

商標

Copyright©PLANETTechnology Corp.2016。

内容は予告なく改訂される場合があります。

PLANETは、PLANET Technology Corp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 Technology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適切に機能することを保証するものではありません。

品質、パフォーマンス、商品性、または適合性に関する、黙示または明示の保証および表明

特定の目的。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ました。PLANETは責任を放棄します
発生した可能性のある不正確または脱落について。

このユーザーズマニュアルの情報は、予告なしに変更されることがあり、の責任を表すものではありません。

惑星。PLANETは、このユーザーズマニュアルに含まれている可能性のある不正確さについて責任を負いません。PLANETは

この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義務はなく、改善を行う権利を留保します。

このユーザーズマニュアルおよび/またはこのユーザーズマニュアルに記載されている製品に対して、いつでも予告なしに。

このマニュアルに不正確、誤解を招く、または不完全な情報を見つけた場合は、コメントをいただければ幸いです。

提案。

FCC警告

この機器はテスト済みであり、FCCのパート15に準拠したクラスAデジタルデバイスの制限に準拠していることが確認されています。

ルール。これらの制限は、機器の操作時に有害な干渉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

商業環境で。この機器は、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、設置されていない場合は、

取扱説明書に従って使用すると、無線通信に有害な干渉を引き起こす可能性があります。この操作

住宅地の機器は有害な干渉を引き起こす可能性があります。その場合、ユーザーは修正する必要があります

彼自身の費用で干渉。

CEマーク警告

これはクラスAの製品です。家庭環境では、この製品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

適切な対策を講じる必要があります。

デバイスの省エネノート

この電力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、電源ケーブルを抜いてください

デバイスを電源回路から切り離します。エネルギーの節約と不要な電力消費の削減の観点から、

このデバイスをアクティブにすることを意図していない場合は、デバイスの電源接続を削除することを強くお勧めします。

WEEE警告

危険物の存在の結果としての環境と人間の健康への潜在的な影響を回避するため

電気電子機器の物質、電気電子機器のエンドユーザーは

取り消し線の付いた車輪付きゴミ箱の記号の意味を理解します。WEEEを未分類として廃棄しないでください

都市ごみとそのようなWEEEを別々に収集する必要があります。

リビジョン

PLANETGS-4210シリーズユーザーズマニュアル

モデルの場合：GS-4210-8P2S / GS-4210-8P2T2S / GS-4210-16P4C / GS-4210-24P4C / GS-4210-24PL4C / GS-4210-48T4S /

GS-4210-48P4S

改訂：1.3（2016年8月）

部品番号：EM-GS-4210-series_v1.3

目次

1.はじめに.....	10
1.1パケットの内容.....	10
1.2製品の説明.....	11
1.3このマニュアルの使用方法.....	14
1.4製品の特徴.....	15
1.5製品仕様.....	18
2.インストール.....	31
2.1ハードウェアの説明.....	31
2.1.1フロントパネルの切り替え.....	31
2.1.2LED表示.....	33
2.1.3スイッチの背面パネル.....	39
2.2スイッチの取り付け.....	41
2.2.1デスクトップのインストール.....	41
2.2.2ラックマウント.....	42
2.2.3SFPトランシーバーの取り付け.....	44
3.スイッチ管理.....	47
3.1要件.....	47
3.2管理アクセスの概要.....	48
3.3管理コンソール.....	49
3.4Web管理.....	50
3.5SNMPベースのネットワーク管理.....	51
3.6PLANETスマートディスカバリユーティリティ.....	51
4.Web構成.....	54
4.1メインWebページ.....	57
4.1.1保存ボタン.....	58
4.1.2構成マネージャー.....	59
4.1.2.1構成の保存.....	60
4.2システム.....	61

4.2.1システム情報.....	61
4.2.2IP構成.....	62
4.2.3IPv6構成.....	64
4.2.4ユーザー設定.....	66
4.2.5時間設定.....	67
4.2.5.1システム時間.....	67
4.2.5.2SNTPサーバー設定.....	70
4.2.6ログ管理.....	71
4.2.6.1ローカルログ.....	71
4.2.6.2ローカルログ.....	72
4.2.6.3リモートSyslog.....	73
4.2.6.4ログメッセージ.....	75
4.2.7SNMP管理.....	77
4.2.7.1SNMPの概要.....	77
4.2.7.2SNMPシステム情報.....	78
4.2.7.3SNMPビュー.....	79
4.2.7.4SNMPアクセスグループ.....	80
4.2.7.5SNMPコミュニティ.....	82
4.2.7.6SNMPユーザー.....	83
4.2.7.7SNMPv1、2通知受信者.....	85
4.2.7.8SNMPv3通知受信者.....	86
4.2.7.9SNMPエンジンID.....	87
4.2.7.10SNMPリモートエンジンID.....	88
4.3ポート管理.....	90
4.3.1ポート構成.....	90
4.3.2ポートカウンター.....	92
4.3.3帯域幅の使用率.....	97
4.3.4ポートミラーリング.....	98
4.3.5ジャンボフレーム.....	100
4.3.6ポートエラー無効構成.....	101
4.3.7ポートエラーの無効化.....	103
4.3.8保護されたポート.....	103
4.3.9EEE.....	106
4.3.10SFPモジュール情報.....	107
4.3.10.1SFPモジュールのステータス.....	107
4.3.10.1SFPモジュールの詳細ステータス.....	109
4.4リンクアグリゲーション.....	110
4.4.1LAG設定.....	112
4.4.2LAG管理.....	113
4.5 VLAN.....	121

4.4.3LAGポート設定.....	114
4.4.4LACP設定.....	116
4.4.5LACPポート設定.....	117
4.4.6LAGステータス.....	118

4.5.1VLANの概要.....	121
4.5.2IEEE 802.1Q VLAN.....	122
4.5.3管理VLAN.....	126
4.5.4VLANの作成.....	127
4.5.5インターフェース設定.....	128
4.5.6VLANへのポート.....	132
4.5.7ポートVLANメンバーシップ.....	133
4.5.8プロトコルVLANグループの設定.....	134
4.5.9プロトコルVLANポート設定.....	136
4.5.10GVRP設定.....	137
4.5.11GVRPポート設定.....	139
4.5.12 GVRP VLAN.....	140
4.5.13GVRP統計.....	141
4.5.14 VLAN設定例：.....	143
4.5.14.12つの別々の802.1QVLAN.....	143
4.5.14.22つの802.1Q対応スイッチ間のVLANトランキング.....	146
4.6スパンニングツリープロトコル.....	149
4.6.1理論.....	149
4.6.2STPグローバル設定.....	156
4.6.3STPポート設定.....	158
4.6.4CISTインスタンスの設定.....	161
4.6.5CISTポート設定.....	163
4.6.6MSTインスタンスの構成.....	165
4.6.7MSTポート設定.....	167
4.6.8STP統計.....	169
4.7マルチキャスト.....	170
4.7.1プロパティ.....	170
4.7.2IGMPスヌーピング.....	171
4.7.2.1IGMP設定.....	175
4.7.2.2IGMPクエリア設定.....	177
4.7.2.3IGMP静的グループ.....	178
4.7.2.4IGMPグループテーブル.....	179
4.7.2.5IGMPルーターの設定.....	180
4.7.2.6IGMPルーターテーブル.....	181

4.7.2.7IGMP転送すべて.....	182
4.7.3IGMPスヌーピング統計.....	183
4.7.4MLDスヌーピング.....	186
4.7.4.1MLD設定.....	186
4.7.4.2MLD静的グループ.....	188
4.7.4.3MLDグループテーブル.....	189
4.7.4.4MLDルーターの設定.....	189
4.7.4.5MLDルーターテーブル.....	191
4.7.4.6MLD転送すべて.....	192
4.7.5MLDスヌーピング統計.....	193

4.7.6マルチキャストスロットリング設定.....	195
4.7.7マルチキャストフィルター.....	196
4.7.7.1マルチキャストプロファイルの設定.....	197
4.7.7.2IGMPフィルター設定.....	198
4.7.7.3MLDフィルター設定.....	199
4.8サービス品質.....	201
4.8.1QoSを理解する.....	201
4.8.2一般.....	202
4.8.2.1QoSプロパティ.....	202
4.8.2.2QoSポート設定.....	203
4.8.2.3キュー設定.....	204
4.8.2.4CoSマッピング.....	205
4.8.2.5DSCPマッピング.....	207
4.8.2.6IP優先順位マッピング.....	208
4.8.3QoS基本モード.....	210
4.8.3.1グローバル設定.....	210
4.8.3.2ポート設定.....	211
4.8.4レート制限.....	212
4.8.4.1入力帯域幅制御.....	212
4.8.4.2出力帯域幅制御.....	213
4.8.4.3出力キュー.....	214
4.8.5音声VLAN.....	215
4.8.5.1音声VLANの概要.....	215
4.8.5.2プロパティ.....	216
4.8.5.3テレフォニーOUIMAC設定.....	217
4.8.5.4テレフォニーOUIポート設定.....	219
4.9セキュリティ.....	221
4.9.1 802.1X.....	221
4.9.1.1 IEEE802.1Xポートベース認証について.....	222

4.9.1.2802.1X設定.....	225
4.9.1.3802.1Xポート設定.....	226
4.9.1.4ゲストVLAN設定.....	228
4.9.1.5認証されたホスト.....	230
4.9.2RADIUSサーバー.....	231
4.9.3 TACACS +サーバー.....	234
4.9.4 AAA.....	236
4.9.4.1ログインリスト.....	237
4.9.4.2有効化リスト.....	238
4.9.5アクセス.....	239
4.9.5.1 Telnet.....	239
4.9.5.2 SSH.....	240
4.9.5.3 HTTP.....	242
4.9.5.4 HTTP.....	243
4.9.6管理アクセス方法.....	244

4.9.6.1	プロファイルルール.....	244
4.9.6.2	アクセスルール.....	246
4.9.7	DHCPスヌーピング.....	247
4.9.7.1	DHCPスヌーピングの概要.....	247
4.9.7.2	グローバル設定.....	248
4.9.7.3	DHCPスヌーピングVLAN設定.....	249
4.9.7.4	ポート設定.....	251
4.9.7.5	統計.....	253
4.9.7.6	データベースエージェント.....	254
4.9.7.7	レート制限.....	256
4.9.7.8	Option82グローバル設定.....	257
4.9.7.9	Option82ポート設定.....	258
4.9.7.10	Option82回路ID設定.....	260
4.9.8	動的ARP検査.....	261
4.9.8.1	グローバル設定.....	261
4.9.8.2	VLAN設定.....	262
4.9.8.3	ポート設定.....	263
4.9.8.4	統計.....	265
4.9.8.5	レート制限.....	266
4.9.9	IPソースガード.....	267
4.9.9.1	ポート設定.....	268
4.9.9.2	バインディングテーブル.....	270
4.9.10	ポートセキュリティ.....	271
4.9.11	DoS.....	273
4.9.11.1	グローバルDoS設定.....	273

4.9.11.2	DoSポート設定.....	276
4.9.12	ストームコントロール.....	277
4.9.12.1	グローバル設定.....	277
4.9.12.2	ポート設定.....	278
4.10	ACL.....	280
4.10.1	MACベースのACL.....	281
4.10.2	MACベースのACE.....	282
4.10.3	IPv4ベースのACL.....	285
4.10.4	IPv4ベースのACE.....	286
4.10.5	IPv6ベースのACL.....	291
4.10.6	IPv6ベースのACE.....	292
4.10.7	ACLバインディング.....	297
4.11	MACアドレステーブル.....	298
4.11.1	静的MAC設定.....	299
4.11.2	MACフィルタリング.....	300
4.11.3	動的アドレス設定.....	301
4.11.4	動的学習.....	302
4.12	LLDP.....	304
4.12.1	リンク層検出プロトコル.....	304

4.12.2LLDPグローバル設定.....	305
4.12.3LLDPポート設定.....	307
4.12.4LLDPローカルデバイス.....	310
4.12.5LLDPデバイスの削除.....	312
4.12.6MEDネットワークポリシー.....	313
4.12.7MEDポート設定.....	317
4.12.8LLDPの過負荷.....	320
4.12.9LLDP統計.....	321

4.13 診断..... 323

4.13.1ケーブル診断.....	323
4.13.2 Ping.....	325
4.13.3pingテスト.....	325
4.13.4 IPv6Pingテスト.....	326
4.13.5トレーススレーター.....	327

4.14 RMON 328

4.14.1RMON統計.....	328
4.14.2RMONイベント.....	330
4.14.3RMONイベントログ.....	331
4.14.4RMONアラーム.....	332

4.14.5RMONの履歴.....	335
4.14.6RMON履歴ログ.....	336

4.15 Power over Ethernet..... 337

4.15.1 Power overEthernet搭載デバイス.....	338
4.15.2システム構成.....	339
4.15.3 Power overEthernet構成.....	340
4.15.4PoEスケジュール.....	343
4.15.5PoEアライブチェック構成.....	346

4.16 メンテナンス..... 348

4.16.1工場出荷時のデフォルト.....	348
4.16.2スイッチの再起動.....	348
4.16.3バックアップマネージャ.....	349
4.16.4アップグレードマネージャー.....	349
4.16.5デュアルイメージ.....	351

5.スイッチ操作..... 352

5.1 アドレステーブル..... 352

5.2 学習..... 352

5.3 転送とフィルタリング..... 352

5.4 ストアアンドフォワード..... 352

5.5 オートネゴシエーション..... 353

6.トラブルシューティング 354

付録AスイッチのRJ45ピン割り当て..... 356

A.1 1000Mbps、1000BASE-T..... 356

A.2 10 / 100Mbps、10 / 100BASE-TX 356

1.はじめに

複数のギガビットイーサネット銅線とが付属するPLANETGS-4210マネージドスイッチシリーズをお買い上げいただきありがとうございます
SFP光ファイバー接続と堅牢なレイヤー2およびレイヤー4の機能。このモデルの説明を以下に示します。

GS-4210-8P2S	8ポート10/100 / 1000T 802.3at PoE +2ポート100 / 1000XSFPマネージドスイッチ
GS-4210-8P2T2S	8ポート10/100 / 1000BASE-T 802.3at PoE Plus +2ポート10/100 / 1000BASE-T +2ポート100 / 1000BASE-X SFPマネージドスイッチ (240W)
GS-4210-16P4C	16ポート10/100 / 1000BASE-T PoE Plus Plus +4ポートギガビットTP / SFPコンボマネージドスイッチ (220W)
GS-4210-24P4C	24ポート10/100 / 1000BASE-T PoE Plus Plus +4ポートギガビットTP / SFPコンボマネージドスイッチ (220W)
GS-4210-24PL4C	24ポート10/100 / 1000BASE-T PoE Plus Plus +4ポートギガビットTP / SFPコンボマネージドスイッチ (440W)
GS-4210-48T4S	48ポート10/100 / 1000BASE-T +4ポート100 / 1000BASE-XSFPマネージドギガビットスイッチ
GS-4210-48P4S	48ポート10/100 / 1000T 802.3at PoE +4ポート100 / 1000BASE-X SFPマネージドスイッチ (440W)

このユーザズマニュアルでは、別名「**マネージドスイッチ**」を使用しています。

1.1パケットの内容

管理対象スイッチのボックスを開き、慎重に開梱します。ボックスには、次のアイテムが含まれている必要があります。

モデル名					
	GS-4210-8P2S	GS-4210-8P2T2S	GS-4210-16P4C	GS-4210-24P4C GS-4210-24PL4C	GS-4210-48T4S GS-4210-48P4S
項目					
マネージドスイッチ	■	■	■	■	■
クイックインストールガイド	■	■	■	■	■

5.23からRJ45コンソール	バツ	■	■	■	バツ
ゴム足	■	■	■	■	■
2つのラックマウント アタッチメント付きブラケット ネジ	■	■	■	■	■
電源コード	■	■	■	■	■
SFPダストキャップ	2	2	4	4	4

不足または破損しているアイテムが見つかった場合は、最寄りの販売店に連絡して交換してください。

1.2 製品の説明

フルPoE + パワーバジェットを備えた完璧なマネージドPoE + スイッチ

PLANET GS-4210 PoEシリーズは、PLANETインテリジェントを搭載した新世代のPLANETマネージドギガビットPoE + スイッチです。

PoEは、重要なビジネスアプリケーションの可用性を向上させるために機能します。迅速、安全、費用効果の高いパワーオーバーを提供します
中小企業および企業向けのIPセキュリティ監視に対するイーサネットネットワークソリューション。

パワードデバイス管理用の組み込みの独自のPoE機能

GS-4210 PoEシリーズは、監視、ワイヤレス、およびVoIPネットワーク用のマネージドPoEスイッチとして、特別なPoEを備えています。

管理機能：

- PDアライブチェック
- 定期的な電力リサイクル
- PoEのスケジュール
- PoEの使用状況の監視

インテリジェントパワードデバイスアライブチェック

GS-4210 PoEシリーズは、pingアクションを介して接続されたPD（受電装置）のステータスをリアルタイムで監視するように構成できます。一度

PDが動作を停止して応答すると、GS-4210 PoEシリーズはPoEポートの電力を再開し、PDを動作に戻します。

PoEポートがPDの電源をリセットし、管理者を削減することで、ネットワークの信頼性を大幅に向上させます。

管理負担。

定期的な電力リサイクル

GS-4210 PoEシリーズを使用すると、接続されている各PoE IPカメラまたはPoEワイヤレスアクセスポイントを特定の場所で再起動できます。

毎週の時間。したがって、バッファオーバーフローが原因でIPカメラまたはAPがクラッシュする可能性が低くなります。

省エネのためのPoEスケジュール

世界的な省エネと環境保護への貢献のトレンドの下で、GS-4210PoEシリーズは

高ワットの電力を供給する能力に加えて、電源を効果的に制御します。「**PoEスケジュール**」機能はあなたがするのを助けます

指定された時間間隔で各PoEポートのPoE給電を有効または無効にします。これは、SMBを支援する強力な機能です。

または企業は電力とお金を節約します。また、使用してはならないPDの電源をオフにすることで、セキュリティを強化します。

営業時間外。

PoE使用状況の監視

GS-4210 PoEシリーズは、Web管理インターフェイスの電力使用量チャートを介して、管理者が

接続されたPDの電力使用量のステータスをリアルタイムで。したがって、それはの管理効率を大幅に向上させます

施設。

サイレント操作のための環境に優しいスマートファン設計

GS-4210シリーズは、デスクトップサイズの金属製ハウジング、低騒音設計、効果的な換気システムを備えています。サポートしています

内蔵ファンの速度を自動的に制御して騒音を低減し、の温度を維持するスマートファンテクノロジ

最適な電力出力機能のためのPoEスイッチ。GS-4210シリーズは、どのような場所でも確実に、安定して、静かに動作することができます。

そのパフォーマンスに影響を与えることなく環境。

IPv6 / IPv4デュアルスタック

IPv6プロトコルとIPv4プロトコルの両方をサポートするGS-4210シリーズは、SMBが最小の投資でIPv6時代に踏み出すのに役立ちます

IPv6 FTTxエッジネットワークが設定されている場合は、ネットワーク機能を交換またはオーバーホールする必要がないためです。

堅牢なレイヤー2機能

GS-4210シリーズは、動的ポートリンクアグリゲーションなどの高度なスイッチ管理機能用にプログラムできます。

802.1QVLANおよびQ-in-QVLAN、**マルチスパンニングツリープロトコル（MSTP）**、ループおよびBPDUガード、IGMPスヌーピング、および**MLDスヌーピング**。リンクアグリゲーションを介して、GS-4210シリーズは高速トランクの操作を組み合わせることを可能にします。16Gbpsファットパイプなどの複数のポート。フェイルオーバーもサポートします。また、Link Layer Discovery Protocol（LLDP）はローカルブロードキャストドメイン上の隣接デバイスに関する基本情報の検出に役立つレイヤー2プロトコルが含まれています。

効率的な交通管制

GS-4210シリーズには、堅牢なQoS機能と強力なトラフィック管理が搭載されており、ビジネスクラスのサービスを強化します。

データ、音声、およびビデオソリューション。機能には、ブロードキャスト/マルチキャスト**ストーム制御**、ポートごとの**帯域幅制御**、IPが含まれます。DSCPQoSの優先順位とリマーケティング。VoIPおよびビデオストリーム送信の最高のパフォーマンスを保証し、権限を与えます。企業は限られたネットワークリソースを最大限に活用します。

強力なセキュリティ

PLANET GS-4210シリーズは、セキュリティを強化するための包括的なIPv4 / IPv6レイヤー2からレイヤー4の**アクセス制御リスト（ACL）**を提供します。端末まで。送信元と宛先のIPアドレスに基づいてパケットを拒否することにより、ネットワークアクセスを制限するために使用できます。

TCP / UDPポートまたは定義された一般的なネットワークアプリケーション。その保護メカニズムには、**802.1Xポートベースのユーザーとデバイス認証**。RADIUSとともに展開して、ポートレベルのセキュリティを確保し、不正なユーザーをブロックできます。とともに

保護ポート機能、エッジポート間の通信を防止して、ユーザーのプライバシーを保証できます。さらに、**ポートセキュリティ**機能により、特定のポート上のネットワークデバイスの数を制限できます。

高度なネットワークセキュリティ

GS-4210シリーズは、**DHCPスヌーピング**、**IPソースガード**、および**動的ARP検査**機能も提供してIPを防止します。

攻撃からスヌーピングし、無効なMACアドレスを持つARPパケットを破棄します。ネットワーク管理者は高度に構築できるようになりました。以前よりも大幅に少ない時間と労力で企業ネットワークを保護しました。

フレンドリーで安全な管理

効率的な管理のために、GS-4210シリーズには、コンソール、**Web**、**Telnet**、および**SNMP**管理インターフェイスが装備されています。

組み込みのWebベースの管理インターフェイスであるGS-4210シリーズは、プラットフォームに依存しない使いやすい管理を提供します。

および構成機能。標準の簡易ネットワーク管理プロトコル（SNMP）をサポートすることにより、スイッチは次のようになります。

標準の管理ソフトウェアを介して管理されます。テキストベースの管理の場合、スイッチにはTelnetおよび

コンソールポート。さらに、GS-4210シリーズは、**SSH**、**SSL**、および**SNMPv3**をサポートすることにより、安全なリモート管理を提供します。

各セッションでパケットコンテンツを暗号化する接続。

柔軟性と拡張ソリューション

GS-4210シリーズは、10/100 / 1000BASE-T RJ45銅線をサポートするギガビットTP / SFPインターフェイスを提供します。

監視管理を容易にするNVR、ビデオストリーミングサーバー、NASなどの監視ネットワークデバイス。またはを通して

これらのデュアルスピードファイバーSFPスロットは、**100BASE-FX / 1000BASE-SX / LX** SFP（スモールフォームファクター）とも接続できます。

プラグ可能な）ファイバートランシーバー、そして長距離のバックボーンスイッチとモニタリングセンターへ。距離は

550メートルから2キロメートル（マルチモードファイバー）および最大10/20/30/40/50/70/120キロメートル（シングルモードファイバーまたは

WDMファイバー）。これらは、エンタープライズデータセンターおよびディストリビューション内のアプリケーションに最適です。

インテリジェントSFP診断メカニズム

GS-4210シリーズはSFP-DDM（**デジタル診断モニター**）機能をサポートしており、ネットワーク管理者が

光出力パワー、光入力パワー、温度、レーザバイアスなどのSFPのリアルタイムパラメータを簡単に監視できます

電流とトランシーバーの供給電圧。

1.3 このマニュアルの使用方法

このユーザズマニュアルは次のように構成されています。

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、マネージド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、マネージド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るマネージドスイッチの管理方法について説明します。

セクション5、スイッチ操作

この章では、マネージドスイッチのスイッチ操作の方法について説明します。

セクション6、トラブルシューティング

この章では、マネージドスイッチのトラブルシューティング方法について説明します。

付録A

このセクションには、マネージドスイッチのケーブル情報が含まれています。

1.4 製品の特徴

物理ポート

■ 10/100 / 1000BASE-TギガビットRJ45銅

- 100 / 1000BASE-XミニGBIC / SFPスロット。
- スイッチの基本的な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

Power over Ethernet (GS-4210 PoEシリーズ)

- IEEE802.3atハイパワーオーバーイーサネットエンドスパンPSEに準拠
- イーサネットエンドスパンPSEを介したIEEE802.3afパワーに準拠
- IEEE802.3af/802.3atデバイスを搭載
- 各PoEポートで最大30.8ワットのPoE電力をサポート
- 受電装置 (PD) の自動検出
- 回路保護により、ポート間の電力干渉を防ぎます
- 最大100メートルのリモート給電
- PoE管理
 - トータルPoEパワーバジェット制御
 - ポートごとのPoE機能の有効化/無効化
 - PoEポート給電の優先順位
 - PoEポートごとの電力制限
 - PD分類の検出
 - PDアライブチェック
 - PoEスケジュール

レイヤー2の機能

- バックプレッシャー (半二重) およびIEEE 802.3xポーズフレームフロー制御 (全二重) によるパケット損失を防止します
- 高性能のストアアンドフォワードアーキテクチャ、ブロードキャストストーム制御、ラント/ CRCフィルタリングによりエラーが排除されます
- ネットワーク帯域幅を最適化するためのパケット

■ VLANをサポート

- IEEE802.1Qタグ付きVLAN
- プロバイダーブリッジング (VLAN Q-in-Q) サポート (IEEE 802.1ad)
- プロトコルVLAN
- 音声VLAN
- プライベートVLAN
- 管理VLAN
- GVRP

■スパンニングツリープロトコルをサポート

- STP (スパンニングツリープロトコル)
- RSTP (高速スパンニングツリープロトコル)
- MSTP (マルチスパンニングツリープロトコル)
- STP BPDUガード、BPDUフィルタリング、およびBPDU転送

■リンクアグリゲーションをサポート

- IEEE 802.3adリンク集約制御プロトコル (LACP)
- Ciscoイーサチャネル (スタティックトラंक)

15

- 最大8つのトランクグループ、トランクグループごとに最大8つのポート
- ポートミラーを提供します (多対1)
- ブロードキャストループを回避するためのループ保護

サービスの質

- ポート帯域幅制御ごとの入力/出力レート制限
- ストームコントロールのサポート
 - ブロードキャスト/不明なユニキャスト/不明なマルチキャスト
- トラフィック分類

- IEEE 802.1p CoS
- IPv4 / IPv6パケットのTOS / DSCP / IP優先順位

■厳格な優先順位と加重ラウンドロビン（WRR）CoSポリシー

マルチキャスト

- IGMPスヌーピングv2およびv3をサポートします
- MLDスヌーピングv1、v2をサポートします
- IGMPクエリアモードのサポート
- IGMPスヌーピングポートフィルタリング
- MLDスヌーピングポートフィルタリング

セキュリティ

- 認証
 - IEEE802.1Xポートベースのネットワークアクセス認証
 - RADIUSサーバーと連携するための組み込みRADIUSクライアント
 - RADIUS / TACACS +ログインユーザーアクセス認証
- アクセス制御リスト
 - IPv4 / IPv6IPベースのACL
 - MACベースのACL
- MACセキュリティ
 - 静的MAC
 - MACフィルタリング
- 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
- 信頼できないDHCPメッセージをフィルタリングするためのDHCPスヌーピング
- 動的ARP検査は、無効なMACアドレスからIPアドレスへのバインディングを持つARPパケットを破棄します
- IPソースガードはIPスプーフィング攻撃を防ぎます
- DoS攻撃の防止
- SSH / SSL

管理

- IPv4およびIPv6デュアルスタック管理
- スイッチ管理インターフェイス
 - Webスイッチ管理
 - Telnetコマンドラインインターフェイス
 - SNMP v1、v2c、およびv3
 - SSH / SSLセキュアアクセス
- ユーザー特権レベルの制御
- 組み込みのトリビアルファイル転送プロトコル（TFTP）クライアント
- IPアドレス割り当て用のBOOTPおよびDHCP
- システムメンテナンス
 - HTTP / TFTPを介したファームウェアのアップロード/ダウンロード
 - Webインターフェイスを介した構成のアップロード/ダウンロード
 - デュアルイメージ
 - システムを再起動するか、工場出荷時のデフォルトにリセットするためのハードウェアリセットボタン
- SNTPネットワークタイムプロトコル

- ケーブル診断
- LinkLayer Discovery Protocol（LLDP）およびLLDP-MED
- インターフェイスのリンクアップおよびリンクダウン通知用のSNMPトラップ
- リモートSyslogサーバーへのイベントメッセージログ
- 4つのRMONグループ（履歴、統計、アラーム、およびイベント）
- PLANETスマートディスカバリユーティリティ
- 速度制御付きのスマートファン

1.5製品仕様

GS-4210-8P2S / GS-4210-8P2T2S

製品	GS-4210-8P2S	GS-4210-8P2T2S
ハードウェア仕様		
銅のポート	8 x 10/100 / 1000BASE-T RJ45 自動MDI / MDI-Xポート	10 x 10/100 / 1000BASE-T RJ45 自動MDI / MDI-Xポート
SFP / ミニGBICスロット	2 x 100 / 1000BASE-X SFPインターフェイス ポート9からポート10。 100 / 1000Mbpsデュアルモードをサポートし、 DDM	2 x 100 / 1000BASE-XSFPインターフェイス ポート11からポート12まで。 100 / 1000Mbpsデュアルモードをサポート およびDDM
PoEインジェクターポート	802.3at / afPoEインジェクターを備えた8ポート ポート1からポート8で機能	802.3at / afPoEインジェクターを備えた8ポート ポート1からポート8で機能
コンソール	---	1 x RS-232-to-RJ45シリアルポート（115200、 8、N、1）
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	20Gbps / ノンブロッキング	24Gbps / ノンブロッキング
Switch Throughput @ 64Bytes	14.88Mpps	17.76Mpps
アドレステーブル	8Kエントリ	

共有データバッファ	4.1メガビット	
フロー制御	全二重用のIEEE802.3xボーズフレーム	
	半二重の背圧	
ジャンボフレーム	10Kバイト	
リセットボタン	<5秒：システムの再起動 > 5秒：工場出荷時のデフォルト	
導いた	PWR、ファンアラート、LNK / ACT、使用中のPoE、1000	PWR、SYS、LNK / ACT、使用中のPoE、1000
スマートファン	1	1
寸法（W x D x H）	330 x 155 x 43.5 mm、高さ1U	330 x 200 x 44.5 mm、高さ1U
重量	1687g	2kg
電力要件	AC 100～240V、50 / 60Hz、自動検知	
ESD保護	2KV DC	6KV DC
消費電力/ 散逸	165ワット（最大） / 563 BTU	320ワット（最大） /1091.8BTU
エンクロージャー	金属	
Power over Ethernet		
PoE標準	IEEE 802.3af / 802.3at PoE / PSE	
PoE電源タイプ	エンドスパン	
PoE電力出力	ポートあたり52VDC、36ワット（最大）	ポートあたり54VDC、36ワット（最大）
電源ピンの割り当て	1/2（+）、3/6（-）	

GS-4210シリーズのユーザーズマニュアル

PoEパワーバジェット	120ワット（最大）@摂氏25度 100ワット（最大）@摂氏50度	240ワット（最大）@摂氏25度 200ワット（最大）@摂氏50度
PoEアビリティPD @ 9ワット	8ユニット	8ユニット
PoEアビリティPD @ 15ワット	8ユニット	8ユニット
PoEアビリティPD @ 30ワット	4ユニット	8ユニット
レイヤー2機能		
ポートミラーリング	TX / RX /両方 多対1モニター 802.1QタグベースのVLAN 4094のVLANIDのうち、最大256のVLANグループ 802.1adQ-in-Qトンネリング	
VLAN	音声VLAN プロトコルVLAN プライベートVLAN（保護ポート） GVRP	
リンクアグリゲーション	IEEE 802.3adLACPと静的トランク 8つのグループ、トランクグループごとに8つのポートをサポート	
スパンニングツリープロトコル	STP、RSTP、MSTP	
IGMPスヌーピング	IGMP（v2 / v3）スヌーピング IGMPクエリア 最大256のマルチキャストグループ	
MLDスヌーピング	MLD（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	IPv4 / IPv6IPベースのACL / MACベースのACL 8つのマッピングIDを8つのレベルの優先度キューに - ポート番号	

QoS

- 802.1pの優先度
- 802.1QVLANタグ
- IPパケットのDSCPフィールド
- トラフィック分類ベース、厳密な優先順位、およびWRR
- IEEE 802.1X -ポートベースの認証
- RADIUSサーバーと連携するための組み込みRADIUSクライアント
- RADIUS / TACACS +ユーザーアクセス認証
- IP-MACポートバインディング
- MACフィルター

セキュリティ

- 静的MACアドレス
- DHCPスヌーピングとDHCPオプション82
- STP BPDUガード、BPDUフィルタリング、およびBPDU転送
- DoS攻撃の防止
- ARP検査
- IPソースガード

管理機能

基本的な管理インターフェース

- ウェブブラウザ; Telnet; SNMP v1、v2c
- イーサネットネットワークを介したHTTP / TFTPプロトコルによるファームウェアのアップグレード
- リモート/ローカルSyslog

- システムログ
- LLDPプロトコル
- SNTP

安全な管理インターフェースSSH / SSL、SNMP v3

SNMPMIB

- RFC 1213 MIB-II
- RFC1215汎用トラップ
- RFC1493ブリッジMIB
- RFC2674ブリッジMIB拡張
- RFC 2737エンティティMIB (バージョン2)
- RFC 2819 RMON (1、2、3、9)
- RFC2863インターフェイスグループMIB
- RFC3635イーサネットのようなMIB

規格への適合

企業コンプライアンス

- FCCパート15クラスA、CE
- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX / 100BASE-FX
- IEEE802.3zギガビットSX / LX
- IEEE802.3abギガビット1000T
- IEEE802.3xフロー制御と背圧
- LACPを備えたIEEE802.3adポートトラUNK
- IEEE802.1Dスパンニングツリープロトコル
- IEEE802.1w高速スパンニングツリープロトコル
- IEEE802.1sマルチスパンニングツリープロトコル
- IEEE802.1pサービスクラス
- IEEE 802.1QVLANタギング
- IEEE802.1xポート認証ネットワーク制御
- IEEE 802.1ab LLDP
- IEEE 802.3af Power over Ethernet
- IEEE802.3atハイパワーオーバーイーサネット
- RFC 768 UDP
- RFC 793 TFTP
- RFC 791 IP
- RFC 792 ICMP
- RFC 2068 HTTP
- RFC 1112IGMPバージョン1
- RFC 2236IGMPバージョン2

標準への準拠

	RFC 3376IGMPバージョン3
	RFC 2710MLD/バージョン1
	RFC 3810MLD/バージョン2
環境	
オペレーティング	温度：0～50℃ 相対湿度：5～95%（結露しないこと）
ストレージ	温度：-20～70℃ 相対湿度：5～95%（結露しないこと）

GS-4210シリーズのユーザーズマニュアル

GS-4210-16P4C

製品	GS-4210-16P4C
ハードウェア仕様	
銅のポート	20 x 10/100 / 1000BASE-T RJ45自動MDI / MDI-Xポート
SFP / ミニGBICスロット	ポート17からポート20で共有される4x 100 / 1000BASE-XSFPインターフェイス。 100 / 1000MbpsデュアルモードとDDMをサポート
PoEインジェクターポート	ポート1からポート16までの802.3at / afPoEインジェクター機能を備えた16ポート
コンソール	1 x RS-232-to-RJ45シリアルポート（115200、8、N、1）
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	40Gbps / ノンブロッキング
Switch Throughput @ 64Bytes	29.76Mpps
アドレステーブル	8Kエントリ
共有データバッファ	4.1メガビット
フロー制御	全二重用のIEEE802.3xポーズフレーム 半二重の背圧
ジャンボフレーム	10Kバイト
リセットボタン	<5秒：システムの再起動 > 5秒：工場出荷時のデフォルト
導いた	PWR、SYS、LNK / ACT、使用中のPoE、1000、FAN 1アラート、FAN 2アラート、PoEPWRアラート
スマートファン	2
寸法（W x D x H）	440 x 300 x 44.5 mm、19インチ、高さ1U
重量	4.132kg
電力要件	AC 100～240V、50 / 60Hz、自動検知
ESD保護	6KV DC
消費電力/ 散逸	251ワット（最大） / 861.2BTU
エンクロージャー	金属
Power over Ethernet	
PoE標準	IEEE 802.3af / 802.3at PoE / PSE
PoE電源タイプ	エンドスパン
PoE電力出力	ポートあたり52VDC、30.8ワット（最大）
電源ピンの割り当て	1/2（+）、3/6（-）
PoEパワーバジェット	220ワット（最大） @ 摂氏25度

