-O から VTU-R に送信される最終的な電気長です。 CO-MIB。 値の範囲は 0 ~ 128 dB で、ステップ数は 0.1 dB です。
xdsI2ラインバンドステータス SnrMargin	SNR マージンは、VTU で受信されるノイズ電力の dB の最大増加です (下流方向のバンドの場合はVTU-R、アップストリーム方向のバンドの場合は VTU-C)。 要件は、VT U で受信されるすべてのベアラ チャンネルに対して満たされ、0.1 dB 単位で -640 ~ 630 の範囲です (物理値は -64 ~ 63 dB)。 0x7FFFFFFF (2147483647) の特殊値は、SNR マージンが表現される範囲外であることを示します。0x7FFFFFFE (2147483646) の特殊値は、測定中のSNR Marg が現在 利用
xdsI2PMLCurr15M経過時間	この間隔の合計経過秒数
xdsI2PMLCurr15MFecs	この間隔中に、少なくとも 1 つの FEC があつた秒数 この行の 1 つ以上のベアラ チャンネルの修正イベント。このパラメーターは、UAS または SES の間に禁止されます。

この間隔中に次の秒数が存在した場合の数:

xdsI2PMLCur15M

VTU-C: CRC-8 ≥ 1 1 つ以上のベアラ チャネルまたは

LOS ≥ 1 OR SEF ≥ 1 LPR ≥ 1

VTU-R: FEBE ≥ 1 1 1 つ以上のベアラ チャネルまたは

	<p>LOS-FE >=1 または RDI >=1 または LPR-FE >=1 .</p> <p>このパラメーターは UAS 中に禁止されます。</p>
	<p>この間隔中に次の秒数が存在した場合の数:</p> <p>VTU-C: (受信したベアラ チャンネルの 1 つ以上の CRC-8 異常)</p> <p>>= 18 または LOS >= 1 OR SEF >= 1 OR LPR >= 1</p> <p>VTU-R: (受信したベアラ チャンネルの 1 つ以上の FEBE 異常)</p> <p>>= 18 または LOS-FE >= 1 OR RDI >= 1 OR</p> <p>LPR-FE >= 1</p> <p>このパラメーターは、UAS 中に禁止されます。</p>
xdsI2PMLCur15の	
	<p>この間隔中に LOS (または LOS-FE が存在した秒数)</p> <p>VTU-R</p>
xdsI2PMLCurr15MLossLoss	
	<p>この間隔中の使用不可状態の秒数です。使用不可は、10 秒連続で重大なエラーが発生し、終了します。</p> <p>10 連続秒の開始時に、重大なエラー秒なし</p>
xdsI2PMLCur15MUas	
	<p>この間隔の合計経過秒数</p>
xdsI2PMLCurr1日勤経過	
	<p>この回線に 1 つ以上のベアラ・チャンネルに対して少なくとも 1 つの FEC 訂正イベントがあった場合の、この間隔中の秒数。これ</p> <p>UAS または SES の間にパラメーターが禁止される</p> <p>この間隔中に次の秒数が存在した場合の数:</p> <p>VTU-C: CRC-8 >= 1 1 つ以上のベアラ チャンネルまたは</p> <p>LOS >= 1 OR SEF >= 1 または LPR >= 1</p> <p>VTU-R: FEBE >= 1 1 つ以上のベアラ チャンネルまたは</p> <p>LOS-FE >= 1 または RDI >= 1 または LPR-FE >= 1.</p> <p>このパラメーターは、UAS 中に禁止されます。</p>
xdsI2PMLCurr1DayFecs	
	<p>この間隔中に次の秒数が存在した場合の数:</p> <p>VTU-C: (受信したベアラ チャンネルの 1 つ以上の CRC-8 異常) >= 18 または LOS >= 1 OR SEF >= 1</p> <p>OR LPR >= 1</p> <p>VTU-R: (FEBE 異常の 1 つ以上</p> <p>受信ベアラ チャンネル) >= 18 または LOS-FE >= 1</p> <p>OR RDI >= 1 OR LPR-FE >= 1 .</p> <p>このパラメーターはUAS中に禁止されます。</p>
xdsI2PMLCurr1DayEs	
	<p>この間隔中に LOS (または LOS-FE が存在した秒数)</p> <p>VTU-R</p>
xdsI2PMLCurr1DaySes	
	<p>この間隔中の使用不可状態の秒数です。使用不可は、10 個の連続した重大なエラー秒の開始時に開始され、10 秒の連続秒の開始時に終了します。</p>
xdsI2PMLCurr1DayLoss	
	<p>この間隔中の使用不可状態の秒数です。使用不可は、10 個の連続した重大なエラー秒の開始時に開始され、10 秒の連続秒の開始時に終了します。</p>
xdsI2PMLCurr1DayUas	

5. コンソール管理

PLANET VDSL2 マネージ スイッチ シリーズには、RS-232 DB9 コネクタがデフォルトで装備されています。また、2つのモデルはどちらも Telnet 管理をサポートしています。

5.1 コンソールインターフェイスへのログイン

コンソール モードでシステムを構成するには、シリアル ケーブルを PC またはノートブック コンピュータの COM ポートに接続し、管理対象スイッチの RJ45 タイプシリアル(コンソール)ポートに接続します。管理対象スイッチのコンソール ポートは既に DCE であるため、ヌル モデムを必要とせずに PC 経由でコンソール ポートを直接接続できます。

Microsoft Windows プラットフォーム上のハイパーターミナルを使用して VC-820M のコンソール インターフェイスに接続する方法の詳細については、[第 3.5 章管理コンソール](#)を参照してください。

端末がデバイスに接続されると、VC-820Mの電源が入ると、端末はテスト手順を実行していることを示します。

次に、ログイン パスワードを確認する次のメッセージが表示されます。工場出荷時のデフォルトパスワードは次の値です。次のように、ログイン画面で図 5-1-1表示。

ユーザー:
以下の場合:

```
portid=9,loid=2.1.30,value=3f3338
MIB value has set.
>>interface xdsl set oid 9 2.1.32 400010

portid=9,loid=2.1.32,value=400010
MIB value has set.
>># Setup Profile

>>interface xdsl set initprofile

Init port1 use profile name:default
Init port2 use profile name:default
Init port3 use profile name:default
Init port4 use profile name:default
Init port5 use profile name:default
Init port6 use profile name:default
Init port7 use profile name:default
Init port8 use profile name:default

Username: admin
Password:
Switch#
```

図 5-1-1: VDSL2 管理対象スイッチ コンソールログイン画面



1. セキュリティ上の理由から、この最初のセットアップ後に新しいユーザー名とパスワードを変更して記憶してください。

ユーザー名最大: **6**、最小: **1** 文字

パスワードの最大値: **6**, 最小: **1** 文字

2. コンソール インターフェイス の下の小文字のコマンドのみを受け入れます。

5.2 IPアドレスの構成

VC-820M管理スイッチは、次に示すデフォルトの IP アドレスで出荷されます。

Ip: **192.168.0.100**

サブ・ス: **255.255.255.0**

現在の IP アドレスを確認するか、スイッチの新しい IP アドレスを変更するには、次の手順を実行してください。

■ 現在の IP アドレスを表示する

1. [スイッチ#] " プロンプトで、「構成」と入力します。
2. "スイッチ(config)# " プロンプトで、「show ip」と入力します。
3. 画面には、[図5-2-1](#)に示すように、c urrent IP アドレス、サブネット マスク、およびゲートウェイが表示されます。

```

QinQ.....OK
Forwarding.....OK
IP Mcst.....OK
IGMP.....OK
STP/RSTP/MSTP...OK
MIB.....OK
802.1X.....OK
Port.....OK
ACL.....OK
SNMP.....OK
Port interval...OK
TOS/DSCP.....OK
MAC.....OK
Completed!!

Username: admin
Password:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# _

```

図 5-2-1: IP 情報画面

■ IPアドレスの構成

1. オン "スイッチ(構成)#"プロンプトで、次のコマンドを入力し、<Enter>に示すように図 5-2-2.

次の値を取得します。 **ip 192.168.1.100 255.255.255.0**

次の値を取得します。 **ip 192.168.1.254**

前のコマンドは、スイッチの次の設定を適用します。

IP:192.168.1.100

サブネットマスク:255.255.255.0

ゲートウェイ: 192.168.1.254

```

Port.....OK
ACL.....OK
SNMP.....OK
Port interval...OK
TOS/DSCP.....OK
MAC.....OK
Completed!!

Username: admin
assword:
Switch# configure
Switch(config)# show ip
IP address: 192.168.0.100
Subnet mask: 255.255.255.0
Gateway: 192.168.0.254
Switch(config)# ip address 192.168.1.100 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.254
Switch(config)# show ip
IP address: 192.168.1.100
Subnet mask: 255.255.255.0
Gateway: 192.168.1.254
Switch(config)# copy running-config startup-config
Switch(config)# _

```

図 5-2-2: IP アドレスの設定画面

2. 手順1 を繰り返して、IP アドレスが変更されているかどうかを確認します。

IP が正常に構成されると、管理対象スイッチは新しい IP アドレス設定を直ちに適用します。新しい IP アドレスを使用して、管理対象スイッチの Web インターフェイスにアクセスできます。



コンソール コマンドまたは関連するパラメータに慣れていない場合は、コンソールに「help」と入力してヘルプの説明を取得してください。

これらの設定は、必要に応じてログオン後に変更できます。この管理方法は、システムの再起動中も接続したままシステムを監視できるため、多くの場合、推奨されます。また、関連付けられたアクションが開始されたインターフェイスに関係なく、特定のエラーメッセージがシリアルポートに送信されます。Macintosh または PC 接続は、端末シリアル・ポートに接続するための任意の端末エミュレーション・プログラムを使用できます。UNIX の下で workstation 添付ファイルは、TIP などのエミュレーターを使用できます。

5.3 コマンドレベル

次の表に、CLI コマンドと説明を示します。

モード	アクセス方法	プロンプト	終了メソッド	このモードについて1
ユーザー EXEC	スイッチとのセッションを開始します。	スイッチ>	ログアウトを入力するか、終了します。	ユーザー・レベルで使用可能なユーザー・コマンドは、特権レベルで使用可能なユーザー・コマンドのサブセットです。 このモードは、次の場合に使用します。 <ul style="list-style-type: none"> • 基本的なテストを実行します。 • システム情報を表示します。
特権 Exec	ユーザー EXEC モードで enable コマンドを入力します。	スイッチ#	disable と入力して終了します。	特権コマンドは、拡張モードです。 このモードを使用して、 <ul style="list-style-type: none"> • 高度な機能ステータスの表示 • 構成の保存
グローバル構成	特権 EXEC で configure コマンドを入力します。 モード。	スイッチ (構成)#	特権 EXEC モードを終了するには、exit または終了	このモードを使用して、スイッチ。

6. コマンドラインインターフェイス

6.1 操作に関する通知

「コンフィギュレーション」モードに入るには、特権モードにする必要があります。
を構成します。

(#一時は
内 ()#

6.1.1. コマンドライン編集

キー機能

<Ctrl>-B	;← カーソルを 1 文字後ろに移動します。
<Ctrl>-D	カーソル位置の文字を削除します。
<Ctrl>-E	現在のコマンドラインの末尾にジャンプします。
<Ctrl>-F	;→ カーソルを 1 文字前方に移動します。
<Ctrl>-K	カーソルからコマンドラインの末尾までを削除します。
<Ctrl>-N	;↓ コマンド履歴の次のコマンドラインを入力します。
<Ctrl>-P	;↑ コマンド履歴の前のコマンドラインを入力します。
<Ctrl>-U	カーソルからコマンドラインの先頭までを削除します。
Ctrl	-W 最後に入力した単語を削除します。
<Esc> B	カーソルを 1 単語後ろに移動します。
<Esc> D	カーソルから単語の末尾までを削除します。
<Esc> F	カーソルを 1 単語前方に移動します。
[バックスペース >	カーソルの前の文字を削除します。
	カーソル位置の文字を削除します。

以下の汎用ファンクションキーは、すべてのメニューの機能を提供します。

6.1.2. コマンドヘルプ

あなたは? 任意のコマンドモードでは、CLIはその時点で可能なコマンドを返し、いくつかの説明と共に

6.2 システムコマンド

実行構成の表示

説明:

スイッチの実行コンフィギュレーションを表示します。

おとなしい

説明:

スイッチ構成をバックアップします。

・・・を含む

説明:

次回の起動時にデフォルトの工場出荷時の設定にリセットします。

クリアアープ

説明:

<ip-addr> クリアする IP アドレスを指定します。IP アドレスを入力しない場合は、ARP キャッシュ全体がクリアされます。

arp を表示ス・ス・ス

説明:

IP ARP 変換テーブルを表示します。

Ping

説明:

ICMP ECHO_REQUESTをネットワーク ホストに送信します。

パラメーター:

<1..999> 繰り返し回数を指定します。入力しない場合は、<Ctrl>-C キーを押して停止するまで ping を続行します。

syslog-server

説明：

syslog サーバ情報を設定します。

構文

syslog-サーバー <IP アドレス > [<0-2>]

パラメーター：

<0-2 >はログの種類を指定します。"0" は既定値です。

0: なし

1: メジャー

2: すべて

[いいえ]sntp

説明：

SNTP を有効または無効にします。

構文

[いいえ]sntp

Sntp

説明：

SNTP サービスを開始します。

構文

sntp <IP アドレス > [<タイム ゾーン オフセット>][<時間範囲>]

パラメーター：

<タイム ゾーン オフセット> は、UTC の前または後のタイム ゾーン オフセットを指定します。

前- UTC: 前 -UTC 後 -

UTC: 後 UTC

<0-24 > 時間範囲 <単位: 時間>

6.3 スイッチスタティック設定

6.3.1 ポート設定とステータスの表示

ポートの状態

ポートの状態をオンまたはオフにします。

構文：

ポートの状態<a0> オン | オフ > [<ポートリスト>]

パラメーター：

<ポート一覧> を指定します。入力しない場合、すべてのポートのオンとオフが切り離されます。

ポートネゴ

説明：

ポート ネゴシエーションを設定します。

構文

ポートネゴ <フォース | 自動 | nway-force> [<ポートリスト>]

パラメーター：

<ポート一覧> 設定するポートを指定します。入力しない場合は、すべてのポートが設定されます。

ポート速度

説明：

ポート速度(mbps)とデュプレックスを設定します。

構文：

ポート速度<10 | 100 | 1000> <フル | 半分> [<ポート一覧>]

パラメーター：

<ポート一覧> 設定するポートを指定します。入力しない場合は、すべてのポートが設定されます。

ポートフロー

説明：

ポート フロー制御を有効または無効にします。

構文：

ポート フロー <有効 |> [<ポート一覧>]を無効にします

パラメーター：

<有効 |無効> フロー制御を有効または無効にします。

<ポート一覧> 設定するポートを指定します。入力しない場合は、すべてのポートが設定されます。

ポートレート

説明：

ポートの有効な入り口または出力レートを設定します。

構文：

ポートレート<入力 |出力> <0..8000> [<ポートリスト>]

パラメーター：

<0..8000> 入力レートまたは出力レートを指定します。

<ポート一覧> 設定するポートを指定します。入力しない場合は、すべてのポートが設定されます。

ポートの優先順位

説明：

ポートの優先順位を設定します。

構文：

ポートの優先順位<無効 |0..7> [<ポートリスト>]

パラメーター：

<ポート一覧> 設定するポートを指定します。入力しない場合は、すべてのポートが設定されます。

ポートジャンボフレーム

説明：

ポートジャンボフレームを設定します。ポート ジャンボ フレームがイネーブルの場合、ポートフォワード ジャンボ フレーム パケット

構文：

ポートジャンボフレーム <有効 |> [<ポート一覧>]を無効にします

パラメーター：

<ポート一覧> 設定するポートを指定します。入力しない場合は、すべてのポートが設定されます。

ポートの状態を表示する

説明：

ポートの状態、リンク、トランキング、VLAN、ネゴシエーション、速度、デュプレックス、フロー制御、Rate 制御、プライオリティ、セキュリティ、BSF 制御を含むポートステータスを表示します。

モード(構成)#

1 おとな内語

::

日:ス: VLAN:

: 以下の場合:

```

Port 2 Information
-----
State: on
Link: down
Trunking: none
VLAN: DEFAULT
Priority: disable
Security: off
-----
Port 3 Information
-----
State: on
Link: down
--More--

```

ポート統計情報の表示

説明：

TxGoodPkt、TxBadPkt、RxGoodPkt、RxBadPkt、TxAbort、衝突、ドロッププットなどのポート統計情報を表示します。

パラメーター：

<ポート ID> は、表示するポートを指定します。

```

モード(構成)#
-----
1 分の一
-----
TxGoodPkt: 0
TxBadPkt: 0
RxGoodPkt: 0
RxBadPkt: 0
TxAbort: 0
次の場合:0
おしり: 0
-----
2 分の一
-----
TxGoodPkt: 0
TxBadPkt: 0
RxGoodPkt: 0
RxBadPkt: 0
TxAbort: 0
次の場合:0
おしり: 0
-----
3 分の一
-----

```

ポート保護を表示する

説明：

保護されたポート情報を表示します。

スイッチ(config)#はポート保護を表示		
ポート	保護	グループ
1	オフ	1
2	オフ	1
3	オフ	1
4	オフ	1
5	オフ	1
6	オフ	1
7	オフ	1
8	オフ	1
9	オフ	1
10	オフ	1
トルク1	オフ	1

6.4 トランク構成

トランクを使用すると、スイッチはポートを結合して、単一の高速リンクのように機能させることができます。これは、高速リンクを提供するために、一部のデバイスへの帯域幅を増やすために使用することができます。たとえば、トランクは、接続をtween スイッチにしたり、サーバをスイッチに接続したりする場合に便利です。トランクは、フォールトトレランスのための冗長リンクを提供することもできます。トランク内の 1 つのリンクに障害が発生した場合、スイッチは残りのリンク間でトラフィックのバランスを取ることができます。



1. 10/100 Mbps ポートは、Gigabit ポート(ポート 9 およびポート 10)ではトランクできません。
2. 同じトランクグループ内のすべてのポートは、1 つのポートとして扱われます。トランクグループが存在する場合、そのトランクに属するポートは VLAN 設定画面で"TRUNK #"に置き換えられます。次の例では、ポート 1~ ポート 2 を「TRUNK 1」として設定します。

6.4.1 トランキングコマンド

トランクを表示する

説明：

トランキング情報を表示します。

```

スイッチ(config)# show trunk
グループ ID |LACP | ポート |LACP アクティブ
-----+-----+-----+-----
1 |はい| 1, 2 | 1, 2

```

トランクの追加

説明：

新しいトランク グループを追加します。

構文：

トランク 追加 <トランク ID> <lacp | いいえ-ラック> <ポートリスト> <アクティブポートリスト>

パラメーター：

<トランク ID> は、追加するトランク グループを指定します。

<lacp | no-lacp>を使用して、追加されたトランク グループを LACP 対応に指定します。

<ポート一覧> 設定するポートを指定します。

<アクティブポート リスト>は、LACP に設定するポートをアクティブにするかどうかを指定します。

トランクなし

説明：

既存のトランク グループを削除します。

構文：

トランクなし<トランク ID>

パラメーター：

<トランク ID> は、削除するトランク グループを指定します。

6.4.2 LACPコマンド

[いいえ]ラック

説明：

LACP を有効または無効にします。

ラックシステム優先

説明：

LACP システムの優先順位を設定します。

構文：

lACPシステム優先 <1..65535>

パラメーター：

<1..65535> は LACP システムの優先順位を指定します。

ラックシステム優先なし

説明：

LACP システムの優先順位をデフォルト値 32768 に設定します。

ラックの状態を表示する

説明：

LACP の有効化/無効化ステータスとシステムプライオリティを表示します。

オプション(構成)#ス・ス・ス・データ内を一時

LACPは、シークをする。

LACP の使用価格: 32768

ラックを表示する

説明：

LACP 情報を表示します。

ラックアッグを表示する

説明：

LACP アグリゲータ情報を表示します。

構文：

ラック アッグ <トランク ID を表示する<トランク ID>

パラメーター：

<トランク ID> は、表示するトランク グループを指定します。

ラックポートを表示する

説明：

ポート別に LACP 情報を表示します。

構文：

ラックポート <ポート ID を表示>

パラメーター：

<ポート ID> は、表示するポートを指定します。



VLAN グループが存在する場合、スタティック トランク グループのすべてのメンバーが同じ VLAN グループ内に存在する必要があります。

6.5 VLAN設定

6.5.1 仮想LAN

仮想 LAN (VLAN) は、ブロードキャスト ドメインを制限する論理ネットワーク グループです。これにより、VLAN のメンバーのみが同じ VLAN メンバーからトラフィックを受信できるように、ネットワーク トラフィックを分離できます。基本的に、スイッチ内に VLAN を作成することは、ネットワーク デバイスのグループを別のレイヤ 2 スイッチに再接続することと論理的に同じです。ただし、すべてのネットワーク デバイスは、同じスイッチに物理的に接続されます。ステーションは複数の VLAN グループに属することができます。VLAN は、ユーザーが同じ LAN 上の別のネットワーク リソースにアクセスできないようにするため、ユーザーは同じ建物内の別のユーザーのハード ディスクとプリンタを見ることができません。VLAN は、ブロードキャスト トラフィックを減らすことでネットワーク パフォーマンスを向上させ、グループを分離することでネットワークのセキュリティを強化することもできます。

管理対象スイッチは、次の 2 種類の VLAN をサポートします。

- ポートベース
- IEEE 802.1Q (タグ)ベース

一度に有効にできるのは、2 つの VLAN タイプのうちの 1 つだけです。

ポート ベースの VLAN は VLAN で、宛先 MAC アドレスとそれに関連付けられたポートに基づいてパケット転送の決定が行われます。ポート ベースの VLAN を使用する場合は、各ポートで許可される発信ポートを定義する必要があります。

ポート ベースの VLAN では、1 つのポートから受信したパケットは、同じ VLAN に設定されているポートにのみ送信できます。次の図に示すように、スイッチ管理者はポート 1~2 を VLAN 1 として設定し、ポート 3~4 を VLAN 2 として設定しました。ポート 1 から受信したパケットは、ポート 2 にのみ転送できます。ポート 2 から受信したパケットは、ポート 1 にのみ転送できます。つまり、コンピュータ A はコンピュータ B にパケットを送信でき、その逆も可能です。VLAN 2 でも同じ状況が発生しました。コンピュータ C と D は相互に通信できます。ただし、VLAN1 のコンピュータは、異なる VLAN に属していたため、VLAN 2 のコンピュータを見ることができません。

IEEE 802.1Q(タグ)ベースの VLAN を使用すると、イーサネット機能はタグ付きパケットをブリッジ全体に伝播し、ネットワーク内に VLAN を作成し、ネットワーク上にまたがっていく統一された方法を提供します。出力パケットの場合は、このポートに関連付けられた VLAN ID でタグ付けするかしないかを選択できます。入力パケットの場合は、同じ VLAN グループ内にある限り、このパケットを特定のポートに転送できます。

802.1Q V LAN は、イーサネット パケットに追加されたタグを使用して動作します。このタグには、特定の VLAN グループに属する VLAN 識別子(VID)が含まれています。また、ポートは複数の VLAN に属することができます。

ポート ベースの VLAN とタグ ベース VLAN の違いは、タグ ベース VLAN がネットワークを論理的に接続された複数の LAN に本当に分割した点です。スイッチの周囲を取り取るパケットは、よりインテリジェントに転送できます。次の図では、タグを識別することにより、VLAN1 のコンピュータ A から送信されるブロードキャスト パケットを VLAN1 に直

接転送できます。

ただし、スイッチはポートベースの VLAN メカニズムでそれほどスマートではありませんでした。ブロードキャスト パケットは、sw2 のポート 4 にも転送されます。これは、ポートベースのVLANがスイッチ間で論理 VLAN グループを操作できないことを意味します。

VC-820M シリーズは、ポートベース VLAN とタグベース(802.1Q)VLAN モードの両方をサポートします。既定の構成は次のとおりです。

タグベース(802.1Q)VLAN。802.1Q VLAN では、最初はスイッチ上のすべてのポートがデフォルト VLAN に属し、VID は 1 です。



802.1Q VLAN モードでは、デフォルト VLAN グループを削除できません。

6.5.2 VLAN モード:ポートベース

パケットは、同じ VLAN グループのメンバー間でのみ送信できます。選択されていないすべてのポートは、別の単一の VLAN に属するものとして扱われます。ポートベースの VLAN が有効になっている場合、VLAN タグ付けは無視されます。