PoEアビリティ PD @ 9ワット	190ワット（最大）@摂氏50度
PoEアビリティ PD@15.4ワット	16台
PoEアビリティ PD @ 30ワット	14ユニット
レイヤー2機能	7台
ポートミラーリング	TX / RX /両方

VLAN	<p>多対1モニター</p> <p>802.1QタグベースのVLAN</p> <p>4094のVLANIDのうち、最大256のVLANグループ</p> <p>802.1adQ-in-Qトンネリング</p> <p>音声VLAN</p> <p>プロトコルVLAN</p> <p>プライベートVLAN（保護ポート）</p> <p>GVRP</p>
リンクアグリゲーション	<p>IEEE 802.3adLACPと静的トランク</p> <p>8つのグループ、トランクグループごとに8つのポートをサポート</p>
スパンニングツリープロトコル	<p>STP、RSTP、MSTP</p>
IGMPスヌーピング	<p>IGMP（v2 / v3）スヌーピング</p> <p>IGMPクエリア</p> <p>最大256のマルチキャストグループ</p>
MLDスヌーピング	<p>MLD（v1 / v2）スヌーピング、最大256のマルチキャストグループ</p>
アクセス制御リスト	<p>IPv4 / IPv6IPベースのACL / MACベースのACL</p> <p>8つのマッピングIDを8つのレベルの優先度キューに</p> <ul style="list-style-type: none"> - ポート番号 -802.1pの優先度 --802.1QVLANタグ -IPパケットのDSCPフィールド <p>トラフィック分類ベース、厳密な優先順位、およびWRR</p> <p>IEEE 802.1X -ポートベースの認証</p> <p>RADIUSサーバーと連携するための組み込みRADIUSクライアント</p> <p>RADIUS / TACACS +ユーザーアクセス認証</p> <p>IP-MACポートバインディング</p> <p>MACフィルター</p> <p>静的MACアドレス</p> <p>DHCPスヌーピングとDHCPオプション82</p> <p>STP BPDUガード、BPDUフィルタリング、およびBPDU転送</p> <p>DoS攻撃の防止</p> <p>ARP検査</p> <p>IPソースガード</p>
セキュリティ	
管理機能	
基本的な管理インターフェース	<p>ウェブブラウザ; Telnet; SNMP v1、v2c</p> <p>イーサネットネットワークを介したHTTP / TFTPプロトコルによるファームウェアのアップグレード</p> <p>リモート/ローカルSyslog</p> <p>システムログ</p> <p>LLDPプロトコル</p> <p>SNTP</p>
安全な管理インターフェース	<p>SSH / SSL、SNMP v3</p>
SNMPMIB	<p>RFC 1213 MIB-II</p> <p>RFC1215汎用トラップ</p> <p>RFC1493ブリッジMIB</p>

規格への適合

企業コンプライアンス

標準への準拠

環境

オペレーティング

ストレージ

- RFC 2819 RMON (1、2、3、9)
- RFC2863インターフェイスグループMIB
- RFC3635イーサネットのようなMIB
- FCC/パート15クラスA、CE
- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX / 100BASE-FX
- IEEE802.3zギガビットSX / LX
- IEEE802.3abギガビット1000T
- IEEE802.3xフロー制御と背圧
- LACPを備えたIEEE802.3adポートトラंक
- IEEE802.1Dスパンニングツリープロトコル
- IEEE802.1w高速スパンニングツリープロトコル
- IEEE802.1sマルチスパンニングツリープロトコル
- IEEE802.1pサービスクラス
- IEEE 802.1QVLANタギング
- IEEE802.1xポート認証ネットワーク制御
- IEEE 802.1ab LLDP
- IEEE 802.3af Power over Ethernet
- IEEE802.3at/ハイパワーオーバーイーサネット
- RFC 768 UDP
- RFC 793 TFTP
- RFC 791 IP
- RFC 792 ICMP
- RFC 2068 HTTP
- RFC 1112IGMPバージョン1
- RFC 2236IGMPバージョン2
- RFC 3376IGMPバージョン3
- RFC 2710MLD/バージョン1
- RFC 3810MLD/バージョン2

- 温度：0～50℃
- 相対湿度：5～95%（結露しないこと）
- 温度：-20～70℃
- 相対湿度：5～95%（結露しないこと）

GS-4210-24P4C / GS-4210-24PL4C

製品	GS-4210-24P4C	GS-4210-24PL4C
ハードウェア仕様		
銅のポート	28 x 10/100 / 1000BASE-T RJ45自動MDI / MDI-Xポート	
SFP / ミニGBIC スロット	ポート 25 からポート 28 で共有される 4 x 100 / 1000BASE-X SFP インターフェイス。 100 / 1000Mbps デュアルモードと DDM をサポート	
PoE インジェクターポート	ポート 1 からポート 24 までの 802.3at / af PoE インジェクター機能を備えた 24 ポート	
コンソール	1 x RS-232-to-RJ45 シリアルポート (115200、8、N、1)	
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	56Gbps / ノンブロッキング	
Switch Throughput @ 64Bytes	41.67Mpps	
アドレステーブル	8K エントリ	
共有データバッファ	4.1メガビット	
フロー制御	全二重用の IEEE802.3x ポーズフレーム 半二重の背圧	
ジャンボフレーム	10K バイト	
リセットボタン	<5秒：システムの再起動 >5秒：工場出荷時のデフォルト	
導いた	PWR、SYS、LNK / ACT、使用中の PoE、1000、FAN 1 アラート、FAN 2 アラート、PoEPWR アラート	
スマートファン	2	3
寸法 (W x D x H)	440 x 300 x 44.5 mm、19-インチ、高さ 1U	
重量	4.214kg	4.814kg
電力要件	AC 100~240V、50 / 60Hz、自動検知	
ESD 保護	2KV DC	
消費電力 / 散逸	275ワット (最大) / 938.3 BTU	544ワット (最大) / 1856.2BTU
エンクロージャー	金属	
Power over Ethernet		
PoE 標準	IEEE 802.3af / 802.3at PoE / PSE	
PoE 電源タイプ	エンドスパン	
PoE 電力出力	ポートあたり 52VDC、30.8ワット (最大)	
電源ピンの割り当て	1/2 (+)、3/6 (-)	
PoE パワーバジェット	220ワット (最大) @ 摂氏 25 度 190ワット (最大) @ 摂氏 50 度	440ワット (最大) @ 摂氏 25 度 380ワット (最大) @ 摂氏 50 度
PoE アビリティ PD @ 9ワット	24 ユニット	
PoE アビリティ PD @ 15.4ワット	14 ユニット	24 ユニット
PoE アビリティ PD @ 30ワット	7 台	14 ユニット
レイヤー 2 機能		
ポートミラーリング	TX / RX / 両方	

多対1モニター
802.1QタグベースのVLAN

	4094のVLANIDのうち、最大256のVLANグループ 802.1adQ-in-Qトunnel
VLAN	音声VLAN プロトコルVLAN プライベートVLAN（保護ポート） GVRP
リンクアグリゲーション	IEEE 802.3adLACPと静的トランク 8つのグループ、トランクグループごとに8つのポートをサポート
スパニングツリープロトコル	STP、RSTP、MSTP
IGMPスヌーピング	IGMP（v2 / v3）スヌーピング IGMPクエリア 最大256のマルチキャストグループ
MLDスヌーピング	MLD（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	IPv4 / IPv6IPベースのACL / MACベースのACL 8つのマッピングIDを8つのレベルの優先度キューに - ポート番号 -802.1pの優先度 --802.1QVLANタグ -IPパケットのDSCPフィールド トラフィック分類ベース、厳密な優先順位、およびWRR IEEE 802.1X -ポートベースの認証 RADIUSサーバーと連携するための組み込みRADIUSクライアント RADIUS / TACACS +ユーザーアクセス認証 IP-MACポートバインディング MACフィルター 静的MACアドレス DHCPスヌーピングとDHCPオプション82 STP BPDUガード、BPDUフィルタリング、およびBPDU転送 DoS攻撃の防止 ARP検査 IPソースガード
セキュリティ	
管理機能	
基本的な管理インターフェース	ウェブブラウザ; Telnet; SNMP v1、v2c イーサネットネットワークを介したHTTP / TFTPプロトコルによるファームウェアのアップグレード リモート/ローカルSyslog システムログ LLDPプロトコル SNTP
安全な管理インターフェース	SSH、SSL、SNMP v3
SNMPMIB	RFC 1213 MIB-II RFC1215汎用トラップ RFC1493ブリッジMIB RFC2674ブリッジMIB拡張 RFC 2737エンティティMIB（バージョン2）

規格への適合	RFC 2819 RMON（1、2、3、9） RFC2863インターフェイスグループMIB RFC3635イーサネットのようなMIB
企業コンプライアンス	FCCパート15クラスA、CE IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX / 100BASE-FX IEEE802.3zギガビットSX / LX

IEEE802.3ab デジタルトランシーバー制御と9999	IEEE802.3ab デジタルトランシーバー制御と9999
LACPを備えたIEEE802.3adポートトラUNK	LACPを備えたIEEE802.3adポートトラUNK
IEEE802.1Dスバニングツリープロトコル	IEEE802.1Dスバニングツリープロトコル
IEEE802.1w高速スバニングツリープロトコル	IEEE802.1w高速スバニングツリープロトコル
IEEE802.1sマルチスバニングツリープロトコル	IEEE802.1sマルチスバニングツリープロトコル
IEEE802.1pサービスクラス	IEEE802.1pサービスクラス
IEEE 802.1QVLANタギング	IEEE 802.1QVLANタギング
IEEE802.1xポート認証ネットワーク制御	IEEE802.1xポート認証ネットワーク制御
IEEE 802.1ab LLDP	IEEE 802.1ab LLDP
IEEE 802.3af Power over Ethernet	IEEE 802.3af Power over Ethernet
IEEE802.3at/ハイパワオーバーイーサネット	IEEE802.3at/ハイパワオーバーイーサネット
RFC 768 UDP	RFC 768 UDP
RFC 793 TFTP	RFC 793 TFTP
RFC 791 IP	RFC 791 IP
RFC 792 ICMP	RFC 792 ICMP
RFC 2068 HTTP	RFC 2068 HTTP
RFC 1112IGMPバージョン1	RFC 1112IGMPバージョン1
RFC 2236IGMPバージョン2	RFC 2236IGMPバージョン2
RFC 3376IGMPバージョン3	RFC 3376IGMPバージョン3
RFC 2710MLDバージョン1	RFC 2710MLDバージョン1
RFC 3810MLDバージョン2	RFC 3810MLDバージョン2

環境

オペレーティング

温度：0～50℃
 相対湿度：5～95%（結露しないこと）

ストレージ

温度：-20～70℃
 相対湿度：5～95%（結露しないこと）

GS-4210-48T4S

製品	GS-4210-48T4S	GS-4210-48P4S
ハードウェア仕様		
銅のポート	48 x 10/100 / 1000BASE-TRJ45自動MDI / MDI-Xポート	
SFP/ミニGBICスロット	4 100 / 1000BASE-X SFPインターフェイス、 100 / 1000MbpsデュアルモードとDDMをサポート	
PoEインジェクターポート	---	802.3at / afPoEインジェクターを備えた48ポート ポート1からポート48で機能
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	104Gbps / ノンブロッキング	
Switch Throughput @ 64Bytes	77.38Mpps @ 64Bytes	
アドレステーブル	16Kエントリ	

共有データバッファ	12MビットSRAM/バケットバッファ	
フロー制御	全二重用のIEEE802.3xポーズフレーム	
ジャンボフレーム	半二重の背圧	
リセットボタン	10Kバイト	
	<5秒：システムの再起動	
	> 5秒：工場出荷時のデフォルト	
	システム：	システム：
	PWR（電源）（緑）	PWR（電源）（緑）
	SYS（システム）（緑）	SYS（システム）（緑）
	10/100 / 1000T RJ45インターフェイス（ポート1からポート48）：	10/100 / 1000T RJ45インターフェイス（ポート1からポート48）：
	1000Mbps（オレンジ）、LNK / ACT（緑）	10/100 / 1000Mbps、LNK / ACT（緑）
	10 / 100Mbps（なし）、LNK / ACT（緑）	使用中のPoE（オレンジ）
	100 / 1000Mbps SFPインターフェイス（ポート49ポート52へ）：	100 / 1000Mbps SFPインターフェイス（ポート49ポート52へ）：
	1000Mbps、LNK / ACT（緑）	1000Mbps、LNK / ACT（緑）
	100Mbps、LNK / ACT（オレンジ）	100Mbps、LNK / ACT（オレンジ）
サーマルファン	ファンレス設計（ファンなし）	3xスマートファン
電力要件	AC 100〜240V、50 / 60Hz、自動検知。	100〜240V AC、50 / 60Hz、自動検知
ESD保護	6KV DC	6KV DC
消費電力/散逸	34ワット/ 116BTU	481ワット（最大） / 1641 BTU
寸法（W x D x H）	440 x 300 x 44.5 mm、高さ1U	440 x 300 x 44.5 mm、高さ1U
重量	3.7 kg	5.476 kg
エンクロージャー	金属	金属
Power over Ethernet		
PoE標準	---	IEEE 802.3af / 802.3at PoE + PSE
PoE電源タイプ	---	エンドスパン

GS-4210シリーズのユーザーズマニュアル

PoE電力出力	---	ポートあたり52VDC、36ワット（最大）
電源ピンの割り当て	---	1/2（+）、3/6（-）
PoEパワーバジェット	---	440ワット（最大）@摂氏25度
		380ワット（最大）@摂氏50度
PoEアビリティPD @ 9ワット	---	48ユニット
PoEアビリティPD @ 15ワット	---	29台
PoEアビリティPD @ 30ワット	---	14ユニット
レイヤー2機能		
ポートミラーリング	TX / RX /両方	
	多対1モニター	
	802.1QタグベースのVLAN	
	4094のVLANIDのうち、最大256のVLANグループ	
	802.1ad Q-in-Qトンネリング（VLANスタッキング）	
VLAN	音声VLAN	
	プロトコルVLAN	
	プライベートVLAN（保護ポート）	
	GVRP	
	管理VLAN	

リンクアグリゲーション	IEEE 802.3adLACPと静的トラUNK 8つのグループ、トラUNKグループごとに8つのポートをサポート
スパニングツリープロトコル	IEEE 802.1Dスパニングツリープロトコル（STP） IEEE 802.1wラビッドスパニングツリープロトコル（RSTP） IEEE 802.1sマルチスパニングツリープロトコル（MSTP） STP BPDUガード、BPDUフィルタリング、およびBPDU転送
IGMPスヌーピング	IGMP（v2 / v3）スヌーピング IGMPクエリア 最大256のマルチキャストグループ
MLDスヌーピング	IPv6 MLD（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	IPv4 / IPv6IPベースのACL / MACベースのACL IPv4 / IPv6IPベースのACE / MACベースのACE 8つのマッピングIDを8つのレベルの優先度キューに - ポート番号 -802.1pの優先度 -IPv4 / IPv6 / パケットのDSCP / IP優先順位 トラフィック分類ベース、厳密な優先順位、およびWRR ポート帯域幅制御ごとの入力/出力レート制限
QoS	IEEE802.1Xポートベースの認証 RADIUSサーバーと連携するための組み込みRADIUSクライアント RADIUS / TACACS +認証 IP-MACポートバインディング MACフィルタリング 静的MACアドレス
セキュリティ	

管理機能	DHCPスヌーピングとDHCPオプション82 STP BPDUガード、BPDUフィルタリング、およびBPDU転送 DoS攻撃の防止 ARP検査 IPソースガード ストームコントロールのサポート -ブロードキャスト/不明なユニキャスト/不明なマルチキャスト
基本的な管理インターフェース	ウェブブラウザ; Telnet; SNMP v1、v2c、v3 イーサネットネットワークを介したHTTP / FTPプロトコルによるファームウェアのアップグレード HTTP / TFTPを介した構成のアップロード/ダウンロード リモート/ローカルSyslog システムログ LLDPプロトコル SNTP PLANETスマートディスカバリユーティリティ
安全な管理インターフェース	SSH、SSL、SNMP v3
SNMPMIB	RFC3635イーサネットのようなMIB RFC2863インターフェイスグループMIB RFC 2819 RMON（1、2、3、9） RFC1493ブリッジMIB
規格への適合	
企業コンプライアンス	FCCパート15クラスA、CE IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX / 100BASE-FX

標準への準拠

- IEEE802.3zギガビットSX / LX
- IEEE802.3abギガビット1000BASE-T
- IEEE802.3xフロー制御と背圧
- LACPを備えたIEEE802.3adポートトラUNK
- IEEE802.1Dスバニングツリープロトコル
- IEEE802.1w高速スバニングツリープロトコル
- IEEE802.1sマルチスバニングツリープロトコル
- IEEE802.1pサービスクラス
- IEEE 802.1QVLANタギング
- IEEE802.1xポート認証ネットワーク制御
- IEEE 802.1ab LLDP
- RFC 768 UDP
- RFC 793 TFTP
- RFC 791 IP
- RFC 792 ICMP
- RFC 2068 HTTP
- RFC 1112IGMPバージョン1
- RFC 2236IGMPバージョン2
- RFC 3376IGMPバージョン3

環境

オペレーティング

ストレージ

- RFC 2710MLD/バージョン1
- RFC 3810MLD/バージョン2
- 温度：0～50℃
- 相対湿度：5～95%（結露しないこと）
- 温度：-20～70℃
- 相対湿度：5～95%（結露しないこと）

2.インストール

このセクションでは、ハードウェア機能と、デスクトップまたはラックマウントへのマネージドスイッチのインストールについて説明します。簡単にマネージドスイッチの管理と制御、その表示インジケータとポートについてよく理解してください。フロントパネル
この章の図は、ユニットのLEDインジケータを示しています。ネットワークデバイスをマネージドスイッチに接続する前に、この章を完全に読んでください。

2.1ハードウェアの説明

2.1.1スイッチのフロントパネル

フロントパネルは、マネージドスイッチの簡単なインターフェイスモニタリングを提供します。[図2-1-1a](#)から[2-1-1g](#)は、のフロントパネルを示しています。マネージドスイッチ。

GS-4210-8P2Sフロントパネル

図2-1-1aGS -4210-8P2Sフロントパネル

GS-4210-8P2T2Sフロントパネル

図2-1-1bGS -4210-8P2T2Sフロントパネル

GS-4210-16P4Cフロントパネル

図2-1-1cGS -4210-16P4Cフロントパネル

GS-4210-24P4Cフロントパネル

図2-1-1dGS -4210-24P4Cフロントパネル

GS-4210-24PL4Cフロントパネル

図2-1-1eGS -4210-24PL4Cフロントパネル

31

GS-4210-48T4Sフロントパネル

図2-1-1fGS -4210-48T4Sフロントパネル

GS-4210-48P4Sフロントパネル

図2-1-1gGS -4210-48P4Sフロントパネル

■ギガビットTPインターフェース

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

■ 100 / 1000BASE-XSFPスロット

各SFP（Small Form-Factor Pluggable）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 トランシーバモジュールの場合：2 km（マルチモードファイバ）から20/40/60 km（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ースです。コンソールポートを介して、IPアドレス設定、出荷時設定へのリセット、ポート管理、リンクステータス、システムなどの豊富な診断情報を提供します設定。

ユーザーは、パッケージに付属のDB9-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、ProComm Plus、Telix、Winterm）を実行できます。など）デバイスの起動画面に入ります。

■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、オンとオフを切り替えずにマネージドスイッチを再起動するように設計されています。パワー。以下は、リセットボタン機能の要約表です。

リセットボタンを押して放した

<5秒：システムの再起動

> 5秒：工場出荷時のデフォルト

関数

管理対象スイッチを再起動します。

管理対象スイッチを工場出荷時のデフォルト構成にリセットします。

その後、マネージドスイッチが再起動してデフォルトをロードします

以下に示す設定：

- 。 デフォルトのユーザー名：admin
- 。 デフォルトのパスワード：admin

- 。 デフォルトの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

2.1.2LED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ステータスを示します。監視とトラブルシューティングに役立ちます
必要です。図2-1-2aから2-1-2fは、これらのマネージドスイッチのLED表示を示しています。

GS-4210-8P2SLED表示

図2-1-2aGS -4210-8P2SLED/パネル

■システム

導いた	色	関数
PWR	緑色のライト	スイッチに電力が供給されていることを示します。
ファン	ファンがダウンしていることを示すオレンジ色のライト。	

■ 10/100 / 1000BASE-Tインターフェイス

導いた	色	関数
LNK / ACT	緑	点灯：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データをアクティブに送信または受信していることを示します。
1000	緑	点灯：ポートが1000Mbpsで動作していることを示します。 オフ： LNK / ACT LEDが点灯している場合は、ポートが10 / 100Mbpsで動作していることを示しています。 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。

■ 100 / 1000BASE-XSFPインターフェイス

導いた	色	関数
LNK / ACT	緑	点灯：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データをアクティブに送信または受信していることを示します。 点灯：ポートが1000Mbpsで動作していることを示します。
1000	緑	オフ： LNK / ACT LEDが点灯している場合は、ポートが100Mbpsで動作していることを示しています。 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。

GS-4210-8P2T2SLED表示

図2-1-2bGS -4210-8P2T2SLEDパネル

■システム

導いた	色	関数
PWR	緑色のライト	は、スイッチに電力が供給されていることを示します。
SYS	緑	システムが機能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ために点滅します。

■ 10/100 / 1000BASE-Tインターフェイス

導いた	色	関数
LNK / ACT	緑	点灯：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データをアクティブに送信または受信していることを示します。 点灯：ポートが1000Mbpsで動作していることを示します。
1000	オレンジオフ：	LNK / ACT LEDが点灯している場合は、ポートが10 / 100Mbpsで動作していることを示しています。 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。

■ 100 / 1000BASE-XSFPインターフェイス

導いた	色	関数
LNK / ACT	緑	点灯：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データをアクティブに送信または受信していることを示します。 点灯：ポートが1000Mbpsで動作していることを示します。
1000	オレンジ	オフ： LNK / ACT LEDが点灯している場合は、ポートが100Mbpsで動作していることを示しています。 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

GS-4210-16P4CLED表示

図2-1-2cGS -4210-16P4CLEDパネル

システムアラート

導いた	色	関数
PWR	緑色のライト	は、スイッチに電力が供給されていることを示します。
SYS	緑	システムが機能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ために オフ 。
ファン1	赤	FAN1がダウンしていることを示す ライト 。
ファン2	赤	FAN2がダウンしていることを示す ライト 。
PoE PWR	赤	PoE電源がダウンしていることを示すために 点灯 します。

■ 10/100 / 1000BASE-Tインターフェイス（ポート-1からポート-16）

導いた	色	関数
LNK / ACT	緑	点灯 ：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データをアクティブに送信または受信していることを示します。
PoE	オレンジ	ライト ：ポートが56VDCインライン電力を供給していることを示します。 オフ ：接続されたデバイスがPoE給電デバイス（PD）ではないことを示します。

■ 10/100 / 1000BASE-Tインターフェイス（ポート-17からポート-20）

導いた	色	関数
LNK / ACT	緑	点灯 ：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データをアクティブに送信または受信していることを示します。 点灯 ：ポートが1000Mbpsで動作していることを示します。
1000	オレンジ	オフ ：LNK / ACT LEDが点灯している場合は、ポートが10 / 100Mbpsで動作していることを示しています。 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。

■ 100 / 1000BASE-SX / LX SFPインターフェイス（ポート-17からポート-20）

導いた	色	関数
LNK / ACT	緑	点灯 ：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データをアクティブに送信または受信していることを示します。 点灯 ：ポートが1000Mbpsで動作していることを示します。
1000	オレンジ	オフ ：LNK / ACT LEDが点灯している場合は、ポートが100Mbpsで動作していることを示しています。 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。

■システム/アラート

導いた	色	関数
PWR	緑色のライト	は、スイッチに電力が供給されていることを示します。
SYS	緑	システムが機能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ためにオフ。
ファン1	赤	FAN1がダウンしていることを示すライト。
ファン2	赤	FAN2がダウンしていることを示すライト。
PoE PWR	赤	PoE電源がダウンしていることを示すために点灯します。

■ 10/100 / 1000BASE-Tインターフェイス（ポート1からポート24）

導いた	色	関数
LNK / ACT	緑	点灯：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データをアクティブに送信または受信していることを示します。
PoE	オレンジ	ライト：ポートが56VDCインライン電力を供給していることを示します。
		オフ：接続されたデバイスがPoE給電デバイス（PD）ではないことを示します。

■ 10/100 / 1000BASE-Tインターフェイス（ポート25からポート28）

導いた	色	関数
LNK / ACT	緑	点灯：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データをアクティブに送信または受信していることを示します。
		点灯：ポートが1000Mbpsで動作していることを示します。
1000	オレンジ	オフ：LNK / ACT LEDが点灯している場合は、ポートが10 / 100Mbpsで動作していることを示しています。 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。

■ 100 / 1000BASE-SX / LX SFPインターフェイス（ポート25からポート28）

導いた	色	関数
LNK / ACT	緑	点灯：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データをアクティブに送信または受信していることを示します。
		点灯：ポートが1000Mbpsで動作していることを示します。
1000	オレンジ	オフ：LNK / ACT LEDが点灯している場合は、ポートが100Mbpsで動作していることを示しています。 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。

GS-4210-48T4SLED表示

図2-1-2cGS -4210-48T4SLEDパネル

■ システム

導いた	色	関数
PWR	緑色のライト	は、スイッチに電力が供給されていることを示します。
SYS	緑色のライト	システムが機能していることを示す緑色のライト。

■ 10/100 / 1000Mbps RJ45インターフェイス（ポート1からポート48）ごと

導いた	色	関数
速度	オレンジ	そのポートを介したリンクが1000Mbpsで正常に確立されたことを示します。
	なし	そのポートを介したリンクが10 / 100Mbpsで正常に確立されたことを示します。
LNK / ACT	緑	点滅：スイッチがそのポートを介してデータをアクティブに送信または受信していることを示します。

■ 100 / 1000Mbps SFPインターフェイスごと（ポート49からポート52）

導いた	色	関数
LNK / ACT	緑	点灯：そのポートを介したリンクが1000Mbpsで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データをアクティブに送信または受信していることを示します。
	オレンジ	点灯：そのポートを介したリンクが100Mbpsで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データをアクティブに送信または受信していることを示します。

GS-4210-48P4SLED表示

図2-1-2fGS -4210-48P4SLED/パネル

システム

導いた	色	関数
PWR	緑色	緑色のライトは、スイッチに電力が供給されていることを示します。
SYS		システムが機能していることを示す緑色のライト。

■ 当たり10/100 / 1000MbpsのRJ45インタフェース（ポート1ポート48へ）

導いた	色	関数
LNK / ACT	緑	点灯：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データをアクティブに送信または受信していることを示します。
PoE	オレンジ	ライト：ポートが52VDCインライン電力を供給していることを示します。 オフ： 接続されたデバイスがPoE給電デバイス（PD）ではないことを示します。

■ バー100 / 1000MbpsのSFPインターフェイス（ポート49ポート52へ）

導いた	色	関数
LNK / ACT	緑	点灯：そのポートを介したリンクが1000Mbpsで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データをアクティブに送信または受信していることを示します。
	オレンジ	点灯：そのポートを介したリンクが100Mbpsで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データをアクティブに送信または受信していることを示します。

2.1.3スイッチの背面パネル

マネージドスイッチの背面パネルには、100～240VACの入力電力を受け入れるACインレット電源ソケットが示されています。

50～60Hz。図2-1-3aから2-1-3gは、これらのマネージドスイッチのリアパネルを示しています。

GS-4210-8P2Sリアパネル

図2-1-3aGS - 4210-8P2Sの背面パネル

GS-4210-8P2T2Sリアパネル

図2-1-3bGS - 4210-8P2T2Sの背面パネル

GS-4210-16P4Cリアパネル

図2-1-3cGS - 4210-16P4Cの背面パネル

GS-4210-24P4Cリアパネル

図2-1-3dGS -4210-24P4Cのリアパネル

GS-4210-24PL4Cリアパネル

図2-1-3eGS - 4210-24PL4Cの背面パネル

GS-4210-48T4Sリアパネル

図2-1-3fGS - 4210-48T4Sの背面パネル

GS-4210-48P4Sリアパネル

図2-1-3gGS - 4210-48P4Sの背面パネル

■ AC電源レセプタクル

世界のほとんどの地域での電気サービスとの互換性のために、マネージドスイッチの電源は自動的に調整されます
100-240VACおよび50 / 60Hzの範囲のライン電力に。

電源コードのメス側をマネージドスイッチの背面パネルのレセプタクルにしっかりと差し込みます。他のプラグ
電源コードの端をコンセントに差し込むと、電源の準備が整います。

パワー通知： このデバイスは電力が必要なデバイスです。つまり、電力が供給されるまで機能しません。ネットワークの場合
常にアクティブである必要があります。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ネットワークのダウンタイムを防ぐことができます。

パワー通知：一部の地域では、サージ抑制デバイスをインストールすると、マネージドスイッチの保護にも役立つ場合があります。調整されていないサージまたはマネージドスイッチへの電流による損傷から。

2.2スイッチの取り付け

このセクションでは、マネージドスイッチをインストールしてマネージドスイッチに接続する方法について説明します。をお読みください

以下のトピックを参照し、提示されている順序で手順を実行します。管理対象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、次の手順を実行するだけです。

2.2.1デスクトップインストール

マネージド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、次の手順に従ってください。

ステップ1： マネージドスイッチの下部にあるくぼんだ領域にゴム製の脚を取り付けます。

手順2： [図2-1-4](#)に示すように、管理対象スイッチをデスクトップまたはAC電源の近くのシェルフに配置します。

図2-1-4管理対象スイッチをデスクトップに配置する

手順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確保します。

場所を選択するときは、第1章で説明した環境制限に留意してください。

セクション4、および仕様。

手順4 : マネージドスイッチをネットワークデバイスに接続します。

標準のネットワークケーブルの一方の端を、マネージドスイッチの前面にある10/100 / 1000RJ45ポートに接続します。

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。

管理対象スイッチに接続するには、RJ45チップを備えたUTPカテゴリ5ネットワークケーブルが必要です。多くのための詳細については、付録Aのケーブル仕様を参照してください。

ステップ5 : マネージドスイッチに電力を供給します。

電源ケーブルの一方の端をマネージドスイッチに接続します。

電源ケーブルの電源プラグを標準の壁コンセントに接続します。

マネージドスイッチに電力が供給されると、電源LEDは緑色に点灯したままになります。

2.2.2ラックマウント

マネージドスイッチを19インチの標準ラックに取り付けるには、以下の手順に従ってください。

手順1 : 管理対象スイッチを硬い平らな面に置き、フロントパネルを前面に向けます。

手順2 : 付属のネジをパッケージに取り付けて、ラックマウントブラケットをマネージドスイッチの両側に取り付けます。

図2-1-5に、マネージドスイッチの片側にブラケットを取り付ける方法を示します。

図2-1-5管理対象スイッチへのブラケットの取り付け。

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。による部品の損傷
間違ったネジを使用すると、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。

手順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。

手順5 : ブラケットをマネージドスイッチに取り付けたら、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2-1-6に示すように。

図2-1-6ラックへのマネージドスイッチの取り付け

手順6 : セッション2.2.1デスクトップの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て電源を供給します。

マネージドスイッチ。

2.2.3 SFP トランシーバーの取り付け

このセクションでは、SFP トランシーバーをSFP スロットに挿入する方法について説明します。SFP トランシーバーはホットプラグ可能であり、ホットスワップ可能。マネージドスイッチの電源を切ることなく、SFP ポートとの間でトランシーバーを接続および接続できます。

図2-1-7に示します。

図2-1-7 SFP トランシーバーのプラグイン

■ 承認されたPLANETSFP トランシーバー

PLANET マネージドスイッチは、シングルモードとマルチモードの両方のSFP トランシーバーをサポートします。承認されたPLANET の次のリスト SFP トランシーバーは、発行時点で正しいものです。

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 mini-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

ファストイーサネットSFPトランシーバモジュール

- **MFB-FX** SFPポート100BASE-FXトランシーバー – 2km
- **MFB-F20** SFPポート100BASE-FXトランシーバー – 20km
- **MFB-F60** SFPポート100BASE-FXトランシーバー – 60km
- **MFB-FA20** SFPポート100BASE-BXトランシーバー（WDM、TX：1310nm） – 20km
- **MFB-FB20** SFPポート100BASE-BXトランシーバー（WDM、TX：1550nm） – 20km

マネージドスイッチではPLANETSFPを使用することをお勧めします。SFPトランシーバーを挿入する場合サポートされていない場合、マネージド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例としてギガビットSFPトランシーバーを使用しています。しかしながら、ファストイーサネットSFPトランシーバーの手順も同様です。

- 1.1。 管理対象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の両側を確認する必要があります
トランシーバーは同じメディアタイプです。たとえば、1000BASE-SXから1000BASE-SX、1000BASE-LXから1000BASE-LX。

1.2。 光ファイバケーブルのタイプがSFPトランシーバの要件と一致するかどうかを確認します。
➤ 1000BASE-SXSFPトランシーバーに接続するには、片側がオスのマルチモードファイバケーブルを使用してください
デュプレックスLCコネクタタイプ。
➤ 1000BASE-LXSFPトランシーバーに接続するには、片側がオス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
デュプレックスLCコネクタタイプ。

■ ファイバケーブルを接続する

- 1.1。 デュプレックスLCコネクタをSFPトランシーバに挿入します。
- 2.2。 ケーブルのもう一方の端を、SFPトランシーバーが取り付けられているデバイスに接続します。
- 3.3。 管理対象スイッチの前面にあるSFPスロットのLNK / ACTLEDを確認します。SFPトランシーバーが動作していることを確認します
正しく。
- 4.4。 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てください。一部のファイバーNICまたはメディアコンバーターで機能するには、ユーザーが設定する必要があります
「1000Force」または「100Force」へのポートリンクモード。

■ トランシーバモジュールを取り外します

- 1.1。 ネットワークアクティビティがもうないことを確認してください。
- 2.2。 光ファイバケーブルをそっと取り外します。
- 3.3。 MGBモジュールのレバーを持ち上げ、水平位置に回します。
- 4.4。 レバーからモジュールをそっと引き出します。

図2-1-8SFPトランシーバーを引き出す方法

モジュールのレバーを持ち上げて水平にしないでモジュールを引き出さないでください

ポジション。モジュールを直接引き抜くと、モジュールとのSFPモジュールスロットが損傷する可能性があります。

マネージドスイッチ。

3.スイッチ管理

この章では、マネージドスイッチへの管理アクセスを設定するために使用できる方法について説明します。それは説明します

管理アプリケーションの種類と、ユーザー間でデータを配信する通信および管理プロトコル

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ー）およびシステム。ポート接続に関する情報も含まれています
オプション。

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、および関連資料

3.1要件

- Windows 2000 / XP、2003、Vista / 7 / 8、2008、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
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にはイーサネットNIC（ネットワークインターフェイスカード）がインストールされています。
- シリアルポート接続（ターミナル）
•上記のPCには、COMポート（DB9 / RS-232）またはUSB-RS-232コンバーターが付属しています
- イーサネットポート接続
•ネットワークケーブル-RJ45コネクタ付きの標準ネットワーク（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ブラウザとJavaランタイム環境プラグインとともにインストールされます。

管理対象スイッチにアクセスするには、Internet Explorer8.0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

マネージドスイッチは、次の方法のいずれかまたはすべてを使用してアクセスおよび管理する柔軟性を提供します。

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

管理コンソールとWebブラウザインターフェイスはマネージドスイッチソフトウェアに組み込まれており、次の目的で使用できます。

すぐに使用できます。これらの管理方法にはそれぞれ独自の利点があります。表3-1は、3つの管理を比較しています
メソッド。

方法	利点	短所
コンソール	•IPアドレスやサブネットは必要ありません •テキストベース	•スイッチの近くにあるか、ダイヤルアップを使用する必要があります 接続

<ul style="list-style-type: none"> •Telnet機能とハイパーターミナルWindowsに組み込まれています 95/98 / NT / 2000 / ME / XP動作システム •安全 	<ul style="list-style-type: none"> •リモートユーザーには不便 •モデム接続は信頼できないことが判明する場合があります または遅い
<p>Webブラウザ・スイッチをリモートで構成するのに理想的</p> <ul style="list-style-type: none"> •すべての一般的なブラウザと互換性があります •どこからでもアクセスできます •最も視覚的に魅力的 	<ul style="list-style-type: none"> •セキュリティが危険にさらされる可能性があります（ハッカーはIPアドレスとサブネットマスクのみを知るため） •接続不良でラグタイムが発生する可能性があります
<p>SNMPエージェント・でスイッチ機能と通信します</p> <p>MIBレベル</p> <ul style="list-style-type: none"> •オープンスタンダードに基づく 	<ul style="list-style-type: none"> •SNMPマネージャーソフトウェアが必要です •3つの方法すべての中で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 •セキュリティが危険にさらされる可能性があります（ハッカーはコミュニティ名のみを知るため）

表3-1管理方法の比較

3.3管理コンソール

管理コンソールは、システムを実行するための内部の文字指向のコマンドラインユーザーインターフェイスです。

統計の表示やオプション設定の変更などの管理。この方法を使用すると、管理を表示できます

マネージドスイッチのコンソールポートに接続された端末、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のコンソール。

図3-1-1：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、端末またはを備えたPCを直接接続することによって実現されます。

ターミナルエミュレーションプログラム（ハイパーターミナルなど）をマネージドスイッチコンソール（シリアル）ポートに接続します。これを使用する場合

管理方法では、スイッチをPCに接続するには、RS-232からRJ45へのストレートケーブルが必要です。これを作った後接続するには、次のパラメータを使用するようにターミナルエミュレーションプログラムを構成します。

デフォルトのパラメータは次のとおりです。

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

図3-1-2：端末パラメータ設定

必要に応じて、ログイン後にこれらの設定を変更できます。この管理方法は、次のことができるため、多くの場合好まれます。接続を維持し、システムの再起動中にシステムを監視します。また、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。関連するアクションが開始されたインターフェイスに関係なく。MacintoshまたはPCの添付ファイルは、端末のシリアルポートに接続するための端末エミュレーションプログラム。UNIXでのワークステーションアタッチメントはエミュレーターを使用できますTIPなど。

コンソールインターフェイスは、GS-4210-8P2S、GS-4210-48T4S、およびGS-4210-48P4Sでは使用できません。

3.4Web管理

マネージドスイッチは、ユーザーがマネージドスイッチをどこからでも管理できるようにする管理機能を提供します。Microsoft InternetExplorerなどの標準ブラウザを介したネットワーク。スイッチのIPアドレスを設定した後、次のことができます。のIPアドレスを入力して、WebブラウザでマネージドスイッチのWebインターフェイスアプリケーションに直接アクセスします。マネージドスイッチ。

図3-1-3Web管理

次に、Webブラウザを使用して、マネージドスイッチ構成/パラメーターを1つの中央の場所から一覧表示および管理できます。

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かのように。Web管理にはMicrosoftのいずれかが必要です

Internet Explorer 8.0以降、Google Chrome、Safari、またはMozilla Firefox1.5以降。

図3-1-4 マネージドスイッチのWebメイン画面

3.5SNMP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、SNMPネットワークなどのマネージドスイッチを構成および管理できます。

マネージャ、HP Openview Network Node Management (NNM) またはWhat's UpGold。この管理方法にはSNMPが必要で

スイッチ上のエージェントと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します。この管理

：この方法は、実際には、2つのコミュニティストリング使用GETコミュニティ文字列と設定コミュニティ文字列を。SNMPネットワークの場合

管理ステーションは、設定されたコミュニティ文字列のみを認識し、MIBの読み取りと書き込みを行うことができます。ただし、取得を知っているだけの場合

コミュニティ文字列。MIBのみを読み取ることができます。マネージドスイッチのデフォルトの取得および設定コミュニティストリングはパブリックです。

3.6 PLANET SmartDiscoveryユーティリティ

イーサネット環境でマネージドスイッチを簡単に一覧表示するには、ユーザーズマニュアルのPlanet Smart DiscoveryUtility CD-ROMは理想的なソリューションです。次のインストール手順は、Planet SmartDiscoveryを実行するためのガイドです。ユーティリティ。

- 1.管理者PCにPlanetSmart DiscoveryUtilityをデポジットします。
- 2.次の画面が表示されたら、このユーティリティを実行します。

図3-1-6： Planet SmartDiscoveryユーティリティ画面

同じ管理者PCに2枚以上のLANカードがある場合は、別のLANカードを選択してください
使用して「選択アダプタ」ツールを。

- 3.3。 押して「リフレッシュ」以下の画面が示すように検出リストで現在接続されたデバイスのためのボタン：

- 1.このユーティリティは、MACアドレス、デバイス名、ファームウェアバージョンなど、デバイスから必要なすべての情報を表示します。
デバイスのIPサブネットアドレス。また、新しいパスワード、IPサブネットアドレス、および説明をデバイスに割り当てることもできます。

- 2.セットアップが完了したら、「**デバイスの更新**」、「**マルチの更新**」、または「**すべての更新**」ボタンを押して有効にします。定義
上記の3つのボタンのうち以下に示します。

■ **デバイスの更新**：1つのデバイスで現在の設定を使用します。

■ **マルチの更新**：マルチデバイスで現在の設定を使用します。

■ **すべて更新**：リスト内のデバイス全体で現在の設定を使用します。

上記と同じ機能は、「**オプション**」ツールバーにもあります。

- 3.「**パケット強制ブロードキャストの制御**」機能をクリックすると、WebSmartに新しい設定値を割り当てることができます。
別のIPサブネットアドレスで切り替えます。
- 4.「**デバイスに接続**」ボタンを押すと、[図3-1-4](#)にWebログイン画面が表示されます。
- 5.「**終了**」ボタンを押して、Planet SmartDiscoveryユーティリティをシャットダウンします。

4.Web構成

このセクションでは、Webベースの管理の構成と機能を紹介します。

Webベースの管理について

マネージドスイッチは、ユーザーがマネージドスイッチをどこからでも管理できるようにする管理機能を提供します。

Microsoft Internet Explorerなどの標準ブラウザを介したネットワーク。

Webベースの管理はInternet Explorer 8.0をサポートします。これは、ネットワークを削減することを目的としたJavaアプレットに基づいています。

帯域幅の消費、アクセス速度の向上、見やすい画面の表示。

デフォルトでは、IE 8.0以降のバージョンではJavaアプレットがソケットを開くことができません。ユーザーはする必要があります
ブラウザ設定を明示的に変更して、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します。

マネージドスイッチはイーサネット接続を介して構成できるため、マネージャーPCと同じに設定する必要があります。

管理対象スイッチとしてのIPサブネットアドレス。

たとえば、マネージドスイッチのデフォルトのIPアドレスが**192.168.0.100の場合**、マネージャーPCは次のように設定する必要があります。

192.168.0.x（xは100を除く1から254までの数値）であり、デフォルトのサブネットマスクは255.255.255.0です。

コンソールを介してマネージドスイッチのデフォルトIPアドレスをサブネットマスク255.255.255.0で192.168.1.1に変更した場合、

次に、マネージャーPCを192.168.1.x（xは2～254の数値）に設定して、で相対的な構成を行う必要があります。

マネージャーPC。

図4-1-1 Web管理

■スイッチへのログイン

1.1。 Internet Explorer 8.0以降のWebブラウザを使用してください。工場出荷時のデフォルトのIPアドレスを入力して、Webインターフェイスにアクセスします。ザ・

工場出荷時のデフォルトのIPアドレスは次のとおりです。

http://192.168.0.100

- 2.2。 次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**」とパスワード「**admin**」（または
コンソールで変更したユーザー名/パスワード）を使用して、マネージドスイッチのメイン画面にログインします。のログイン画面
[図4-1-2](#)が表示されます。

図4-1-2ログイン画面

デフォルトのユーザー名：**admin**

デフォルトのパスワード：**admin**

ユーザー名とパスワードを入力すると、メイン画面が[図4-1-3](#)のように表示されます。

図4-1-3デフォルトのメインページ

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、Managed Switch by Webを管理したりできます。
インターフェース。Webページの左側にあるスイッチメニューを使用すると、マネージドスイッチのすべてのコマンドと統計にアクセスできます。
提供します。

- 管理対象スイッチにアクセスするには、Internet Explorer 8.0以降を使用することをお勧めします。
- 変更されたIPアドレスは、[保存]ボタンをクリックした直後に有効になります。必要がある新しいIPアドレスを使用してWebインターフェイスにアクセスします。
- 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記憶してください。
- Webインターフェイスでは小文字のコマンドのみを受け入れます。

4.1メインWebページ

管理対象スイッチは、それを構成および管理するためのWebベースのブラウザーインターフェイスを提供します。このインターフェイスを使用すると、選択したWebブラウザを使用してマネージドスイッチにアクセスします。この章では、マネージドスイッチの使用法について説明します。

それを構成および管理するためのWebブラウザインターフェイス。

図4-1-4メインページ

パネルディスプレイ

Webエージェントは、マネージドスイッチのポートのイメージを表示します。モードは、のさまざまな情報を表示するように設定できます。

リンクアップまたはリンクダウンを含むポート。ポートの画像をクリックすると、**[ポート統計]**ページが開きます。

ポートの状態は次のように示されます。

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ことにより、システムパラメータを定義し、マネージドスイッチとそのすべてのポートを管理および制御できます。

またはネットワークの状態を監視します。管理者は、Web管理を介して、を選択してマネージドスイッチを設定できます。

MainFunctionにリストされている機能。[図4-1-5](#)の画面が表示されます。

図4-1-5 マネージドスイッチの主な機能メニュー

ボタン

：クリックして変更を保存するか、デフォルトにリセットします。

：クリックして、マネージドスイッチからログアウトします。

：クリックして管理対象スイッチを再起動します。

：クリックしてページを更新します。

4.1.1 保存ボタン

この保存ボタンを使用すると、実行/起動/バックアップ構成またはリセットスイッチをデフォルトパラメータで保存できます。の画面 [図4-1-6](#)が表示されます。

図4-1-6 保存ボタン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
・構成をに保存	クリックして構成を保存します。詳細については、 を参照してください。
閃光	4.1.2章
・デフォルトに戻す	クリックして、デフォルトパラメータのスイッチをリセットします。詳細については、 4.15.1章を参照してください

4.1.2 構成マネージャー

システムファイルフォルダには、構成設定が含まれています。 [図4-1-7](#)の画面が表示され **ます**。

図4-1-7保存ボタン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
・実行コンフィギュレーションスイッチ	で使用する実行コンフィギュレーションシーケンスを指します。 スイッチでは、実行コンフィギュレーションファイルはRAMに保存されます。現在のバージョンでは、実行コンフィギュレーションシーケンスrunning-configはRAMから保存できます 「ソースファイル=実行コンフィギュレーション」を「宛先」に保存してフラッシュに ファイル=スタートアップ構成」、つまり実行構成シーケンス スタートアップコンフィギュレーションファイルになります。これはコンフィギュレーションセーブと呼ばれます。 不正なファイルのアップロードを防ぎ、設定を簡単にするために、スイッチは名前を義務付けています 実行中の構成ファイルのrunning-config。
・スタートアップコンフィギュレーションスイッチ	の起動で使用する構成シーケンスを参照します。 スタートアップコンフィギュレーションファイルは、 いわゆる構成の保存。デバイスがマルチ構成ファイルをサポートしている場合は、 構成ファイルは.cfgファイルになり、デフォルトはstartup.cfgです。 デバイスがマルチ構成ファイルをサポートしていない場合は、スタートアップの名前を義務付けます

	設定ファイルはstartup-configになります。
・バックアップ 構成	FLASHではバックアップ構成は空です。バックアップを保存してください 最初に「メンテナンス>バックアップマネージャ」で構成します。
ボタン	
	: クリックして構成を保存します。

4.1.2.1構成の保存

マネージドスイッチでは、実行コンフィギュレーションファイルがRAMに保存されます。現在のバージョンでは、実行コンフィギュレーション running-configのシーケンスは、「構成をFLASHに保存」機能によってRAMからFLASHに保存できるため、
実行中の構成シーケンスは、構成保存と呼ばれるスタートアップ構成ファイルになります。

適用されたすべての変更を保存し、現在の構成をスタートアップ構成として設定します。スタートアップコンフィギュレーションファイルはシステムの再起動時に自動的にロードされます。

- 1.1。 「保存>構成をフラッシュに保存」をクリックして、「構成マネージャ」 ページにログインします。

2.2。 「ソースファイル=実行コンフィギュレーション」および「宛先ファイル=スタートアップコンフィギュレーション」を選択します。

3.3。 「適用」ボタンを押して実行中の構成を保存し、構成を開始します。

4.2システム

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

■システム情報	スイッチシステム情報はここにあります。
■IP構成	このページでスイッチ管理のIP情報を構成します。
■IPv6構成	このページでスイッチ管理のIPv6情報を構成します。
■ユーザー設定	このページで新しいユーザー名とパスワードを設定します。
■時間設定	このページでSNTPを構成します。
■ログ管理	スイッチログ情報はここにあります。
■SNMP管理	このページでSNMPを構成します。

4.2.1システム情報

[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。システム情報ページは、スイッチ管理者がハードウェアのMACアドレス、ソフトウェアのバージョン、およびシステムの稼働時間を特定します。図4-2-1および図4-2-2の画面が表示されます。

図4-2-1システム情報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
・システム名	現在のシステム名を表示する
・システムの場所	現在のシステムの場所を表示する
・システムの連絡先	現在のシステム連絡先を表示する
・MACアドレス	このマネージドスイッチのMACアドレス。
・IPアドレス	このマネージドスイッチのIPアドレス。
・サブネットマスク	このマネージドスイッチのサブネットマスク。
・ゲートウェイ	このマネージドスイッチのゲートウェイ。
・ローダーバージョン	このマネージドスイッチのローダーバージョン。
・ローダーの日付	このマネージドスイッチのローダーの日付。
・ファームウェアバージョン	このマネージドスイッチのファームウェアバージョン。
・ファームウェアの日付	このマネージドスイッチのファームウェアの日付。
・システムオブジェクトID	管理対象スイッチのシステムオブジェクトID。
・システム稼働時間	デバイスが動作している期間。
・PCN / HWバージョン	このマネージドスイッチのハードウェアバージョン。

ボタン

：クリックしてパラメータを編集します。

4.2.2IP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。構成された列は、IP構成。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4-2-2および図4-2-3の画面現れる。

図4-2-2IPアドレス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
・モード	<p>IPアドレスモードの動作を示します。可能なモードは次のとおりです。</p> <p>静的：NTPモード操作を有効にします。</p> <p>NTPモードの動作を有効にすると、エージェントは転送および転送しますクライアントとサーバーがオンになっていないときのNTPメッセージ同じサブネットドメイン。</p> <p>DHCP：DHCPクライアントモードの操作を有効にします。</p> <p>このチェックボックスをオンにして、DHCPクライアントを有効にします。DHCPが失敗し、構成されたIPアドレスがゼロの場合、DHCPは再試行します。DHCPが失敗し、構成されたIPアドレスがゼロ以外の場合、DHCPは停止し、構成されたIP設定が使用されます。DHCPクライアントは構成済みをアナウンスしますDNS/ルックアップを提供するためのホスト名としてのシステム名。</p>
・IPアドレス	<p>このスイッチのIPアドレスをドット付き10進表記で指定します。</p>
・サブネットマスク	<p>このスイッチのサブネットマスクをドット付き10進表記で指定します。</p>
・ゲートウェイ	<p>ルーターのIPアドレスをドット付き10進表記で指定します。</p>
・DNSサーバー1/2	<p>DNSサーバーのIPアドレスをドット付き10進表記で指定します。</p>
ボタン	<p>：クリックして変更を適用します。</p>

図4-2-3IP情報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
• DHCP状態	現在のDHCP状態を表示します。
• IPアドレス	現在のIPアドレスを表示します。
• サブネットマスク	現在のサブネットマスクを表示します。
• ゲートウェイ	現在のゲートウェイを表示します。
• DNSサーバー1/2	現在のDNSサーバーを表示します。

4.2.3IPv6構成

IPv6構成には、自動構成、IPv6アドレス、およびゲートウェイが含まれます。構成された列は、表示またはIPv6構成を変更します。デバイスの自動構成、IPv6アドレス、およびゲートウェイを入力します。図の画面4-2-4と図4-2-5が表示されます。

図4-2-4IPv6アドレス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
• 自動構成	<p>このチェックボックスをオンにして、IPv6自動構成を有効にします。</p> <p>失敗した場合、構成されたIPv6アドレスはゼロです。ルーターが応答を遅らせる可能性があります 数秒間のルーター要請。完了するのに必要な合計時間</p> <p>自動構成は大幅に長くなる可能性があります。</p>
• IPv6アドレス	<p>このスイッチのIPv6アドレスを指定します。</p> <p>IPv6アドレスは、最大4つの8つのフィールドとして表される128ビットレコードにあります 各フィールドをコロンで区切った16進数 (:)。例えば、 'fe80 :: 215 : c5ff : fe03 : 4dc7'。</p> <p>記号 '::'は、次の省略形として使用できる特別な構文です。</p> <p>連続するゼロの複数の16ビットグループを表します。しかし、それは現れることができます</p>

一度。また、次の合法的なIPv4アドレスを使用します。たとえば、「:192.1.2.34」。

このスイッチのIPv6プレフィックスを指定します。許容範囲は1~128です。

このスイッチのIPv6ゲートウェイアドレスを指定します。

IPv6アドレスは、最大4つの8つのフィールドとして表される128ビットレコードにあります

各フィールドをコロンで区切った16進数 (:)。例えば、

'fe80::215:c5ff:fe03:4dc7'。

このマネージドスイッチが**動的ホスト**からの構成を受け入れることができるようにするには

構成プロトコルバージョン6 (DHCPv6) サーバー。デフォルトでは、マネージ

スイッチはDHCPv6クライアントアクションを実行しません。DHCPv6クライアントは

個々のローカルホストにプッシュできる、存続期間の長いプレフィックスの委任。

ボタン

: クリックして変更を適用します。

図4-2-5IPv6情報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
•自動構成	現在の自動構成状態を表示します
•IPv6使用中アドレス	現在のIPv6使用中アドレスを表示します
•IPv6使用中ルーター	現在使用中のゲートウェイを表示する
•IPv6静的アドレス	現在のIPv6静的アドレスを表示します
•IPv6スタティックルーター	現在のIPv6静的ゲートウェイを表示する
•DHCPv6クライアント	現在のDHCPv6クライアントのステータスを表示する

4.2.4ユーザー設定

このページでは、現在のユーザーと特権タイプの概要を説明します。現在、別のユーザーとしてログインする唯一の方法はWebサーバーは、ブラウザを閉じて再度開きます。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。お願いします新しいユーザー名とパスワードでWebインターフェイスにログインします。図4-2-6および図4-2-7の画面が表示されます。

図4-2-6ローカルユーザー情報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
•ユーザー名	ユーザーを識別する名前。 最大長：32文字。 最大ユーザー数：8
•パスワードタイプ	ユーザーのパスワードタイプ。
•パスワード	ここにユーザーの新しいパスワードを入力します。 (範囲：0～32文字のプレーンテキスト、大文字と小文字を区別)
•パスワードの再入力	確認のため、ここにユーザーの新しいパスワードをもう一度入力してください。
•特権タイプ	ユーザーの特権タイプ。 オプション： •管理者 •ユーザー •その他

ボタン

：クリックして変更を適用します。

図4-2-7ローカルユーザー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
•ユーザー名	現在のユーザー名を表示する
•パスワードタイプ	現在のパスワードタイプを表示します
•特権タイプ	現在の特権タイプを表示します
•変更	クリックしてローカルユーザーエントリを変更します

: 現在のユーザーを削除します

4.2.5時間設定

4.2.5.1システム時間

このページでSNTPを構成します。SNTPは、同期するためのネットワークプロトコルであるSimple Network TimeProtocolの頭字語です。コンピュータシステムの時計。SNTPサーバーを指定し、GMTタイムゾーンを設定できます。のSNTP設定画面 [図4-2-8](#)と[図4-2-9](#)が表示されます。

図4-2-8SNTPセットアップ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
・SNTPを有効にする	有効：SNTPモード操作を有効にします。 SNTPモードの動作を有効にすると、エージェントは転送および転送します クライアントとサーバーがそうでない場合のSNTPメッセージ

	同じサブネットドメイン上。 無効：SNTPモードの操作を無効にします。
・手動時間	手動で時間を設定します。 ・年-開始年を選択します。 ・月-開始月を選択します。 ・日-開始日を選択します。 ・時間-開始時間を選択します。 ・分-開始分を選択します。 ・秒-開始秒を選択します。
・タイムゾーン	スイッチの現在の場所に応じてタイムゾーンを選択できます。
・夏時間	これは、構成に応じてクロックを前後に設定するために使用されます

	定義された夏時間の期間について、以下に設定します。[無効にする]を選択して無効にします
	夏時間の構成。「定期的」を選択し、
	毎年構成を繰り返す夏時間。選択する
	「非繰り返し」および単一時間の夏時間の期間を構成します
	構成。（デフォルト：無効）。
・夏時間	夏時間中に追加する分数を入力します。（範囲：1～
オフセット	1440）
・からの繰り返し	・週-開始週番号を選択します。
	・日-開始日を選択します。
	・月-開始月を選択します。
	・時間-開始時間を選択します。
	・分-開始分を選択します。
・繰り返し	・週-開始週番号を選択します。
	・日-開始日を選択します。
	・月-開始月を選択します。
	・時間-開始時間を選択します。
	・分-開始分を選択します。
・非定期的なFrom	・週-開始週番号を選択します。
	・日-開始日を選択します。
	・月-開始月を選択します。
	・時間-開始時間を選択します。
	・分-開始分を選択します。
・非定期的	・週-開始週番号を選択します。
	・日-開始日を選択します。
	・月-開始月を選択します。
	・時間-開始時間を選択します。
	・分-開始分を選択します。

ボタン

: クリックして変更を適用します。

図4-2-9時間情報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
•現在のデータ/時間	現在のデータ/時間を表示する
•SNTP	現在のSNTP状態を表示します
•タイムゾーン	現在のタイムゾーンを表示する
•夏時間	現在の夏時間の状態を表示します
•夏時間 オフセット	現在の夏時間オフセット状態を表示します
•から	から現在の夏時間を表示します
•へ	現在の夏時間を表示します

4.2.5.2SNTPサーバー設定

図4-2-10および図4-2-11のSNTPサーバー設定画面が表示されます。

図4-2-10SNTPセットアップ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
•SNTPサーバーアドレス	SNTPサーバーのIPアドレスまたはドメイン名を入力します
•サーバーポート	SNTPのポート番号を入力します

ボタン

：クリックして変更を適用します。

図4-2-11 SNTTPサーバー情報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
・SNTTPサーバーアドレス	現在のSNTTPサーバーアドレスを表示します
・サーバーポート	現在のSNTTPサーバーポートを表示します

4.2.6ログ管理

マネージドスイッチのログ管理はここで提供されます。ローカルログを使用すると、システムメッセージを構成および制限できます。フラッシュまたはRAMメモリに記録されます。デフォルトでは、イベントレベル0〜3がフラッシュに記録され、レベル0〜6が記録されます。羊。次の表に、マネージドスイッチのイベントレベルを示します。

レベル重大度名		説明
7	デバッグ	メッセージのデバッグ
6	情報	情報メッセージのみ
5	通知	コールドスタートなどの正常だが重大な状態
4	警告	警告条件（例：falseを返す、予期しない戻り）
3	エラー	エラー状態（例、無効な入力、デフォルトで使用）
2	クリティカル	重大な状態（例：メモリ割り当て、または空きメモリエラー/リソース使い果たされた）
1	アラート	早急な対応が必要
0	緊急	システムが使用できません

4.2.6.1ローカルログ

スイッチシステムのローカルログ情報はここにあります。図4-2-12および図4-2-13のローカルログ画面が表示されます。

図4-2-12ログ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
・ログサービス	有効：ログサービスの操作を有効にします。 無効：ログサービスの操作を無効にします。

ボタン

：クリックして変更を適用します。

図4-2-13ログ情報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
・ログサービス	現在のロギングサービスのステータスを表示します

4.2.6.2ローカルログ

スイッチシステムのローカルログ情報はここにあります。図4-2-14および図4-2-15のローカルログ画面が表示されます。

図4-2-14ローカルログターゲット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
・ターゲット	ローカルログエントリのターゲット。次のターゲットタイプがサポートされています。 ■パッファ：ローカルログのパッファをターゲットにします。 ■ファイル：ローカルログのファイルを対象とします。
・重大度	ローカルログエントリの重大度。次の重大度タイプがサポートされています。

- **EMERG** : ローカルログの不安定なシステムの緊急レベル。
- **警告** : ローカルログに必要な緊急行動の警告レベル。
- **クリティカル** : ローカルログのための重要な条件のクリティカルレベル。
- **エラー** : ローカルログのエラー状態のエラーレベル。
- **警告** : ローカルログの警告条件の警告レベル。
- **予告** : ローカルログの通常だが重要な条件の通知レベル。
- **情報** : ローカルログの情報メッセージの情報レベル。
- **デバッグ** : ローカルログのデバッグメッセージのデバッグレベル。

72

ボタン

: クリックして変更を適用します。

図4-2-15ローカルログ設定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
・ステータス	現在のローカルログの状態を表示します
・ターゲット	現在のローカルログターゲットを表示する
・重大度	現在のローカルログの重大度を表示します
・アクション	: 現在のステータスを削除します

4.2.6.3リモートSyslog

このページでリモートsyslogを構成します。[リモートSyslog]ページでは、送信されるメッセージのログを構成できます

Syslogサーバーまたは他の管理ステーションに。送信されるイベントメッセージを、以下のメッセージのみに制限することもできます。

指定されたレベル。

図4-2-16および図4-2-17のリモートSyslog画面が表示されます。

図4-2-16リモートログターゲット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
・サーバーアドレス	このスイッチのリモートsyslogIPアドレスを指定します。
・サーバーポート	リモートsyslogサーバーのポート番号を指定します。 デフォルトのポート番号：514
・重大度	ローカルログエントリの重大度。次の重大度タイプがサポートされています。 <ul style="list-style-type: none"> ■ EMERG：ローカルログの不安定なシステムの緊急レベル。 ■ 警告：ローカルログに必要な緊急行動の警告レベル。 ■ クリティカル：ローカルログのための重要な条件のクリティカルレベル。 ■ エラー：ローカルログのエラー状態のエラーレベル。 ■ 警告：ローカルログの警告条件の警告レベル。 ■ 予告：ローカルログの通常だが重要な条件の通知レベル。 ■ 情報：ローカルログの情報メッセージの情報レベル。 ■ デバッグ：ローカルログのデバッグメッセージのデバッグレベル。
・施設	Local0～7：ローカルユーザー0～7

ボタン

：クリックして変更を適用します。

図4-2-17リモートログ設定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
・ステータス	現在のリモートsyslog状態を表示します

・サーバー情報	現在のリモートsyslogサーバー情報を表示します
・重大度	現在のリモートsyslogの重大度を表示します
・施設	現在のリモートsyslog機能を表示します
・アクション	: リモートサーバーエントリを削除します

4.2.6.4ログメッセージ

スイッチログビューはここにあります。図4-2-18、図4-2-19、および図4-2-20のログビュー画面が表示されます。

図4-2-18ログ情報スクリーンショットの選択

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
・ターゲット	ログビューエントリのターゲット。次のターゲットタイプがサポートされています。 ■バッファリング：ログビューのバッファリングをターゲットにします。 ■ファイル：ログビューのファイルを対象とします。
・重大度	ログビューエントリの重大度。次の重大度タイプがサポートされています。 ■EMERG：ログ・ビューのための不安定なシステムの緊急レベル。 ■警告：ログ・ビューのために必要な緊急行動の警告レベル。 ■クリティカル：ログ・ビューのための重要な条件のクリティカルレベル。 ■エラー：ログビューのエラー状態のエラーレベル。 ■警告：ログビューの警告条件の警告レベル。 ■通知：ログビューの通常の重要な状態の通知レベル。 ■情報：ログ・ビューのための情報メッセージの情報レベル。 ■デバッグ：ログ・ビューのためのデバッグメッセージのデバッグレベル。
・カテゴリ	ログビューのカテゴリは次のとおりです。 AAA、ACL、CABLE_DIAG、DAI、DHCP_SNOOPING、Dot1X、GVRP、 IGMP_SNOOPING、IPSG、L2、LLDP、ミラー、MLD_SNOOPING、プラットフォーム、PM、 ポート、PORT_SECURITY、QoS、レート、SNMP、およびSTP

ボタン

: クリックしてログを表示します。

図4-2-19ログ情報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
・ターゲット	現在のログターゲットを表示する
・重大度	現在のログの重大度を表示します
・カテゴリ	現在のログカテゴリを表示する
・エントリー総数	現在のログエントリを表示する

図4-2-20ログメッセージ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
・いいえ。	これはログの数です
・タイムスタンプ	ログの時間を表示します
・カテゴリ	カテゴリタイプを表示する
・重大度	重大度タイプを表示します
・メッセージ	ログメッセージを表示する

ボタン

: クリックしてログをクリアします。

: クリックしてログを更新します。

4.2.7SNMP管理

4.2.7.1SNMPの概要

SNMP（Simple Network Management Protocol）はの交換を容易にするためのアプリケーションレイヤプロトコルです

ネットワークデバイス間の管理情報。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）の一部です。**

プロトコルスイート。SNMPを使用すると、ネットワーク管理者はネットワーク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、ネットワークの成長を計画します。

SNMP管理ネットワークは、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）とネットワーク管理プロトコル：

- 。 **ネットワーク管理ステーション（NMS）**：コンソールと呼ばれることもあるこれらのデバイスは、管理アプリケーションを実行します
ネットワーク要素を監視および制御します。物理的には、NMSは通常、ワークステーションレベルのコンピュータをエンジニアリングしています。
高速CPU、メガピクセルカラーディスプレイ、十分なメモリ、および豊富なディスク容量。少なくとも1つのNMSがに存在する必要があります
各管理環境。
- 。 **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。彼らは管理情報を収集して保存します
ネットワーク要素が受信したエラーパケットの数など。
- 。 **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コレクションです。
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、エージェント間で管理情報を伝達するために使用されます
およびNMS。SNMPは、インターネットコミュニティの事実上の標準管理プロトコルです。

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**-エージェントがNMSにイベントを非同期的に通知するために使用します。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と管理ステーションが属するグループです。どこを定義するのに役立ちます

情報が送信されます。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に属している可能性があります

SNMPコミュニティ。いずれかのコミュニティに属していない管理ステーションからの要求には応答しません。SNMP

デフォルトのコミュニティは次のとおりです。

- 。 **書き込み**=プライベート
- 。 **読み取り**=公開

4.2.7.2SNMPシステム情報

このページでSNMP設定を構成します。図4-2-21および図4-2-22のSNMPシステムグローバル設定画面が表示されます。

図4-2-21SNMPグローバル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
・ステータス	SNMPモードの動作を示します。可能なモードは次のとおりです。 有効：SNMPモード操作を有効にします。 無効：SNMPモードの操作を無効にします。

ボタン

：クリックして変更を適用します。

図4-2-22SNMP情報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
・SNMP	現在のSNMPステータスを表示します

4.2.7.3SNMPビュー

このページでSNMPv3ビューテーブルを構成します。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。SNMPv3ビューテーブル [図4-2-23](#)および[図4-2-24](#)の設定画面が表示されます。

図4-2-23SNMPv3ビューテーブル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
・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。 許可される文字列の長さは1～16です。
・サブツリーOID	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。
・サブツリーOIDマスク	ビットマスクは、指定されたオブジェクト識別子のどの位置になるかを識別します パターンマッチングの目的では「ワイルドカード」と見なされます。
・ビュータイプ	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。 含まれる ：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。 除外 ：このビューサブツリーを除外する必要があることを示すオプションのフラグ。 一般に、ビューエントリのビュータイプが「除外」されている場合は、別のビューが存在する必要があります ビュータイプが「含まれる」であり、そのOIDサブツリーが「除外される」を超えるエントリ エントリを表示します。

ボタン

：クリックして新しいビューエントリを追加します。

図4-2-24SNMPビューテーブル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
・ビュー名	現在のSNMPビュー名を表示します
・サブツリーOID	現在のSNMPサブツリーOIDを表示します
・OIDマスク	現在のSNMPOIDマスクを表示します
・ビュータイプ	現在のSNMPビュータイプを表示します
・アクション	：ビューテーブルエントリを削除します。

4.2.7.4SNMPアクセスグループ

このページでSNMPv3アクセスグループを構成します。エントリ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4-2-25および図4-2-26のSNMPv3アクセスグループ設定画面が表示されます。

図4-2-25SNMPv3アクセスグループ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
・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。 許可される文字列の長さは1～16です。
・セキュリティモデル	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。 考えられる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用に予約されています。■ v2c : SNMPv2c用に予約されています。■ V3 : SNMPv3またはユーザーベースのセキュリティモデル（USM）用に予約済み
・セキュリティレベル	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。 考えられる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、プライバシーセキュリティレベルなし グループに割り当てられます。
・ビュー名を読む	読み取りビュー名は、コンテンツのみを表示できるビューの名前です。 エージェントの。 許可される文字列の長さは1～16です。
・ビュー名を書き込む	書き込みビュー名は、データを入力して構成するビューの名前です。 エージェントの内容。 許可される文字列の長さは1～16です。
・ビュー名を通知する	通知ビュー名は、通知、通知、または通知を指定するビューの名前です。 トラップ。

ボタン

：クリックして新しいアクセスエントリを追加します。

：チェックしてエントリを削除します。

図4-2-26SNMPビューテーブル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
・グループ名	現在のSNMPアクセスグループ名を表示します
・セキュリティモデル	現在のセキュリティモデルを表示する
・セキュリティレベル	現在のセキュリティレベルを表示する
・ビュー名を読む	現在の読み取りビュー名を表示します
・ビュー名を書き込む	現在の書き込みビュー名を表示します
・ビュー名を通知する	現在の通知ビュー名を表示します
・アクション	<div> <div></div> <div>：アクセスグループエントリを削除します。</div> </div>

4.2.7.5SNMPコミュニティ

このページでSNMPコミュニティを構成します。図4-2-27および図4-2-28のSNMPコミュニティ画面が表示されます。

図4-2-27コミュニティ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
・コミュニティ名	SNMPへのアクセスを許可するコミュニティの読み取り/書き込みアクセス文字列を示します エージェント。 許可される文字列の長さは0～16です。
・コミュニティモード	SNMPコミュニティがサポートするモードを示します。可能なバージョンは次のとおりです。 ■基本：SNMPコミュニティモードでサポートされているバージョン1および2cを設定します。 ■詳細：SNMPコミュニティモードでサポートされているバージョン3を設定します。
・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。 許可される文字列の長さは1～16です。
・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。 許可される文字列の長さは1～16です。
・アクセス権	SNMPコミュニティタイプの操作を示します。可能なタイプは次のとおりです。 RO =読み取り専用：アクセス文字列タイプを読み取り専用モードに設定します。 RW = Read-Write：読み取り/書き込みモードでアクセス文字列タイプを設定します。

ボタン

: クリックして変更を適用します。

図4-2-28コミュニティ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
・コミュニティ名	現在のコミュニティタイプを表示する
・グループ名	現在のSNMPアクセスグループの名前を表示します
・ビュー名	現在のビュー名を表示する
・アクセス権	現在のアクセスタイプを表示します
・削除	<div></div> : コミュニティエントリを削除します

4.2.7.6SNMPユーザー

このページでSNMPv3ユーザーテーブルを構成します。各SNMPv3ユーザーは、一意の名前で定義されます。ユーザーは、特定のセキュリティレベルで、グループに割り当てられます。SNMPv3グループは、ユーザーを特定の読み取り、書き込み、および通知ビューに制限します。ザ・エントリインデックスキーは**ユーザー名**です。図4-2-29および図4-2-30のSNMPv3ユーザー設定画面が表示されます。

図4-2-29SNMPv3ユーザー構成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
・ユーザー名	このエントリが属するユーザー名を識別する文字列。 許可される文字列の長さは1～16です。
・グループ	SNMPアクセスグループ。このエントリがグループ名を識別する文字列 に属する必要があります。
・特権モード	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：認証もプライバシーもありません。■ 認証：認証とプライバシーなし。■ プライベート：認証とプライバシー。

・認証

プロトコル

エントリがすでに存在する場合、セキュリティレベルの値は変更できません。つまり、まず、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。

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

認証プロトコルは次のとおりです。

- なし：なし認証プロトコル。

83

・認証

パスワード

・暗号化プロトコル

エントリがすでに存在する場合、セキュリティレベルの値は変更できません。つまり、まず、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。