VLANモードを表示する

説明：

現在の VLAN モードを表示します。

VLANモード

説明：

VLAN モードを変更します。

構文：

VLANモード (無効|ポートベース|dot1q)

パラメーター：

(無効 | ポートベース | dot1q) は VLAN モードを指定します。



VLAN モードが変更されるたびに、ユーザは有効な値を取得するためにスイッチを再起動する必要があります。

6.5.3 高度な 802.1Q VLAN設定

入力フィルターの構成

パケットがポートで受信されると、スイッチを適用してドロップするか、タグなしパケットでない場合はドロップしないように制御できます。さらに、受信パケットがタグ付けされていても、受信ポートの同じ VLAN グループに属していない場合は、パケットを転送またはドロップするようにスイッチを制御することもできます。次の例では、同じ VLAN グループに属していない packet をドロップし、VLAN タグを含まないパケットを転送するようにスイッチを設定します。

VLAN コマンド:

VLANモードを表示する

説明:

現在の VLAN モードを表示します。

VLANモード

説明:

VLAN モードを変更します。

構文:

VLANモード (無効|ポートベース|dot1q)

パラメータ:

(無効 | ポートベース | dot1q) は VLAN モードを指定します。



VLAN モードが変更されるたびに、ユーザは有効な値を取得するためにスイッチを再起動する必要があります。

VLAN追加

説明:

VLAN エントリを追加または編集します。

構文:

VLAN追加 <1-4094> NAME (CPUポート|CPU ポートなし)

LIST [LIST] パラメータ:

<1-4094>は、VLAN ID またはグループ ID を指定します(ポート ベースの VLAN モードの場合)。

NAME はVLAN グループ名を指定します。

(CPU ポート|CPU ポートなし)この VLAN グループに属する CPU ポートを指定します。

LISTは、VLAN メンバーに設定するポートを指定します。

[リスト]タグ付きメンバーに設定するポートを指定します。入力しない場合、すべてのメンバーがタグなしに設定されます。

例えば。スイッチ(config)# VLANは 1 VLAN1 CPU-ポート 1-4を追加します。

この VLAN エントリには 4 つのメンバー(port1 から port4 まで)があり、すべてのメンバーにタグが付け解除されます。

VLANなし

説明：

VLAN エントリを削除します。

構文：

VLAN なし <1-

4094> パラメータ：

<1-4094> は、VLAN ID またはグループ ID (ポート ベースの VLAN の場合) を指定します。

例えば、VLAN 1なし

VLANを表示する

説明：

VLAN エントリ情報を表示します。

構文：

vlan を表示する [<1-

4094>] パラメータ：

<a0-4094> は VLAN ID を指定し、null はすべての有効なエ

ントリを意味します。

```
オプション(構成)#Vlan 1 より内の一時
```

```
Vlan          1
タイプ        :おとな
作成時間 (秒): 43 CPUポー
ト            :は
い
```

```
私
```

```
-----+-----
   ポート1 |タグな
   しポート2 |タグな
   しポート3 |タグな
   し Port4 |タグな
   しポート5 |タグな
   しポート6 |タグな
   し Port7 |タグな
   し Port8 |タグな
   しポート9 |タグな
```

VLAN を静的に表示

説明：

静的 VLAN エントリ情報を表示します。

vlan pvid を表示する

説明：

ポートの既定の VLAN ID を表示します。

構文：

vlan pvid [LIST] パ

ラメータを表示する：

[LIST] は、表示するポートを指定します。入力しない場合は、すべてのポートの PVID が表示されます。例えば。

```
オプション(構成)#Vlan pvidの一時。
```

```
>Pvid
```

```
-----+-----
```

```
ポート1 |1
```

```
ポート2 |1
```

```
ポート3 |1
```

```
ポート4 |1
```

```
ポート5 |1
```

```
ポート6 |1
```

```
ポート7 |1
```

```
ポート8 |1
```

```
ポート9 |1
```

```
ポート10 |1
```

VLANフィルタ

説明：

イングレスフィルタルールを設定します。

構文：

VLANフィルタ <有効 | 無効化> <有効 | 無効化> LIST

パラメータ：

<有効にする | disable> は、非メンバー パケットが転送されるかどうかを指定します。enable に設定されている場合は、このポートの設定された VID に一致する VID を持つパケットのみを転送します。

<有効にする | disable>は、タグなしフレームを削除するかしないかを指定します。有効に設定されている場合は、タグなしフレームをドロップします。

VLANフィルタを表示する

説明：

VLAN フィルタ設定を表示します。

構文：

VLAN フィルタを表示

[LIST] パラメータ：

[LIST] は、表示するポートを指定します。入力しない場合は、すべてのポートのフィルタルールが表示されます。

```

Switch(config)# show vlan filter
  Port | Rule 1 | Rule 2
  Filter (nonmbr) (untag)
-----+-----+-----
  Port1 | Drop    | Forward
  Port2 | Drop    | Forward
  Port3 | Drop    | Forward
  Port4 | Drop    | Forward
  Port5 | Drop    | Forward
  Port6 | Drop    | Forward
  Port7 | Drop    | Forward
  Port8 | Drop    | Forward
  Port9 | Drop    | Forward
  Port10 | Drop   | Forward
  Trk1  | Drop    | Forward

```

6.6 その他の構成

[いいえ] マックエイジタイム

説明：

MAC アドレスの期限切れを無効にするか、MAC アドレスの期限切れ時間を設定します。

構文：

mac-age-time MAC アドレスの期限切れを有効または無効にします。

マック年齢時間<6..1572858>

パラメーター：

<6.1572858> は、MAC アドレスの経過時間を指定します。MAC の経過時間は 6 で割り切れる必要があります。非アクティブな MAC アドレスがスイッチのアドレス テーブルに残っている秒数を入力します。

マック年齢を表示

説明：

MAC アドレスの経過時間を表示する

放送

説明：

ブロードキャスト ストーム フィルタ モードをオフ、1/2、1/4、1/8、1/16 に設定します。

構文：

ブロードキャストモード <オフ | 1/2 | 1/4 | 1/8 | 1/16>

ブロードキャスト選択

説明：

ブロードキャスト ストーム フィルタ パケットの種類を選択します。

- ユニキャスト/マルチキャスト: フラッドユニキャスト/マルチキャストフィルタ
- 制御パケット: 制御パケットフィルタ
- IP マルチキャスト: IP マルチキャストパケットフィルタ
- ブロードキャストパケット: ブロードキャストパケットフィルタ

構文:

ブロードキャスト選択<ユニキャスト/マルチキャスト | 制御パケット | ip-マルチキャスト | ブロードキャスト>

衝突再試行

説明:

衝突再試行の設定

構文:

衝突再試行 <オフ |16 |32 |48> パラ

メータ:

<16 |32 |48> – 半二重では、衝突再試行の最大値は 16 回(または 32,48 回)で、衝突が引き続き発生する場合はパケットがドロップされます。

off – 半二重では、衝突が発生した場合は永久に再試行します(デフォルト)。

6.7 管理の構成

6.7.1 ユーザー名とパスワードの変更

ホスト

説明:

スイッチ名を設定します。

構文:

ホスト名<名前-str>

パラメーター:

<name-str> スイッチ名を指定します。名前内にスペースを入きたい場合は、名前を引用符 (") で囲みます。

ホスト名なし

スイッチ名を工場出荷時のデフォルト設定にリセットします。

[いいえ]パスワード

説明:

マネージャまたはオペレーターのユーザー名とパスワードを設定または削除します。

構文：

[いいえ]パスワード <マネージャ | オペレータ | すべて>

パラメーター：

マネージャのユーザー名とパスワードは、Web UI でも使用されます。

6.7.2 IP構成

ユーザーは IP 設定を構成し、新しい値を入力できます。

IPアドレス**説明：**

IP アドレスとサブネット マスクを設定します。

構文：

IPアドレス <IP-addr> <IPマスク>

IPデフォルト ゲートウェイ**説明：**

デフォルト ゲートウェイの IP アドレスを設定します。

構文：

IPデフォルト ゲートウェイ <IP-addr>

ipを表示する**説明：**

IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを表示します。

情報の表示**説明：**

システム情報、MAC アドレス、バージョンなどの基本情報を表示します。

モード(構成)#[入数]

マチマ:VC-820M

: 8 10/100Mbps + 2G TP/SFP .ファックス:44:55:66

バージョン情報: 1.08

Cli: 1.07 802.1x:

y Dウィギンス:

イルド・イルDP:

igMP:

Dhcp

説明：

スイッチをdhcpクライアントとして設定すると、dhcpサーバから IP を取得できます。



このコマンドを設定すると、スイッチが再起動します。

dhcp を表示

説明：

dhcp の有効化/無効化を示します。

6.7.3 スイッチの再起動

ブート

説明：

スイッチを再起動 (ウォームスタート) します。

6.7.4 既定値にリセット

スタートアップ構成を消去する

説明：

次回の起動時に構成を既定の工場出荷時の設定にリセットします。

6.7.5 TFTP アップデートファームウェア

tftp ファームウェアのコピー

説明：

TFTP サーバからファームウェアをダウンロードします。

構文：

tftp ファームウェア <ip-addr> <リモートファイル> をコピーします。

パラメーター：

<ip-addr> TFTP サーバの IP アドレスを指定します。

<リモート ファイル> TFTP サーバからダウンロードするファイルを指定します。

6.7.6 構成ファイルの復元

tftp <実行構成をコピーする |フラッシュ>

説明：

TFTP サーバから設定を取得します。リモート・ファイルが CLI コマンドのテキスト・ファイルである場合は、キーワード **running-config** を使用します。

リモート ファイルがスイッチの設定フラッシュ イメージである場合は、キーワード **flash** を使用します。

構文：

コピー **tftp** <ランニング **config** |フラッシュ> <IP-addr> <リモートファイル>

パラメーター：

<ip-addr> TFTP サーバーの IP アドレスを指定します。

<リモート ファイル> TFTP サーバーからダウンロードするファイルを指定します。

6.7.7 バックアップ構成ファイル

<実行構成をコピーする |フラッシュ > **tftp**

説明：

TFTP サーバに設定を送信します。CLI コマンドのテキスト・ファイルに設定を保存する場合は、キーワード **RUNNING-config** を使用します。代わりに設定フラッシュ イメージを保存する場合は、キーワード **flash** を使用します。

構文：

コピー <実行構成 |フラッシュ> **tftp** <IP-addr> <リモートファイル>

パラメーター：

<ip-addr> TFTP サーバーの IP アドレスを指定します。

6.8 MACリミット

MAC 制限を使用すると、ユーザーは MAC アドラー **ess** テーブルに格納する MAC アドレスの最大数を設定できます。

MAC アドレス テーブルに格納するように選択された MAC アドレスは、先入れ先保存ポリシーの結果です。MAC アドレスが MAC アドレス テーブルに格納されると、タイムアウトになるまで残ります。「開口部」が使用可能な場合、スイッチはその開口部に表示される最初の新しい MAC アドレスを保存します。MAC アドレス テーブルにない MAC アドレスからのパケットはすべてブロックする必要があります。

ユーザーは MAC 制限設定を設定し、新しい値を入力できます。

マックリミット

説明：

MAC 制限を有効にします。

マックリミットなし

説明：

MAC 制限を無効にします。

マックリミット

説明：

ポートの MAC 制限値をオフにするには、0 を設定します。

構文：

Mac 制限 <ポートリスト> <1-64>

Mac-limit を表示する

説明：

MAC 制限情報 (MAC 制限の有効化/無効化、ポートごとの MAC 制限設定など) を表示します。

6.9 ポート ミラーリングの構成

ポート モニタリングは、すべてのポートで発生したトラフィックをスイッチの指定されたモニタリング ポートにリダイレクトする機能です。この機能を使用すると、ネットワーク管理者は LAN セグメント全体のトラフィックを監視および分析できます。管理対象スイッチでは、監視対象ポートに 1 つのポートを指定し、任意の 1 つのポートをモニタリング ポートとして指定できます。監視するトラフィックの方向を指定することもできます。適切に設定されると、モニタ対象の port から指定された方向のパケットがモニタリング ポートに転送されます。