認証パスフレーズを識別する文字列。MD5とSHAの両方

認証プロトコルでは、許可される文字列の長さは8～16です。

このエントリが属する必要があるブライバシープロトコルを示します。可能なブライバシープロトコルは次のとおりです。

- なし：なしブライバシープロトコル。
- DES：このユーザーがDESを使用していることを示すオプションのフラグ
認証プロトコル。

・暗号化キー

ブライバシーパスフレーズを識別する文字列。

許可される文字列の長さは8～16です。

ボタン

：クリックして、新しいユーザーエントリを追加します。

図4-2-30SNMPv3ユーザーの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

・ユーザー名

現在のユーザー名を表示します

・グループ

現在のグループを表示する

・特権モード

現在の特権モードを表示する

・認証プロトコル

現在の認証プロトコルを表示する

・暗号化プロトコル

現在の暗号化プロトコルを表示する

・アクセス権

現在のアクセス権を表示する

・アクション

：ユーザーエントリを削除します

4.2.7.7 SNMPv1、2通知受信者

このページでSNMPv1および2の通知受信者を構成します。図4-2-31のSNMPv1、2通知受信者画面

そして図4-2-32表示されます。

図4-2-31SNMPv1、2通知受信者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
・サーバーアドレス	SNMPトラップの宛先アドレスを示します。で有効なIPアドレスを許可します ドット付き10進表記（'xyzw'）。また、法的に有効なIPv4を表すこともできます 住所。たとえば、「:: 192.1.2.34」。
・SNMPバージョン	SNMPトラップがサポートされているバージョンを示します。可能なバージョンは次のとおりです。 ■ SNMP v1D：設定SNMPトラップは、バージョン1をサポートしていました。 ■ SNMPのV2C：設定SNMPトラップは、バージョン2cをサポートしていました。
・通知タイプ	トラップまたはインフォームに通知タイプを設定します。
・コミュニティ名	SNMPトラップパケットを送信するときのコミュニティアクセス文字列を示します。
・UDPポート	SNMPトラップの宛先ポートを示します。SNMPエージェントはSNMPメッセージを送信します このポートを介して、ポート範囲は1～65535です。
・タイムアウト	SNMPトラップ通知タイムアウトを示します。許容範囲はある1に300。
・再試行	SNMPトラップ通知の再試行時間を示します。許容範囲は、からである1に255。

ボタン

：クリックして、新しいSNMPv1、2ホストエントリを追加します。

図4-2-32SNMPv1、2ホスト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
・サーバーアドレス	現在のサーバーアドレスを表示する
・SNMPバージョン	現在のSNMPバージョンを表示する
・通知タイプ	現在の通知タイプを表示します
・コミュニティ名	現在のコミュニティ名を表示する
・UDPポート	現在のUDPポートを表示する
・タイムアウト	現在のタイムアウトを表示する
・再試行	現在の再試行時間を表示します
・アクション	 : SNMPv1、2ホストエントリを削除します。

4.2.7.8SNMPv3通知受信者

このページでSNMPv3通知受信者を構成します。[図4-2-33のSNMPv1、2通知受信者画面](#)および[図4-2-34](#)が表示されます。

図4-2-33SNMPv3通知受信者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
・サーバーアドレス	SNMPトラップの宛先アドレスを示します。で有効なIPアドレスを許可します ドット付き10進表記（'xyzw'）。また、法的に有効なIPv4を表すこともできます 住所。たとえば、「:: 192.1.2.34」。
・通知タイプ	トラップまたはインフォームに通知タイプを設定します。
・ユーザー名	SNMPトラップパケットを送信するときのユーザー文字列を示します。
・UDPポート	SNMPトラップの宛先ポートを示します。SNMPエージェントはSNMPメッセージを送信します このポートを介して、ポート範囲は1〜65535です。
・タイムアウト	SNMPトラップ通知タイムアウトを示します。許容範囲はある1に300。
・再試行	SNMPトラップ通知の再試行時間を示します。許容範囲は、からである1に255。

ボタン

: クリックして、新しいSNMPv3ホストエントリを追加します。

図4-2-34SNMPv3ホスト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
・サーバーアドレス	現在のサーバーアドレスを表示する
・通知タイプ	現在の通知タイプを表示します
・ユーザー名	現在のユーザー名を表示します
・UDPポート	現在のUDPポートを表示する
・タイムアウト	現在のタイムアウトを表示する
・再試行	現在の再試行時間を表示します
・アクション	<div></div> : SNMPv3ホストエントリを削除します

4.2.7.9SNMPエンジンID

このページでSNMPv3エンジンIDを構成します。エントリーインデックスキーはエンジンIDです。リモートエンジンIDは、リモートホスト上のユーザーに送信されるパケットを認証および暗号化するためのセキュリティダイジェスト。SNMPv3エンジンID設定 [図4-2-35](#)および[図4-2-36](#)の画面が表示されます。

図4-2-35SNMPv3エンジンID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
・エンジンID	このエントリが属するエンジンIDを識別するオクテット文字列。ザ・文字列には、10～64桁の偶数が含まれている必要がありますが、すべてゼロおよびすべて「F」は許可されていません。
ボタン	

: クリックして変更を適用します。

図4-2-36SNMPv3エンジンID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
・ユーザーデフォルト	現在のステータスを表示する
・エンジンID	現在のエンジンIDを表示する

4.2.7.10SNMPリモートエンジンID

このページでSNMPv3リモートエンジンIDを構成します。図4-2-37のSNMPv3リモートエンジンID設定画面と図4-2-38が表示されます。

図4-2-37SNMPv3リモートエンジンID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
・リモートIPアドレス	SNMPリモートエンジンIDアドレスを示します。で有効なIPアドレスを許可します ドット付き10進表記（'xyzw'）。
・エンジンID	このエントリが属するエンジンIDを識別するオクテット文字列。

ボタン

: クリックして変更を適用します。

90ページ

GS-4210シリーズのユーザズマニュアル

ポートメニューを使用して、マネージドスイッチのポートを表示または構成します。このセクションには、次の項目があります。

4.3.1 ポート構成

このページには、現在のポート構成とステータスが表示されます。ここでポートを構成することもできます。テーブルには、それぞれに1つの行があります

選択したスイッチのいくつかの列のポート：次のとおりです。

図4-3-1および図4-3-2の[PortConfiguration]画面が表示されます。

図4-3-1ポート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
•ポート選択	このドロップダウンリストからポート番号を選択します。
•有効	ポートステート操作を示します。考えられる状態は次のとおりです。 有効-ポートを手動で起動します。 無効-ポートを手動でシャットダウンします。

•速度	特定のスイッチポートで使用可能なリンク速度を選択します。メニューバーをに描画します モードを選択します。 ■ 自動-オートネゴシエーションを設定します。 ■ Auto-10M -10Mオートネゴシエーションを設定します。 ■ Auto-100M -100M自動ネゴシエーションを設定します。 ■ Auto-1000M -1000Mオートネゴシエーションを設定します。 ■ 自動-10 / 100M-セットアップ10 / 100Mオートネゴシエーション。 ■ 10M -10Mフォースモードを設定します。 ■ 100M -100M強制モードを設定します。 ■ 1000M -1000M強制モードを設定します。
•デュプレックス	指定されたスイッチポートで使用可能なリンクデュプレックスを選択します。メニューバーをに描画します モードを選択します。 ■ 自動-オートネゴシエーションを設定します。 ■ Full -Forceは全二重モードを設定します。 ■ Half -Forceは半二重モードを設定します。
•フロー制御	ポートに自動速度が選択されている場合、このセクションはフロー制御を示します リンクパートナーにアダプタイズされる機能。固定速度設定が 選択された、それが使用されます。現在の受信列は、一時停止するかどうかを示します ポートのフレームは順守されます。現在のTx列は、一時停止するかどうかを示します ポート上のフレームが送信されます。RxとTxの設定は、 前回のオートネゴシエーションの結果。フローを使用するように構成された列を確認してください コントロール。この設定は、構成済みリンク速度の設定に関連しています。

ボタン

: クリックして変更を適用します。

図4-3-2ポート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
•ポート	これは、この行の論理ポート番号です
•説明	クリック ポート名を示す
•状態を有効にする	現在のポート状態を表示します
•リンクステータス	現在のリンクステータスを表示します
•速度	ポートの現在の速度ステータスを表示します
•デュプレックス	ポートの現在のデュプレックスステータスを表示します
•フロー制御	ポートの現在のフロー制御構成を表示します
構成	
•フロー制御ステータス	ポートの現在のフロー制御ステータスを表示します

4.3.2ポートカウンター

このページでは、すべてのスイッチポートのトラフィックとトランクの統計情報の概要を説明します。図4-3-3の[PortStatistics]画面
図4-3-4、図4-3-5、および図4-3-6が表示されます。

図4-3-3ポートMIBカウンター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
--------	----

- ポート

このドロップダウンリストからポート番号を選択します。
- モード

ポートカウンターモードを選択します。
- オプション：

••

すべて

••

インターフェース

••

エーテルリンク

••

RMON

図4-3-4インターフェイスカウンターのスクリーンショット

オブジェクト	説明
•受け取ったオクテット	フレーミングを含む、インターフェイスで受信されたオクテットの総数文字。
•ユニキャストを受信しました パケット	上位層プロトコルに配信されたサブネットワークユニキャストパケットの数。
•不明な受信 ユニキャストパケット	インターフェイスを介して受信されたパケットの数。 不明またはサポートされていないプロトコル。
•受け取った破棄 パケット	破棄されるように選択されたインバウンドパケットの数 上位層への配信を妨げるエラーは検出されませんでした プロトコル。このようなパケットを破棄する理由の1つとして、解放することが考えられます。 バッファスペース。
•オクテットの送信	フレーミングを含む、インターフェイスから送信されたオクテットの総数文字。
•ユニキャストを送信する パケット	上位プロトコルが要求したパケットの総数が送信されます 破棄されたアドレスや送信されなかったアドレスを含む、サブネットワークユニキャストアドレスへ。
•不明な送信 ユニキャストパケット	上位プロトコルが要求したパケットの総数が送信されます 破棄されたアドレスや送信されなかったアドレスを含む、サブネットワークユニキャストアドレスへ。
•送信破棄	ないにもかかわらず破棄されるように選択されたインバウンドパケットの数

パケット	上位層への配信を防ぐためにエラーが検出されました プロトコル。このようなパケットを破棄する理由の1つとして、解放することが考えられます。 バッファスペース。
•受信したマルチキャスト パケット	このサブレイヤーによって上位（サブ）レイヤーに配信されるパケットの数は次のとおりです。 このサブレイヤーのマルチキャストアドレスにアドレス指定されます。

93

•受信したブロードキャスト パケット	このサブレイヤーによって上位（サブ）レイヤーに配信されるパケットの数。 このサブレイヤーのブロードキャストアドレスにアドレス指定されます。
•マルチキャストの送信 パケット	上位プロトコルが要求したパケットの総数が送信されます そして、このサブレイヤーのマルチキャストアドレスにアドレス指定されます。 破棄されたか、送信されませんでした。
•ブロードキャストを送信する パケット	上位レベルのプロトコルが要求したパケットの総数は、 このサブレイヤーのブロードキャストアドレスにアドレス指定されました。 破棄または送信されません。

図4-3-5イーサネットリンクカウンターのスクリーンショット

オブジェクト	説明
•アライメントエラー	アラインメントエラー（同期されていないデータパケット）の数。
•FCSエラー	特定のインターフェイスで受信されたフレームの数で、 長さはオクテットですが、FCSチェックに合格しません。このカウントには含まれていません frame-toolongまたはframe-too-shortエラーで受信されたフレーム。
•単一の衝突 フレーム	送信が禁止されている、正常に送信されたフレームの数 ちょうど1回の衝突で。
•複数の衝突 フレーム	によって送信が禁止されている、正常に送信されたフレームの数 複数の衝突。
•延期 トランスミッション	特定のインターフェイスで最初の送信が試行されたフレームの数 メディアがビジーだったために遅れています。
•後期衝突	512ビット時間以降に衝突が検出された回数 パケットの送信。
•過度の衝突	特定のインターフェイスでの送信が原因で失敗したフレームの数

	全二重モードで動作します。
・フレームが長すぎます	最大値を超える特定のインターフェイスで受信されたフレームの数 許容されるフレームサイズ。
・シンボルエラー	受信および送信されたシンボルエラーの数
・不明なコントロール オペコード	受信したコントロールの不明なオペコードの数
・一時停止フレーム内	受信した一時停止フレームの数
・フレームを一時停止します	送信された一時停止フレームの数

図4-3-6RMONカウンターのスクリーンショット

オブジェクト	説明
・ドロップイベント	不足のためにパケットがドロップされたイベントの総数 リソース。
・オクテット	インターフェイスで送受信されたオクテットの総数。 フレーミング文字。
・パケット	インターフェイスで送受信されたパケットの総数。
・ブロードキャストパケット	ブロードキャストに向けられた、受信された良好なフレームの総数。 住所。これにはマルチキャストパケットが含まれないことに注意してください。

・マルチキャストパケット	このマルチキャストに送信された、受信した正常なフレームの総数。 住所。
・CRC /アライメント エラー	CRC /アライメントエラー（FCSまたはアライメントエラー）の数。
・アンダーサイズパケット	長さが64オクテット未満の受信フレームの総数（除く フレーミングビット（ただしFCSオクテットを含む）およびその他の点では整形式でした。
・特大パケット	1518オクテットより長い受信フレームの総数（除く フレーミングビット（ただしFCSオクテットを含む）およびその他の点では整形式でした。
・フラグメント	長さが64オクテット未満の受信フレームの総数 （フレーミングビットを除くが、FCSオクテットを含む）FCSまたは アライメントエラー。
・ジャバ	1518オクテットより長い受信フレームの総数 （フレーミングビットを除くが、FCSオクテットを含む）、FCSまたは アライメントエラー。
・衝突	このイーサネットセグメントでの衝突の総数の最良の見積もり。
・64バイトフレーム	送受信されたフレーム（不良パケットを含む）の総数 長さは64オクテットでした（フレーミングビットを除くが、FCSオクテットを含む）。
・65～127バイトのフレーム	受信および送信されたフレーム（不良パケットを含む）の総数
128～255バイトのフレーム	オクテットの数指定された範囲内にある場合（フレーミングを除く）
256～511バイトのフレーム	ビット（ただしFCSオクテットを含む）。
512-1023バイトフレーム	
1024-1518バイト フレーム	

[帯域幅使用率]ページには、ポートで使用されている使用可能な帯域幅の合計のパーセンテージが表示されます。帯域幅使用統計は、折れ線グラフを使用して表示できます。[図4-3-7の](#)[帯域幅使用率]画面が表示されます。

ポート使用率を表示するには、[ポート管理]フォルダーをクリックしてから、[帯域幅使用率]リンクをクリックします。

図4-3-7ポート帯域幅使用率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
更新期間	これは、最後の更新と次の更新の間の期間間隔を示しています。 オプション： ■2秒 ■5秒 ■10秒
IFG	ユーザーがこの機能を有効または無効にできるようにする

4.3.4ポートミラーリング

このページでポートミラーリングを構成します。この機能は、各着信のコピーを転送するネットワークトラフィックの監視を提供します
または、ネットワークスイッチの1つのポートから、パケットを調査できる別のポートへの発信パケット。それはマネージャーがすることを可能にします
スイッチのパフォーマンスを綿密に追跡し、必要に応じて変更します。
•ネットワークの問題をデバッグするために、選択したトラフィックをミラーポートにコピーまたはミラーリングして、フレームアナライザーを使用できます。
フレームフローを分析するために取り付けられています。

- ・マネージドスイッチは、任意のポートからモニターポートへのトラフィックを目立たないようにミラーリングできます。その後、プロトコルを添付できます
- ・トラフィック分析を実行し、接続の整合性を検証するために、このポートへのアナライザーまたはRMONプローブ。

図4-3-8ポートミラーアプリケーション

ミラーポートにコピーされるトラフィックは、次のように選択されます。

- ・特定のポートで受信されたすべてのフレーム（入力またはソースミラーリングとも呼ばれます）。
- ・特定のポートで送信されるすべてのフレーム（出力または宛先ミラーリングとも呼ばれます）。

ミラーポート構成

図4-3-9および図4-3-10の[ポートミラー設定]画面が表示されます。

図4-3-9ポートミラーリング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
・セッションID	ポートミラーセッションIDを設定します。 可能なIDは次のとおりです：1から4。
・セッション状態の監視	ポートミラーリング機能を有効または無効にします。
・宛先ポート	宛先ポートをミラーリングするポートを選択します。
・許可-入力	ソース（rx）または宛先（tx）ミラーリングが有効になっているポートからのフレームはこのポートにミラーリングされます。
・スニファTXポート	これらのポートから送信されたフレームは、ミラーリングポートにミラーリングされます。受信したフレームミラーリングされていません。
・スニファRXポート	これらのポートで受信されたフレームは、ミラーリングポートにミラーリングされます。

送信されたフレームはミラーリングされません。

ボタン

: クリックして変更を適用します。

図4-3-10ミラーリング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
・セッションID	セッションIDを表示する
・宛先ポート	これはミラーリングポートエントリです
・入力状態	入力状態を表示する
・送信元TXポート	現在のTXポートを表示します
・ソースRXポート	現在のRXポートを表示する

4.3.5ジャンボフレーム

このページでは、スイッチポートに許可される**最大フレームサイズ**を選択できます。[図4-3-11](#)のジャンボフレーム画面
そして[図は4-3-12](#)表示されます。

図4-3-11ジャンボフレーム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
・ジャンボフレーム (バイト)	FCSを含め、スイッチポートに許可される最大フレームサイズを入力します。 許可される範囲は64バイトから9216バイトです。

ボタン

: クリックして変更を適用します。

図4-3-12ジャンボフレーム情報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
・ジャンボ	現在の最大フレームサイズを表示します

4.3.6ポートエラー無効構成

このページでは、ポートエラー無効化機能を設定します。図4-3-13および図の[PortError DisableConfiguration]画面4-3-14が表示されます。

図4-3-13エラー無効化リカバリ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
・回復間隔	ポートが発生した場合にポートが無効に保たれる期間（秒単位） エラーが検出されました（そして、ポートアクションによってポートがシャットダウンされます）。
・BPDUガード	ポートエラー無効化機能を有効または無効にして、BPDUガードでステータスを確認します。
・セルフループ	ポートエラー無効化機能を有効または無効にして、セルフループでステータスを確認します。
・放送洪水	ポートエラー無効化機能を有効または無効にして、ブロードキャストでステータスを確認します 洪水。
・不明なマルチキャスト 洪水	ポートエラー無効化機能を有効または無効にして、不明な状態でステータスを確認します マルチキャストフラッド。
・ユニキャストフラッド	ポートエラー無効化機能を有効または無効にして、ユニキャストフラッドによるステータスを確認します。
・ACL	ポートエラー無効化機能を有効または無効にして、ACLでステータスを確認します。
・ポートセキュリティ 違反	ポートエラー無効機能を有効または無効にして、ポートセキュリティでステータスを確認します 違反。
・DHCPレート制限	DHCPレートでステータスを確認するには、ポートエラー無効化機能を有効または無効にします 制限
・ARPレート制限	ポートエラー無効化機能を有効または無効にして、ARPレート制限でステータスを確認します

ボタン

: クリックして変更を適用します。

図4-3-14エラー無効化情報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
・回復間隔	現在の回復間隔時間を表示します
・BPDUガード	現在のBPDUガードステータスを表示します
・セルフループ	現在のセルフループステータスを表示します

・ 放送洪水	現在のブロードキャストフラッドステータスを表示します
・ 不明なマルチキャスト	現在の不明なマルチキャストフラッドステータスを表示します
・ 洪水	
・ ユニキャストフラッド	現在のユニキャストフラッドステータスを表示します
・ ACL	現在のACLステータスを表示します
・ ポートセキュリティ違反	現在のポートセキュリティ違反ステータスを表示します
・ DHCPレート制限	現在のDHCPレート制限ステータスを表示します
・ ARPレート制限	現在のARPレート制限ステータスを表示します

4.3.7ポートエラーが無効

このページでは、ポートをエラー無効化に移行する無効化と回復オプションを提供します。
ポートは、BPDUガード、ループバック、UDLDなどの一部のプロトコルによって無効にされました。のポートエラー無効化画面
[図4-3-15](#)が表示されます。

図4-3-15ポートエラー無効化のスクリーンショット

表示されるカウンターは次のとおりです。

オブジェクト	説明
・ ポート名	エラー無効化のためにポートを表示します
・ エラー無効化理由	ポートのエラー無効化理由を表示します
・ 残り時間（秒）	残り時間を表示する

4.3.8保護されたポート

概要概要

スイッチポートが**保護されたグループ**（**プライベートVLAN**とも呼ばれる）のメンバーになるように構成されている場合、そのグループ内の保護されたポートを防ぐことができます。このセクションでは、2つのアプリケーション例を示します。

- ・ISPに接続している顧客は、保護されたグループのメンバーになることができますが、通信することはできません。そのVLAN内で互いに。
- ・非武装地帯（DMZ）内のWebサーバーのファーム内のサーバーは、外部との通信が許可され、内部セグメントにデータベースサーバーがありますが、相互に通信することはできません

保護されたポートグループを適用するには、最初に管理対象スイッチを標準VLAN操作用に構成する必要があります。のポート保護されたポートグループは、次の2つのグループのいずれかに分類されます。

■ **無差別（保護されていない）ポート**

- トラフィックをプライベートVLAN内のすべてのポートに転送できるポート
- プライベートVLAN内のすべてのポートからトラフィックを受信できるポート

■ **分離された（保護された）ポート**

- トラフィックをプライベートVLAN内の無差別ポートにのみ転送できるポート
- プライベートVLAN内の無差別ポートからのみトラフィックを受信できるポート

無差別で分離されたポートの構成は、すべてのプライベートVLANに適用されます。トラフィックが無差別ポートに着信したときプライベートVLANでは、VLANテーブルのVLANマスクが適用されます。トラフィックが分離されたポートに着信すると、プライベートVLAN VLANテーブルのVLANマスクに加えてマスクが適用されます。これにより、転送を実行できるポートが減少します。プライベートVLAN内の無差別ポートのみ。

ポート設定は、ページヘッダーに反映されているように、現在のユニットに関連しています。で、ポートアイソレーションの設定画面を[図](#)

図4-3-16保護ポート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
・ポートリスト	このドロップダウンリストからポート番号を選択します。
・ポートタイプ	保護されたポートタイプを表示します。 -保護：1つの無差別ポートを含む単一のスタンドアロンVLAN および1つ以上の分離（またはホスト）ポート。このVLANは、 分離されたポートと1つの無差別ポート。 -保護されていない：無差別ポートはすべてのインターフェイスと通信できます プライベートVLAN内。これがデフォルト設定です。

ボタン

：クリックして変更を適用します。

図4-3-17ポート分離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
・保護されたポート	現在保護されているポートを表示する
・保護されていないポート	現在保護されていないポートを表示する

4.3.9 EEE

EEEとは

EEEは、トラフィック使用率が低いかまったくない場合に電力使用量を削減する省電力オプションです。EEEは電力を供給することで機能します。トラフィックがないときに回線をダウンします。ポートが送信するデータを取得すると、すべての回路の電源がオンになります。にかかる時間回路の電源投入はウェイクアップ時間と呼ばれます。デフォルトのウェイクアップ時間は、1ギガビットリンクの場合は17 us、その他のリンク速度の場合は30usです。EEEデバイスは、受信と送信の両方を確実にするために、ウェイクアップ時間の値について合意する必要があります。トラフィックが送信されると、デバイスのすべての回路の電源がオンになります。デバイスは、を使用してウェイクアップ時間情報を交換できます。LLDPプロトコル。EEEは、ポートが1Gまたは100Mビット全二重のいずれかにネゴシエーションされる自動ネゴシエーションモードのポートで機能します。モード。EEEに対応していないポートの場合、対応するEEEチェックボックスはグレー表示されているため、有効にすることはできません。EEEfor。EEEポート設定は、ページヘッダーに反映されているように、現在の単位に関連しています。

電力を節約するためにポートの電源を切ると、ポートの電源を再び入れるまで、発信トラフィックはバッファに保存されます。なぜならポートを上下に切り替えるにはオーバーヘッドがあります。トラフィックが大きくなるまでバッファリングできれば、より多くの電力を節約できます。トラフィックのバーストを送信できます。トラフィックをバッファリングすると、トラフィックにある程度の遅延が生じます。
[図4-3-18](#)および[図4-3-19](#)の[EEEポート設定]画面が表示されます。

図4-3-18EEEポート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
•ポート	このドロップダウンリストからポート番号を選択します
•有効にする	EEE機能を有効または無効にします

ボタン

: クリックして変更を適用します。

図4-3-19EEEイネーブル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
•ポート	論理ポートのスイッチポート番号
•EEE状態	現在のEEE状態を表示します

4.3.10SFPモジュール情報

マネージドスイッチは、**デジタル診断モニタリング（DDM）**機能を備えたSFPモジュールをサポートしています。この機能もデジタル光学モニタリング（DOM）として知られています。SFPを介してSFPモジュールの物理的または動作状態を確認できますモジュール情報ページ。このページには、トランシーバーのタイプ、速度、波長、光などの動作ステータスが表示されますリアルタイムでの出力電力、光入力電力、温度、レーザーバイアス電流およびトランシーバー供給電圧。使用することもできますポート番号のハイパーリンク。特定のインターフェイスの統計を確認します。

4.3.10.1SFPモジュールのステータス

図4-3-20および図4-3-21のSFPモジュールステータス画面が表示されます。

図4-3-20サンプルスイッチを使用したポート選択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
•ポート	このドロップダウンリストからポート番号を選択します

図4-3-21ファイバーポート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
• OE-現在	現在のSFPOEの存在を表示します
• LOS	現在のSFPLOSを表示します

4.3.10.1SFPモジュールの詳細ステータス

図4-3-22のSFPモジュール詳細ステータス画面が表示されます。

図4-3-22サンプルスイッチを使用したSFPモジュールの詳細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
•ポート	同じ行に含まれる設定の論理ポート
•温度	現在のSFP温度を表示します
•電圧	現在のSFP電圧を表示します
•現在	現在のSFP電流を表示します
•出力電力	現在のSFP出力電力を表示します
•入力電力	現在のSFP入力電力を表示します
•送信障害	現在のSFP送信障害を表示する
•信号の喪失	現在のSFP信号損失を表示します。
•レートレディ	現在のSFPレートレディを表示します。

4.4リンクアグリゲーション

ポートアグリゲーションは、ポートのグループをリンクして単一のリンクアグリゲーショングループ（LAG）を形成することにより、ポートの使用を最適化します。ポート集約により、デバイス間の帯域幅が増加し、ポートの柔軟性が向上し、リンクの冗長性が提供されます。

各LAGは同じ速度のポートで構成され、全二重動作に設定されています。LAGのポートは、さまざまなメディアタイプにすることができます（UTP/ファイバー、または異なるファイバータイプ）同じ速度で動作する場合。

集約リンクは、手動（**ポートトランク**）またはリンク集約制御プロトコルを有効にすることで自動的に割り当てることができます（**LACP**）関連リンク。

集約リンクは、システムによって単一の論理ポートとして扱われます。具体的には、集約リンクには同様のポート属性がありますオートネゴシエーション、速度、スープレックス設定などを含む、集約されていないポートへ。

デバイスは、次の集約リンクをサポートしています。

- **静的LAG（ポートトランク）** →選択された集約ポートを強制的にトランクグループにします。

- **リンクアグリゲーション制御プロトコル (LACP)** LAG-LACP LAGは、他のLACPとアグリゲーションポートリンクをネゴシエートします別のデバイスにあるポート。他のデバイスポートもLACPポートである場合、デバイスはLAGを確立します

それらの間の。

図4-4-1リンクアグリゲーション

リンクアグリゲーション制御プロトコル (LACP) は、パートナーとの間で情報を交換するための標準化の手段を提供します

高速冗長リンクを必要とするシステム。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つにグループ化できます

専用接続。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操作には全二重が必要です

モード。詳細については、IEEE802.3ad規格を参照してください。

ポートリンクアグリゲーションを使用して、ネットワーク接続の帯域幅を増やしたり、障害を確実に回復したりできます。リンク

集約により、最大8つの連続するポートを、任意の2つのスイッチまたはその他の間の単一の専用接続にグループ化できます。

レイヤー2スイッチ。ただし、デバイス間で物理的な接続を行う前に、リンクアグリゲーション構成を使用してください

メニューを使用して、両端のデバイスのリンクアグリゲーションを指定します。ポートリンクアグリゲーションを使用する場合は、次の点に注意してください。

- リンクアグリゲーションで使用されるポートは、すべて同じメディアタイプ（RJ45、100 Mbpsファイバー）である必要があります。
 - 同じリンクアグリゲーションに割り当てることができるポートには、他にも特定の制限があります（以下を参照）。
 - ポートは、1つのリンクアグリゲーションにのみ割り当てることができます。
 - 接続の両端のポートは、リンクアグリゲーションポートとして構成する必要があります。
 - リンクアグリゲーションのどのポートも、ミラー送信元ポートまたはミラーターゲットポートとして設定できません。
 - リンクアグリゲーション内のすべてのポートは、VLANとの間で移動したり、VLANから追加または削除したりするときに、全体として処理する必要があります。
 - スパンニングツリープロトコルは、リンクアグリゲーション内のすべてのポートを全体として扱います。
 - データループの作成を回避するために、スイッチ間にケーブルを接続する前にリンクアグリゲーションを有効にします。
 - ポートリンクアグリゲーションを削除する前に、すべてのリンクアグリゲーションポートケーブルを切断するか、リンクアグリゲーションポートを無効にします。
- データループの作成は避けてください。

最大8つのポートを同時に集約できます。マネージドスイッチは、ギガビットイーサネットポート（最大8つ）をサポートします

グループ)。グループがLACP静的リンクアグリゲーショングループとして定義されている場合、選択された追加のポートはすべてスタンバイ状態になります。他のポートの1つに障害が発生した場合の冗長性のためのモード。グループがローカル静的リンクアグリゲーショングループとして定義されている場合、

ポートの数は、グループメンバーのポートと同じである必要があります。

リンクアグリゲーションメニューを使用して、トランク機能を表示または構成します。このセクションには、次の項目があります。

■	LAG設定	負荷分散アルゴリズムの構成設定を構成します
■	LAG管理	LAG構成設定を構成します
■	LAGポート設定	LAGポート設定を構成します
■	LACP設定	LACP優先度設定を構成します
■	LACPポート設定	LACP構成設定を構成する
■	LAGステータス	LAGステータス/ LACP情報を表示する

4.4.1LAG設定

このページでは、負荷分散アルゴリズムの構成設定を構成できます。図4-4-2および図のLAG設定画面4-4-3が表示されます。

図4-4-2LAG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
・負荷分散	負荷分散アルゴリズムモードを選択します。
アルゴリズム	■MACアドレス：MACアドレスを使用して、 フレーム。 ■IP / MACアドレス：IPおよびMACアドレスを使用して、 フレームのポート。

ボタン

：クリックして変更を適用します。

図4-4-3LAG情報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
・負荷分散 アルゴリズム	現在の負荷分散アルゴリズムを表示する

4.4.2LAG管理

このページは、LAG管理を構成するために使用されます。図4-4-4および図4-4-5のLAG管理画面が表示されます。

図4-4-4LAG管理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
・LAG	このドロップダウンリストからLAG番号を選択します
・名前	各LAG名を示します
・タイプ	トランクタイプを示します 静的：集約された選択されたポートを強制的にトランクグループにします。 LACP：LACP LAGは、アグリゲーションポートリンクを他のLACPポートとネゴシエートします別のデバイスで。他のデバイスポートもLACPポートである場合、デバイスそれらの間にLAGを確立します。
・ポート	このドロップダウンリストからポート番号を選択して、リンクアグリゲーションを確立します

図4-4-5LAG管理情報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
・LAG	同じ行に含まれる設定のLAG
・名前	現在の名前を表示する
・タイプ	現在のタイプを表示します
・リンク状態	リンク状態を表示する
・アクティブメンバー	アクティブなメンバーを表示します
・スタンバイメンバー	スタンバイメンバーを表示する
・変更	クリック LAG構成を変更するには

4.4.3LAGポート設定

このページでは、各LAGの構成を設定できます。図4-4-6および図4-4-7のLAGポート設定画面が表示されます。

図4-4-6LAGポート設定情報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
・LAGSelect	このドロップダウンリストからLAG番号を選択します。
・有効にする	LAG状態の操作を示します。考えられる状態は次のとおりです。 有効-LAGを手動で起動します。 無効-LAGを手動でシャットダウンします。
・速度	特定のスイッチポートで使用可能なリンク速度を選択します。メニューバーをに描画します

- モードを選択します。
- **自動** -自動ネゴシエーションを設定します。
 - **Auto -10M** -10Mオートネゴシエーションを設定します。
 - **Auto -100M** -100Mオートネゴシエーションを設定します。

- **自動1000M** - 1000Mオートネゴシエーションに設定。
- **Auto -10/ 100M** - 10 / 100Mオートネゴシエーションを設定します。
- **10M** - 10Mフォースモードに設定。
- **100M** - 100Mフォースモードに設定。
- **1000M** - 1000Mフォースモードに設定。

・フロー制御

ポートに自動速度が選択されている場合、このセクションはフロー制御を示します
リンクパートナーにアダプタイズされる機能。固定速度設定が
選択された、それが使用されます。現在のRx列は、一時停止するかどうかを示します
ポートのフレームは順守されます。現在のTx列は、一時停止するかどうかを示します
ポート上のフレームが送信されます。RxとTxの設定は、
前回のオートネゴシエーションの結果。フローを使用するように構成された列を確認してください
コントロール。この設定は、構成済みリンク速度の設定に関連しています。

ボタン

: クリックして変更を適用します。

図4-4-7LAGポート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
・LAG	同じ行に含まれる設定のLAG
・説明	現在の説明を表示する
・ポートタイプ	現在のポートタイプを表示します
・状態を有効にする	現在の有効状態を表示します
・速度	現在の速度を表示する

・デブプレックス	現在のデブプレックスモードを表示します
・フロー制御構成	現在のフロー制御構成を表示します
・フロー制御ステータス	現在のフロー制御ステータスを表示します

4.4.4LACP設定

このページは、LACPシステムの優先順位設定を構成するために使用されます。図4-4-8および図4-4-9のLACP設定画面
現れる。

図4-4-8LACP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
・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。 値が最も小さいマネージドスイッチの優先度が最も高く、 トランクグループのアクティブなLACPピアとして選択されています。

ボタン

：クリックして変更を適用します。

図4-4-9LACP情報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
・システムの優先順位	現在のシステム優先度を表示します。

4.4.5LACPポート設定

このページは、LACPポート設定を構成するために使用されます。図4-4-10および図4-4-11のLACPポート設定画面が表示されます。

図4-4-10LACPポート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
•ポート選択	このドロップダウンリストからポート番号を選択して、LACPポート設定を設定します。
•優先度	優先度は、ポートの優先度を制御します。 LACPパートナーが、このデバイスでサポートされているよりも大きなグループを形成したい場合は、次に、このパラメータは、アクティブになるポートとアクティブになるポートを制御します バックアップの役割で。 数値が小さいほど、優先度が高くなります。
•タイムアウト	タイムアウトは、BPDUS送信間の期間を制御します。 ShortはLACPパケットを毎秒送信し、Longは30を待機します LACPパケットを送信する数秒前。

ボタン

: クリックして変更を適用します。

図4-4-11LACPポート情報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
•ポート名	論理ポートのスイッチポート番号

・優先度	現在のLACP優先度パラメータを表示します
・タイムアウト	現在のタイムアウトパラメータを表示する

4.4.6LAGステータス

このページにはLAGステータスが表示されます。図4-4-12および図4-4-13のLAGステータス画面が表示されます。

図4-4-12LAG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
・LAG	現在のトランクエントリを表示します
・名前	現在のLAG名を表示します
・タイプ	現在のトランクタイプを表示します
・リンク状態	現在のリンク状態を表示します
・アクティブメンバー	現在アクティブなメンバーを表示します
・スタンバイメンバー	現在のスタンバイメンバーを表示します

図4-4-13LACP情報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
• トランク	現在のトランクIDを表示します
• ポート	現在のポート番号を表示します
• PartnerSysId	リンクパートナーのシステムID。このフィールドは、ポートが受信すると更新されます リンクパートナーからのLACPPDU
• PnKey	パートナーのポートキー。このフィールドは、ポートがLACPを受信すると更新されます リンクパートナーからのPDU
• AtKey	アクターのポートキー。キーはトランクIDと同じになるように設計されています。
• SelD	ポートのLACP選択ロジックステータス <ul style="list-style-type: none">■ 「S」は選択されたことを意味します■ 「U」は未選択を意味します■ 「D」はスタンバイを意味します
• マルチプレクサ	ポートのLACPマルチプレクサステートマシンのステータス <ul style="list-style-type: none">■ 「DETACH」は、ポートがデタッチ状態にあることを意味します■ 「WAIT」は待機状態を意味します■ 「ATTACH」はアタッチ状態を意味します■ 「CLLCT」は状態の収集を意味します■ 「DSTRBT」は状態の配布を意味します
• 受信	LACPはポートのステートマシンステータスを受信します <ul style="list-style-type: none">■ 「INIT」は、ポートが初期化状態であることを意味します■ 「PORTds」は、ポートが無効な状態を意味します■ 「EXPR」は期限切れ状態を意味します■ 「LACPds」は、LACPが無効な状態を意味します■ 「DFLT」はデフォルト状態を意味します■ 「CRRNT」は現在の状態を意味します
• PrdTx	ポートのLACP定期送信ステートマシンステータス <ul style="list-style-type: none">■ 「PRDなし」は、ポートが定期的な状態にないことを意味します■ 「FstPRD」は高速周期状態を意味します■ 「SlwPRD」は遅い周期状態を意味します■ 「PrdTX」は定期的なTX状態を意味します
• AtState	LACPPDU記述のアクター状態フィールド。 左から右へのフィールドは、「LACP_Activity」、「LACP_Timeout」、

「集約」、「同期」、「収集」、「配布」、「デフォルト」、および「期限切れ」。	
内容は真または偽である可能性があります。内容が偽の場合、Webには「_」が表示されます。もし内容が真実である場合、ウェブには「A」、「T」、「G」、「S」、「C」、「D」、「F」、「E」が表示されます。それぞれのコンテンツ。	
• PnState	LACPPDU記述のパートナー状態フィールド。 左から右へのフィールドは、「LACP_Activity」、「LACP_Timeout」、 「集約」、「同期」、「収集」、「配布」、「デフォルト」、および「期限切れ」。 内容は真または偽である可能性があります。内容が間違っている場合、ウェブは表示されます 「_」; 内容が正しい場合、Webには「A」、「T」、「G」、「S」、「C」、「D」、「F」、「E」が表示されます。 それぞれのコンテンツに対して。

4.5 VLAN

4.5.1VLANの概要

仮想ローカルエリアネットワーク（VLAN）は、物理的ではなく論理的スキームに従って構成されたネットワークポロジです。

レイアウト。VLANを使用して、LANセグメントの任意のコレクションを単一のように見える自律ユーザーグループに結合できます。

LAN。VLANはまた、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て、パケットが間でのみ転送されるようにします。

VLAN内のポート。通常、VLANは特定のサブネットに対応しますが、必ずしもそうとは限りません。

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によってグループ化されたエンドノードのコレクションです。頻繁に通信するエンドノード

ネットワーク上の物理的な場所に関係なく、相互に同じVLANに割り当てられます。論理的には、VLANは

ブロードキャストパケットは、ブロードキャストドメインが存在するVLANのメンバーにのみ転送されるため、ブロードキャストドメインと同等です。

放送が開始されました。

- 1.1。 エンドノードを一意に識別し、これらのノードにVLANを割り当てるためにどのような基準が使用されてもメンバーシップ、パケットは、ネットワークデバイスがルーティングを実行しないとVLANを通過できませんVLAN間の機能。
- 2.2。 マネージドスイッチはIEEE802.1QVLANをサポートします。ポートタグ解除機能を使用できますパケットヘッダーから802.1タグを削除して、次のデバイスとの互換性を維持します。タグを認識しません。

マネージドスイッチのデフォルトは、すべてのポートをという名前の単一の802.1QVLANに割り当てることです。

DEFAULT_VLAN。新しいVLANが作成されると、新しいVLANに割り当てられるメンバーポートは次のようになります。

DEFAULT_VLANポートメンバーリストから削除されました。**DEFAULT_VLAN**のVID = 1です。

このセクションには、次の項目があります。

■ 管理VLAN	管理VLANを構成します
■ VLANを作成する	VLANグループを作成します
■ インターフェイス設定	VLANポートでモードとPVIDを構成します
■ VLANへのポート	VLANメンバーシップを構成します
■ ポートVLANメンバーシップ	VLANメンバーシップを表示します
■ プロトコルVLANグループ設定	プロトコルVLANグループを構成します
■ プロトコルVLANポート設定	プロトコルVLANポート設定を構成します
■ GVRP設定	GVRPグローバル設定を構成します
■ GVRPポート設定	GVRPポート設定を構成します
■ GVRP VLAN	GVRPVLANデータベースを表示します
■ GVRP統計	GVRPポート統計を表示します

4.5.2 IEEE 802.1Q VLAN

大規模なネットワークでは、ルーターを使用して、各サブネットのブロードキャストトラフィックを個別のドメインに分離します。このマネージドスイッチVLANを使用して、ネットワークノードの任意のグループを個別のブロードキャストドメインに編成することにより、レイヤ2で同様のサービスを提供します。

VLANは、ブロードキャストトラフィックを発信元グループに制限し、大規模ネットワークでのブロードキャストストームを排除できます。これもまたより安全でクリーンなネットワーク環境を提供します。

IEEE 802.1Q VLANは、ネットワーク内のどこにでも配置できるポートのグループですが、それらが属しているかのように通信します。同じ物理セグメントに。

VLANは、デバイスを変更せずに新しいVLANに移動できるようにすることで、ネットワーク管理を簡素化するのに役立ちます。

物理的な接続。VLANは、部門グループ（マーケティングや研究開発など）、使用グループを反映するように簡単に編成できます。

（電子メールなど）、またはマルチキャストグループ（ビデオ会議などのマルチメディアアプリケーションに使用されます）。

VLANは、ブロードキャストトラフィックを削減することでネットワーク効率を高め、ネットワークを変更することなく変更できるようにします。

IPアドレスまたはIPサブネットを更新します。トラフィックは通過する必要があるため、VLANは本質的に高レベルのネットワークセキュリティを提供します。別のVLANに到達するように構成されたレイヤー3リンク。

このマネージドスイッチは、次のVLAN機能をサポートしています。

- IEEE802.1Q標準に基づく最大255のVLAN
- ポートがオーバーラップし、ポートが複数のVLANに参加できるようにする
- エンドステーションは複数のVLANに属することができます
- VLAN対応デバイスとVLAN非対応デバイス間でのトラフィックの受け渡し

■ IEEE802.1Q標準

IEEE 802.1Q（タグ付き） VLANがスイッチに実装されています。802.1Q VLANにはタグ付けが必要です。これにより、VLANはネットワーク全体（ネットワーク上のすべてのスイッチがIEEE 802.1Qに準拠していると想定）。

VLANを使用すると、ブロードキャストドメインのサイズを縮小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）に転送されます。これにはブロードキャストが含まれます。不明なソースからのマルチキャストおよびユニキャストパケット。

VLANは、ネットワークに一定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、ステーション間でのみパケットを配信します。VLANのメンバーです。任意のポートは、**タグ付け**または**タグ付け解除**のいずれかとして構成できます。

- IEEE802.1QVLANのタグ付け解除機能により、VLANはVLANタグを認識しないレガシースイッチと連携できます。パケットヘッダー内。

- タグ付け機能により、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ことができます。スパンニングツリーをすべてのポートで有効にして、正常に動作できるようにします。

いくつかの関連用語：

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

■ 802.1QVLANタグ

次の図は、802.1QVLANタグを示しています。送信元MACアドレスの後に4つの追加オクテットが挿入されています。彼らの

存在は、**EtherType**フィールドの**0x8100**の値で示されます。パケットのEtherTypeフィールドが0x8100に等しい場合、

パケットはIEEE802.1Q/802.1pタグを伝送します。タグは次の2つのオクテットに含まれ、3ビットのユーザー優先度で構成されます。

1ビットのCanonicalFormat Identifier（CFI-トークンリングパケットをカプセル化してイーサネット経由で伝送できるようにするために使用）

バックボーン）、および12ビットの**VLAN ID（VID）**。ユーザー優先度の3ビットは802.1pによって使用されます。VIDはVLAN識別子であり、802.1Q標準で使用されます。VIDは12ビット長であるため、4094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。元々含まれていたすべての情報パケット内に保持されます。

		ユーザー優先度		CFI	VLAN ID (VID)	
		3ビット		1ビット	12ビット	
TPID (タグプロトコル識別子) TCI (タグ制御情報)						
		2バイト		2バイト		
前文	先	ソース	VLANタグ	イーサネット	データ	FCS
	住所	住所		タイプ		
	6バイト	6バイト		4バイト		

EtherTypeとVLANIDは、MAC送信元アドレスの後、元のEther Type / LengthまたはLogicalの前に挿入されます。

リンク制御。パケットが元の値より少し長くなっているため、巡回冗長検査（CRC）は再計算されました。

IEEE802.1Qタグの追加

目的地。Addr。	Src。Addr。	長さ/ E。タイプ	データ	古いCRC	オリジナルイーサネット		
目的地。Addr。	Src。Addr。	E.タイプ	鬼ごっこ	長さ/ E。タイプ	データ	新しいCRC	新しいタグ付きパケット
		優先	CFI	VLAN ID			

■ポートVLANID

タグ付けされた（802.1Q VID情報を伝送している）パケットは、1つの802.1Q準拠ネットワークから送信できます。
VLAN情報がそのままの状態ですべてのポートを別のポートに接続します。これにより、802.1Q VLANがネットワークデバイス（実際には全体）にまたがることができます。
ネットワーク-すべてのネットワークデバイスが802.1Qに準拠している場合）。

スイッチ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のPVIDも割り当てられます。VLANがない場合に、スイッチで定義されたすべてのポートが、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、それらが受信されたポートのPVID。VLANに関する限り、転送の決定はこのPVIDに基づいています。
タグ付きパケットは、タグ内に含まれるVIDに従って転送されます。タグ付けされたパケットにも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が、VIDは使用されます。

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に関連付けるためのテーブルを保持する必要があります。スイッチはVIDを比較します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。2つのVIDが異なる場合、スイッチはドロップしますパケット。タグなしパケットのPVIDとタグ付きパケットのVIDが存在するため、タグ対応およびタグを認識しないネットワークデバイスは、同じネットワーク上に共存できます。

スイッチポートはPVIDを1つだけ持つことができますが、スイッチがVLANテーブルにメモリを格納するのと同じ数の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を認識しない可能性があるため、タグ認識デバイスの各ポートで事前に決定を行う必要があります
パケットが送信されます-送信されるパケットにタグを付ける必要がありますか？送信ポートがに接続されている場合
タグを認識しないデバイスの場合、パケットはタグなしである必要があります。送信ポートがタグ対応デバイスに接続されている場合、パケット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「デフォルト」と呼ばれる1つのVLAN、VID = 1を構成します。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」。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が「デフォルト」から削除されます。

■VLANへのポートの割り当て

スイッチのVLANを有効にする前に、まず各ポートを、それが参加するVLANグループに割り当てする必要があります。デフォルトではすべてのポートは、タグなしポートとしてVLAN1に割り当てられます。1つ以上のトラフィックを伝送する場合は、タグ付きポートとしてポートを追加しますVLAN、および接続のもう一方の端にある中間ネットワークデバイスまたはホストはVLANをサポートします。次に、ポートを割り当てますこのトラフィックを手動または手動で同じVLANに伝送するパスに沿った他のVLAN対応ネットワークデバイス上GVRPを動的に使用します。ただし、このスイッチのポートを1つ以上のVLANに参加させたいが、中間ネットワークデバイスも接続のもう一方の端にあるホストもVLANをサポートしている場合は、このポートをに追加する必要があります。タグなしポートとしてのVLAN。

VLANタグ付きフレームは、VLAN対応またはVLAN非対応のネットワーク相互接続を通過できます
ただし、VLANタグは、エンドノードホストに渡す前に削除する必要があります。
VLANタギングをサポートしていません。

■VLAN分類

スイッチがフレームを受信すると、2つの方法のいずれかでフレーム进行分类します。フレームがタグ付けされていない場合、スイッチは関連付けられたVLANへのフレーム（受信ポートのデフォルトVLAN IDに基づく）。ただし、フレームにタグが付けられている場合、スイッチはフレームのポートブロードキャストドメインを識別するためのタグ付きVLANID。

■ポートの重複

ポートオーバーラップを使用して、次のような異なるVLANグループ間で共通に共有されるネットワークリソースへのアクセスを許可できます。ファイルサーバーまたはプリンター。オーバーラップしないが通信する必要があるVLANを実装する場合は、接続できることに注意してくださいこのスイッチでルーティングを有効にすることでそれらを実現します。

■タグなしVLAN

タグなし（または静的）VLANは通常、ブロードキャストトラフィックを削減し、セキュリティを強化するために使用されます。ネットワークユーザーのグループVLANに割り当てられると、スイッチに設定されている他のVLANとは別のブロードキャストドメインが形成されます。パケットは同じVLANに指定されているポート間でのみ転送されます。タグなしVLANを使用して、ユーザーを手動で分離できますグループまたはサブネット。

4.5.3管理VLAN

このページで管理VLANを構成します。図4-5-1および図4-5-2の画面が表示されます。

図4-5-1管理VLAN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
•管理VLAN	管理対象VLANIDを提供します

ボタン

：クリックして変更を適用します。

図4-5-2管理VLAN状態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
•管理VLAN	現在の管理VLANを表示します。

4.5.4VLANの作成

このページでVLANを作成/削除します。図4-5-3および図4-5-4の画面が表示されます。

図4-5-3VLAN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
• VLANリスト	この特定のVLANのIDを示します。
• VLANアクション	この列により、ユーザーはVLANを追加または削除できます。
• VLAN名プレフィックス	この特定のVLANの名前を示します。

ボタン

: クリックして変更を適用します。

図4-5-4VLANテーブル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
• VLANID	現在のVLANIDエントリを表示します
• VLAN名	現在のVLANID名を表示します
• VLANタイプ	現在のVLANIDタイプを表示します
• 変更	クリック VLAN構成を変更するには

4.5.5インターフェース設定

このページは、マネージドスイッチポートVLANを構成するために使用されます。[ポート構成ごとのVLAN]ページには、次のフィールドが含まれています。

VLANの一部であるポートの管理。ポートの**デフォルトVLANID（PVID）**は、[VLANポート構成]ページで構成されます。
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。

スイッチの命名法を理解する

■ IEEE802.1Qタグ付きおよびタグなし

802.1Q標準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構成できます。

- **タグ付き：**

タグ付けが有効になっているポートは、VID番号、優先度、およびその他のVLAN情報をそれらのポートに流入するすべてのパケットのヘッダー。パケットが以前にタグ付けされている場合、ポート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。のVLAN情報タグは、ネットワーク上の他の802.1Q標準デバイスで使用して作成できます。パケット転送の決定。
- **タグなし：**

タグ付け解除が有効になっているポートは、それらに流入するすべてのパケットから802.1Qタグを取り除きます。ポート。パケットに802.1QVLAN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、タグ付け解除ポートによって受信および転送されるすべてのパケットには、802.1QVLANがありません。情報。（PVIDはスイッチの内部でのみ使用されることに注意してください）。タグの解除は802.1Q標準のネットワークデバイスから非標準の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端末。

フレーム収入	収入フレームは タグ付けされています	収入フレームは タグなしです
フレームリーブ		
ポートを離れるはタグ付けされてい ます	フレームはタグ付けされたままです	タグが挿入されます
ポートをタグ付けしない	タグが削除されました	フレームはタグなしのまま

表4-5-1：VLANVIDタグ付きの入力/出力ポート/タグ解除テーブル

■ IEEE802.1Qトンネリング（Q-in-Q）

IEEE 802.1Qトンネリング（QinQ）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ー向けに設計されています。
QinQトンネリングは、異なる顧客の場合でも、顧客固有のVLANおよびレイヤー2プロトコル構成を維持するために使用されます
同じ内部VLANIDを使用します。これは、**サービスプロバイダーVLAN（SPVLAN）**タグをお客様のフレームがサービスプロバイダーのネットワークに入るときにフレームを作成し、フレームがネットワークを離れるときにタグを削除します。

サービスプロバイダーの顧客は、内部VLANIDとサポートされるVLANの数について特定の要件を持っている場合があります。
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、トラフィックが通過する可能性があります
インフラストラクチャを介して混合される可能性があります。各顧客に一意の範囲のVLANIDを割り当てると、顧客が制限されます
構成では、VLANマッピングテーブルの集中的な処理が必要であり、VLANの最大制限を簡単に超える可能性があります。
4096。

マネージドスイッチは複数の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ます。

多数の独立した顧客LANからのトラフィックを**MAN（メトロアクセスネットワーク）**スペースに集約します。一つ

プロバイダーブリッジの目的は、VLANタグを認識して使用し、MANスペースのVLANを使用できるようにすることです。

お客様のVLANから独立しています。これは、入力するフレームにMAN関連のVIDを持つVLANタグを追加することで実現されます。

その男。MANを離れると、タグが削除され、顧客関連のVIDを持つ元のVLANタグが再び使用可能になります。

これにより、干渉することなく、共通のMANスペースを介してリモートコスチュームVLANを接続するトンネリングメカニズムが提供されます。

VLANタグ付き。すべてのタグは、イーサタイプを使用**0x8100**または**0x88A8** 0x8100が顧客タグと0x88A8のために使用され、使用されています

サービスプロバイダータグ用。

特定のサービスVLANのスイッチにメンバーポートが2つしかない場合、特定の学習を無効にすることができます。

VLANであるため、2つのポート間の転送メカニズムとしてフラッディングに依存できます。このように、MACテーブル

要件が軽減されます。

インターフェイス設定の編集

図4-5-5および図4-5-6の[インターフェイス設定/ステータスの編集]画面が表示されます。

図4-5-5 インターフェイス設定のスクリーンショットの編集

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
・ポート選択	このドロップダウンリストからポート番号を選択して、VLANポート設定を設定します。
・インターフェイスVLANモード	ポートをアクセス、トランク、ハイブリッド、およびトンネルモードに設定します。 ■トランクは、ポートが複数のVLANのトラフィックを許可することを意味します。 ■アクセスは、ポートが1つのVLANのみに属していることを示します。 ■ハイブリッドとは、ポートがマルチVLANのトラフィックをタグまたはタグ解除モード。 ■トンネルは、別のポートへのダウンリンクポートのIEEE802.1Qトンネリングを構成します顧客ネットワーク内のデバイス。
・PVID	選択したポートにPVIDを割り当てることができます。 PVIDは、入力ポートに入るすべてのタグなしフレームに挿入されます。ザ・

	<p>PVIDは、ポートがVLANグループに属するVLANIDと同じである必要があります。 タグなしのトラフィックはドロップされます。</p> <p>PVIDの範囲は1～4094です。</p>
•受け入れられるタイプ	<p>ポートがすべてのフレームを受け入れるか、タグ付きフレームのみを受け入れるかを決定します。このパラメータはVLAN入力処理に影響します。ポートがタグ付きのみを受け入れる場合フレーム、ポートで受信されたタグなしフレームは破棄されます。</p> <p>オプション：</p> <ul style="list-style-type: none"> ■すべて ■タグのみ ■タグを外すのみ
•イングレスフィルタリング	<p>デフォルトでは、フィールドは[すべて]に設定されています。</p> <p>•イングレスフィルタリングが有効になっている場合（チェックボックスがオンになっている場合）、フレームは</p> <p>ポートがメンバーではないVLANは破棄されます。</p> <p>•イングレスフィルタリングが無効になっている場合、ポートがVLANではないVLANに分類されたフレームのメンバーが受け入れられ、スイッチエンジンに転送されます。</p> <p>ただし、ポートは、VLANに分類されていないフレームを送信することはありません。</p> <p>のメンバー。</p>
•アップリンク	<p>トランクポートのアップリンク機能を有効/無効にします。</p>
•TPID	<p>スイッチトランクポートのプロトコルのタイプ（TPID）を構成します。</p>

ボタン

：クリックして変更を適用します。

図4-5-6 インターフェース設定のスクリーンショットの編集

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	論理ポートのスイッチポート番号
・インターフェイスVLANモード	現在のインターフェースVLANモードを表示します
・PVID	現在のPVIDを表示する
・受け入れられるフレームタイプ	現在のアクセスフレームタイプを表示します
・インGRESフィルタリング	現在のインGRESフィルタリングを表示する
・アップリンク	現在のアップリンクモードを表示する
・TPID	現在のTPIDを表示する

4.5.6VLANへのポート

VLAN静的テーブルを使用して、選択したVLANインデックスのポートメンバーを設定します。このページでは、ポートを追加および削除できます
各VLANのメンバー。図4-5-7の画面が表示されます。

図4-5-7ポートからVLANへ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
• VLANID	このドロップダウンリストからVLANIDを選択して、VLANメンバーシップを割り当てます。
• ポート	論理ポートのスイッチポート番号。
• インターフェイスVLANモード	現在のインターフェイスVLANモードを表示します。
• メンバーシップ	適切な無線をマークして、各インターフェイスのVLANメンバーシップを選択します ポートまたはトランクのボタン： 禁止 ：インターフェイスは、経由でVLANに自動的に参加することを禁止されています GVRP。 除外 ：インターフェイスはVLANのメンバーではありません。に関連付けられたパケット このVLANはインターフェイスによって送信されません。 タグ付き ：インターフェイスはVLANのメンバーです。によって送信されたすべてのパケット ポートはタグ付けされます。つまり、タグを伝送するため、VLANまたは CoS情報。 タグなし ：インターフェイスはVLANのメンバーです。によって送信されたすべてのパケット

GS-4210シリーズのユーザズマニュアル

	ポートはタグ付けされません。つまり、タグが付けられないため、タグが付けられません。 VLANまたはCoS情報を伝送します。インターフェイスは次のようにする必要がありますに注意してください タグなしポートとして少なくとも1つのグループに割り当てられます。
• PVID	現在のPVIDを表示する

ボタン

：クリックして変更を適用します。

4.5.7ポートVLANメンバーシップ

このページでは、VLANユーザのメンバーシップステータスの概要を説明します。[図4-5-8](#)の[VLANメンバーシップステータス]画面
が表示されます。

図4-5-8ポートVLANメンバーシップテーブル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
•ポート	論理ポートのスイッチポート番号
•モード	現在のVLANモードを表示します
•管理VLAN	現在の管理VLANを表示します
•運用VLAN	現在稼働中のVLANを表示する
•変更	クリック VLANメンバーシップを変更するには

4.5.8プロトコルVLANグループ設定

複数のプロトコルをサポートするために必要なネットワークデバイスは、共通のVLANに簡単にグループ化することはできません。これには必要な場合があります。特定の参加しているすべてのデバイスを網羅するために、異なるVLAN間でトラフィックを渡す非標準デバイスプロトコル。この種の構成では、セキュリティや簡単なアクセスなど、VLANの基本的な利点がユーザーから奪われます。

これらの問題を回避するために、物理ネットワークを分割するプロトコルベースのVLANを使用してこのマネージドスイッチを構成できます。必要なプロトコルごとに論理VLANグループに変換します。フレームがポートで受信されると、そのVLANメンバーシップは次のようになります。インバウンドパケットで使用されているプロトコルタイプに基づいて決定されます。

コマンドの使用法

プロトコルベースのVLANを構成するには、次の手順に従います。

- 1.1. まず、使用する**プロトコルのVLANグループ**を構成します。必須ではありませんが、ネットワーク上で実行されている主要なプロトコルごとに個別のVLAN。この時点では、ポートメンバーを追加しないでください。
- 2.2. プロトコルVLAN設定を使用して、VLANに割り当てるプロトコルごとに**プロトコルグループ**を作成します。
 ページ。
- 3.3. 次に、[Protocol VLAN Port Configuration]ページを使用して、各インターフェイスのプロトコルを適切なVLANにマッピングします。

このページでは、プロトコルベースのVLANグループ設定を構成できます。図4-5-9のプロトコルベースのVLAN画面と図4-5-10が表示されます。

図4-5-9プロトコルVLANグループの追加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
•グループID	特別プロトコルVLANグループに割り当てられたプロトコルグループID。
•フレームタイプ	フレームタイプには、次のいずれかの値を指定できます。
	■イーサネットII

- IEEE802.3_LLC_Other
- RFC_1042

注：[フレームタイプ]フィールドを変更すると、次のテキストフィールドの有効な値が変更されます
選択した新しいフレームタイプによって異なります。

・プロトコル値

このテキストフィールドに入力できる有効な値は、選択したオプションによって異なります

(0x0600-0xFFFE)

前のフレームタイプ選択メニューから。

フレームタイプの有効な値の範囲は0x0600～0xFFFEです。

ボタン

：クリックして変更を適用します。

図4-5-10プロトコルVLANグループの状態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	
・グループID	現在のグループIDを表示する	
・フレームタイプ	現在のフレームタイプを表示します	
・プロトコル値	現在のプロトコル値を表示します	
・削除	クリック	グループIDエントリを削除するには

4.5.9プロトコルVLANポート設定

このページでは、すでに設定されているグループ名をスイッチのVLAN /ポートにマッピングできます。プロトコルVLANポート
図4-5-11および図4-5-12の設定/状態画面が表示されます。

図4-5-11プロトコルVLANポート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
・ポート	このドロップダウンリストからポートを選択して、プロトコルVLANポートを割り当てます
・グループ	このドロップダウンリストからグループIDをプロトコルVLANグループに選択します
・VLAN	特別プロトコルVLANグループに割り当てられたVLANID

ボタン

：クリックしてプロトコルVLANポートエントリを追加します。

図4-5-12プロトコルVLANポート状態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
・ポート	現在のポートを表示する
・グループID	現在のグループIDを表示する
・VLANID	現在のVLANIDを表示します
・削除	クリックグループIDエントリを削除するには

4.5.10 GVRP設定

GARP VLAN登録プロトコル（GVRP）は、スイッチが登録するためにVLAN情報を交換する方法を定義します。ネットワーク全体のポートのVLANメンバー。

VLANは、ホストデバイスによって発行され、ネットワーク全体に伝播される参加メッセージに基づいて動的に構成されます。自動VLAN登録を許可し、ローカルスイッチを超えて拡張するVLANをサポートするには、GVRPを有効にする必要があります。

図4-5-13および図4-5-14のGVRPグローバル設定/情報画面が表示されます。

図4-5-13 GVRPグローバル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
・GVRP	このスイッチでGVRPを有効にするか無効にするかを制御します。
・参加タイムアウト	VLANに参加するための要求/クエリの送信間隔 グループ。 範囲：20～16375センチ秒 デフォルト：20センチ秒
・タイムアウトを残す	ポートがVLANグループを離れる前に待機する間隔。今回はに設定する必要があります 参加時間の2倍以上。これにより、LeaveまたはLeaveAllの後に メッセージが発行され、申請者は実際に港の前に再参加することができます グループを離れます。 範囲：45～32760センチ秒 デフォルト：60センチ秒
・LeaveAllタイムアウト	VLANグループのLeaveAllクエリメッセージを送信する間隔 参加者とグループを去る港。この間隔はかなりあるはずです ノードによって生成されるトラフィックの量を最小限に抑えるために、LeaveTimeよりも大きい グループに再び参加します。 範囲：65～32765センチ秒。 デフォルト：1000センチ秒

タイマー設定は次のルールに従う必要があります。

2 x (タイマーに参加) < タイマーを離れる < leaveAllタイマー

ボタン

: クリックして変更を適用します。

図4-5-14GVRPグローバル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
・GVRPステータス	現在のGVRPステータスを表示します
・参加タイムアウト	現在の参加タイムアウトパラメータを表示します
・タイムアウトを残す	現在の休暇タイムアウトパラメータを表示します

4.5.11GVRPポート設定

図4-5-15および図4-5-16のGVRPポート設定/ステータス画面が表示されます。

図4-5-15GVRPグローバル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
•ポート選択	このドロップダウンリストからポートを選択して、プロトコルVLANポートを割り当てます
• GVRPが有効	ポートでGVRPを有効にするか無効にするかを制御します
•登録モード	デフォルトでは、GVRPポートは 通常 の登録モードです。これらのポートはGVRPを使用します隣接するスイッチからのメッセージに参加して、802.1Qトランクリンク。反対側のデバイスがGVRPを送信できない場合メッセージ、またはスイッチがVLANをブルーニングすることを許可したくない場合は、 固定 モードを使用します。固定モードポートは、に存在するすべてのVLANに転送されますデータベースを切り替えます。 禁止 モードのポートは、VLAN1に対してのみ転送されます。
• VLANの作成	GVRPは、トランキングの目的でスイッチ上にVLANを動的に作成できます。沿ってGVRP動的VLAN作成を有効にすると、スイッチはデータベースにVLANを追加します持っていないVLANに関するGVRP参加メッセージを受信したとき。

ボタン

: クリックして変更を適用します。

図4-5-16GVRPポート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
•ポート	論理ポートのスイッチポート番号
•ステータスを有効にする	現在のGVRPポートの状態を表示します
•登録モード	現在の登録モードを表示する
•VLAN作成ステータス	現在のVLAN作成ステータスを表示します

4.5.12 GVRP VLAN

図4-5-17のGVRPVLANデータベース画面が表示されます。

図4-5-17GVRPVLANデータベースの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
•VLANID	現在のVLANIDを表示します
•メンバーポート	現在のメンバーポートを表示します
•動的ポート	現在の動的ポートを表示します
•VLANタイプ	現在のVLANタイプを表示します

4.5.13GVRP統計

図4-5-18および図4-5-19のGVRPポート統計およびエラー統計画面が表示されます。

図4-5-18GVRPポート統計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
•ポート	論理ポートのスイッチポート番号
•空に参加 (Rx / Tx)	現在の参加空 (TX / RX) パケットを表示します
•空 (Rx / Tx)	現在の空の (TX / RX) パケットを表示します
•空のままにする (Rx / Tx)	現在のLeaveempty (TX / RX) パケットを表示します
•参加 (Rx / Tx)	現在の結合を (TX / RX) パケットで表示します
•そのままにしておく (Rx / Tx)	現在のリーブイン (TX / RX) パケットを表示します
• LeaveAll (Rx / Tx)	現在のleaveall (TX / RX) パケットを表示します

図4-5-19GVRPポートエラー統計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
•ポート	論理ポートのスイッチポート番号。
•無効なプロトコルID	現在の無効なプロトコルIDを表示します
•無効な属性タイプ	現在の無効な属性タイプを表示します
•無効な属性値	現在の無効な属性値を表示します
•無効な属性 長さ	現在の無効な属性の長さを表示する

ボタン

：クリックしてGVRPエラー統計をクリアします。

：クリックしてGVRPエラー統計を更新します。

4.5.14 VLAN設定例：

-個別のVLAN

-802.1QVLANトランク

4.5.14.12つの別々の802.1QVLAN

この図は、マネージドスイッチが2つのVLANのタグ付きおよびタグなしのトラフィックフローを処理する方法を示しています。VLANグループ2およびVLANグループ3は分離されたVLANです。各VLANはネットワークトラフィックを分離するため、VLANのメンバーのみが同じVLANメンバー。図4-5-20の画面が表示され、表4-5-2にマネージドのポート構成が示されています。

スイッチ。

VLANグループ	VID	タグなしメンバー	タグ付きメンバー
VLANグループ1	1	ポート-7～ポート-8	該当なし
VLANグループ2	2	ポート-1、ポート-2	ポート3
VLANグループ3	3	ポート-4、ポート-5	ポート-6

表4-5-2VLANとポートの構成

シナリオは次のように説明されます。

■ VLAN2に入るタグなしパケット

- 1.1。 ときにPC-1は、送信**タグなし**の入力パケットの**ポート-1**を、マネージドスイッチは、でそれをタグ付けします**VLANタグ= 2**。
PC-2とPC-3は、**ポート2とポート3**を介してパケットを受信します。
- 2.2。 PC-4、PC-5、PC-6はパケットを受信しません。

143

- 3.3。 パケットが**ポート2**を離れると、**タグがタグなし**パケットになることでパケットが取り除かれます。
- 4.4。 パケットが**ポート3**を離れると、**VLAN Tag = 2のタグ付き**パケットとして保持されます。

■ VLAN2に入るタグ付きパケット

- 1.1。 場合PC-3送信**タグ付き**でパケット**VLANタグ= 2**入射**ポート3**、PC-1とPC-2がパケットを受信します
ポート1およびポート2を介して。
- 2.2。 パケットが**ポート1とポート2**を離れると、**タグ**によって削除され、**タグなし**パケットになります。

■ VLAN3に入るタグなしパケット

- 1.1。 場合PC-4送信**タグなし**入るパケット**ポート4**を、スイッチでそれをタグ付けします**VLANタグ= 3**。PC-5およびPC-6
ポート5とポート6を介してパケットを受信します。
- 2.2。 パケットが**ポート5**を離れると、**タグがタグなし**パケットになることでパケットが取り除かれます。
- 3.3。 パケットが**ポート6**を離れると、**VLAN Tag = 3のタグ付き**パケットとして保持されます。

この例では、VLANグループ1がデフォルトVLANとして設定されていますが、VLAN2およびVLAN3トラフィックのみに焦点を当てています。
フロー。

セットアップ手順

1.VLANグループ2および3を作成します

VLANグループ2とグループ3を追加します

2.VLANモードとPVIDを各ポートに割り当てます。

ポート1、ポート2、およびポート3：VLANモード=ハイブリッド、PVID = 2

ポート4、ポート5、およびポート6：VLANモード=ハイブリッド、PVID = 3

3.タグ付き/タグなしを各ポートに割り当てます。

VLAN ID = 2 :

ポート-1および2 = タグなし、

ポート-3 = タグ付き、

ポート-4～6 = 除外。

VLAN ID = 3 :

ポート-4および5 = タグなし、

ポート-6 = タグ付き、

ポート-1～3 = 除外。

4.5.14.22つの802.1Q対応スイッチ間のVLANトランッキング

ほとんどの場合、これらは他のスイッチへの「アップリンク」に使用されます。VLANは異なるスイッチで分離されていますが、同じVLANグループ内の他のスイッチにアクセスします。図4-5-21の画面が表示されます。

セットアップ手順

1.1。 VLANグループ2および3を作成します

VLANグループ2とグループ3を追加します

2.2。 VLANモードとPVIDを各ポートに割り当てます。

ポート1、ポート2、およびポート3 : VLANモード=ハイブリッド、PVID = 2

ポート4、ポート5、およびポート6 : VLANモード=ハイブリッド、PVID = 3

ポート7 : VLANモード=ハイブリッド、PVID = 1

3.3。 タグ付き/タグなしを各ポートに割り当てます。

VLAN ID = 1 :

ポート1~6 =タグなし、

ポート7 =除外。

VLAN ID = 2 :

ポート1および2 =タグなし、

ポート3および7 =タグ付き、

ポート4~6 =除外。

VLAN ID = 3 :

ポート-4および5 = タグなし、

ポート-6および7 = タグ付き、

ポート-1 ~ 3 = 除外。

4.6 スパニングツリープロトコル

4.6.1 理論

スパニングツリープロトコルを使用して、ネットワークループを検出して無効にしたり、スイッチ間のバックアップリンクを提供したりできます。

ブリッジまたはルーター。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、1つのルートのみを確保できます。

ネットワーク上の任意の2つのステーション間に存在し、プライマリリンク時に自動的に引き継ぐバックアップリンクを提供します

低下する。このスイッチでサポートされるスパンニングツリーアルゴリズムには、次のバージョンが含まれます。

- STP –スパンニングツリープロトコル (IEEE 802.1D)
- RSTP –高速スパンニングツリープロトコル (IEEE 802.1w)
- MSTP –マルチスパンニングツリープロトコル (IEEE 802.1s)

IEEE 802.1DスパンニングツリープロトコルおよびIEEE 802.1w高速スパンニングツリープロトコルは、リンクの遮断を可能に

ネットワーク内でループを形成するスイッチ間。スイッチ間の複数のリンクが検出された場合、プライマリリンクは

設立。重複したリンクは使用がブロックされ、スタンバイリンクになります。プロトコルは、重複リンクが

プライマリリンクに障害が発生した場合に使用されます。スパンニングツリープロトコルを設定して有効にすると、プライマリリンクは次のようになります。

確立され複製されたリンクは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（プライマリリンク時）

失敗）も、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は、ネットワークユーザーに最大の稼働時間を提供します。ただし、スパンニングの概念

ツリーアルゴリズムとプロトコルは複雑で複雑な主題であり、十分に調査して理解する必要があります。可能です

スパンニングツリーが正しく構成されていない場合、ネットワークのパフォーマンスが大幅に低下します。をお読みください

デフォルト値から変更を加える前に、以下に従ってください。

スイッチSTPは、次の機能を実行します。

- スイッチ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ンニングツリーを作成します。
- ユーザー指定で、単一のスイッチ内に含まれるポートの任意の組み合わせから、複数のスパンニングツリーを作成しますグループ。
- スパンニングツリーを自動的に再構成して、の要素の障害、追加、または削除を補正します。木。
- オペレーターの介入なしにスパンニングツリーを再構成します。