既定のポート監視設定は無効です。

ミラー ポート

説明：

ポート監視情報を設定します。(RXのみ|TXのみ|RXとTXの両方)

構文：

ミラー ポート<rx |tx |両方> <ポート ID> <ポートリスト>

パラメータ：

rxは監視 rxのみを指定します。

txは監視 txのみを指定します。

両方ともrxと txの両方を監視します。

<ポート ID> は分析ポート ID を指定します。このポートは、監視対象のすべてのポートからトラフィックを受信します。

<ポート一覧> 監視対象のポート一覧を指定します。

ミラー ポートを表示する

説明：

ポ一ト監視情報ノ表示

6.10 サービスの品質

管理対象スイッチには、**最上位**、**SecHigh**、**SecLow**、**最低**の4つのトラ nsmission キューがあります。管理対象スイッチは、QoS モード設定に従って4つのキューからパケットを取得します。QoS モードが「無効」に設定されている場合、管理対象スイッチウィルはスイッチド ネットワーク上で QoS を実行しません。QoS モードが「高空から低」に設定されている場合、優先順位の高いキューが空になるまで、管理対象スイッチはキューからパケットを使い果たしません。QoS モードが "ウェイト比" に設定されている場合、管理d スイッチは比率に従ってキューからパケットを使い果たします。QoS モードのデフォルト値は"**重み 8:4:2:1**"です。つまり、スイッチは最初に最も高い優先順位を持つキューから8パケットを排気し、次に2番目に高い優先順位でキューから4パケットを排気します。

スイッチがパケットを受信すると、スイッチは受信パケットを入れるキューを決定する必要があります。管理対象スイッチでは、「802.1p プライオリティ」および「Sタティック ポート入力プライオリティ」の設定に従って、受信パケットをキューに入れます。受信パケットが 802.1p タグ付きパケットの場合、スイッチは 802.1p Priority 設定に従ってパケットをキューに入れます。

それ以外の場合、スイッチはスタティックポート入力プライオリティの設定に従ってパケットをキューに入れます。

- **802.1pプライオリティ:** 802.1p パケットのパケットヘッダーにはプライオリティタグがあります。優先度の範囲は 7~0 です。管理対象スイッチは、802.1p プライオリティと4つの伝送キュー間のマッピングを指定できます。デフォルト設定では、802.1p プライオリティ 0~1 のパケットは最も低い優先順位のキューに入れ、802.1p プライオリティ 2~3 のパケットは2番目に低い優先順位で que ue に入れられます。
- **スタティック ポートイングレスプライオリティ:** 各ポートには1つのプライオリティ 7~0 が割り当てられます。1つのポートから受信したパケットの優先順位は、受信ポートと同じ優先順位に設定されます。受信パケットの優先順位が決定されると、パケットはその優先順位を持つ 802.1p パケットとして扱われ、802.1p 優先度設定。

6.10.1 QoS構成

QoS モード:

- **ファーストカムファーストサービス:**送信されるパケットのシーケンスは、到着注文によって異なります。
- **低より前のすべての高:** 優先度の低いパケットの前に送信される優先度の高いパケット。
- **WRR:** 重み付けラウンドロビン。スイッチの優先度の高いキュー内のパケットに与えられるプリファレンスを選択します。これらのオプションは、優先度の低いパケットが送信される前に送信される優先度の高いパケットの数を表します。たとえば、8 高:4 秒高は、スイッチが4秒の優先順位パケットを送信する前に、8つの最も優先度の高いパケットを送信することを意味します。
- **Qosレベル:** 0~7 の優先度レベルは、最高、2番目、2番目に低い、最低のキューにマップできます。

コマンド:

qos優先順位

説明：

802.1p 優先順位を設定します。

構文：

qos優先順位 <先來サービス | 低前にすべて高い | 重み付けラウンドロビン> パラメータ：

[<最高>] [<秒-高重量>] [<秒低重量>] [<最も低い重量>]

例: qos 優先順位加重ラウンドロビン 8,4,2,1

qos レベル

説明：

優先度レベルを最高、2番目、2番目に低い、低に設定します。

構文：

qosレベル <最高 | 2番目に高い | 2番目に低い | 最低> <レベルリスト>

パラメーター：

<レベル リスト> 優先度レベルを高または低に指定しま

す。レベルは 0 ~ 7 の間でなければなりません。

例えば、qos レベル最高 7

例えば、qos レベルの最低値 0

qos を表示する

説明：

QoS 設定 (802.1p プライオリティを含む)、優先度 I を表示Evel

。例えば。

```

オプション(構成)#qosの一時。
QoS:
QoSの日:セクツの円を取り付け
: 8
4 秒 秒(秒): 2
00000000000000000000
00000000000000000000
00000000000000000000
0000000000-10-71

```

6.10.2 ポートごとの優先順位

ポートの優先順位

説明：

ポートの優先順位を設定します。

構文：

ポートの優先順位 <無効 [[0-7]> [<ポートリスト>]

パラメーター：

<ポート一覧> 設定するポートを指定します。入力しない場合は、すべてのポートが設定されます。

例えば、ポートプライオリティは1-5を無効にする

6.11 MAC アドレスの設定

クリアマックアドレステーブル

説明：

すべての動的 MAC アドレス テーブル エントリをクリアします。

mac アドレス テーブル 静的

説明：

スタティックユニキャストまたはマルチキャスト MAC アドレスを設定します。マルチキャスト MAC アドレス (01:00:5E で始まるアドレス) を指定する場合、最後のパラメータは *port-list* である必要があります。それ以外の場合は、*port-id* である必要があります。

構文：

mac アドレス テーブルスタティック <mac-addr> <VLAN-id> <ポート ID | ポート-リスト>

mac アドレス テーブルの静的な Mac-addrがありません

説明：

スタティックユニキャストまたはマルチキャスト MAC アドレス テーブル エントリを削除します。

構文：

mac アドレス テーブルなしスタティック *mac-addr* <vlan-id>

Mac アドレス テーブルを表示する

説明：

MAC アドレス テーブルエントリを表示します。

スイッチ(config)#は mac アドレス テーブルを表示します。

MACアドレス	VLAN	タイプ	ソース
00:08:B6:00:06:90	1	ダイナミック	9
00:40:63:00:65:30	1	ダイナミック	トルク1
00:03:63:F7:80:7F	1	ダイナミック	9

Mac アドレス テーブルを静的に表示する

説明：

静的 MAC アドレス テーブル エントリを表示します。

Mac アドレス テーブルマルチキャストを表示する

説明：

マルチキャスト関連の MAC アドレス テーブルを表示します。

smac-アドレステーブル静的

説明：

セカンダリ MAC アドレス テーブルでスタティック ユニキャストまたはマルチキャスト MAC アドレスを設定します。マルチキャスト MAC アドレス (01:00:5E で始まるアドレス) を指定する場合、最後のパラメータは *port-list* である必要があります。それ以外の場合は、*port-id* である必要があります。

構文：

smac-アドレス テーブル静的 <mac-addr> <VLAN-id> <ポート ID | ポートリスト>

smac-アドレステーブルを表示

説明：

セカンダリ MAC アドレス テーブル エントリを表示します。

smac-アドレステーブルマルチキャストを表示する

説明：

マルチキャスト関連のセカンダリ MAC アドレス テーブルを表示します。

[いいえ] フィルタ

説明：

MAC アドレス フィルタを設定します。宛先 MAC アドレスと VLAN タグの両方がフィルタ エントリと一致する場合、パケットはフィルタリングされます。パケットに VLAN タグがない場合は、VLAN ID 1 のエントリと一致します。

構文：

[なし] フィルタ <mac-addr> <VLAN-id>

フィルタの表示

説明：

フィルタの MAC アドレス テーブルを表示します。

6.12 STP/MSTPコマンド

[いいえ]スパニングツリー

説明：

スパニングツリーを有効または無効にします。

スパニングツリーの前方遅延

説明：

CIST のスパニング ツリー転送遅延を秒単位で設定します。

構文：

スパニングツリー前方遅延 <4-30> パ

ラメータ：

<4-30> は、転送遅延を秒単位で指定します。デフォルト値は 15 です。



aaを含む場合は、以下の場合があります。2*(1) <= 次の値
を持つ値を入力する場合 <= 2*(1=

スパニングツリーこんにちは時間

説明：

CIST のスパニング ツリーの hello 時間を秒単位で設定します。

構文：

スパニングツリーこんにちは時間

<1-10> パラメータ：

<1-10> は、こんにちは時間を秒単位で指定します。デフォルト値は 2 です。



aaを含む場合は、以下の場合があります。2*(こんにちは時
間 + 1) <= イマズ -= 2*(1 つの分の 1)

スパニングツリーの最大経過時間

説明：

スパニング ツリーの CIST の最大経過時間を秒単位で設定します。

構文：

スパニングツリーの最大経過時間 <6-

40> パラメータ：

<6 ~ 40> は、最大経過時間を秒単位で指定します。デフォルト値は 20 です。



The parameters must enforce the following relationships:

$$2*(hello-time + 1) \leq maximum-age \leq 2*(forward-delay - 1)$$

スパニングツリーの優先順位

説明：

CIST およびすべての MST のスパニング ツリー ブリッジプライオリティを設定します。

構文：

スパニングツリーの優先順位 <0-

61440> パラメータ:

<0 から 61440> はブリッジの優先順位を指定します。値は 4096 のステップでなければなりません。デフォルト値は 32768 です。

スパニングツリーを表示する

説明：

スパニングツリー情報を表示します。

スパニングツリー ポートを表示する

説明：

ポート情報ごとにスパニング ツリーを表示します。

構文：

スパニングツリー ポートを表示する [<

ポートリスト>] パラメータ:

<ポート一覧> 表示するポートを指定します。Null は、すべてのポートを意味します。

スパニングツリープロトコルバージョン

説明：

CIST のスパニング ツリー プロトコル バージョンを変更します。

構文：

スパニングツリー プロトコル バージョン <stp

[mstp>] パラメータ:

stp は、元のスパニングツリー プロトコル(STP,802.1d)を指定し

ます。mstp は、複数のスパニング ツリー プロトコル

(MSTP,802.1s)を指定します。

スパニングツリーの最大ホップ

説明：

CIST およびすべての MST のスパニング ツリー ブリッジの最大ホップを設定します。

構文：

スパニングツリーの最大ホップ <1-40>

パラメーター :

<1-40> は、ブリッジの最大ホップを指定します。既定値は **20** です。

スパニングツリー名

説明 :

CIST のスパニング ツリー ブリッジ名を設定します。

構文 :

スパニングツリー名 [**<名前文字列>**] パ

ラメータ :

<名前文字列> はブリッジ名を指定します。既定の名前は null です。

スパニングツリーリビジョン

説明 :

CIST のスパニング ツリー ブリッジ リビジョンを設定します。

構文 :

スパニングツリーリビジョン <0-

65535> パラメータ :

<0-65535> はブリッジリビジョンを指定します。既定値は **0** です。

スパニングツリーポートパス コスト

説明 :

CIST のスパニング ツリー ポート パス コストを設定します。

構文 :

スパニング ツリー ポート パスコスト <1-200000000> [<ポートリスト>]

パラメーター :

<1-200000000> ポート パスのコストを指定します。

<ポート一覧> 設定するポートを指定します。Null は、すべてのポートを意味します。

スパニングツリー ポートの優先順位

説明 :

CIST のスパニング ツリー ポートの優先順位を設定します。

構文 :

スパニングツリー ポートの優先順位 <0 - 240> [<

ポートリスト>] パラメータ :

<0 ~ 240> ポートの優先順位を指定します。値は 16 のステップでなければなりません。

<ポート一覧> 設定するポートを指定します。Null は、すべてのポートを意味します。

[いいえ] スパニングツリー ポート mcheck**説明：**

CIST のポートに MST BPDU を強制的に送信します。フォーマットがないということは、CIST のポートが MST BPDU を強制的に送信しないことを意味します。

構文：

[いいえ] スパニングツリー ポート mチェック

[<ポートリスト>] パラメータ：

<ポート一覧> 設定するポートを指定します。Null は、すべてのポートを意味します。

[いいえ] スパニングツリー ポート エッジ ポート**説明：**

CIST のポートをエッジ接続に設定します。[形式なし] は、CIST のポートを非エッジ接続に設定することを意味します。

構文：

[いいえ] スパニングツリー ポート エッジ ポート [<ポートリスト>]

パラメーター：

<ポート一覧> 設定するポートを指定します。Null は、すべてのポートを意味します。

[いいえ] スパニングツリー ポート 非stp**説明：**

CIST ポートでスパニング ツリー プロトコルを無効または有効にします。

構文：

[no] スパニングツリー ポート 非stp [<ポート

リスト>] Parameters:

<ポート一覧> 設定するポートを指定します。Null は、すべてのポートを意味します。

スパニングツリー ポートポイントツーポイント マック**説明：**

CIST のポートをポイントツーポイント接続に設定します。

構文：

スパニングツリー ポート ポイントツーポイント mac <auto |真 |false> [<

ポートリスト>] パラメータ：

autoはポイントツーポイントリンク自動接続を指定します。

trueは、ポイントツーポイントリンク **true** を指定します。

falseは、ポイントツーポイントリンク **false** を指定します。

<ポート一覧> 設定するポートを指定します。Null は、すべてのポートを意味します。

スパニングツリー mst

説明：

MSTI のスパニング ツリー ブリッジプライオリティを設定します。

構文：

スパニングツリー **mst <0-15> 優先度 <0-**

61440> パラメータ：

<0-15> は MSTI インスタンス ID を指定します。

<0 から 61440> MSTI ブリッジの優先順位を指定します。値は 4096 のステップでなければなりません。デフォルト値は 32768 です。

スパニング ツリー **mst <0-15> VLAN [<vlan-list>]**

説明：

VLAN リストをマップするように MSTI を設定します。

構文：

スパニングツリー **mst <0-15> vlan [<vlan-**

list>] パラメータ：

<0-15> は MSTI インスタンス ID を指定します。

<vlan-list> は、マップされた VLAN リストを指定します。Null は、すべての VLAN を意味します。

スパニング ツリー **MSt <0-15> ポート パス コスト <1-20000000> [<ポート リスト>]**

説明：

MSTI のスパニング ツリー ポート パス コストを設定します。

構文：

スパニング ツリー **mst <0-15> ポート パス コスト <1-20000000> [<**

ポート リスト>] パラメータ：

<1-200000000> はポート パスのコストを指定します。

<ポート一覧> 設定するポートを指定します。Null は、すべてのポートを意味します。

スパニング ツリー **MSt <0-15> ポートの優先順位 <0-240> [<ポートリスト>]**

説明：

MSTI のスパニング ツリー ポートの優先順位を設定します。

構文：

スパニング ツリー **mst <0-15> ポートの優先順位 <0-240> [<**

ポートリスト>] パラメータ：

<0 ~ 240> ポートの優先順位を指定します。値は16 のテップでなければなりません。

<ポート一覧> 設定するポートを指定します。Null は、すべてのポートを意味します。

スパニングツリー **mstなし**

説明：

特定の MSTI を削除します。

構文：

スパニングツリー mst <0-

15> パラメータなし:

<0-15> は MSTI インスタンス ID を指定します。

スパニングツリーを表示する

説明：

CIST のスパニングツリー情報を表示します。

スパニングツリー ポートを表示する

説明：

CIST のスパニング ツリー ポート情報を表示します。

構文：

スパニングツリー ポートを表示する [<

ポートリスト>] パラメータ：

<ポート一覧> 表示するポートを指定します。Null は、すべてのポートを意味します。

スパニングツリー MST 設定の表示

説明：

MST インスタンス マップを表示します。

構文：

スパニングツリー MST 設定の表示

スパニングツリー MST <0-15>

説明：

MST インスタンス情報を表示します。

構文：

スパニングツリー mst <0-15>

パラメータを表示する：

<0-15> は MSTI インスタンス ID を指定します。

スパニングツリー mst <0-15> ポート <1-10>

説明：

MST インスタンスの特定のポート情報を表示します。

構文：

スパニングツリー mst <0-15> ポート <1-10>

パラメータを表示する：

<0-15> は MSTI インスタンス ID を指定します。

<1-10> はポート番号を指定します。

VLAN スパニングツリーを表示する

説明：

port スパニング ツリーのステータスごとに VLAN ごとに表示します。

構文：

VLAN スパニングツリーを表示する

6.13 Snmp

単純なネットワーク管理プロトコル(SNMP)を実行するネットワーク管理は、スイッチを管理できます。

6.13.1 システムオプション

[いいえ]snmp

説明：

SNMP を有効または無効にします。

snmp ステータスの表示

説明：

SNMP の有効または無効の状態を表示します。

snmpシステム名

説明：

エージェント システム名文字列を設定します。

構文：

snmpシステム名 <名前-str>

パラメーター：

<名前-str>はシステム名文字列を指定します。

例: snmp システム名スイッチ

snmpシステムロケーション

説明：

エージェントの場所の文字列を設定します。

構文：

snmpシステムロケーション <ロケーション-str>

パラメーター：

場所の文字列を指定します。

例えば、snmpシステムロケーションオフィス

snmpシステムコンタクト

説明：

エージェント システムの連絡先文字列を設定します。

構文：

snmpシステムコンタクト <コンタクト str>

パラメーター :

<contact-str> は連絡先文字列を指定します。

例えば、snmpシステムコンタクトabc@sina.com

snmp システムを表示する

説明：

SNMP システム情報を表示します。

6.13.2 コミュニティストリング

snmp コミュニティ

説明：

SNMP コミュニティ ストリングを設定します。

構文：

snmp コミュニティ <read-sysinfo-only | 読み取り専用 | 読み取り/書き込みすべて > <コ

ミュニティ-str> パラメータ：

<コミュニティ str> はコミュニティ文字列を指定します。

例えば、snmp コミュニティ読み取り専用パブリック

snmp コミュニティなし

説明：

SNMP コミュニティ ストリングを削除します。

構文：

snmp コミュニティなし <コミュニティ-str>

パラメーター：

<コミュニティ str> はコミュニティ文字列を指定します。

例えば、snmp コミュニティなし

snmp コミュニティを表示する

説明：

SNMP コミュニティ ストリングを表示します。

6.13.3 トラップマネージャ

snmp トラップ

説明：

SNMP トラップ レシーバの IP アドレス、コミュニティ ストリング、およびポート番号を設定します。

構文：

snmp **トラップ** <ip-addr> [<コミュニティ-str>] [<1..65535>]

パラメーター：

<ip-addr> は IP アドレスを指定します。

<コミュニティ str> はコミュニティ文字列を指定します。

<1..65535> は、トラップ受信側のポート番号を指定します。指定しない場合、デフォルト値は 162 です。

例: snmp トラップ 192.168.200.1 パブリック

snmp トラップなし

説明：

トラップ受信機のIPアドレスとポート番号を削除します。

構文：

snmp トラップ<ip-addr> [<1..65535>]

パラメーター：

<ip-addr> は IP アドレスを指定します。

<1..65535> は、トラップ受信側のポート番号を指定します。

例えば、snmp トラップなし 192.168.200.1

snmp トラップを表示する

説明：

すべてのトラップ受信機を表示します。

6.14 Icmp

インターネットグループ管理電子化プロトコル (IGMP) は、インターネットプロトコル (IP) スイートの内部プロトコルです。

[いいえ]イグム

説明：

IGMP スヌーピングを有効/無効にします。

構文：

[なし]イグム

[いいえ]igmp ファストリー

説明：

IGMP スヌーピング高速休暇を有効/無効にします。有効にすると、スイッチは休暇レポートを送信するメンバーを高速削除し、それ以外の場合は 1 秒間待機します。

構文：

[なし]igmp ファストリー

【いいえ】イグムクエリア

説明：

IGMP スヌーピング クエリアを有効または無効にします。

構文：

[なし]イグムクエリア

[いいえ]イグムクロスVLAN

説明：

IGMP スヌーピングクロス VLANの有効化/無効化

構文：

[なし]イグムクロスVLAN

igmpを表示する

説明：

IGMP スヌーピング情報を表示します。

構文：

igmp <ステータスを表示する|ルーター |

グループ |表> パラメータ：

status はIGMP スヌーピングステータスおよび統計情報を指定します。

ルータはIGMP スヌーピング ルータの IP アドレスを指

定します。**グループ**は IGMP スヌーピング マルチキャ

スト グループ リストを指定します。**テーブル**は IGMP

スヌーピング IP マルチキャスト テーブル エントリを指

定します。

igmp clear_statistics

説明：

IGMP スヌーピング統計カウンタをクリアします。

6.15 802.1xプロトコル

[なし] ドット1x

説明：

802.1x を有効または無効にします。

構文：

[なし]ドット1x

RADIUS サーバーホスト

説明：

RADIUS サーバの IP、ポート番号、およびアカウンティング ポート番号を設定します。

構文：

RADIUS サーバー ホスト<IP-addr> <1024.. 65535> <1024..65535>

パラメーター：

<ip-addr> サーバーの IP アドレスを指定します。

最初の <1024.65535> は、サーバーのポート番号を指定します。

2 番目の <1024.65535> はアカウンティング・ポート番号を指定します。

RADIUS サーバーキー

説明：

802.1x 共有キーを設定します。

構文：

RADIUS サーバー キー <キー str>

パラメーター：

<key-str> は共有キー文字列を指定します。

半径サーバー nas

説明：

802.1x NAS 識別子を設定します。

構文：

RADIUS サーバー nas <ID-str>

パラメーター：

<id-str> は NAS 識別子文字列を指定します。

半径サーバーを表示する

説明：

RADIUS サーバ IP、ポート番号、アカウンティング ポート番号、共有キー、NAS 識別子などの RADIUS サーバ
情報を表示します。

dot1x timeout quiet-period

説明：

802.1x 静かな期間を設定します。(デフォルト: 60 秒)

構文：

dot1x タイムアウトサイレントピリオド<10-65535>

パラメーター：

<10-65535> は、静かな期間を秒単位で指定します。

dot1x タイムアウトtx-期間

説明：

802.1x Tx 期間を設定します。(デフォルト: 15 秒)。

構文：

dot1x タイムアウトtx-期間 <10-65535>

パラメーター：

<10-65535> は Tx 期間を秒単位で指定します。

ドット1x

説明：

802.1x サプリカント タイムアウトを設定する(デフォルト: 30 秒)

構文：

dot1x タイムアウト サプリカント<10-300>

パラメーター：

<10-300> はサプリカント タイムアウトを秒単位で指定します。

dot1x

説明：

RADIUS サーバのタイムアウトを設定します(デフォルト: 30 秒)。

構文：

dot1x タイムアウト半径サーバー <10-300>

パラメーター：

<10-300> は、半径サーバーのタイムアウトを秒単位で指定します。

1x-60

説明：

要求の最大再試行回数を 802.1x に設定します (デフォルト: 2 回)。

構文：

ドット1x 最大 req <1-10>

パラメーター :

<1-10> は、要求の最大再試行回数を指定します。

dot1x タイムアウト再認証期間

説明：

802.1x の再認証期間を設定します (デフォルト: 3600 秒)。

構文：

dot1x タイムアウト再認証期間 <30-65535>

パラメーター：

<30-65535> は、再認証期間を秒単位で指定します。

ドット1xを表示

説明：

802.1x 情報、静かな期間、Tx 期間、サブリカント タイムアウト、サーバー タイムアウト、最大要求数、および再認証期間を表示します。

ドット1xポート

説明：

ポート情報あたり 802.1x を設定します。

構文：

ドット1xポート<fu |fa | au |なし> <ポートリスト>

パラメーター：

fuは強制承認を指定します。**fa**

は強制許可を指定します。**au** は

承認を指定します。

noは、承認を無効にします。

<ポート一覧> 設定するポートを指定します。

ドット1xポートを表示

説明：

ポート通知ごとに 802.1x を表示します。

構文：

ドット 1x ポート<ポート一覧>を表示する

パラメーター：

<ポート一覧> 設定するポートを指定します。

6.16 アクセス制御リスト

ACL ルールによって転送またはドロップされるパケットには、IPv4 または非 IPv4 が含まれます。管理対象スイッチは、送信元と宛先の IP アドレス、プロトコルなどによってインデックス付けされたパケット フラグメントのテーブルを維持することで、パケットをブロックするために使用できます。