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ために、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、Bridge Protocol Data Unit (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：

- 送信スイッチが現在ルートスイッチであると信じているスイッチの一意の識別子
- 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、スパンニングツリートポロジを通信および構築します。LANに接続されているすべてのスイッチ

送信されたパケットは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、受信スイッチは

BPDUを計算するためのフレーム内の情報、およびトポロジが変更された場合は、BPDU送信を開始します。

BPDUを介したスイッチ間の通信により、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。
- ルートスイッチまでの最短距離は、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、パケットが転送されるルートスイッチに最も近いスイッチです。ルートに。
- 各スイッチのポートが選択されます。これは、スイッチ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するためです。すべてのスイッチでデフォルト設定でSTPが有効になっている場合、MACが最も低いスイッチネットワーク内のアドレスがルートスイッチになります。最適なスイッチの優先度を上げる（優先度番号を下げる）ことにより、STPは、ルートスイッチとして最適なスイッチを選択するように強制できます。

デフォルトのパラメータを使用してSTPが有効になっている場合、スイッチドネットワーク内の送信元ステーションと宛先ステーション間のパス理想的ではないかもしれません。たとえば、現在のルートポートよりも番号が大きいポートに高速リンクを接続すると、ルートポートの変更を引き起こします。

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、トポロジが変更される可能性があります。ブロッキング状態からフォワーディング状態に直接移行すると、一時的なデータループが発生する可能性があります。ポートは新しいものを待つ必要があります。パケットの転送を開始する前にネットワーク全体に伝播するネットワークトポロジ情報。彼らはまた待つ必要があります。古いトポロジに基づいて転送されたBPDU/パケットの有効期限が切れるパケットの有効期間。転送遅延タイマーが使用されます。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。さらに、STPは、ポートが必要とする一連の状態を指定します。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、移行します。

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

- **ブロッキング**—ポートはパケットの転送または受信をブロックされます
- **リスニング**—ポートは、ブロッキング状態に戻るようにポートに指示する可能性のあるBPDU/パケットの受信を待機しています。
- **学習**—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
- **転送**—ポートはパケットを転送しています
- **無効**—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1つの状態から別の状態に遷移します。

- 初期化（スイッチブート）からブロッキングまで
- ブロッキングからリスニングまたは無効化まで
- 聞くことから学ぶことへまたは障害者へ
- 学習から転送または障害者へ
- 転送から無効へ

- 無効からブロックへ

図4-6-1STPポートの状態遷移

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を有効にすると、のすべてのスイッチのすべてのポートがネットワークはブロッキング状態を経て、電源投入時にリスニングとラーニングの状態に移行します。適切な場合設定すると、各ポートは転送状態またはブロッキング状態に安定します。パケット（BPDUを除く）は転送または受信されませんによって、転送状態がそのポートで有効になるまで、STPが有効なポート。

2.STPパラメータ

STPの運用レベル

スイッチでは、スイッチレベルとポートレベルの2つのレベルの操作が可能です。スイッチレベルはスパンニングツリーを形成します1つ以上のスイッチ間のリンクで構成されます。ポートレベルは、1つ以上のグループで構成されるスパンニングツリーを構築します。ポート。STPは、両方のレベルでほぼ同じように動作します。

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てからルートを設定します
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
ポート。

以下は、スイッチレベルのユーザー設定可能なSTPパラメータです。

パラメータ	説明	デフォルト値
ブリッジ識別子（ユーザーではありません）	ユーザー設定の優先度との組み合わせ	32768 + MAC
構成可能	スイッチのMACアドレス。	

優先順位を設定する以外 未満)	ブリッジ識別子は2つの部分で構成されています。 16ビットの優先度と48ビットのイーサネットMAC アドレス32768+ MAC	
優先	各スイッチの相対的な優先度-低い 数字は優先度が高く、 特定のスイッチがとして選出される可能性 ルートブリッジ	32768
こんにちは時間	の放送間の時間の長さ スイッチによるハローメッセージ	2秒
最大年齢タイマー	受信したBPDUの経過時間を測定します。 ポートし、BPDUが確実に破棄されるようにします その年齢がの値を超えると 最大年齢タイマー。	20秒
フォワードディレイタイマー	のポートが費やした時間 学習とリスニングの状態は ポートをに戻す可能性のあるBPDU ブロッキング状態。	15秒

以下は、ポートまたはポートグループレベルのユーザー設定可能なSTPパラメータです。

変数	説明	デフォルト値
----	----	--------

ポートの優先順位	それぞれの相対的な優先順位	128
	ポート-数値が小さいほど優先度が高くなります	
	特定のポートが存在する可能性が高くなります	
	ルートポートとして選出	
ポートコスト	バスを評価するためにSTPが使用する値-	200,000-100Mbpsファストイーサネットポート
	STPはバスコストを計算し、	20,000~1000Mbpsギガビットイーサネット
	アクティブとして最小コストのバス	ポート
	道	0-自動

デフォルトのスパンニングツリー構成

特徴	デフォルト値
状態を有効にする	すべてのポートでSTPが無効になっています
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

ユーザーが変更可能なSTAパラメーター

スイッチの工場出荷時のデフォルト設定は、インストールの大部分をカバーする必要があります。ただし、デフォルトのままにしておくことをお勧めします。どうしても必要な場合を除き、工場出荷時の設定です。スイッチのユーザーが変更可能なパラメーターは次のとおりです。

優先度-スイッチの優先度は0~65535の範囲で設定できます。0は最高の優先度と同じです。

152

ハロータイム-ハロータイムは1~10秒です。これは、送信されたBPDUパケットの2つの送信間の間隔です。

ルートブリッジによって、他のすべてのスイッチに、それが実際にルートブリッジであることを通知します。スイッチにハロータイムを設定したが、そうではない場合ルートブリッジ。スイッチがルートブリッジになると、設定されたハロータイムが使用されます。

ハロータイムは最大値より長くすることはできません。年齢。それ以外の場合、構成エラーは起こる。

最大年齢-最大年齢は6~40秒です。最大経過時間の終了時に、BPDUがまだ受信されていない場合

ルートブリッジの場合、スイッチは、ルートブリッジになる許可を得るために、他のすべてのスイッチに独自のBPDUの送信を開始します。それであればスイッチのブリッジ識別子が最も低いことが判明すると、ルートブリッジになります。

転送遅延タイマー-転送遅延は4~30秒です。これは、上の任意のポートの時間です

スイッチは、ブロッキング状態からフォワーディング状態に移行する間、リスニング状態で消費します。

上記のパラメータを設定するときは、次の式に従ってください。

最大年齢_2 x (転送遅延-1秒)

最大年齢_2 x (ハロータイム+ 1秒)

ポートの優先度-ポートの優先度は0~240です。数値が小さいほど、ポートが選択される可能性が高くなります。

ルートポート。

ポートコスト-ポートコストは0から200000000まで設定できます。数値が小さいほど、ポートが発生する可能性が高くなります。

パケットを転送するために選択されました。

3.STPの図

ループに接続された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支援が適用されない場合、いくつかの主要なネットワークの問題。

スイッチAがパケットをスイッチBに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はパケットをスイッチにブロードキャストします。Aなど。ブロードキャストパケットはループで無期限に渡され、ネットワーク障害を引き起こす可能性があります。この例では、STPは、スイッチBとCの間の接続をブロックすることにより、ループを切断します。特定の接続をブロックする決定は、最新のブリッジとポート設定のSTP計算について。

ここで、スイッチAがスイッチCにパケットをブロードキャストすると、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てSTPを設定することは、複雑になる可能性があります。したがって、デフォルトのファクトリを維持することをお勧めします。設定と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。特定を選択するためにSTPに影響を与える優先度設定を使用してルートブリッジとして切り替えるか、ポート優先度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に影響を与えます。ただし、ポートコストの設定は比較的簡単です。

図4-6-2STAルールを適用する前

この例では、デフォルトのSTP値のみが使用されます。

図4-6-3STAルールを適用した後

154

ブリッジIDが最小のスイッチ（スイッチC）がルートブリッジとして選択され、ポートは高いポートを提供するように選択されました。

スイッチBとスイッチC間のコスト。スイッチAの2つの（オプションの）ギガビットポート（デフォルトのポートコスト= 20,000）はに接続されています。

スイッチBとCの両方に1つの（オプションの）ギガビットポート。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（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することもできますが、ポートコストを増やす必要があります
デフォルトから、スイッチBとスイッチC間のリンクがブロックされたリンクであることを確認します。

このセクションには、次の項目があります。

- | | | |
|---|--------------|-----------------|
| ■ | STPグローバル設定 | STPシステム設定を構成します |
| ■ | STPポート設定 | ポートごとの構成STP設定 |
| ■ | CISTインスタンス設定 | システム構成を構成します |
| ■ | CISTポート設定 | CISTポート設定を構成します |
| ■ | MSTインスタンス設定 | 各MSTインスタンス設定の構成 |
| ■ | MSTポート設定 | ポートごとの構成MST設定 |
| ■ | STP統計 | STP統計を表示します |

4.6.2STPグローバル設定

このページでは、STPシステム設定を構成できます。この設定は、スイッチ内のすべてのSTPブリッジインスタンスによって使用されます。ザ・マネージドスイッチは、次のスパンニングツリープロトコルをサポートしています。

- ・**互換性-スパンニングツリープロトコル（STP）**：エンドステーション間に単一のパスを提供し、ループを排除します。
- ・**通常-高速スパンニングツリープロトコル（RSTP）**：より高速なネットワークポロジを検出して使用します
転送ループを作成せずに、スパンニングツリーコンバージェンス。
- ・**拡張機能-マルチスパンニングツリープロトコル（MSTP）**：RSTPの拡張機能を定義して、
仮想LAN（VLAN）の有用性。この「VLANごとの」マルチスパンニングツリープロトコルは、個別の
各VLANグループのスパンニングツリー。各スパンニング内の可能な代替パスの1つを除くすべてをブロックします。
木。

図4-6-4および図4-6-5のSTPグローバル設定画面が表示されます。

図4-6-4グローバル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
・有効にする	STP機能を有効または無効にします。 デフォルト値は「無効」です。
・BPDU転送	BPDU転送方式を設定します。
・PathCostメソッド	パスコスト法は、デバイス間の最適なパスを決定するために使用されます。 したがって、より高速なメディアに接続されているポートには、より低い値を割り当てる必要があります。 メディアが遅いポートには、より高い値が割り当てられます。
・強制バージョン	STPプロトコルのバージョン設定。有効な値は STP互換 です。

RSTP-操作およびMSTP-操作。

- ・構成名 現在使用されている構成を識別するために使用される識別子。
- ・現在使用されている構成を識別するために使用される構成リビジョン識別子。

許可される値は0～65535です。

デフォルト値は0です。

ボタン

: クリックして変更を適用します。

図4-6-5STP情報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
・STP	現在のSTP状態を表示します
・BPDU転送	現在のBPDUフォワードモードを表示します
・原価法	現在のコスト方法を表示する
・強制バージョン	現在のフォースバージョンを表示する
・構成名	現在の構成名を表示します
・構成リビジョン	現在の構成リビジョンを表示します

4.6.3STPポート設定

このページでは、ポートごとのSTP設定を構成できます。図4-6-6および図4-6-7のSTPポート設定画面が表示されます。

図4-6-6STPポート構成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
•ポート選択	このドロップダウンリストからポート番号を選択します。
•外部コスト（0 = 自動）	ポートで発生するバスコストを制御します。 自動設定は、物理リンク速度によって適切にバスコストを設定します。 802.1D推奨値を使用します。特定の設定を使用して、 ユーザー定義の値を入力できます。 バスコストは、ネットワークのアクティブなトポロジを確立するときに使用されます。 バスコストが高いポートを優先して、転送ポートとしてバスコストが低いポートが選択されます ポート。有効な値は1〜200000000の範囲です。
•エッジポート	operEdgeフラグを設定またはクリアして開始するかどうかを制御します。（ ポートが初期化されたときの初期operEdge状態）。
•BPDUフィルタ	Edgeとして明示的に構成されたポートが送受信するかどうかを制御します BPDU。
•BPDUガード	Edgeとして明示的に構成されたポートがそれ自体を無効にするかどうかを制御します BPDUの受信。 ポートはエラーディセーブル状態になり、アクティブから削除されます トポロジ。
•P2PMAC	ポートが共有ではなくポイントツーポイントLANに接続するかどうかを制御します 中。 これは自動的に決定されるか、trueまたはfalseのいずれかを強制されます。への移行 転送状態は、共有メディアよりもポイントツーポイントLANの方が高速です。 （これは物理ポートにのみ適用されます。集約は常に強制されますPoint2Point）。
•移行する	スイッチがSTPBPDUを検出した場合はいつでも、設定または トポロジ変更通知BPDU、選択したものを自動的に設定します 強制STP互換モードへのインターフェイス。 ただし、[プロトコル移行]ボタンを使用して手動で再確認することもできます

選択したで送信する適切なBPDUフォーマット（RSTPまたはSTP互換）
インターフェイス。
（デフォルト：無効）

ボタン

：クリックして変更を適用します。

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、バスコストを設定します
以下に示す値に従います。バスコスト「0」は、自動構成モードを示すために使用されます。ショートバスコストがかかる場合
メソッドが選択され、IEEE 802.1w標準で推奨されているデフォルトのバスコストが65,535を超える場合、デフォルトはに設定されます。
65,535。

ポートタイプ	IEEE 802.1D-1998	IEEE 802.1w-2001
イーサネット	50～600	200,000～20,000,000
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4-6-1推奨されるSTPバスのコスト範囲

ポートタイプ	リンクタイプ	IEEE 802.1D-1998	IEEE 802.1w-2001
イーサネット	半二重	100	2,000,000
	全二重	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	19	200,000
	全二重	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4-6-2推奨されるSTPバスコスト

ポートタイプ	リンクタイプ	IEEE 802.1w-2001
イーサネット	半二重	2,000,000
	全二重	1,000,000
	トランク	500,000
ファストイーサネット	半二重	200,000
	全二重	100,000
	トランク	50,000
ギガビットイーサネット	全二重	10,000
	トランク	5,000

表4-6-3デフォルトのSTPバスコスト

図4-6-7STPポート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
•ポート	論理STPポートのスイッチポート番号。
•管理者の有効化	現在のSTPポートモードステータスを表示します
•外部コスト	現在の外部コストを表示します。
•エッジポート	現在のエッジポートのステータスを表示します。
•BPDUフィルタ	現在のBPDUフィルタ設定を表示します。
•BPDUガード	現在のBPDUガード設定を表示します。
•P2PMAC	現在のP2PMACステータスを表示します。

4.6.4CISTインスタンス設定

このページでは、CISTインスタンス設定を構成できます。図4-6-8のCISTインスタンス設定および情報画面
そして、図4-6-9に表示されます。

図4-6-8 : CISTインスタンス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
•優先度	<p>ブリッジの優先度を制御します。数値が小さいほど優先順位が高くなります。橋</p> <p>優先度とMSTIインスタンス番号、6バイトのMACと連結</p> <p>スイッチのアドレスはブリッジ識別子を形成します。</p> <p>MSTP操作の場合、これはCISTの優先順位です。それ以外の場合、これが優先されます</p> <p>STP / RSTPブリッジの。</p>
•最大ホップ数	<p>これは、で生成されたMSTI情報の残りのホップの初期値を定義します。</p> <p>MSTI領域の境界。ルートブリッジができるブリッジの数を定義します</p> <p>BPDU情報を配布します。有効な値は6〜40ホップの範囲です。</p>
•転送遅延	<p>ルートポートと指定ポートをに移行するためにSTPブリッジが使用する遅延</p> <p>転送（STP互換モードで使用）。有効な値は4からの範囲です</p> <p>30秒まで</p> <p>-デフォルト : 15</p> <p>-最小 : 4または[(最大メッセージ経過時間 / 2) + 1]のいずれか高い方</p> <p>-最大 : 30</p>
•最大年齢	<p>ブリッジが送信する情報の最大経過時間</p> <p>ルートブリッジ。有効な値は6〜40秒の範囲です。</p> <p>-デフォルト : 20</p> <p>-最小 : 6または[2 x (Hello Time + 1)]のいずれか高い方。</p> <p>-最大 : 40または[2 x (転送遅延-1)]の低い方</p>

•送信ホールドカウント	<p>ブリッジポートが1秒間に送信できるBPDUの数。</p> <p>超過すると、次のBPDUの送信が遅延します。有効な値は次のとおりです</p> <p>1秒あたり1〜10BPDUの範囲です。</p>
•ハロータイム	<p>STPをチェックするためにBPDUパケットを送信するようにスイッチを制御する時間</p> <p>現在の状態。</p> <p>1〜10の値を入力します。</p>

ボタン

: クリックして変更を適用します。

図4-6-9CISTインスタンス情報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
・優先度	現在のCIST優先度を表示します
・マックスホップ	現在の最大値を表示します。ホップ
・転送遅延	現在の転送遅延を表示します
・最大年齢	現在の最大年齢を表示します
・送信ホールドカウント	現在のTxホールドカウントを表示します
・ハロータイム	現在のハロータイムを表示する

4.6.5CISTポート設定

このページでは、ポートごとのCISTの優先度とコストを設定できます。図4-6-10のCISTポート設定およびステータス画面
そして図は4-6-11表示されます。

図4-6-10CISTポート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
・ポート選択	このドロップダウンリストからポート番号を選択します。
・優先度	ポートの優先順位を制御します。これは、ポートの優先度を制御するために使用できます。 同一のポートコスト。（上記を参照）。 デフォルト：128 範囲：0～240、16刻み
・内部バスコスト	ポートで発生するバスコストを制御します。

(0 =自動)

自動設定は、物理リンク速度によって適切なバスコストを設定します

802.1D推奨値を使用します。**特定**の設定を使用することにより、

ユーザー定義の値を入力できます。

バスコストは、ネットワークのアクティブなトポロジを確立するときに使用されます。

バスコストが高いポートを優先して、転送ポートとしてバスコストが低いポートが選択されます

ポート。有効な値は1～200000000の範囲です。

ボタン

: クリックして変更を適用します。

図4-6-11CISTポート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
・ポート	論理STPポートのスイッチポート番号
・識別子（優先度/ポートID）	現在の識別子（優先度/ポートID）を表示します
・外部バスコスト 会議/操作	現在の外部バスのコストを表示するconf / oper
・内部バスコスト 会議/操作	現在の内部バスのコスト/操作を表示します
・指定されたルートブリッジ	現在指定されているルートブリッジを表示する
・外部ルートコスト	現在の外部ルートコストを表示する

•地域ルートブリッジ	現在の地域ルートブリッジを表示する
•内部ルートコスト	現在の内部ルートコストを表示します
•指定橋	現在指定されている橋を表示する
•内部ポートバスコスト	現在の内部ポートバスコストを表示します
•エッジポート会議/操作	現在のエッジポートのconf / operを表示します
•P2PMAC会議/操作	現在のP2PMAC conf / operを表示します
•ポートの役割	現在のポートの役割を表示する
•ポートステート	現在のポート状態を表示します

4.6.6MSTインスタンスの構成

このページでは、ユーザーがMSTインスタンス構成を構成できます。MSTインスタンス設定、情報、ステータス画面
[図4-6-12](#)、[図4-6-13](#)及び[図4-6-14](#)に表示されます。

図4-6-12MSTインスタンス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
• MSTID	MSTIIDの割り当てを許可します。 MSTI IDの範囲は1〜15です。
• VLANリスト (1-4096)	VLANリストを特別なMSTIIDに割り当てることができます。 VLANリストの範囲は1〜4094です。
•優先度	ブリッジの優先度を制御します。数値が小さいほど優先されます。 ブリッジの優先度とMSTIインスタンス番号（6バイトで連結） スイッチのMACアドレスはブリッジ識別子を形成します。

ボタン

: クリックして変更を適用します。

図4-6-13MSTIインスタンス設定情報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
・MSTI	現在のMSTIエントリを表示します
・ステータス	現在のMSTIステータスを表示します

・VLANリスト	現在のVLANリストを表示する
・VLANカウント	現在のVLAN数を表示する
・優先度	現在のMSTI優先度を表示します

図4-6-14MSTインスタンス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
・MSTID	MSTIDを表示します。
・地域のルートブリッジ	現在指定されているルートブリッジを表示する
・内部ルートコスト	現在の内部ルートコストを表示します
・指定橋	現在指定されている橋を表示する
・ルートポート	現在のルートポートを表示します。
・最大年齢	現在の最大値を表示します。年齢。
・転送遅延	現在の転送遅延を表示します。
・残りのホップ	現在の残りのホップを表示します。
・最後のトポロジ変更現在の最後のトポロジ変更	現在の最後のトポロジ変更を表示します。

4.6.7MSTポート設定

このページでは、ユーザーは現在のSTP MSTIポート構成を検査し、場合によってはそれらも変更できます。

MSTIポートは仮想ポートであり、各MSTIインスタンスのアクティブなCIST（物理）ポートごとに個別にインスタンス化されます。
ポートに設定および適用可能。実際のMSTIポート構成を表示する前に、MSTIインスタンスを選択する必要があります
オプション。

このページには、物理ポートと集約ポートのMSTIポート設定が含まれています。集計設定はグローバルです。MSTIポート
[図4-6-15](#)および[図4-6-16](#)の設定画面が表示されます。

図4-6-15MSTポート構成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
• MSTID	特別なMSTIDを入力して、パスのコストと優先度を設定します。
•ポート選択	このドロップダウンリストからポート番号を選択します。
•優先度	ポートの優先順位を制御します。これは、ポートの優先度を制御するために使用できます。 同一のポートコスト。
•内部バスコスト（0 = 自動）	ポートで発生するバスコストを制御します。 自動設定は、物理リンク速度によって適切なバスコストを設定します 802.1D推奨値を使用します。特定の設定を使用して、 ユーザー定義の値を入力できます。 バスコストは、ネットワークのアクティブなトポロジを確立するときに使用されます。 バスコストが高いポートを優先して、転送ポートとしてバスコストが低いポートが選択されます ポート。 有効な値は1〜2000000000の範囲です。

ボタン

: クリックして変更を適用します。

図4-6-16MSTポート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
• MSTID	現在のMSTIDを表示します
• ポート	論理STPポートのスイッチポート番号
• 識別子 (優先度/ ポートID)	現在の識別子 (優先度/ポートID) を表示します
• 内部バスコスト 会議/操作	現在の内部バスコストの構成/操作を表示します
• 地域のルートブリッジ	現在の地域のルートブリッジを表示する
• 内部ルートコスト	現在の内部ルートコストを表示します
• 指定橋	現在指定されている橋を表示する
• 内部バスコスト	現在の内部バスコストを表示します
• ポートの役割	現在のポートの役割を表示する
• ポートステート	現在のポート状態を表示します

このページには、STP統計が表示されます。図4-6-17のSTP統計画面が表示されます。

図4-6-17STP統計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
・ポート	論理STPポートのスイッチポート番号
・受信した設定BPDU	受信した現在の設定BPDUを表示します
・受信したTCNBPDU	受信した現在のTCNBPDUを表示します
・受信したMSTPBPDU	受信した現在のMSTPBPDUを表示します
・設定BPDU	送信された設定BPDUを表示します
送信	
・送信されたTCNBPDU	送信された現在のTCNBPDUを表示します
・送信されたMSTPBPDU	送信された現在のBPDUを表示します

4.7マルチキャスト

このセクションには、次の項目があります。

■ プロパティ	マルチキャストプロパティを構成します
■ IGMPスヌーピング	IGMPスヌーピング設定を構成します
■ IGMPスヌーピング統計	IGMPスヌーピング統計を表示します
■ MLDスヌーピング	MLDスヌーピング設定を構成します

■	MLDスヌーピング統計	MLDスヌーピング統計を表示します
■	マルチキャストスロットリング 設定	マルチキャストスロットリング設定を構成します
■	マルチキャストフィルター	マルチキャストフィルターを構成します

4.7.1プロパティ

このページでは、マルチキャストプロパティに関連する構成について説明します。

図4-7-1および図4-7-2のマルチキャストの[プロパティと情報]画面が表示されます。

図4-7-1プロパティ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
・不明なマルチキャスト アクション	不明なマルチキャストトラフィック方式： ドロップ、フラッド、またはルーターポートに送信します。
・IPv4転送方式	IPv4マルチキャスト転送方式を構成します
・IPv6転送方式	IPv6マルチキャスト転送方式を構成します

ボタン

：クリックして変更を適用します。

図4-7-2プロパティ情報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
--------	----

<ul style="list-style-type: none"> • 不明なマルチキャスト 	現在の不明なマルチキャストアクションステータスを表示します
<ul style="list-style-type: none"> <ul style="list-style-type: none"> アクション 	
<ul style="list-style-type: none"> • IPv4の転送方法 	現在のIPv4マルチキャスト転送方法を表示します
<ul style="list-style-type: none"> • IPv6の転送方法 	現在のIPv6マルチキャスト転送方法を表示します

4.7.2IGMPスヌーピング

インターネットグループ管理プロトコル (IGMP) はマルチキャストグループについて、ホストおよびルータの情報共有をすることができます。メンバーシップ。IGMPスヌーピングは、IGMPメッセージの交換を監視し、それらをCPUにコピーするスイッチ機能です。機能処理用。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次のポートのみに制限することです。マルチキャストグループのメンバー。

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

マルチキャスト送信を受信したいコンピューターとネットワークデバイスは、近くのルーターに通知する必要があります。マルチキャストグループのメンバーになります。**インターネットグループ管理プロトコル (IGMP)** は、これを通信するために使用されます。情報。また、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。その場合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つのルーターが「照会済み」として選択されます。その後、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から受信した情報は、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かどうかを決定します。ルータは、IGMPを使用して、次のことを確認できます。特定のサブネットワークには、マルチキャストグループのメンバーが少なくとも1つあります。サブネットワークにメンバーがいない場合、パケットそのサブネットワークには転送されません。

図4-7-3マルチキャストサービス

図4-7-4マルチキャストフラッディング

172

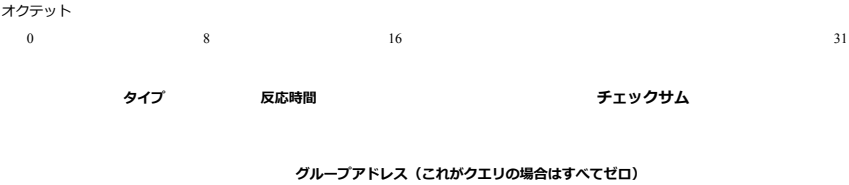
図4-7-5IGMPスヌーピングマルチキャストストリーム制御

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会できます。IGMPは、メンバーとマルチキャストルーターに次の方法を提供します。

マルチキャストグループに参加または脱退するときに通信します。
IGMPバージョン1はRFC1112で定義されています。パケットサイズは固定されており、オプションのデータはありません。
IGMPパケットの形式を以下に示します。

IGMPメッセージ形式



IGMPタイプコードを以下に示します。

タイプ	定義
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）
0x12	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現在）

0x16	メンバーシップレポート（バージョン2）
0x17	グループを脱退（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パケットにより、マルチキャストルーター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。

以下に、IGMPを使用してマルチキャストルーター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IGMP「レポート」を送信してグループに参加します

ホストがグループを離れたときにレポートを送信することはありません（バージョン1の場合）。

ホストは、グループを脱退するときに「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ーは、IGMPクエリを定期的に（すべてのホストのグループアドレス：224.0.0.1に）送信して、グループメンバーがいるかどうかを確認します。

サブネットワーク上に存在します。特定のグループからの応答がない場合、ルータはグループメンバーがいないと見なします

ネットワーク上。

クエリメッセージの存続可能時間（TTL）フィールドは1に設定されているため、クエリは他のサブネットワークに転送されません。

IGMPバージョン2では、LANごとに照会されたマルチキャストを選択する方法、明示的な脱退など、いくつかの拡張機能が導入されています。

メッセージ、および特定のグループに固有のクエリメッセージ。

コンピューターがマルチキャストグループに参加または脱退するために通過する状態を以下に示します。

図4-7-6IGMPの状態遷移

■ IGMPクエリアー

ルーターまたはマルチキャスト対応スイッチは、ホストにマルチキャストトラフィックを受信するかどうかを定期的に尋ねることができます。もっとあるならIPマルチキャストを実行するLAN上の1つのルーター/スイッチよりも、これらのデバイスの1つが「クエリアー」として選出され、LANにグループメンバーを照会する役割。次に、サービス要求をアップストリームマルチキャストに伝播します
スイッチ/ルーターを使用して、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。

マルチキャストルーターは、この情報を、次のようなマルチキャストルーティングプロトコルとともに使用します。
DVMRPまたはPIM、インターネットを介したIPマルチキャストをサポートします。

4.7.2.1IGMP設定

このページでは、IGMPスヌーピング関連の設定を提供します。
ページに反映されているように、ほとんどの設定はグローバルですが、ルーターポートの構成は現在のユニットに関連しています
ヘッダ。図4-7-7、図4-7-8、および図4-7-9のIGMPスヌーピング設定および情報画面が表示されます。

図4-7-7IGMPスヌーピン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
・IGMPスヌーピングステータス	IGMPスヌーピングを有効または無効にします。デフォルト値は「無効」です。
・IGMPスヌーピングバージョン	IGMPスヌーピング操作のバージョンを設定します。可能なバージョンは次のとおりです。 <div>■ V2：設定IGMPスヌーピングは、IGMPバージョン2をサポート。 ■ V3：設定IGMPスヌーピングは、IGMPバージョン3をサポートしていました。</div>

・IGMPスヌーピングレポート抑制	マルチキャスト対応ルーターに送信されるメンバーシップレポートトラフィックを制限します。 レポートの抑制を無効にすると、すべてのIGMPレポートがそのまま送信されます。 マルチキャスト対応ルーター。 デフォルトで有効になっています。
-------------------	--

ボタン

: クリックして変更を適用します。

図4-7-8IGMPスヌーピング情報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スヌーピングステータス	現在のIGMPスヌーピングステータスを表示します。
・IGMPスヌーピングバージョン	現在のIGMPスヌーピングバージョンを表示します。
・IGMPスヌーピングV2レポート抑制	現在のIGMPスヌーピングv2レポート抑制を表示します。

図4-7-9IGMPスヌーピング情報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
・エントリー番号	現在のエントリー番号を表示します
・VLANID	現在のVLANIDを表示します
・IGMPスヌーピング操作状態	現在のIGMPスヌーピング操作ステータスを表示します
・ルーターポートの自動学習	現在のルーターポートの自動学習を表示する
・クエリの堅牢性	現在のクエリの堅牢性を表示する

・クエリ間隔（秒）	現在のクエリ間隔を表示する
・クエリの最大応答 間隔（秒）	現在のクエリの最大応答間隔を表示します

・最後のメンバーのクエリ数	現在の最後のメンバーのクエリ数を表示します
・最後のメンバーのクエリ 間隔（秒）	現在の最後のメンバーのクエリ間隔を表示します
・即時休暇	現在の即時休暇を表示する
・変更	クリック パラメータを編集するには

4.7.2.2IGMPクエリア設定

このページでは、IGMPクエリア設定を提供します。図4-7-10および図4-7-11のIGMPクエリア設定画面が表示されます。

図4-7-10IGMPVLAN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
・VLANID	このドロップダウンリストからVLANIDを選択します。
・QuerierState	クエリア状態を有効または無効にします。 デフォルト値は「無効」です。
・Querierバージョン	ネットワーク上の他のデバイスとの互換性のためにクエリアのバージョンを設定します。 バージョン：2または3; デフォルト：2

ボタン

：クリックして変更を適用します。

図4-7-11IGMPクエリア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
• VLANID	現在のVLANIDを表示します
• QuerierState	現在のクエリア状態を表示します
• クエリアステータス	現在のクエリアステータスを表示します
• Querierバージョン	現在のクエリアのバージョンを表示する
• QuerierIP	現在のクエリアIPを表示します

4.7.2.3IGMP静的グループ

マルチキャストフィルタリングは、上記のように、IGMPスヌーピングおよびIGMPクエリメッセージを使用して動的に構成できます。
セクション。より厳密な制御が必要な特定のアプリケーションでは、マルチキャストサービスを静的に構成する必要がある場合があります。
マネージドスイッチ。まず、参加しているホストに接続されているすべてのポートを共通のVLANに追加してから、マルチキャストを割り当てます
そのVLANグループへのサービス。

- 静的マルチキャストアドレスが期限切れになることはありません。
- マルチキャストアドレスが特定のVLANのインターフェイスに割り当てられている場合、対応するトラフィックは次のようになります。
そのVLAN内のポートに転送されます。

図4-7-12および図4-7-13のIGMP静的グループ設定画面が表示されます。

図4-7-12IGMP静的グループの追加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
• VLANID	このドロップダウンリストからVLANIDを選択します
• グループIPアドレス	特定のマルチキャストサービスのIPアドレス
• メンバーポート	このドロップダウンリストからポート番号を選択します

: クリックしてIGMPルーターポートエントリを追加します。

図4-7-13IGMP静的グループ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
・VLANID	現在のVLANIDを表示します
・グループIPアドレス	現在のグループIPアドレスを表示します
・メンバーポート	現在のメンバーポートを表示します
・変更	クリック パラメータを編集するには

4.7.2.4IGMPグループテーブル

このページはマルチキャストデータベースを提供します。図4-7-14のIGMPグループテーブル画面が表示されます。

図4-7-14IGMPグループテーブル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
・VLANID	現在のVIDを表示する
・グループIPアドレス	特定のマルチキャストサービスのマルチキャストIPアドレスを表示する
・メンバーポート	現在のメンバーポートを表示する
・タイプ	表示されるメンバータイプには、選択に応じて静的または動的が含まれます オプション
・寿命（秒）	現在の生活を表示する

4.7.2.5IGMPルーター設定

ネットワーク接続によっては、IGMPスヌーピングが常にIGMPクエリアを見つけることができるとは限りません。したがって、IGMPクエリアは、ネットワークを介してマネージドのインターフェイス（ポートまたはトランク）に接続されている既知のマルチキャストルーター/スイッチです。スイッチを使用すると、インターフェイス（および指定したVLAN）を手動で構成して、でサポートされている現在のすべてのマルチキャストグループに参加できます。接続されたルーター。これにより、マルチキャストトラフィックがマネージドスイッチ内のすべての適切なインターフェイスに確実に渡されます。

図4-7-15および図4-7-16のIGMPルーター設定およびステータス画面が表示されます。

図4-7-15 ルーターポートの追加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
・VLANID	接続されたから来るすべてのマルチキャストトラフィックを伝播するVLANを選択します マルチキャストルーター。
・タイプ	ルーターのポートタイプを設定します。ルーターポートの種類は次のとおりです。 <div>■ 静的</div> <div>■ 禁止</div>
・静的ポートの選択	どのポートがルーターポートとして機能するかを指定します。ルーターポートはイーサネット上のポートです レイヤ3マルチキャストデバイスまたはIGMPクエリアにつながるスイッチ。
・ポート選択を禁止する	どのポートがルーターポートとして機能しないかを指定します

ボタン

：クリックしてIGMPルーターポートエントリを追加します。

図4-7-16 ルーターポート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
・VLANID	現在のVLANIDを表示します
・静的ポート	現在の静的ポートを表示する
・禁止されているポート	現在禁止されているポートを表示する
・変更	<div>クリック パラメータを編集するには</div> <div>クリック グループIDエントリを削除するには</div>

4.7.2.6IGMPルーターテーブル

このページはルーターテーブルを提供します。図4-7-17、図4-7-18、および図4-7-18の動的、静的、および禁止ルーターテーブルの画面図4-7-19が表示されます。

図4-7-17ダイナミックルーターテーブル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
•VLANID	現在のVLANIDを表示します
•ポート	現在の動的ルーターポートを表示する
•有効期限（秒）	現在の有効期限を表示します

図4-7-18静的ルーターテーブル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
•VLANID	現在のVLANIDを表示します
•ポートマスク	現在のポートマスクを表示する

図4-7-19禁止ルーターテーブル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
•VLANID	現在のVLANIDを表示します

4.7.2.7IGMP転送すべて

このページでは、IGMP ForwardAllを提供しています。[図4-7-20の](#)[すべて転送]画面が表示されます。

図4-7-20 すべての設定を転送する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
・VLANID	このドロップダウンリストからVLANIDを選択して、IGMPメンバーシップを割り当てます
・ポート	論理ポートのスイッチポート番号
・メンバーシップ	各インターフェイスのIGMPメンバーシップを選択します。 禁止： インターフェイスは、MVRを介してIGMPに自動的に参加することを禁じられています。 無し： インターフェイスはVLANのメンバーではありません。これに関連するパケット VLANはインターフェースによって送信されません。 静的： インターフェイスはIGMPのメンバーです。

ボタン

：クリックして変更を適用します。

4.7.3IGMPスヌーピング統計

このページでは、IGMPスヌーピング統計を提供します。[図4-7-20の](#)IGMPスヌーピング統計画面が表示されます。

図4-7-20すべての設定を転送する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
・トータルRX	現在の合計RXを表示
・有効なRX	現在有効なRXを表示する
・無効なRX	現在の無効なRXを表示する
・その他のRX	現在の他のRXを表示する
・RXを離れる	電流リープRXを表示
・レポートRX	現在のレポートRXを表示する
・一般的なクエリRX	現在の一般的なクエリRXを表示する
・特別なグループクエリ 処方箋	現在の特別なグループクエリRXを表示する
・特別グループと ソースクエリRX	現在の特別なグループとソースクエリRXを表示します

184

・TXを離れる	現在の休暇TXを表示します
・レポートTX	現在のレポートTXを表示する
・一般的なクエリTX	現在の一般的なクエリTXを表示する
・特別なグループクエリ TX	現在の特別なグループクエリTXを表示する
・特別グループと ソースクエリTX	現在の特別なグループとソースクエリTXを表示します

ボタン

：クリックして、IGMPスヌーピング統計をクリアします。

：クリックして、IGMPスヌーピング統計を更新します。

4.7.4MLDスヌーピング

4.7.4.1MLD設定

このページでは、MLDスヌーピング関連の設定を提供します。

ページに反映されているように、ほとんどの設定はグローバルですが、ルーターポートの構成は現在のユニットに関連しています

ヘッダ。図4-7-21、図4-7-22、および図4-7-23のMLDスヌーピング設定、情報、およびテーブル画面が表示されます。

図4-7-21MLDスヌーピング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
• MLDスヌーピングステータス	MLDスヌーピングを有効または無効にします。デフォルト値は「無効」です。
• MLDスヌーピングバージョン	MLDスヌーピング操作のバージョンを設定します。可能なバージョンは次のとおりです。 v1 : MLDスヌーピングでサポートされているMLDバージョン1を設定します。 v2 : MLDスヌーピングでサポートされているMLDバージョン2を設定します。
• MLDスヌーピングレポート抑制	マルチキャスト対応ルーターに送信されるメンバーシップレポートトラフィックを制限します。あなたがレポート抑制を無効にすると、すべてのMLDレポートがそのままマルチキャスト対応に送信されますルーター。デフォルトで有効になっています。

ボタン

: クリックして変更を適用します。

図4-7-22MLDスヌーピング情報スクリーンショット

186

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
・MLDスヌーピングステータス	現在のMLDスヌーピングステータスを表示します
・MLDスヌーピングバージョン	現在のMLDスヌーピングバージョンを表示する
・MLDスヌーピングレポート抑制	現在のMLDスヌーピングレポート抑制を表示します

図4-7-23MLDスヌーピングテーブル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
・エントリー番号	現在のエントリー番号を表示します
・VLANID	現在のVLANIDを表示します
・MLDスヌーピング操作状態	現在のMLDスヌーピング操作ステータスを表示します
・ルーターポートの自動学習	現在のルーターポートの自動学習を表示する
・クエリの堅牢性	現在のクエリの堅牢性を表示する
・クエリ間隔（秒）	現在のクエリ間隔を表示する
・クエリの最大応答間隔（秒）	現在のクエリの最大応答間隔を表示します
・最後のメンバーのクエリ数	現在の最後のメンバーのクエリ数を表示します
・最後のメンバーのクエリ間隔（秒）	現在の最後のメンバーのクエリ間隔を表示します
・即時休暇	現在の即時休暇を表示する
・変更	クリック パラメータを編集するには

4.7.4.2MLD静的グループ

図4-7-24および図4-7-25のMLDスタティックグループ設定画面が表示されます。

図4-7-24MLD静的グループ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
・VLANID	このドロップダウンリストからVLANIDを選択します
・グループIPアドレス	特定のマルチキャストサービスのIPアドレス
・メンバーポート	このドロップダウンリストからポート番号を選択します

ボタン

：クリックしてIGMPルーターポートエントリを追加します。

図4-7-25MLD静的グループ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
・VLANID	現在のVLANIDを表示します
・グループIPv6アドレス	現在のグループのIPv6アドレスを表示します
・メンバーポート	現在のメンバーポートを表示します
・変更	クリック パラメータを編集します。

4.7.4.3MLDグループテーブル

このページはMLDグループテーブルを提供します。図4-7-26のMLDグループテーブル画面が表示されます。

図4-7-26MLDグループテーブル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
・VLANID	現在のVIDを表示する
・グループIPアドレス	特定のマルチキャストサービスのマルチキャストIPアドレスを表示する
・メンバーポート	現在のメンバーポートを表示する
・タイプ	表示されるメンバータイプには、選択に応じて静的または動的が含まれます オプション
・寿命（秒）	現在の生活を表示する

4.7.4.4MLDルーター設定

ネットワーク接続によっては、MLDスヌーピングがMLDクエリアを常に見つけることができるとは限りません。したがって、MLDクエリアは、ネットワークを介してマネージドのインターフェイス（ポートまたはトランク）に接続されている既知のマルチキャストルーター/スイッチです。スイッチを使用すると、インターフェイス（および指定したVLAN）を手動で構成して、でサポートされている現在のすべてのマルチキャストグループに参加できます。接続されたルーター。これにより、マルチキャストトラフィックがマネージドスイッチ内のすべての適切なインターフェイスに確実に渡されます。図4-7-27および図4-7-28のMLDルーター設定画面が表示されます。

図4-7-27ルーターポートの追加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
・VLANID	接続されたから来るすべてのマルチキャストトラフィックを伝播するVLANを選択します マルチキャストルーター

・タイプ	ルーターのポートタイプを設定します。ルーターポートの種類は次のとおりです。 <div>静的</div> <div>禁止する</div>
・静的ポートの選択	どのポートがルーターポートとして機能するかを指定します。ルーターポートはイーサネット上のポートです レイヤ3マルチキャストデバイスまたはMLDクエリアにつながるスイッチ。
・ポート選択を禁止する	どのポートがルーターポートとして機能しないかを指定します

ボタン

：クリックしてMLDルーターポートエントリを追加します。

図4-7-28ルーターポート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
・VLANID	現在のVLANIDを表示します
・静的ポート	現在の静的ポートを表示する
・禁止されているポート	現在禁止されているポートを表示する
・変更	<div>クリック パラメータを編集するには</div> <div>クリック グループIDエントリを削除するには</div>

4.7.4.5MLDルーターテーブル

このページはルーターテーブルを提供します。図4-7-29、図4-7-30、および図4-7-30の動的、静的、および禁止ルーターテーブルの画面
図4-7-31が表示されます。

図4-7-29ダイナミックルーターテーブル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
•VLANID	現在のVLANIDを表示します
•ポート	現在の動的ルーターポートを表示する
•有効期限（秒）	現在の有効期限を表示します

図4-7-30静的ルーターテーブル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
•VLANID	現在のVLANIDを表示します
•ポートマスク	現在のポートマスクを表示する

図4-7-31禁止ルーターテーブル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
•VLANID	現在のVLANIDを表示します
•ポートマスク	現在のポートマスクを表示する

4.7.4.6MLD転送すべて

このページでは、MLD ForwardAllを提供します。図4-7-32の[すべて転送]画面が表示されます。

このページには、次のフィールドが含まれています。

192

このページでは、MLDスヌーピング統計を提供します。図4-7-33のMLDSnoopingStatics画面が表示されます。

図4-7-33すべての設定を転送する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
・トータルRX	現在の合計RXを表示
・有効なRX	現在有効なRXを表示する
・無効なRX	現在の無効なRXを表示する
・その他のRX	現在の他のRXを表示する
・RXを離れる	電流リープRXを表示
・レポートRX	現在のレポートRXを表示する
・一般的なクエリRX	現在の一般的なクエリRXを表示する

・特別なグループクエリ 処方箋	現在の特別なグループクエリRXを表示する
・特別なグループと ソースクエリRX	現在の特別なグループとソースクエリRXを表示します
・TXを離れる	現在の休暇TXを表示します
・レポートTX	現在のレポートTXを表示する
・一般的なクエリTX	現在の一般的なクエリTXを表示する
・特別なグループクエリ TX	現在の特別なグループクエリTXを表示する
・特別なグループと ソースクエリTX	現在の特別なグループとソースクエリTXを表示します

ボタン

：クリックしてMLDスヌーピング統計をクリアします。

：クリックしてMLDスヌーピング統計を更新します。

4.7.6マルチキャストスロットリング設定

マルチキャストスロットリングは、ポートが同時に参加できるマルチキャストグループの最大数を設定します。最大のときポートでグループの数に達すると、スイッチは2つのアクションのいずれかを実行できます。「拒否」または「置換」のいずれか。アクションがに設定されている場合拒否すると、新しいマルチキャスト参加レポートはすべて削除されます。アクションが置換するように設定されている場合、スイッチは既存のものをランダムに削除しますグループ化し、新しいマルチキャストグループに置き換えます。

マルチキャストプロファイルを設定したら、それらをマネージドスイッチのインターフェイスに割り当てることができます。また、あなたは設定することができますインターフェイスが同時に参加できるマルチキャストグループの数を制限するマルチキャストスロットリング番号。MAXグループと

[図4-7-34](#)および[図4-7-35](#)の情報画面が表示されます。

図4-7-34最大グループとアクション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
• IPタイプ	このドロップダウンリストからIPv4またはIPv6を選択します
• ポート選択	このドロップダウンリストからポート番号を選択します
• 最大グループ	インターフェイスが同時に参加できるマルチキャストグループの最大数を設定します 時間。 範囲：0-256; デフォルト：256
• アクション	のマルチキャストグループの最大数が発生したときに実行するアクションを設定します

インターフェイスを超えました。

(デフォルト : 拒否)

~~-拒否~~-新しいマルチキャストグループ参加レポートは削除されます

~~-置換~~-新しいマルチキャストグループが既存のグループを置き換えます

ボタン

: クリックして変更を適用します。

図4-7-3SIGMPポートの最大グループ情報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
・ポート	論理ポートのスイッチポート番号
・最大グループ	現在の最大グループを表示します
・アクション	現在のアクションを表示する

4.7.7マルチキャストフィルター

特定のスイッチアプリケーションでは、管理者はエンドユーザーが利用できるマルチキャストサービスを制御したい場合があります。にとって
たとえば、IP / TVサービスは特定のサブスクリプションプランに基づいています。マルチキャストフィルタリング機能は、次の方法でこの要件を満たします。
スイッチポート上の指定されたマルチキャストサービスへのアクセスを制限します。

マルチキャストフィルタリングを使用すると、で許可または拒否されるマルチキャストグループを指定するスイッチポートにプロファイル割り当てることができます。
ポート。マルチキャストフィルタープロファイルには、1つ以上のマルチキャストアドレスまたは1つの範囲のマルチキャストアドレスを含めることができます。ただし、プロファイルは1つだけです。
ポートに割り当てられます。有効にすると、ポートで受信したマルチキャスト参加レポートがフィルタープロファイルと照合されます。要求された場合
マルチキャストグループが許可されている場合、マルチキャスト参加レポートは通常どおり転送されます。要求されたマルチキャストグループが拒否された場合、
マルチキャスト参加レポートは削除されます。

マルチキャストプロファイル番号を作成したら、アクセスをフィルタリングおよび設定するようにマルチキャストグループを構成できます。
モード。

コマンドの使用法

・各プロファイルには1つのアクセスモードしかありません。いずれかの許可または拒否。

- アクセスモードが**許可**に設定されている場合、マルチキャストグループがに含まれるときにマルチキャスト参加レポートが処理されます。
制御範囲。
- アクセスモードが**拒否**に設定されている場合、マルチキャスト参加レポートは、マルチキャストグループがに含まれていない場合にのみ処理されます。
制御範囲。

4.7.7.1 マルチキャストプロファイル設定

図4-7-36および図4-7-37の[プロファイルの追加]画面と[プロファイルステータス]画面が表示されます。

図4-7-36 プロファイル設定の追加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
・IPタイプ	このドロップダウンリストからIPv4またはIPv6を選択します
・プロファイルインデックス	この特定のプロファイルのIDを示します
・からのグループ	プロファイルに含めるマルチキャストグループを指定します。マルチキャストグループを指定します 開始IPアドレスを入力して範囲を指定します。
・グループ化する	プロファイルに含めるマルチキャストグループを指定します。マルチキャストグループを指定します 終了IPアドレスを入力して範囲を指定します。
・アクション	プロファイルのアクセスモードを設定します。いずれかの 許可 または 拒否 。 <div><div>- 許可</div>マルチキャスト参加レポートは、マルチキャストグループが該当する場合に処理されます 制御範囲内。<div>- 拒否</div>アクセスモードがに設定されている場合、マルチキャスト参加レポートは マルチキャストグループが制御対象にない場合に処理されます 範囲。</div>
ボタン	<div>：クリックしてマルチキャストプロファイルエントリを追加します。</div>

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	
・インデックス	現在のインデックスを表示する	
・IPタイプ	現在のIPタイプを表示します	
・からのグループ	から現在のグループを表示します	
・グループ化する	現在のグループを表示して	
・アクション	現在のアクションを表示する	
・変更	クリック	パラメータを編集します。
	クリック	MLD / IGMPプロファイルエントリを削除します。

4.7.7.2IGMPフィルター設定

図4-7-38および図4-7-39の[フィルター設定]画面と[ステータス]画面が表示されます。

図4-7-38フィルター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
・ポート選択	このドロップダウンリストからポート番号を選択します
・フィルタープロファイルID	このドロップダウンリストからフィルタープロファイルIDを選択します

ボタン

: クリックして変更を適用します。

図4-7-39ポートフィルター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	
・ポート	現在のポートを表示する	
・フィルタープロファイルID	現在のフィルタープロファイルIDを表示します	
・アクション	クリック	詳細プロファイルパラメータを表示するには
	クリック	IGMPフィルタープロファイルエントリを削除するには

4.7.7.3MLDフィルター設定

図4-7-40および図4-7-41の[フィルター設定]画面と[ステータス]画面が表示されます。

図4-7-40フィルター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
・ポート選択	このドロップダウンリストからポート番号を選択します
・フィルタープロファイルID	このドロップダウンリストからフィルタープロファイルIDを選択します

ボタン

: クリックして変更を適用します。

図4-7-41ポートフィルター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	
•ポート	現在のポートを表示する	
•フィルタープロファイルID	現在のフィルタープロファイルIDを表示します	
•アクション	クリック	詳細プロファイルパラメータを表示するには
	クリック	MLDフィルタープロファイルエントリを削除するには

4.8サービス品質

4.8.1QoSを理解する

Quality of Service (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優先順位付け機能です。QoS

マルチメディア、ビデオ、プロトコル固有など、さまざまな種類のトラフィックにさまざまなグレードのネットワークサービスを割り当てることができます。

タイムクリティカルなファイルバックアップトラフィック。

QoSは、帯域幅の制限、遅延、損失、およびジッターを低減します。また、データ配信の信頼性が向上し、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。スイッチでの処理方法を正確に定義できます

選択したアプリケーションとトラフィックの種類。

システムでQoSを使用して、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进行分类します。
- トラフィックに優先順位を割り当てる（たとえば、タイムクリティカルまたはビジネスクリティカルなアプリケーションに高い優先順位を設定するため）。
- 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。
- 最小化することにより、ビデオ会議やVoice over 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
遅延とジッター。
- 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応じてパフォーマンスを維持します。
- ネットワークに帯域幅を絶えず追加する必要性を減らします。
- ネットワークの輻輳を管理します。

ネットワークにQoSを実装するには、次のアクションを実行する必要があります。

- 1.1。 トラフィックに適用される優先度を決定するためのサービスレベルを定義します。
- 2.2。 分類子を適用して、着信トラフィックがどのように分類され、スイッチによって処理されるかを決定します。
- 3.3。 サービスレベルと分類子を関連付けるQoSプロファイルを作成します。
- 4.4。 QoSプロファイルをポートに適用します。

マネージドスイッチのQoSページには、802.1pモード、DSCPモード、またはポートベースモードの3種類のQoSモードが含まれています。

選択できます。3つのモードはどちらも、出力キューを決定するためにパケット内の事前定義されたフィールドに依存しています。

- **802.1pタグ優先モード**—出力キューの割り当ては、IEEE 802.1p VLAN優先タグによって決定されます。
- **IP 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。
- **ポートベース優先モード**—指定された高優先ポートから受信したパケットはすべて高優先として扱われます
パケット。

マネージドスイッチは8つの優先度レベルのキューをサポートします。キューのサービスレートはWRR（ウェイトラウンドロビン）に基づいています。およびWFQ（Weighted Fair Queuing）アロリズム。高優先度と低優先度のWRR比は、「4 : 1と8 : 1」に設定できます。

4.8.2 一般

4.8.2.1 QoSプロパティ

図4-8-1および図4-8-2のQoSグローバル設定および情報画面が表示されます。

図4-8-1 QoSグローバル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
・ QoSモード	QoSモードを有効または無効にします

ボタン

: クリックして変更を適用します。

■ QoSの情報

図4-8-2QoS情報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
・ QoSモード	現在のQoSモードを表示します

4.8.2.2QoSポート設定

図4-8-2および図4-8-3の[QoSポート設定とステータス]画面が表示されます。

図4-8-2QoSポート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
・ポート選択	このドロップダウンリストからポート番号を選択します
・ CoS値	このドロップダウンリストからCoS値を選択します
・備考CoS	備考CoSを無効または有効にする
・備考DSCP	リマークDSCPを無効または有効にする

・RemarkIPPrecedenceリマークIP優先順位を無効または有効にします

ボタン

: クリックして変更を適用します。

■ QoSのポートステータス

図4-8-3QoSポート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
・ポート	論理ポートのスイッチポート番号
・CoS値	現在のCoS値を表示します
・備考CoS	現在の備考CoSを表示する
・備考DSCP	現在の備考DSCPを表示します
・リマークIP優先順位	現在のリマークIP優先順位を表示します

4.8.2.3キュー設定

図4-8-4および図4-8-5の[キューテーブル]および[情報]画面が表示されます。

図4-8-4キューテーブル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
•キュー	現在のキューIDを表示します
•厳格な優先順位	このスイッチポートでスケジューラモードが「StrictPriority」であるかどうかを制御します
•WRR	このスイッチポートでスケジューラモードを「加重」するかどうかを制御します
•重量	このキューの重みを制御します。この値は1〜100に制限されています。この「SchedulerMode」が「Weighted」に設定されている場合にのみ、パラメーターが表示されます。
•WRR帯域幅の%	各キューの現在の帯域幅を表示します

ボタン

: クリックして変更を適用します。

図4-8-5キュー情報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
•情報名	現在のキューメソッド情報を表示します
•情報価値	現在のキュー値情報を表示します

4.8.2.4CoSマッピング

図4-8-6および図4-8-7のCoStoQueueおよびQueueetoCoSマッピング画面が表示されます。

図4-8-6CoSからキューおよびキューからCoSへのマッピン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
・キュー	このドロップダウンリストからキュー値を選択します
・サービスクラス	このドロップダウンリストからCoS値を選択します

ボタン

: クリックして変更を適用します。

■ CoSのマッピング

図4-8-7CoSマッピン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
・ CoS	現在のCoS値を表示します

・キューへのマッピング	キューへの現在のマッピングを表示する
・キュー	現在のキュー値を表示します
・CoSへのマッピング	CoSへの現在のマッピングを表示します

4.8.2.5DSCPマッピング

図4-8-8および図4-8-9の[DSCPtoQueue]および[QueuetoDSCPMapping]画面が表示されます。

図4-8-8DSCPからキューおよびキューからDSCPへのマッピン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
・キュー	このドロップダウンリストからキュー値を選択します
・DSCP	このドロップダウンリストからDSCP値を選択します

ボタン

：クリックして変更を適用します。

図4-8-9DSCPマッピン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
• DSCP	現在のCoS値を表示します
•キューへのマッピング	キューへの現在のマッピングを表示する
•キュー	現在のキュー値を表示します
• DSCPへのマッピング	DSCPへの現在のマッピングを表示します

4.8.2.6IP優先順位マッピング

図4-8-10および図4-8-11の[IPPrecedence toQueue]および[Queueeto IP PrecedenceMapping]画面が表示されます。

図4-8-10IP Precedence toQueueおよびQueueeto IP PrecedenceMapping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
・キュー	このドロップダウンリストからキュー値を選択します
・IPの優先順位	このドロップダウンリストからIP優先順位の値を選択します

ボタン

: クリックして変更を適用します。

図4-8-11IP優先順位マッピン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
・IPの優先順位	現在のCoS値を表示します
・キューへのマッピング	キューへの現在のマッピングを表示する
・キュー	現在のキュー値を表示します
・IPへのマッピング 優先順位	IP優先順位への現在のマッピングを表示します

4.8.3.1グローバル設定

図4-8-12および図4-8-13の「基本モードのグローバル設定およびQoS情報」画面が表示されます。

図4-8-12基本モードのグローバル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
信頼モード	QoSモードを設定します

ボタン

: クリックして変更を適用します。

■ QoSの情報

図4-8-13QoS情報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
信頼モード	現在のQoSモードを表示します

4.8.3.2ポート設定

図4-8-14および図4-8-15の「QoSポート設定およびステータス」画面が表示されます。

図4-8-14基本モードのグローバル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
・ポート	このドロップダウンリストからポート番号を選択します
・信頼モード	信頼モードを有効または無効にします

ボタン

：クリックして変更を適用します。

図4-8-15QoSポート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
・ポート	論理ポートのスイッチポート番号
・信頼モード	現在の信頼タイプを表示します

4.8.4レート制限

このページで、スイッチポートのスイッチポートレート制限を設定します。

4.8.4.1入力帯域幅制御

このページでは、入力帯域幅のプリアンブルを選択できます。の入力帯域幅制御設定およびステータス画面
[図4-8-16](#)と[図4-8-17](#)が表示されます。

図4-8-16入力帯域幅制御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
•ポート	このドロップダウンリストからポート番号を選択します
•州	ポートレートポリサーを有効または無効にします。デフォルト値は「無効」です。
•レート (Kbps)	ポートポリサーのレートを設定します。デフォルト値は「無制限」です。有効値の範囲は0から1000000です。

ボタン

: クリックして変更を適用します。

図4-8-17入力帯域幅制御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
•ポート	論理ポートのスイッチポート番号
•入力レート制限 (Kbps)	現在の入力レート制限を表示します

4.8.4.2出力帯域幅制御

このページでは、出力帯域幅のプリアンブルを選択できます。の出力帯域幅制御設定およびステータス画面 [図4-8-18](#)と [図4-8-19](#)が表示されます。

図4-8-18出力帯域幅制御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
•ポート	このドロップダウンリストからポート番号を選択します
•州	ポートレートポリサーを有効または無効にします。デフォルト値は「無効」です。
•レート (Kbps)	ポートポリサーのレートを設定します。デフォルト値は「無制限」です。有効値の範囲は0から1000000です。

ボタン

: クリックして変更を適用します。

図4-8-19出力帯域幅制御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
•ポート	論理ポートのスイッチポート番号
•出力レート制限 (Kbps)	現在の出力レート制限を表示します

4.8.4.3出力キュー

図4-8-20および図4-8-21の[EgressQueue Bandwidth ControlSettings]および[Status]画面が表示されます。

図4-8-20出力キューの帯域幅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
•ポート	このドロップダウンリストからポート番号を選択します

・キュー ・州	このドロップダウンリストからキュー番号を選択します ポートレートポリサーを有効または無効にします。デフォルト値は「無効」です。
・CIR（Kbps）	ポートポリサーのCIRを構成します。デフォルト値は「無制限」です。有効 値の範囲は0から1000000です。

ボタン

：クリックして変更を適用します。

図4-8-21出力キュー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
・キューID	現在のキューIDを表示します
・レート制限（Kbps）	現在のレート制限を表示します

4.8.5音声VLAN

4.5.8.1音声VLANの概要

このページで、スイッチポートのスイッチポートレート制限を設定します。

音声VLANは、ユーザーの音声データトラフィック用に特別に構成されています。音声VLANを設定し、接続されているポートを追加する
音声機器を音声VLANに接続すると、ユーザーは音声データのQoS（Quality of Service）サービスを構成し、改善することができます。
通話品質を確保するための音声データトラフィック送信の優先順位。

スイッチは、送信元MACアドレスに従って、データトラフィックが指定された機器からの音声データトラフィックであるかどうかを判断できます。
ポートに入るデータパケットのフィールド。システム定義の音声に準拠した送信元MACアドレスを持つパケット
機器OUI（Organizationally Unique Identifier）は、音声データトラフィックと見なされ、Voiceに送信されます。
VLAN。

構成はMACアドレスに基づいており、すべての音声機器が情報を送信するメカニズムを取得します。
ネットワークを介して、固有のMACアドレスを取得します。VLANは、指定されたMACに属するアドレスをトレースします。これにより、
VLANを使用すると、音声機器は、物理的に再配置されたときに常に音声VLANに属することができます。VLANの最大の利点
機器は、指定された場所で送信される音声トラフィックに応じて、音声VLANに自動的に配置できます。
優先。一方、音声機器が物理的に再配置された場合、それはそれ以上のことなく音声VLANに属します。

これは、スイッチポート以外の音声機器に基づいているためです。

音声VLAN機能を使用すると、音声トラフィックを音声VLANで転送してから、
スイッチを分類して、ネットワークトラフィックにスケジュールすることができます。**2つあることをお勧めします**
ポート上のVLAN -1つは音声用、もう1つはデータ用です。

IPデバイスをスイッチに接続する前に、**IP電話で音声VLANを設定する必要があります**
正しくID。独自のGUIを使用して構成する必要があります。

4.8.5.2プロパティ

音声VLAN機能を使用すると、音声トラフィックを音声VLANで転送できます。その後、スイッチを分類して、
ネットワークトラフィックにスケジュールされています。ポートには2つのVLANを配置することをお勧めします。1つは音声用、もう1つはデータ用です。

IPデバイスをスイッチに接続する前に、IP電話は音声VLANIDを正しく設定する必要があります。そのはず
独自のGUIを介して構成されます。このページでは、入力帯域幅のプリアンブルを選択できます。入力帯域幅制御
[図4-8-22](#)および[図4-8-23](#)の設定/ステータス画面が表示されます。

図4-8-22プロパティのスクリーンショット

このページには次のものが含まれています:

オブジェクト	説明	
•音声VLANの状態	音声VLANモードの動作を示します。Mを無効にする必要があります	STP機能
	音声VLANを有効にする前に。ingの競合を回避できます	ressフィルター。可能
	モードは次のとおりです。	
•音声VLANID	■ ■ 有効	音声VLANモードの動作を有効にします。
	■ ■ 無効	音声VLANモードの操作を無効にします
	音声VLANIDを示します。そうすべき	システム内で一意のVLANIDであり、 各ポートのPVIDと等しくすることはできません。紛争防止 管理VID、MVR VID、PVID、等 許容範囲は1〜4095です。

•備考CoS / 802.1p	このドロップダウンリストから802.1p値を選択します
• 1pの発言	802.1prを有効または無効にする emark
•エージングタイム（30-65536分）	VoIPトラフィックが発生したときにポートが音声VLANから削除されるまでの時間 ポートで受信されなくなりました。 (デフォルト：1440分)。

ボタン

: クリックして変更を適用します。

図4-8-23プロパティ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
•音声VLANの状態	現在の音声VLANの状態を表示します。
•音声VLANID	現在の音声VLANIDを表示します。
•備考CoS / 802.1p	現在の備考CoS / 802.1pを表示します。
• 1pの発言	現在の1pコメントを表示します。
•老化	現在のエージングタイムを表示します。

4.8.5.3テレフォニーOUI MAC設定

このページでVOICEVLANOUIテーブルを設定します。テレフォニーOUI MACに設定画面図4-8-24と図4-8-25
現れる。

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
・OUIアドレス	テレフォニーOUIアドレスは、によってベンダーに割り当てられたグローバルに一意の識別子です。 IEEE。 長さは6文字で、入力形式は「xx：xx：xx」（xは16進数）である必要があります。 桁）。
・説明	VoIPデバイスを識別するユーザー定義のテキスト

Buttons

：クリックして音声VLANOUI設定を追加します。

図4-8-25音声VLANOUIグループのスクリーンショット

このページには次の内容が含まれています。

オブジェクト	説明
・OUIアドレス	現在のOUIアドレスを表示します
・説明	Display現在の説明ption
・変更	クリック音声VLANOUIグループパラメータを編集するには
	クリック音声VLANOUIグループパラメータを削除するには

4.8.5.4テレフォニーOUIポート設定

音声VLAN機能により、音声VLANでの音声トラフィック転送が可能になり、スイッチでネットワークを分類およびスケジュールできます。トラフィック。ポートには2つのVLANを配置することをお勧めします。1つは音声用、もう1つはデータ用です。IPデバイスをに接続する前にスイッチを押すと、IP電話は音声VLANIDを正しく設定する必要があります。独自のGUIを使用して構成する必要があります。テレフォニー [図4-8-26](#)および[図4-8-27のOUIMAC](#)設定画面が表示されます。

図4-8-26 音声VLANポート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
•ポート	このドロップダウンリストからポート番号を選択します
•州	音声VLANポート設定を有効または無効にします。デフォルト値は「無効」です。
• CoSモード	現在のCoSモードを選択します

ボタン

: クリックして変更を適用します。

図4-8-27 音声VLANポートの状態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
•ポート	論理ポートのスイッチポート番号
•州	現在の状態を表示する
• CoSモード	現在のCoSモードを表示します

4.9セキュリティ

このセクションでは、ユーザーアクセスや管理制御など、マネージドスイッチのアクセスを制御します。

[セキュリティ]ページには、次の主要トピックへのリンクが含まれています。

- 802.1x

- RADIUSサーバー
- TACACS +サーバー
- AAA
- アクセス
- 管理アクセス方法
- DHCPスヌーピング
- 動的ARP検査
- IPソースガード
- ポートセキュリティ
- DoS
- ストロームコントロール

4.9.1 802.1X

802.1X（ポートベース）認証の概要

802.1Xの世界では、ユーザーはサブリカントと呼ばれ、スイッチはオーセンティケーターであり、RADIUSサーバーは認証サーバー。スイッチはman-in-the-middleとして機能し、サブリカント間で要求と応答を転送します

および認証サーバー。サブリカントとスイッチの間で送信されるフレームは、EAPOLと呼ばれる特別な802.1Xフレームです。

（EAP over LAN）フレーム。EAPOLフレームは、EAP PDU（RFC3748）をカプセル化します。スイッチとの間で送信されるフレーム

RADIUSサーバーはRADIUS/パケットです。RADIUS/パケットは、EAP PDUを他の属性と一緒にカプセル化します。

スイッチのIPアドレス、名前、およびスイッチ上のサブリカントのポート番号。EAPは非常に柔軟性があり、さまざまなことが可能です。

MD5-Challenge、PEAP、TLSなどの認証方法。重要なことは、オーセンティケーター（スイッチ）がそうではないということです

サブリカントと認証サーバーが使用している認証方法、または情報の数を知る必要があります

特定のメソッドには交換フレームが必要です。スイッチは、フレームのEAP部分を単にカプセル化します。

関連するタイプ（EAPOLまたはRADIUS）を転送します。

認証が完了すると、RADIUSサーバーは成功または失敗の表示を含む特別なパケットを送信します。その上

この決定をサブリカントに転送すると、スイッチはそれを使用して、に接続されているスイッチポートのトラフィックを開いたりブロックしたりします。

サブリカント。

ユーザー認証の概要

ローカルを使用した管理アクセスのためにシステムにログインしているユーザーを認証するようにマネージドスイッチを構成することができます

または、telnetやWebブラウザなどのリモート認証方法。このマネージドスイッチは安全なネットワークを提供します

次のオプションを使用した管理アクセス：

221

- リモート認証ダイヤルインユーザーサービス（RADIUS）
- ターミナルアクセスコントローラアクセス制御システムプラス（TACACS +）
- ローカルユーザー名と特権レベルの制御

4.9.1.1 IEEE802.1Xポートベース認証について

IEEE 802.1X標準は、許可されていないものを制限する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を定義しています。

クライアントは、公的にアクセス可能なポートを介してLANに接続できません。認証サーバーは各クライアントを認証します

スイッチまたはLANが提供するサービスを利用可能にする前に、スイッチポートに接続します。

クライアントが認証されるまで、802.1Xアクセス制御はLANを介した拡張認証プロトコル（EAPOL）のみを許可します

クライアントが接続されているポートを介したトラフィック。認証が成功すると、通常のトラフィックはポート。

このセクションには、次の概念情報が含まれています。

- デバイスの役割
- 認証の開始とメッセージ交換
- 許可された状態と許可されていない状態のポート

■ デバイスの役割

802.1Xポートベースの認証では、ネットワーク内のデバイスには、以下に示す特定の役割があります。

図4-9-1

- **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、からの要求に応答するデバイス（ワークステーション）
スイッチ。ワークステーションは、Microsoft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
WindowsXPオペレーティングシステム。（クライアントはIEEE 802.1X仕様のサブリカントです。）
- **認証サーバー**—クライアントの実際の認証を実行します。認証サーバーは、
クライアントのIDであり、クライアントがLANおよびスイッチサービスへのアクセスを許可されているかどうかをスイッチに通知します。
スイッチはプロキシとして機能するため、認証サービスはクライアントに対して透過的です。このリリースでは、リモート
Extensible Authentication Protocol（EAP）を備えた認証ダイヤルインユーザーサービス（RADIUS）セキュリティシステム
サポートされている認証サーバーは拡張機能のみです。Cisco Secure Access ControlServerバージョン3.0で使用できます。
RADIUSは、安全な認証情報がクライアント間で交換されるクライアント/サーバーモデルで動作します。
RADIUSサーバーと1つ以上のRADIUSクライアント。
- **スイッチ（802.1Xデバイス）** —クライアントの認証ステータスに基づいてネットワークへの物理アクセスを制御します。
スイッチは、クライアントと認証サーバー間の仲介（プロキシ）として機能し、IDを要求します
クライアントからの情報、認証サーバーでその情報を確認し、クライアントに応答を中継します。

スイッチには、Extensibleのカプセル化とカプセル化解除を担当するRADIUSクライアントが含まれています
認証プロトコル（EAP）フレームと認証サーバーとの相互作用。スイッチがEAPOLを受信したとき
フレームを作成して認証サーバーに中継すると、イーサネットヘッダーが削除され、残りのEAPフレームは
RADIUS形式で再カプセル化されます。EAPフレームは、カプセル化中に変更または検査されません。
認証サーバーは、ネイティブフレーム形式内でEAPをサポートする必要があります。スイッチがからフレームを受信したとき
認証サーバーの場合、サーバーのフレームヘッダーが削除され、EAPフレームが残ります。このフレームは、
イーサネットとクライアントに送信されます。

■ 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 port-control auto`を使用してポートで認証を有効にした場合
インターフェイスコンフィギュレーションコマンド。スイッチは、ポートリンク状態が遷移すると判断したときに認証を開始する必要があります。
下から上へ。次に、EAP要求/IDフレームをクライアントに送信してIDを要求します（通常、スイッチは
最初のID/要求フレームとそれに続く認証情報の1つ以上の要求）。フレームを受け取ると、
クライアントはEAP応答/IDフレームで応答します。

ただし、起動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、クライアントは開始できます
EAPOL開始フレームを送信することによる認証。これにより、スイッチはクライアントのIDを要求します。

ネットワークアクセスデバイスで802.1Xが有効化またはサポートされていない場合、からのEAPOLフレームは
クライアントは削除されます。クライアントが3回試行してもEAP要求/IDフレームを受信しない場合
認証を開始するために、クライアントはポートが許可された状態にあるかのようにフレームを送信します。のポート
許可された状態は、事実上、クライアントが正常に認証されたことを意味します。

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、クライアントとの間でEAPフレームを渡します。
認証が成功または失敗するまで、認証サーバー。認証が成功すると、スイッチポートは次のようになります。
承認されました。

EAPフレームの具体的な交換は、使用されている認証方法によって異なります。「[図4-9-2](#)」はメッセージを示しています
RADIUSサーバーでワンタイムパスワード（OTP）認証方式を使用してクライアントによって開始された交換。

■ **許可された状態と許可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。ポートは無許可で開始します
状態。この状態の間、ポートは802.1Xプロトコルパケットを除くすべての入力トラフィックと出力トラフィックを許可しません。クライアントが
認証に成功すると、ポートは許可された状態に移行し、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します。

802.1Xをサポートしないクライアントが無許可の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IDを要求します。に
この状況では、クライアントは要求に応答せず、ポートは無許可の状態のままであり、クライアントは許可されません
ネットワークへのアクセス。