6.16.1 IPv4 ACL コマンド

acl なし

デ・クリプション:

ACL グループを削除します。

構文:

acl <1-220>

パラメータがあ

りません:

<1-220> はグループ ID を指定します。

例えば、acl 1 なし

ACL カウントなし

説明:

ACL グループ数をリセットします。

構文:

ACL カウントなし <グル

ープ ID> パラメータ:

グループ ID: <1-220> はグループ ID を指定します。

acl を表示する

説明:

ACL グループ情報を表示します。

構文:

acl を表示する [<1-

220>] パラメータ:

<1-220> はグループ ID を指定し、null はすべての有効なグループを意味します。

オプション(構成)#Acl 1 より内の一時。

Id : 1

とき : 内年:

VlanId : おとなしい

Ip月: SrcIPくしを付け

ス・ス・スおとな

```
Port ID : Any
Hit Octet Count : 165074
Hit Packet count : 472
```

acl (追加|編集)<1-220> (許可|拒否) <0-4094> ipv4 <0-255>

説明：

IPv4 の ACL グループを追加します。

構文：

```
acl追加 <1-220> (許可|拒否) <0-4094> ipv4 <0-255> A.B.C.D A.B.B.C.D (チェック|チェックオフ)
<0-65535> <0-10>
```

パラメーター：

<1-220>はグループ ID を指定します。

(許可|拒否)アクションを指定します。拒否: パケットをドロップします。

<0-4094>はVLAN ID を指定します。

<0-255>は IP プロトコルを指定します。

A.B.C.D は送信元 IP アドレスを指定します。

A.B.C.Dはマスク 0.0.0.0 を指定し、255.255.255.255 はすべてを比較します。

A.B.C.D は宛先 IP アドレスを指定します。

A.B.C.Dはマスク 0.0.0.0 を指定し、255.255.255.255 はすべてを比較します。

(チェック|チェックを取り消す)IP フラグメントを指定します。チェックを外す: IP フラグメント フィールドをチェックしません。

<0-65535> TCP または UDP が気にしない場合は、宛先ポート番号を指定します。

0-10>ポート ID を指定します。0 は気にしない

と言います。例えば。

```
次の値を取得します。Acl 1 1 ipv4 0 192.168.1.1 255.255.255.255 0.0.0 0.0.0.0.000。
```

この ACL ルールは、IP からすべてのパケットをドロップします 192.168.1.1 VLAN ID=1 および IPv4。

acl追加 <1-220> (qosvoip) <0-4094>

説明：

IPv4 の ACL グループを追加します。

構文：

```
acl追加 <1-220> (qosvoip) <0-4094> <0-7> <0-1F> <0-1F> <0-FF> <0-FFFF> <0-FFFF> <0-FFFF>
```

パラメーター：

<1-220> はグループ ID を指定します。

(qosvoip) はアクションを指定します。qos voip パケット調整。

<0-4094> speは VLAN ID を指定します。

<0-1F> はポート ID の値を指定します。

<0-1F> はポート ID マスクを指定します。

<0-FF> はプロトコル値を指定します。

<0-FF> はプロトコル マスクを指定します。

<0-FFFF> は送信元ポートの値を指定します。

<0-FFFF> は送信元ポート マスクを指定します。

<0-FFFF> は宛先ポート値を指定します。

<0-FFFF> は、コピー先のマスクを指定します。

例えば、aclは 1 qosvoip 1 7 1 1 0 0 0 0 を追加します。

6.16.2 非 IPv4 ACL コマンド

acl <1-220> コマンドはなく、acl <1-220> コマンドは IPv4 ACL コマンドと同じです。

acl追加 <1-220> (許可|拒否) <0-4094> nonipv4 <0-65535>

説明：

非 IPv4 の ACL グループを追加します。

構文：

acl追加 <1-220> (許可|拒否) <0-4094> 非 ipv4 <0-65535> パ

ラメータ：

<1-220> はグループ ID を指定します。

(permit|deny) はアクションを指定します。拒否: パケットをドロップします。

<0-4094> は VLAN ID を指定します。0 は気にしないとします。

<0-65535> はエーテルタイプを指定します。0 は気にしないとします。

例えば、aclは 1 拒否 0非ipv4 2054 を追加します。この ACL ルールは、エーテルタイプのすべてのパケットが 0x0806 および非 IPv4をドロップします。

6.17 バインディング

特定の IP アドレスと MAC アドレスを持つデバイスがネットワークを使用できるようにします。特定の IP アドレス、MAC アドレス、VLAN ID、ポート ID をバインドするように設定し、すべての条件が一致する場合はデバイスがスイッチを越えることができます。

6.17.1 SIP/SMAC バインディングコマンド

バインド

説明：

バインド機能を有効にします。

バインドなし

説明：

バインド機能を無効にします。

構文：

バインドなし<1-220>

パラメーター：

<1-220> はグループ ID を指定します。

例えば、バインドなし 1

バインドなし

説明：

バインド グループを削除します。

構文：

バインドなし<1-220>

パラメーター：

<1-220> はグループ ID を指定します。

例えば、バインドなし 1

バインドの表示

説明：

バインド グループ情報を表示します。

構文：

バインドを表示する

[<1-220>] パラメーター：

<1-220> はグループ ID を指定します。

例えば、バインド 1 を表示する

バインドの追加

説明：

バインド グループを追加します。

構文：

バインド追加 <1-220> A:B:C:E:F <0-4094> A.B.C.D <1-10>

パラメーター：

<1-220> はグループ ID を指定します。

A.B.C.D は MAC アドレスを指定します。

<0-4094> は VLAN ID を指定します。0 は気にしないとします。

A.B.C.D は送信元 IP アドレスを指定します。0.0.0.0 は気にしないとします。

A.B.C.D は IP アドレスを指定します。

<1-10> はポート ID を指定

します。

```
モード(構成)#1 00:11:22:33:44:55 0 192.168.1.1 1
```

このバインディング ルールは、デバイスの IP からのすべてのパケットクロス スイッチが 192.168.1.1 で、MAC が 00:11:22:33:44:55 であり、デバイスがスイッチ ポート ID=1 に接続することを許可します。

6.18 DHCP構成

[いいえ]dhcp-option82

説明：

dhcp-option82 機能を有効または無効にします。

構文：

[いいえ] dhcp-option82

dhcp-option82

説明：

dhcp-option82 ポートを有効または無効にします。

構文：

dhcp-option82 <有効 |> [<ポート一覧>]を無効にします

パラメーター：

<有効 |disable> dhcp-option82 ポートを有効または無効にします。

<ポート一覧> 設定するポートを指定します。入力しない場合は、すべてのポートが設定されます。

[いいえ]dhcp-リレー

説明：

dhcp-relay 機能を有効または無効にします。

構文：

[いいえ]dhcp-リレー

dhcp-リレー

説明：

dhcp-option82 ポートを有効または無効にします。

構文：

dhcp-option82 <有効 |> [<ポート一覧>][<IP アドレス>]を無効にする

パラメーター：

<有効 |disable> dhcp-relay ポートを有効または無効にします。

<ポート一覧> 設定するポートを指定します。入力しない場合は、すべてのポートが設定されます。

<IP アドレス> DHCP サーバーの IP アドレスを指定します。

dhcp-ルーター

説明：

ドメイン内の DHCP サーバーに接続するためのポートを割り当てます。

構文：

dhcp-router [<ポート一覧>]

パラメーター：

<ポ一ト一覽> 設定するポ一トを指定します。入力しない場合は、すべてのポ一トが設定されます。

6.19 VDSL2コマンド

インターフェイス	VDSL インターフェイスのコマンド
プロファイル	VDSL プロファイルのコマンド

6.19.1 VDSL2 インターフェイスコマンド

インターフェイスxdsi

説明：

xdsi インターフェイスのコマンド

構文：

インターフェイスxdsi [表示 |設定]

インターフェイスxdsi ショー oid

説明：

VDSL ロジック MIB エントリの表示

構文：

インターフェイスxdsiはoid <ポート

ID> <oid> パラメータを表示します。

<1-8> または <1-24> ポート ID

インターフェイスxdsi ショー ロイド

説明：

VDSL リアル MIB エントリを表示

構文：

インターフェイスxdsiショー roid <ポー

トID> <oid> パラメータ：

<1-8> または <1-24> ポート ID

インターフェイスxdsi 表示ステータス

説明：

明細行ステータスの表示

構文：

インターフェイスxdsi は、ステータ

ス <ポート ID> パラメータを表示します

。

<1-8> または <1-24> ポート ID

スイッチ(config)#インターフェイス **xdsl** はステータス 1 を表示します

行 1 の状態 (基本): ショータイム

	値	の説明
実績データレート	100992	(米国) Kb/s
アクチュアルデータレート	100992	(DS) Kb/s
SNRマージン	79	(米国) 0.1dB
SNRマージン	251	(DS) 0.1dB
ファームウェアのバージョン	10201	

1 行目のステータス (前受):

	アップストリーム	ダウンストリーム	
実際の遅延	5	5	ミリ秒
実際のINP	20	20	0.1 シンボル
15M CV	0	0	
1日CV	0	0	
合計CV	0	0	
15M FEC	0		
1日FEC	728	0	
合計FEC	728	0	
以前のデータレート	0	100992	Kbps
達成可能率	106023	169169	Kbps
電氣的長さ	11 11	0.1dB	
SNRマージン	NA	--	(US0,--) 0.1 dB
SNR マージン	80	251	(US1,DS1) 0.1 dB
SNR マージン	80	250	(US2,DS2) 0.1 dB
SNR マージン	78	251	(US3,DS3) 0.1 dB
SNR マージン		NA	NA
		(US4,DS4) 0.1 dB	
15M経過時間	488	488	秒
15M FECS	0		
15M ES	0		
15M SES	0	0	
15M損失	0	0	
15M UAS	0	0	
1日経過時間	69788	69788	秒 1
日 FECS	7	5	
1日 ES	0	5	
1日 SES	0	0	
1日の損失	0	0	
1日 UAS	0	0	
合計FECS	0	0	
合計ES	0	0	

合計SES	0	0
合計損失	0	0
合計UAS	0	0
スイッチ(構成)#		

インターフェイスxdsl ショー pm_line_curr

説明：

xdsl 線の現在のカウンタを表示します

構文：

インターフェイスxdsl はpm_line_curr

<portid> パラメータを示します。

<1-8> または <1-24> ポート ID

インターフェイスxdsl ショー pm_ch_curr

説明：

xdslチャンネルの現在のカウンタを表示する

シンタx:

インターフェイスxdslは、pm_ch_curr

<portid> パラメータを示しています。

<1-8> または <1-24> ポート ID

インターフェイスxdsl ショー発明

説明：

xdsl明細行の在庫を表示します

構文：

インターフェイスxdsl ショー invent

<portid> パラメータ:

<1-8> または <1-24> ポート ID

インターフェイスxdsl ショーしきい値

説明：

xdsl 回線のしきい値を表示

構文：

インターフェイスxdsl はしきい値

<portid> パラメータを表示します。

<1-8> または <1-24> ポート ID

インターフェイスxdsl ショー テーブル

説明：

xdsl 線のmib テーブルを表示

構文：

インターフェイスxdsi 表示テーブル行

<portid> パラメータ:

<1-8> または <1-24> ポート ID

6.19.2 VDSL2 プロファイルコマンド

プロファイルxdsi-ライン

説明:

xdsi-lineのコマンド

構文:

プロファイルxdsi-線の新しい

<profile_name> プロファイル xdsi-ラ

インデル <profile_name> プロファイ

ル xdsi-線ショー

プロファイルxdsi-ラ

イン保存プロファイ

ル xdsi-line init プロ

ファイル xdsi-line

プロファイルxdsi-ライン new

説明:

新しいxdsi プロファイルを作成する

構文:

プロファイルxdsi-行の新しい <profile_name>

プロファイルxdsi-ラインデル

説明:

xdsi プロファイルの削除

構文:

プロファイルxdsi-線のデル <profile_name>

プロファイルxdsi-ラインショー

説明:

すべてのプロファイル名を表示する、または指定したプロファイルの詳細情報を表示する

シンタx:

プロファイルxdsi-線ショー <プロファイル>

<profile_name> プロファイル xdsl-線ショー <プ

ロファイル>

プロファイルxdsl-ライン ショー <プロファイル>

プロファイルxdsl-行表示プロファイル

説明 :

存在するプロファイル名を表示

構文：

プロファイルxDSL-ラインショー

モード(構成)#内ー Xdsl-?

VDSL・ス・ド・ス

```
=====
VDSL の知名: VDSL の場合、 VDSL
の場合のユーザー 1 の設定の場合の
ユーザーの場合、ユーザー 1 の
VDSL の場合のユーザーの場合のユ
ーザーの場合、ユーザー 2 VDSL の
場合、ユーザー 2 VDSL の次の手順:
ユーザー 2 VDSL の次の手順: user4
VDSL の場合は、ユーザー 5VDSL
の場合は、ユーザー 6 VDSL の場合
は、ユーザー 6 VDSL の場合は、次
の手順を実行します。 7 VDSL の場
合、ユーザー 8 VDSL の設定の場合
は、ユーザー 9 VDSL の設定の場合:
ユーザー 9 VDSL の場合の内諾: ユ
ーザー 10 VDSL の場合は、ユーザ
ー 11 VDSL の設定: ユーザー 11
VDSL の場合もユーザー 12 VDSL
の vDSL の場合は、ユーザー 13
VDSL の使用 user15 VDSL の知見:
```

プロファイルxDSL-ラインショー プロファイル

説明：

システム サポート プロファイル ID の表示

シン税:

プロファイルxDSL-ラインショー プロファイル

モード(構成)#内ー Xdsl-10ス分・その場合

```
AnnexA_R_POTS_D32_EU32_30a
の AnnexA_R_POTS_D 32_17a
32_EU
AnnexA_R_POTS_D32_EU32_EU3
```

AnnexA_R_POTS_D-32_EU-32_12a
 AnnexA_R_POTS_D-32_EU-32_8a
 AnnexA_R_POTS_D-32_EU-32_8b
 AnnexA_R_POTS_D-32_EU-32_8c
 AnnexA_R_POTS_D-32_EU-32_8d
 AnnexA_R_POTS_D-64_EU-64_30a_NUS0
 AnnexA_R_POTS_D-64_EU-64_17a
 AnnexB_B7-1_997-M1c-A-7
 AnnexB_B7-2_997-M1x-M-8
 AnnexB_B7-3_997-M1x-M
 AnnexB_B7-4_997-M2x-M-8
 AnnexB_B7-5_997-M2x-A
 AnnexB_B7-6_997-M2x-M
 AnnexB_B7-9_997E17-M2x-A
 AnnexB_B7-10_997E30-M2x-NUS0
 AnnexB_B8-1_998-M1x-A
 AnnexB_B8-2_998-M1x-B
 AnnexB_B8-4_998-M2x-A
 AnnexB_B8-5_998-M2x-M
 AnnexB_B8-6_998-M2x-B
 AnnexB_B8-8_998E17-M2x-NUS0
 AnnexB_B8-9_998E17-M2x-NUS0-M
 AnnexB_B8-10_998ADE17-M2x-NUS0-M
 AnnexB_B8-11_998ADE17-M2x-A
 AnnexB_B8-12_998ADE17-M2x-B
 AnnexB_B8-13_998E30-M2x-NUS0
 AnnexB_B8-14_998E30-M2x-NUS0-M
 AnnexB_B8-15_998ADE30-M2x-NUS0-M
 AnnexB_B8-16_998ADE30-M2x-NUS0-A
 AnnexC_POTS_25-138_b
 AnnexC_POTS_25-276_b
 AnnexC_TCM-ISDN

プロファイルxdsi-ライン保存

説明：

すべてのプロファイル構成を保存

構文：

プロファイルxdsi-ライン保存

プロファイルxdsi-ライン init

説明：

セーブファイルからプロファイルを初期化する

構文：

プロファイルxdsI-ラインセット

説明：

xdsI プロファイルのコマンドを設定する

プロファイルxdsI-ラインセットdslバンドプラン

説明：

VDSL 設定プロファイルのプロファイルとバンドプランの選択に依存する PSD マスク、PSD レベル、およびサブキャリア マスクの定義済みセットを有効にするには

構文：

プロファイルxdsI-ラインセットdslバンドプラン <profile_name> <値>

プロファイルxdsI-ラインセットの修正率

説明：

プロファイルをビット/s で固定レートを使用するようにSp が設定する

構文：

プロファイルxdsI-ラインセットの修正率 <profile_name> <値>

プロファイルxdsI-ラインセットマージンターゲット-snr-ds

説明：

信号ノイズ比マージンターゲットダウンストリーム設定

構文：

プロファイルxdsI-ラインセットマージンターゲット-snr-ds

<profile_name> <値 -dec> パラメーター:

<0-310>

プロファイルxdsI-ラインセットマージンターゲット-snr-us

説明：

信号ノイズ比マージンターゲットアップストリーム設定

構文：

プロファイルxdsI-ラインセットマージンターゲット-snr-us

<profile_name> <値 -dec> パラメーター:

<0-310>

プロファイルxdsI-ラインセットマージン-最大 snr-ds

説明：

信号ノイズ比マージン最大下流設定

構文：

プロファイルxdsi-ラインセット マージン-最大 snr-ds <profile_name> <値 -dec>

パラメーター :

<0-310>

内一Xdsl-10-0-snr-us

説明 :

信号ノイズ比マージン最大アップストリーム設定

構文 :

プロファイルxdsl-ラインセット マージン-最大-snr-us

<profile_name> <値 -dec> パラメータ:

<0-310>

内一Xdsl- ラ・ド・ラ・ル・ル・スナーds

説明 :

信号ノイズ比マージン最小下流設定

構文 :

プロファイルxdsl-ラインセット マージン-最小-snr-ds

<profile_name> <値 -dec> パラメータ:

<0-310>

内一Xdsl-s

説明 :

信号ノイズ比マージンマージン最小アップストリーム設定

構文 :

プロファイルxdsl-ラインセット マージン-最小-snr-us

<profile_name> <値 -dec> パラメータ:

<0-310>

内一Xdsl-a d-d-s-s1

説明 :

CH1 下流方向設定の最大データレート

構文 :

プロファイルxdsl-ラインセット レート 制限-最大 ds-ch1

<profile_name> <値 -dec> パラメータ:

<0-200000> kbps

内一Xdsl-a-s--s-s-ch1

説明：

CH1 アップストレの最大データレート

構文：

プロファイルxdsi-ラインセット レート 制限-最大-us-ch1

<profile_name> <値 -dec> パラメータ：

<0-200000> kbps

プロファイルxdsi-ラインセットレート-制限-最大 ds-ch2

説明：

下流方向設定の CH2 最大データ レート

構文：

プロファイルxdsi-ラインセット レート 制限-最大 ds-ch2

<profile_name> <値 -dec> パラメータ：

<0-200000> kbps

プロファイルxdsi-ラインセットレート-制限-最大-us-ch2

説明：

上流方向設定の CH2 最大データ レート

構文：

プロファイルxdsi-ラインセット レート 制限-最大-us-ch2

<profile_name> <値 -dec> パラメータ：

<0-200000> kbps

プロファイルxdsi-ラインセットレート-最小 ds-ch1

説明：

下流方向設定の CH1 最小データ レート

構文：

プロファイルxdsi-ラインセットレート-最小-ds-ch1 <profile_name> <値

-dec> パラメータ：

<0-200000> kbps

プロファイルxdsi-ラインセットレート-最小-us-ch1

説明：

上流方向設定の CH1 最小データ レート

構文：

プロファイルxdsi-ラインセットレート-最小-us-ch1 <profile_name> <値

-dec> パラメータ：

<0-200000> kbps

プロファイルxdsi-ラインセットレート-最小 ds-ch2

説明：

下流方向設定のCH2 最小データ レート

構文 :

プロファイルxdsi-ラインセット レート-最小-ds-ch2 <profile_name> <

値 -dec> パラメータ:

<0-200000> kbps

プロファイルxdsi-ラインセットレート-最小-us-ch2

説明 :

上流方向設定の CH2 最小データ レート

構文 :

プロファイルxdsi-ラインセットレート-最小-us-ch2 <profile_name> <値

-dec> パラメータ:

<0-200000> kbps

プロファイルxdsi-ラインセット最大遅延-ds-ch1

説明 :

下流方向設定での CH1 最大インターリーブ遅延

構文 :

プロファイルxdsi-ラインセット最大遅延-ds-ch1<profile_name> <

値 -dec> パラメータ:

<0-63>ミリ秒

プロファイルxdsi-ラインセット最大遅延-us-ch1

説明 :

上流方向設定での CH1 最大インターリーブ遅延

構文 :

プロファイルxdsi-ラインセット最大遅延-us-ch1 <profile_name> <

値 -dec> パラメータ:

<0-63>ミリ秒

プロファイルxdsi-ラインセット inp-min-prot-ds-ch1

説明 :

CH1ダウンストローム最小インパルスノイズプロクシオン4.3125kHz(シンボル)設定

構文 :

プロファイルxdsi-ラインセット inp-min-prot-ds-ch1 <profile_name>

<値 -dec> パラメータ:

profile xdsl-line set inp-min-prot-us-ch1

説明：

CH1 4.3125kHz(シンボル)設定でのCH1アップストローム最小インパルスノイズ保護

構文：

プロファイルxdsl-ラインセット inp-min-prot-us-ch1 <profile_name>

<値-dec> パラメータ：

<1-18>

内一Xdsl-a inp-min-prot8-ds-ch1

説明：

8.625kHz設定のCH1ダウンストローム最小インパルスノイズ保護

構文：

プロファイルxdsl-線セット inp-min-prot8-ds-ch1<profile_name> <値 -

dec> パラメータ：

<1-17>

内一Xdsl-a inp-min-prot8-us-ch1

説明：

8.625kHz設定のCH1アップストローム最小インパルスノイズ保護

構文：

プロファイルxdsl-ラインセット inp-min-prot8-us-ch1 <profile_name>

<値 -dec> パラメータ：

<1-17>

プロファイルxdsl-ラインセット最大遅延-ds-ch2

説明：

下流方向設定での CH2 最大インターリーブ遅延

構文：

プロファイルxdsl-ラインセット最大遅延-ds-ch2 <profile_name> <

値 -dec> パラメータ：

<0-63>ミリ秒

内一Xdsl-a は、a-s-ch2

説明：

上流方向設定での CH2 最大インターリーブ遅延

構文：

プロファイルxdsi-ラインセット最大遅延-us-ch2 <profile_name> <
値 -dec> パラメータ:

<0-63>ミリ秒

プロファイルxdsI-ラインセット inp-min-prot-ds-ch2

説明：

4.3125kHz(シンボル)設定でのCH2ダウンストローム最小インパルスノイズ保護

構文：

プロファイルxdsI-ラインセット inp-min-prot-ds-ch2 <profile_name>

<値 -dec> パラメータ：

<1-18>

プロファイルxdsI-ラインセット inp-min-prot-us-ch2

説明：

4.3125kHz(シンボル)設定でのCH2アップストローム最小インパルスノイズ保護

構文：

プロファイルxdsI-ラインセット inp-min-prot-us-ch2 <profile_name>

<値 -dec> パラメータ：

<1-18>

プロファイルxdsI-ラインセット inp-min-prot8-ds-ch2

説明：

8.625kHz設定のCH2ダウンストローム最小インパルスノイズ保護

構文：

プロファイルxdsI-ラインセット inp-min-prot8-ds-ch2 <profile_name>

<値 -dec> パラメータ：

<1-17>

プロファイルxdsI-ラインセット inp-min-prot8-us-ch2

説明：

8.625kHz設定のCH2アップストローム最小インパルスノイズ保護

構文：

プロファイルxdsI-ラインセット inp-min-prot8-us-ch2 <profile_name>

<値 -dec> パラメータ：

<1-17>

7. SWITCH OPERATION

7.1 住所テーブル

スイッチはアドレス テーブルを使用して実装されます。このアドレス テーブルは、多くのエントリで構成されます。各エントリは、MAC アドレス、ポート番号など、ネットワーク内の一部のノードのアドレス情報を格納するために使用されます。この情報は、イーサネット スwitchの学習手順から取得されます。

7.2 学習

いずれかのポートから1つのパケットが受信されると、スイッチは送信元アドレス、ポート番号を記録します。およびアドレス テーブル内のその他の関連情報。この情報は、future パケットの転送またはフィルタリングを決定するために使用されます。

7.3 転送とフィルタリング

1つのパケットがイーサネット スwitchingの何らかのポートから送信されると、送信元アドレス学習以外の宛先アドレスもチェックされます。イーサネット スwitchingは、宛先広告ドレスのアドレス テーブルをルックアップします。見つからない場合、このパケットは、このパケットが入ってくるポートを除く他のすべてのポートに転送されます。これらのポートは、接続されているネットワークにこのパケットを送信します。見つかり、宛先アドレスがこのパケットの受信ポートとは異なるポートにある場合、イーサネット スwitchingは、アドレス テーブルからの情報に従って、この宛先アドレスが配置されているポートにこのパケットを転送します。ただし、宛先アドレスがこのパケットが受信されたポートと同じポートにある場合、このパケットはフィルタリングされます。それによって、ネットワークのスループットと可用性が向上します。

7.4 ストア アンド フォワード

ストア アンド フォワードは、パケット転送手法の1つです。ストア アンド フォワード イーサネット スwitchingは、着信フレームを内部バッファに格納し、送信前に完全なエラー チェックを実行します。したがって、エラーパケットが発生せず、ネットワークが効率と安定性を必要とする場合に最適です。

イーサネット スwitchはパケット ヘッダーから宛先アドレスをスキャンし、着信ポートに対してルーティング テーブルをサーチし、必要な場合にのみパケットを転送します。高速転送により、サーバーをネットワークに直接接続するためのスイッチが魅力的になり、スループットと可用性が向上します。これまでで最も一般的に存在ハブをセグメント化するために使用される方法は、ほぼ常に全体的なパフォーマンスが向上します。イーサネット スwitchingは、従来のケーブル配線とダブタを使用して帯域幅を大幅に増やすために、任意のイーサネット ネットワーク環境で簡単に設定できます。イーサネット スwitchingの学習機能により、各着信パケットおよび発信パケットの送信元アドレスと対応するポート番号がルーティング テーブルに格納されます。この情報は、宛先アドレスが送信元アドレスと同じセグメント上にあるパケットをフィルタリングするために使用されます。これにより、ネットワーク トラフィックがそれぞれのドメインに限定され、ネットワーク全体の負荷が軽減されます。

スイッチは「ストアアンドフォワード」を実行します。したがって、エラー パケットは発生しません。より確実に、再伝送速度を低減する。パケット損失は発生しません。

7.5 自動ネゴシエーション

スイッチの STP ポートには「自動ネゴシエーション」が組み込まれています。この技術は自動的に可能な限り最高の設定

別のネットワーク デバイスとの接続が確立されるときに帯域幅 (通常は電源オンまたはリセット)。これは、両方のデバイスの 2 番目のモードと速度が接続され、可能な場合、10BASE-T デバイスと 100BASE-TX デバイスの両方が半二重モードまたは全二重モードでポートに接続できることを示します。

接続されているデバイスが次の場合 :	100BASE-TX ポートは次のように設定されます。
10Mbps、自動ネゴシエーションなし	10Mbps。
10Mbps、自動ネゴシエーション付き	10/20Mbps (10BASE-T/全二重)
100Mbps、自動ネゴシエーションなし	100 mbps
100Mbps、自動ネゴシエーション付き	100/200Mbps (100BASE-TX/全二重)

8. トラブルシューティング

この章には、問題の解決に役立つ情報が含まれています。イーサネットスイッチが正常に機能していない場合は、このマニュアルの手順に従ってイーサネットスイッチが設定されていることを確認します。

■ リンク LED が点灯していない。

ソリューション：

ケーブル接続を確認し、イーサネットスイッチのデュプレックスモードを取り外します。

■ 一部のステーションは、他のポートにある他のステーションと通信できません。解決策：

VLAN 設定、トランク設定、またはポートの有効/無効ステータスを確認してください。

■ パフォーマンスが悪い

。

ソリューション：

イーサネットスイッチの全二重ステータスを確認します。イーサネットスイッチが全二重に設定され、パートナーが半二重に設定されている場合、e のパフォーマンスは低下します。ポートの入出力レートもご確認ください。

■ スイッチがネットワークに接続しない理由。ソリューション：

1. スイッチの LNK/ACT LED を確認する
2. スイッチの別のポートを試す
3. ケーブルが正しく取り付けられていることを確認します。
4. cable が正しいタイプであることを確認します。
5. 電源を切ります。しばらくすると、もう一度電源を入れます。

■ 100BASE-TX ポート リンク LED は点灯しますが、トラフィックは不規則です。解決策：

接続されているデバイスが専用の全二重に設定されていないことを確認します。一部のデバイスでは、物理スイッチまたはソフトウェアスイッチを使用してデュプレックスモードを変更します。自動ネゴシエーションでは、この種類の全二重設定が認識されない場合があります。

■ スイッチの電源が入らない。

ソリューション：

1. AC 電源 c が挿入されていないか、障害が発生していません。
2. AC電源コードが正しく挿入されていることを確認します。
3. コードが正しく挿入されている場合は、電源コードを交換してください。スイッチの代わりに別のデバイスを接続して、AC電源が動作していることを確認します。
4. そのデバイスが動作する場合は、次の手順を参照してください。
5. そのデバイスが動作しない場合は、AC電源を確認します。

■ IP アドレスとパスワードが変更されたか、忘れられています。

IP アドレスをデフォルトの IP アドレス "192.168.0.100" にリセットするか、パスワードをデフォルト値にリセットするには、前面パネルのハードウェアリセットボタンを約**10秒間**押します。デバイスを再起動した後、192.168 の同じサブネット内の管理 Web インターフェイスにログインできます。0.xx.

APPENDIX A—RJ45 Pin Assignment

A.1 スイッチの RJ45 ピン割り当て

1000Mbps、1000BASE T

連絡先	Mdi	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

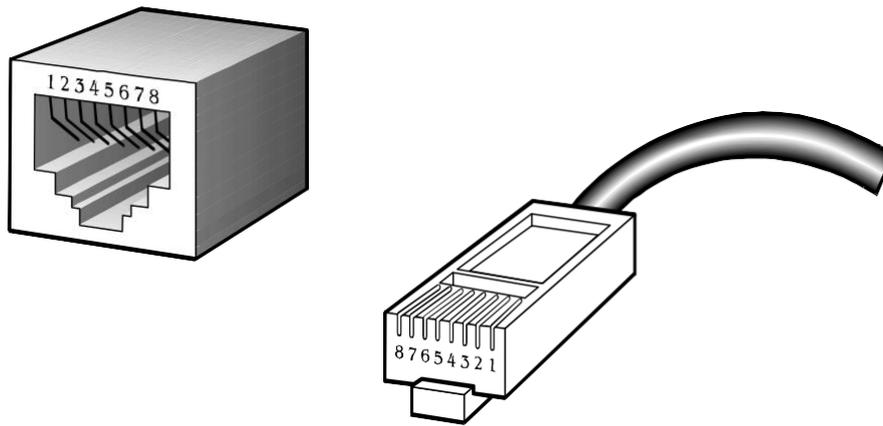
ツイストペアケーブル内または配線パネルでのクロスオーバー機能の暗黙的な実装は、明示的に禁止されていますが、この規格の範囲を超えています。

A.2 10/100Mbps、10/100BASE-TX

10/100Mbps イーサネット スイッチを別のスイッチ、ブリッジ、またはハブに接続する場合は、ストレート ケーブルまたはクロスケーブルが必要です。スイッチの各ポートは、自動 MDI/MDI-X 検出をサポートします。つまり、クロスケーブルを作成しなくても、スイッチを Ether ネットデバイスに直接接続できます。次の表と図は、標準の RJ45 レセプタクル/コネクタとそのピン割り当てを示しています。

RJ45 コネクタピンの割り当て		
連絡先	Mdi メディア依存インターフェイス	MDI-X メディア依存インターフェイスクロス
1	Tx + (送信) Rx + (受信)	
2	Tx - (送信) Rx - (受信)	
3	Rx + (受信) Tx + (送信)	
4, 5	未使用	
6	Rx - (受信) Tx - (送信)	
7, 8	未使用	

標準ケーブル、RJ45ピン割り当て



標準RJ45レセプタクル/コネクタ

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight-through cable and crossover cable connection:

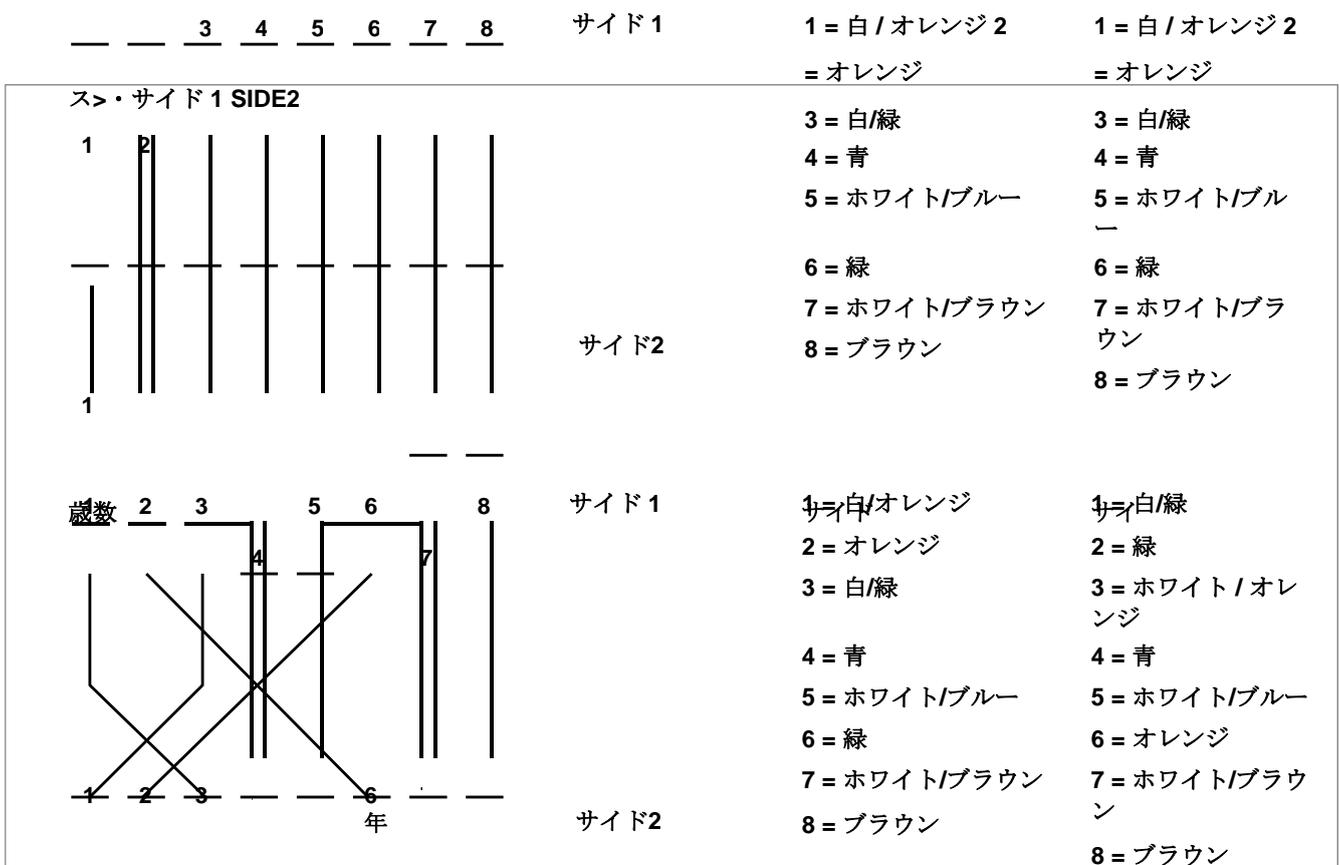


図 A-1: ストレートケーブルとクロスオーバーケーブル

ネットワークにケーブルを展開する前に、接続されているケーブルのピンの割り当てと色が上の図と同じであることを確認してください。