対照的に、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することによる認証プロセス。応答が受信されない場合、クライアントは要求を送信します
固定回数。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に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ると（認証サーバーからAcceptフレームを受信すると）、ポートの状態は次のように変わります。
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通過できるようになります。認証が失敗した場合、ポートは残ります
許可されていない状態ですが、認証を再試行できます。認証サーバーに到達できない場合、スイッチは
リクエストを再送信します。指定された回数試行してもサーバーから応答がない場合、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ログオフ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アップからダウンに移行した場合、またはEAPOLログオフフレームを受信した場合、ポートは無許可に戻ります
状態。

4.9.1.2802.1X設定

このページでは、IEEE802.1X認証システムを構成できます。

IEEE 802.1X標準は、ネットワークへの不正アクセスを防止するポートベースのアクセス制御手順を定義しています。
ユーザーが最初に認証のために資格情報を送信することを要求します。1つ以上の中央サーバーであるバックエンドサーバーが決定します
ユーザーがネットワークへのアクセスを許可されているかどうか。これらのバックエンド（RADIUS）サーバーは、「**セキュリティ**」→**802.1X**で構成されます。
アクセス制御→**802.1X設定**ページ。IEEE802.1X標準はポートベースの操作を定義していますが、非標準のバリエーションです
以下で説明するように、セキュリティの制限を克服します。

図4-9-3および図4-9-4の802.1X設定および情報画面が表示されます。

図4-9-3802.1X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
• 802.1X	NASがスイッチでグローバルに有効か無効かを示します。グローバルに無効になっている場合、 すべてのポートでフレームの転送が許可されます。

ボタン

：クリックして変更を適用します。

図4-9-4802.1X情報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
・802.1X	現在の802.1X状態を表示します

4.9.1.3802.1Xポート設定

このページでは、IEEE802.1Xポート設定を構成できます。図4-9-5および図の802.1Xポート設定画面4-9-6が表示されます。

図4-9-5802.1Xポート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
・ポート	このドロップダウンリストからポートを選択します
・モード	NASがグローバルに有効になっている場合、この選択によりポートの認証モードが制御されます。 次のモードを使用できます。 <div><div>■ 認証なし</div><div>■ 認証</div><div>■ 強制承認</div></div> このモードでは、スイッチは次の場合に1つのEAPOL成功フレームを送信します。

ポートリンクが起動し、ポート上のすべてのクライアントがネットワークを許可されます
認証なしのアクセス。

■ 強制的に無許可

このモードでは、スイッチは次の場合に1つのEAPOL障害フレームを送信します。
ポートリンクが起動し、ポート上のすべてのクライアントがネットワークを許可されなくなります
アクセス。

- ・再認証

有効にする
- チェックすると、正常に認証されたサブリカント/クライアントが再認証されます
再認証期間で指定された間隔の後。の再認証
802.1X対応ポートを使用して、新しいデバイスがに接続されているかどうかを検出できます。

ポートを切り替えるか、サブリカントが接続されていない場合。

- ・再認証

限目
- 接続されたクライアントが必要になるまでの期間を秒単位で決定します
再認証されました。これは、[再認証を有効にする]チェックボックスがオンの場合にのみアクティブになります
チェックしました。
有効な値は30～65535秒の範囲です。
- ・静かな期間
- サブリカント認証の失敗時にサイレントを維持する時間を設定します。
- ・サブリカント期間
- サブリカントがEAP要求/識別フレームを再送信する間隔を設定します。
- ・最大リクエスト

再試行
- スイッチがEAPOLRequestIdentityフレームを送信する回数
ゲストVLANへの入力を検討する前に応答なしで調整されます
この設定。
値は、ゲストVLANオプションがグローバルに有効になっている場合にのみ変更できます。

ボタン

: クリックして変更を適用します。

図4-9-6802.1Xポート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
--------	----

•ポート	論理ポートのスイッチポート番号。
•モード（pps）	現在のモードを表示します。
•ステータス（pps）	現在のステータスを表示します。
•定期的 再認証	現在の定期的な再認証を表示します。

227

•再認証 限目	現在の再認証期間を表示します。
•静かな期間	現在の静止期間を表示します。
•サブリカントタイムアウト	現在のサブリカントのタイムアウトを表示します。
•最大。EAPリクエスト	現在の最大値を表示します。EAPリクエスト。
•変更	クリック 802.1Xポート設定パラメータを編集します。

4.9.1.4ゲストVLAN設定

概要概要

ゲストVLAN対応ポートのリンクがアップすると、スイッチはEAPOLリクエストIDフレームの送信を開始します。番号の場合

そのようなフレームの送信の最大数を超過しています。再認証します。その間、カウントされ、EAPOLフレームは受信されていません。

スイッチはゲストVLANの入力を検討します。EAPOLリクエストIDフレームの送信間隔が設定されます

EAPOLタイムアウトあり。EAPOL Seenが有効になっている場合にゲストVLANを許可すると、ポートはゲストVLANに配置されます。無効になっている場合、

スイッチは最初にその履歴をチェックして、EAPOLフレームが以前にポートで受信されたかどうかを確認します（この履歴は次の場合にクリアされます）

ポートリンクがダウンするか、ポートの管理状態が変更されます）。そうでない場合、ポートはゲストVLANに配置されます。そうでなければそれ

ゲストVLANに移動しませんが、EAPOLによって指定されたレートでEAPOL要求IDフレームを送信し続けます

タイムアウト。

ゲストVLANに入ると、ポートは認証済みと見なされ、ポートに接続されているすべてのクライアントがこれにアクセスできるようになります。

VLAN。ゲストVLANに入るとき、スイッチはEAPOL成功フレームを送信しません。

ゲストVLANにいる間、スイッチはEAPOLフレームのリンクを監視し、そのようなフレームが1つ受信されると、スイッチは

すぐにゲストVLANからポートを取り出し、ポートモードに従ってサブリカントの認証を開始します。もし

EAPOLフレームを受信すると、「EAPOLが表示された場合にゲストVLANを許可する」の場合、ポートはゲストVLANに戻ることができなくなります。

無効になっています。

[図4-9-7](#)および[図4-9-8](#)の802.1XゲストVLAN設定画面が表示されます。

図4-9-7ゲストVLAN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
・ゲストVLANID	これは、ポートがに移動された場合にポートのポートVLANIDが設定される値です。 ゲストVLAN。ゲストVLANオプションがグローバルに有効になっている場合にのみ変更できます。
・ゲストVLANが有効	有効な値は[1~4094]の範囲です。 ゲストVLANは特別なVLANであり、通常はネットワークアクセスが制限されています。 ネットワーク管理者が定義した後に配置される802.1X非対応クライアント タイムアウト。スイッチは、ゲストの出入りに関する一連のルールに従います 以下にリストされているVLAN。 [ゲストVLANを有効にする]チェックボックスを使用すると、グローバルにすばやくアクセスできます ゲストVLAN機能を有効/無効にします。 ■チェックすると、個々のポートの同上設定により、 ポートはゲストVLANに移動できます。 ■チェックを外すと、ゲストVLANに移動する機能が無効になります。 すべてのポート。 ・ゲストVLANポート 設定 ゲストVLANがグローバルに有効になっていて、特定の機能が有効（チェック）になっている場合 ポートの場合、スイッチはポートをゲストVLANに移動することを検討します。 以下に概説するルール。 このオプションは、EAPOLベースのモードでのみ使用できます。 ・ポートベースの802.1X

ボタン

: クリックして変更を適用します。

図4-9-8ゲストVLAN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
•ポート名	論理ポートのスイッチポート番号
•状態を有効にする	現在の状態を表示する
•ゲストVLAN内	現在のゲストVLANを表示する

4.9.1.5認証されたホスト

図4-9-9の[AuthenticatedHostTable]画面が表示されます。

図4-9-9認証されたホストテーブル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
•ユーザー名	現在のユーザー名を表示します
•ポート	現在のポート番号を表示します
•セッション時間	現在のセッション時間を表示する
•認証方法	現在の認証方法を表示します
•MACアドレス	現在のMACアドレスを表示します

4.9.2RADIUSサーバー

このページでは、RADIUSサーバー接続セッションパラメーターを構成します。図4-9-10のRADIUS設定画面、

図4-9-11と図4-9-12が表示されます。

図4-9-10デフォルトパラメータの使用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
・再試行	タイムアウトは、応答を待機する1～10の範囲の秒数です。 要求を再送信する前に、RADIUSサーバーから。
・返信のタイムアウト	再送信は、1～30の範囲のRADIUS要求の回数です。 応答していないサーバーに再送信されます。サーバーが持っていない場合 最後の再送信後に応答すると、停止していると見なされます。
・デッドタイム	0～3600秒の数値に設定できるデッドタイムは スイッチが新しい要求をサーバーに送信しない期間 以前のリクエストに応答できませんでした。これにより、スイッチが継続的に停止します すでに停止していると判断されたサーバーに接続しようとしています。 Dead Timeを0（ゼロ）より大きい値に設定すると、この機能が有効になりますが、 複数のサーバーが構成されている場合のみ。
・キー文字列	RADIUSサーバー間で共有される秘密鍵（最大63文字の長さ） とスイッチ。

ボタン

：クリックして変更を適用します。

図4-9-11新しいRadiusサーバー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
•サーバー定義	サーバー定義を設定する
•サーバーIP	RADIUSサーバーのアドレスIP /名前
•認証ポート	RADIUS認証サーバーで使用するUDPポート。ポートが0に設定されている場合（ゼロ）、デフォルトのポート（1812）がRADIUS認証サーバーで使用されます。
•アカウントポート	RADIUSアカウントingサーバーで使用するUDPポート。ポートが0に設定されている場合（ゼロ）、デフォルトのポート（1813）がRADIUSアカウントingサーバーで使用されます。
•キー文字列	共有キー-RADIUS認証サーバーとスイッチ。
•返信のタイムアウト	1〜30秒の数値に設定できるタイムアウトは、サーバーからの応答を待機する最大時間。 サーバーがこの時間枠内に応答しない場合、サーバーは停止していると見なされます 次に有効になっているサーバー（存在する場合）に進みます。 RADIUSサーバーはUDPプロトコルを使用していますが、これは設計上信頼性がありません。に 失われたフレームに対処するために、タイムアウト間隔は次の3つのサブ間隔に分割されます。 等しい長さ。サブインターバル内に応答が受信されない場合、要求は 再び送信されました。このアルゴリズムにより、RADIUSサーバーは最大でクエリされます。 死んだと見なされる前に3回。
•再試行	タイムアウトは、応答を待機する1〜10の範囲の秒数です。 要求を再送信する前に、RADIUSサーバーから。

•サーバーの優先度	サーバーの優先度を設定する
•デッドタイム	0〜3600秒の数値に設定できるデッドタイムは スイッチが新しい要求をサーバーに送信しない期間 以前のリクエストに回答できませんでした。これにより、スイッチが継続的に停止します すでに停止していると判断されたサーバーに接続しようとしています。 Dead Timeを0（ゼロ）より大きい値に設定すると、この機能が有効になりますが、 複数のサーバーが構成されている場合のみ。
•使用タイプ	使用タイプを設定します。次のモードを使用できます。 ■ログイン ■ 802.1X ■すべて

: クリックしてRadiusサーバー設定を追加します。

図4-9-12ログイン認証リスト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
・IPアドレス	現在のIPアドレスを表示します
・認証ポート	現在の認証ポートを表示します
・アカウントポート	現在のアカウントポートを表示する
・キー	現在のキーを表示します
・タイムアウト	現在のタイムアウトを表示する
・再試行	現在の再試行時間を表示します
・優先度	現在の優先度を表示する
・デッドタイム	現在のデッドタイムを表示する
・使用タイプ	現在の使用タイプを表示します
・変更	
	クリック ログイン認証リストパラメータを編集します。
	クリック ログイン認証リストのエントリを削除します。

4.9.3 TACACS +サーバー

このページでは、RADIUSサーバー接続セッションパラメーターを構成します。図4-9-13のRADIUS設定画面、図4-9-14と図4-9-15が表示されます。

図4-9-13ゲストVLAN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
・キー文字列	秘密鍵（最大63文字の長さ）がTACACS +サーバー間で共有されます とスイッチ。
・返信のタイムアウト	再送信は、1〜30の範囲のTACACS +要求の回数です。

応答していないサーバーに再送信されます。サーバーが持っていない場合最後の再送信後に応答すると、停止していると見なされます。

ボタン

: クリックして変更を適用します。

図4-9-14新しいRadiusサーバー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
•サーバー定義	サーバー定義を設定する
•サーバーIP	TACACS +サーバーのアドレスIP /名前
•サーバーポート	認証メッセージに使用されるTACACS +サーバーのネットワーク（TCP）ポート。 (範囲：1-65535;デフォルト：49)
•サーバーキー	TACACS +認証サーバーとスイッチ間で共有されるキー。
•サーバータイムアウト	スイッチがサーバーからの応答を待機する秒数 リクエストを再送信します。
•サーバーの優先度	サーバーの優先度を設定する

ボタン

: クリックしてRadiusサーバー設定を追加します。

図4-9-15ログイン認証リスト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	
•IPアドレス	現在のIPアドレスを表示します	
•ポート	現在のポートを表示する	
•キー	現在のキーを表示します	
•タイムアウト	現在のタイムアウトを表示する	
•再試行	現在の再試行時間を表示します	
•優先度	現在の優先度を表示する	
•変更	クリック	ログイン認証リストパラメータを編集するには
	クリック	ログイン認証リストのエントリを削除するには

4.9.4 AAA

認証、許可、およびアカウントिंग（AAA）は、マネージドでアクセス制御を設定するためのフレームワークを提供します
スイッチ。3つのセキュリティ機能は次のように要約できます。

- 認証**—ネットワークへのアクセスを要求するユーザーを識別します。
- 承認**—ユーザーが特定のサービスにアクセスできるかどうかを決定します。
- アカウントING**—ユーザーがネットワーク上でアクセスしたサービスのレポート、監査、および請求を提供します。

AAA機能では、ネットワークで設定済みのRADIUSまたはTACACS +サーバを使用する必要があります。セキュリティサーバは
指定されたサービスへのユーザーアクセスを制御する方法として適用される順次グループとして定義されます。例えば、
スイッチがユーザーの認証を試みると、応答がない場合、定義されたグループの最初のサーバに要求が送信されます。
2番目のサーバが試されます。いずれかの時点で合格または不合格が返された場合、プロセスは停止します。

マネージドスイッチは、次のAAA機能をサポートしています。

- マネージドスイッチを介してネットワークにアクセスする**IEEE802.1X認証済みユーザーのアカウントING**。
- コンソールとTelnetを介してマネージドスイッチの**管理インターフェイス**にアクセスするユーザーのアカウントING。
- ユーザーが特定のCLI特権レベルで入力する**コマンドのアカウントING**。アクセスするユーザーの承認
コンソールとTelnetを介したマネージドスイッチの管理インターフェイス。

マネージドスイッチでAAAを設定するには、次の一般的なプロセスに従う必要があります。

- 1.1. RADIUSおよびTACACS +サーバアクセスパラメータを設定します。「**ローカル/リモートログオンの構成**」を参照してください。
認証」。
- 2.2. サービスのアカウントINGと承認をサポートするために、RADIUSおよびTACACS +サーバグループを定義します。
- 3.3. アカウントINGまたは承認を適用する各サービスのメソッド名を定義し、
使用するRADIUSまたはTACACS +サーバグループ。メソッド名をポートまたはラインインターフェイスに適用します。

このガイドは、RADIUSおよびTACACS +サーバーがすでに次のように構成されていることを前提としています。
AAAをサポートします。RADIUSおよびTACACS +サーバーソフトウェアの構成は、
このガイドの範囲については、RADIUSまたはTACACS +に付属のドキュメントを参照してください。
サーバーソフトウェア。

4.9.4.1ログインリスト

このページは、リストパラメータにログインするためのものです。図4-9-17および図4-9-18の認証リスト画面が表示されます。

図4-9-17新しい認証リスト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
・リスト名	認証リストの名前を定義します
・方法1-4	ログイン認証方法を設定します。 空/なし/ローカル/ TACACS + / RADIUS /有効

ボタン

: クリックして認証リストを追加します。

図4-9-18ログイン認証リスト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
・リスト名	現在のリスト名を表示する

・メソッドリスト	現在のメソッドリストを表示する	
・変更	クリック	ログイン認証リストパラメータを編集するには
	クリック	ログイン認証リストのエントリを削除するには

237

4.9.4.2有効化リスト

このページは、リストパラメータにログインするためのものです。図4-9-19および図4-9-20の認証リスト画面が表示されます。

図4-9-19新しい認証リスト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
・リスト名	認証リストの名前を定義します
・方法1-3	ログイン認証方法を設定します。 空/なし/有効/ TACACS + / RADIUS

ボタン

：クリックして認証リストを追加します。

図4-9-20ログイン認証リスト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
・リスト名	現在のリスト名を表示する
・メソッドリスト	現在のメソッドリストを表示する
・変更	クリック ログイン認証リストパラメータを編集するには
	クリック ログイン認証リストのエントリを削除するには

4.9.5アクセス

このセクションでは、Telnet、SSH、HTTP、およびさまざまなアクセス方法を含む、マネージドスイッチのアクセスを制御します。
HTTP。

4.9.5.1 Telnet

図4-9-21および図4-9-22のTelnet設定および情報画面が表示されます。

図4-9-21Telnet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
• Telnetサービス	telnetサービスを無効または有効にする
• ログイン認証リスト	このドロップダウンリストからログイン認証リストを選択します
• 認証リストを有効にする	このドロップダウンリストから[認証リストを有効にする]を選択します
• セッションタイムアウト	セッションタイムアウト値を設定する
• パスワードの再試行回数	パスワードの再試行回数の値を設定する
• サイレントタイム	サイレントタイムの値を設定する

ボタン

：クリックして変更を適用

：クリックしてTelnet通信を切断します

図4-9-21Telnet情報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
• Telnetサービス	現在のTelnetサービスを表示する
• ログイン認証リスト	現在のログイン認証リストを表示する
• 認証リストを有効にする	現在の有効な認証リストを表示する
• セッションタイムアウト	現在のセッションタイムアウトを表示する
• パスワードの再試行回数	現在のパスワードの再試行回数を表示します
• サイレントタイム	現在の無音時間を表示する
• 現在のTelnetセッション カウント	現在のtelnetセッション数を表示します

4.9.5.2 SSH

このページでSSHを構成します。このページには、ポートセキュリティのステータスが表示されます。ポートセキュリティは、直接構成されていないモジュールです。構成は、他のモジュール（ユーザーモジュール）から間接的に行われます。ユーザーモジュールがポートのポートセキュリティを有効にしている場合、ポートはソフトウェアベースの学習用に設定されています。このモードでは、不明なMACアドレスからのフレームがポートに渡されますセキュリティモジュール。これにより、すべてのユーザーモジュールに、この新しいMACアドレスの転送を許可するかブロックするかを尋ねます。MACの場合アドレスを転送状態に設定するには、有効なすべてのユーザーモジュールが、MACアドレスを許可することに全会一致で同意する必要があります。フォワード。1つだけがブロックすることを選択した場合、そのユーザーモジュールが別の方法で決定するまでブロックされます。

[図4-9-23](#)および[図4-9-24](#)のSSH設定および情報画面が表示されます。

図4-9-23SSH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
・SSHサービス	SSHサービスを無効または有効にする
・ログイン認証リスト	このドロップダウンリストからログイン認証リストを選択します
・認証リストを有効にする	このドロップダウンリストから[認証リストを有効にする]を選択します
・セッションタイムアウト	セッションタイムアウト値を設定する
・パスワードの再試行回数	パスワードの再試行回数の値を設定する
・サイレントタイム	サイレントタイムの値を設定する

ボタン

- ：クリックして変更を適用します。
- ：クリックしてTelnet通信を切断します。

図4-9-24SSH情報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
・SSHサービス	現在のSSHサービスを表示する
・ログイン認証リスト	現在のログイン認証リストを表示する
・認証リストを有効にする	現在の有効な認証リストを表示する

・セッションタイムアウト	現在のセッションタイムアウトを表示する
・パスワードの再試行回数	現在のパスワードの再試行回数を表示します
・サイレントタイム	現在の無音時間を表示する
・現在のSSHセッション数現在のSSHセッション数を表示します	

4.9.5.3 HTTP

図4-9-25および図4-9-26の「HTTP設定および情報」画面が表示されます。

図4-9-25HTTP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
・HTTPサービス	HTTPサービスを無効または有効にする
・ログイン認証リスト	このドロップダウンリストからログイン認証リストを選択します
・セッションタイムアウト	セッションタイムアウト値を設定する

ボタン

：クリックして変更を適用します。

図4-9-26HTTP情報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
• HTTPサービス	現在のHTTPサービスを表示する
• ログイン認証リスト	現在のログイン認証リストを表示します
• セッションタイムアウト	現在のセッションタイムアウトを表示する

4.9.5.4 HTTP

図4-9-27および図4-9-28の[HTTPS設定と情報]画面が表示されます。

図4-9-27HTTP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
• HTTPSサービス	HTTPサービスを無効または有効にする
• ログイン認証リスト	このドロップダウンリストからログイン認証リストを選択します
• セッションタイムアウト	セッションタイムアウト値を設定する

ボタン

：クリックして変更を適用します。

図4-9-28HTTPS情報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
• HTTPSサービス	現在のHTTPSサービスを表示する
• ログイン認証リスト	現在のログイン認証リストを表示します
• セッションタイムアウト	現在のセッションタイムアウトを表示する

4.9.6管理アクセス方法

4.9.6.1プロファイルルール

図4-9-29および図4-9-30のプロファイルルールテーブル設定およびテーブル画面が表示されます。

図4-9-29プロファイルルールテーブル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
・アクセスプロファイル名 (1～32文字)	アクセスプロファイル名を示します
・優先度 (1-65535)	優先順位を設定する 許容値は1～65535です。

・管理方法	ホストがからスイッチにアクセスできることを示します HTTP / HTTPS / telnet / SSH / SNMP /ホストIPアドレスが一致したすべてのインターフェース エントリ。
・アクション	IPアドレスには、許可ルールまたは拒否ルールの任意の組み合わせを含めることができます。 (デフォルト：許可ルール) プロファイルのアクセスモードを設定します。どちらかの許可または 拒否します。
・ポート	このドロップダウンリストからポートを選択します
・IPソース	アクセス管理エントリのIPアドレスを示します

ボタン

: クリックして変更を適用します。

図4-9-30プロファイルルールテーブル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	
・アクセスプロファイル名	現在のアクセスプロファイル名を表示します	
・優先度	現在の優先度を表示する	
・管理方法	現在の管理方法を表示する	
・アクション	現在のアクションを表示する	
・ポート	現在のポートリストを表示する	
・ソースIPv4	現在の送信元IPv4アドレスを表示します	
・ソースIPv4マスク	現在のソースIPv4マスクを表示します	
・ソースIPv6	現在の送信元IPv6アドレスを表示します	
・ソースIPv6プレフィックス	現在のソースIPv6プレフィックスを表示します	
・変更	クリック	プロファイルルールパラメータを編集するには
	クリック	プロファイルルールエントリを削除するには

245

4.9.6.2アクセスルール

図4-9-31および図4-9-32のアクセスプロファイル画面が表示されます。

図4-9-31アクセスプロファイル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
・アクセスプロファイル	このドロップダウンリストからアクセスプロファイルを選択します

ボタン

：クリックして変更を適用します。

図4-9-32アクセスプロファイルテーブル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
・アクセスプロファイル	現在のアクセスプロファイルを表示する
・削除	クリック アクセスプロファイルエントリを削除するには

4.9.7DHCPスヌーピング

4.9.7.1DHCPスヌーピングの概要

安全でないポートでDHCPクライアントに割り当てられたアドレスは、登録された動的バインディングを使用して慎重に制御できます
DHCPスヌーピングを使用します。DHCPスヌーピングにより、スイッチは不正なDHCPサーバーやその他のデバイスからネットワークを保護できます。
ポート関連の情報をDHCPサーバーに送信します。この情報は、IPアドレスを追跡して物理ポートに戻すのに役立ちます。

コマンドの使用法

■外部ソースから悪意のあるDHCPメッセージを受信すると、ネットワークトラフィックが中断する可能性があります。**DHCPスヌーピングは**
ネットワークまたはファイアウォールの外部から非セキュアインターフェイスで受信したDHCPメッセージをフィルタリングするために使用されます。DHCPの場合
スヌーピングはグローバルに有効になり、VLANインターフェイスで有効になります。**信頼できないインターフェイスでDHCPメッセージを受信すると**
DHCPスヌーピングテーブルにリストされていないデバイスはドロップされます。

- テーブルエントリは、信頼できるインターフェイスについてのみ学習されます。DHCPスヌーピングテーブルにエントリが動的に追加または削除されます
クライアントがDHCPサーバーからIPアドレスを受信または解放したとき。各エントリには、MACアドレス、IPアドレス、リースが含まれます
時間、VLAN識別子、およびポート識別子。
- DHCPスヌーピングを有効にすると、信頼できないインターフェイスに入るDHCPメッセージは、ダイナミックエントリに基づいてフィルタリングされ
DHCPスヌーピングを介して学習しました。
- フィルタリングルールは次のように実装されます。

247

- グローバルDHCPスヌーピングが無効になっている場合、すべてのDHCPパケットが転送されます。
- DHCPスヌーピングがグローバルに有効になっていて、DHCPパケットを受信するVLANでも有効になっている場合、すべてのDHCP
パケットは信頼できるポートに転送されます。受信したパケットがDHCPACKメッセージの場合、動的DHCP
スヌーピングエントリもバインディングテーブルに追加されます。
- DHCPスヌーピングがグローバルに有効になっていて、DHCPパケットを受信するVLANでも有効になっている場合、
ポートは信頼されていません。次のように処理されます。
 - DHCPパケットがDHCPサーバーからの応答パケット（OFFER、ACK、またはNAKメッセージを含む）である場合、
パケットはドロップされます。
 - DHCPパケットがクライアントからのものである場合（DECLINEまたはRELEASEメッセージなど）、スイッチは
対応するエントリがバインディングテーブルで見つかった場合にのみパケット。
 - DHCPパケットが、DISCOVER、REQUEST、INFORM、DECLINEなどのクライアントからのものである場合
RELEASEメッセージ、MACアドレス検証が無効になっている場合、パケットは転送されます。ただし、MACの場合
アドレス検証が有効になっている場合、パケットはクライアントのハードウェアアドレスの場合にのみ転送されます
DHCPパケットに格納されるのは、イーサネットヘッダーの送信元MACアドレスと同じです。
 - DHCPパケットが認識可能なタイプでない場合、それはドロップされます。
- クライアントからのDHCPパケットが上記のフィルタリング基準に合格した場合、同じVLAN内の信頼できるポートにのみ転送されます。
- DHCPパケットがサーバーからのものである場合、信頼できるポートで受信された場合、DHCPパケットは信頼できるポートと信頼できないポートの両方に転送されます。
同じVLAN。
- DHCPスヌーピングがグローバルに無効になっている場合、すべての動的バインディングがバインディングテーブルから削除されます。
 - スイッチ自体がDHCPクライアントである場合の追加の考慮事項-スイッチが送信するポート
DHCPサーバーへのクライアント要求は、信頼できるものとして構成する必要があります。スイッチは動的エントリを追加しないことに注意してください
DHCPサーバーからACKメッセージを受信すると、バインディングテーブルに自動的に送信されます。また、スイッチが送信するとき
DHCPクライアントパケット自体を出力する場合、フィルタリングは行われません。ただし、スイッチがからメッセージを受信した場合
DHCPサーバー、信頼できないポートから受信したパケットはすべてドロップされます。

4.9.7.2グローバル設定

DHCPスヌーピングは、偽のDHCPを挿入して介入しようとしたときに、スイッチの信頼できないポートへの侵入者をブロックするために使用されます。
DHCPクライアントとサーバー間の正当な会話にパケットを返信します。このページでDHCPスヌーピングを構成します。ザ・
[図4-9-33](#)および[図4-9-34](#)のDHCPスヌーピング設定および情報画面が表示されます。

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
• DHCPスヌーピング	<p>DHCPスヌーピングモードの動作を示します。可能なモードは次のとおりです。</p> <p>■有効：DHCPスヌーピングモード操作を有効にします。</p> <p>DHCPスヌーピングモードの動作を有効にすると、 DHCPメッセージは、信頼できるポートにのみ転送されます 信頼できるポートからの応答パケットを許可しました。</p> <p>■無効：DHCPスヌーピングモードの操作を無効にします。</p>

ボタン

：クリックして変更を適用します。

図4-9-34DHCPスヌーピング情報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
• DHCPスヌーピング	現在のDHCPスヌーピングステータスを表示します

4.9.7.3DHCPスヌーピングVLAN設定

コマンドの使用法

- DHCPは、スイッチ上でグローバルに有効にし、指定されたVLAN上で有効になっているスヌーピングすると、DHCPパケットフィルタリングは次のようになります
VLAN内の信頼されていないポートで実行されます。
- DHCPスヌーピングがグローバルに無効になっている場合、DHCPスヌーピングは、まだ特定のVLANで構成することができますが、変更
DHCPスヌーピングがグローバルに再度有効になるまで有効になりません。
- DHCPスヌーピングがグローバルにイネーブルされ、およびDHCPスヌーピングは、その後、VLAN上で無効になって、すべての動的バインディングがために知ったとき
このVLANはバインディングテーブルから削除されます。

図4-9-35および図4-9-36のDHCPスヌーピングVLAN設定画面が表示されます。

図4-9-35DHCPスヌーピングVLAN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
•VLANリスト	この特定のVLANのIDを示します。
•ステータス	DHCPスヌーピングモードの動作を示します。可能なモードは次のとおりです。 <div>■有効：DHCPスヌーピングモード操作を有効にします。<div>DHCPスヌーピングモードの動作を有効にすると、DHCPメッセージは、信頼できるポートにのみ転送されます信頼できるポートからの応答パケットを許可しました。</div>■無効：DHCPスヌーピングモードの操作を無効にします。</div>

ボタン

：クリックして変更を適用します。

図4-9-36DHCPスヌーピングVLAN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
•VLANリスト	現在のVLANリストを表示する
•ステータス	現在のDHCPスヌーピングステータスを表示します

4.9.7.4ポート設定

スイッチポートを信頼済みまたは信頼できないものとして構成します。

コマンドの使用法

- 信頼できるインターフェースは、ネットワーク内からのメッセージのみを受信するように構成されたインターフェースです。信頼できないインターフェースネットワークまたはファイアウォールの外部からメッセージを受信するように構成されたインターフェースです。
- DHCPスヌーピングは、DHCPパケットフィルタリングは、任意の信頼できないポートで実行され、グローバルおよびVLAN上の両方を有効にするとVLAN内。
- 信頼できないポートが信頼できるポートに変更されると、このポートに関連付けられているすべての動的DHCPスヌーピングバインディングは削除されました。
- ローカルネットワークまたはファイアウォール内のDHCPサーバーに接続されているすべてのポートを信頼できる状態に設定します。他のすべてのポートをローカルネットワークまたはファイアウォールを信頼できない状態にします。

図4-9-37および図4-9-38のDHCPスヌーピングポート設定画面が表示されます。

図4-9-37DHCPスヌーピングポート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
・ポート	このドロップダウンリストからポートを選択します
・タイプ	DHCPスヌーピングポートモードを示します。可能なポートモードは次のとおりです。 <div>■信頼済み：ポートをDHCPメッセージの信頼できる送信元として構成します。</div> <div>■信頼できない：DHCPの信頼できない情報源としてポートを設定します</div> メッセージ。
・Chaddrチェック	選択したポートでChaddrチェック機能が有効になっていることを示します。 Chaddr：クライアントハードウェアアドレス。

ボタン

：クリックして変更を適用します。

図4-9-38DHCPスヌーピングポート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
・ポート	論理ポートのスイッチポート番号
・タイプ	現在のタイプを表示します
・Chaddrチェック	現在のchaddrチェックを表示します

4.9.7.5統計

図4-9-39の[DHCPスヌーピング統計]画面が表示されます。

図4-9-39DHCPスヌーピング統計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
•ポート	論理ポートのスイッチポート番号
•転送	転送された電流を表示します
• Chaddrチェックが削除されました	ドロップされたchaddrチェックを表示します
•信頼できないポートが削除されました	信頼できないポートの表示が削除されました
•ポートを信頼しない Option82が削除されました	option82を削除して信頼できないポートを表示する
•無効なドロップ	無効なドロップを表示

ボタン

：クリックして統計をクリアします。

：クリックして統計を更新します。

4.9.7.6データベースエージェント

DHCPスヌーピングデータベースエージェントの概要

DHCPスヌーピングが有効になっている場合、スイッチはDHCPスヌーピングバインディングデータベースを使用して、信頼できない情報を格納します。インターフェイス。データベースには、最大8192のバインディングを含めることができます。

各データベースエントリ（バインディング）には、IPアドレス、関連付けられたMACアドレス、リース時間（16進形式）、バインディングが適用されるインターフェイス、およびインターフェイスが属するVLAN。チェックサム値は、各エントリの端部は、ありますファイルの先頭からエントリの末尾までのバイト数。各エントリは72バイトで、その後にはスペース、そしてチェックサム値。

スイッチのリロード時にバインディングを保持するには、DHCPスヌーピングデータベースエージェントを使用する必要があります。エージェントが無効になっている場合、動的ARPまたはIPソースガードが有効になっている、DHCPスヌーピングバインディングデータベースに動的バインディングがある場合、スイッチは失われますその接続性。エージェントが無効で、DHCPスヌーピングのみが有効になっている場合、スイッチは接続を失いますが、DHCPはスヌーピングは、DHCPスプーフィング攻撃を防ぐことができない場合があります。

データベースエージェントは、構成された場所にあるファイルにバインディングを格納します。リロード時に、スイッチはバインディングファイルを

DHCPスヌーピングバイディングデータベースを構築します。スイッチは、データベースが変更されたときにファイルを更新することにより、ファイルを最新の状態に保ちます。

スイッチが新しいバイディングを学習したとき、またはバイディングを失ったとき、スイッチはデータベース内のエントリをすぐに更新します。

スイッチは、バイディングファイルのエントリも更新します。ファイルが更新される頻度は、構成可能なものに基づいています

遅延し、更新がバッチ処理されます。ファイルが指定された時間内に更新されない場合（write-delayおよびabort-timeout値によって設定されます）、更新が停止します。

図4-9-40および図4-9-41のDHCPスヌーピングデータベースおよび情報画面が表示されます。

図4-9-40DHCPスヌーピングデータベース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
データベースタイプ	データベースタイプを選択します
ファイル名	ファイル画像の名前
リモートサーバー	リモートサーバーのIPアドレスを入力します
書き込み遅延	バイディング後に転送を遅延させる期間を指定します データベースの変更。範囲は15～86400秒です。デフォルトは300です 秒（5分）。
タイムアウト	データベースのバインド後にデータベース転送プロセスを停止するタイミングを指定します 変化します。 範囲は0～86400です。無限の期間は0を使用します。デフォルトは300です 秒（5分）。

ボタン

：クリックして変更を適用します。

図4-9-41DHCPスヌーピングデータベース情報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
・データベースタイプ	現在のデータベースタイプを表示します
・ファイル名	現在のファイル名を表示する
・リモートサーバー	現在のリモートサーバーを表示する
・書き込み遅延	現在の書き込み遅延を表示します
・タイムアウト	現在のタイムアウトを表示する

4.9.7.7レート制限

DHCPスヌーピングを有効にした後、スイッチはすべてのDHCPメッセージを監視し、ソフトウェア送信を実装します。ザ・
[図4-9-42](#)および[図4-9-43](#)のDHCPレート制限設定および構成画面が表示されます。

図4-9-42DHCPレート制限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
・ポート	このドロップダウンリストからポートを選択します
・州	デフォルトを設定するか、ユーザー定義
・レート制限（pps）	ポートポリサのレート制限を設定します。デフォルト値は「無制限」です。有効 値の範囲は1〜300です。

ボタン

：クリックして変更を適用

図4-9-43DHCPレート制限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
・ポート	論理ポートのスイッチポート番号
・レート制限（pps）	現在のレート制限を表示します

4.9.7.8Option82グローバル設定

DHCPは、スイッチとそのDHCPクライアントに関する情報をDHCPサーバーに送信するためのリレーメカニズムを提供します。として知られているDHCPオプション82、互換性のあるDHCPサーバーがIPアドレスを割り当てるときに情報を使用したり、他のクライアント向けのサービスまたはポリシー。DHCP上の接続されたクライアントからの悪意のあるネットワーク攻撃を防ぐための効果的なツールでもありますIPスプーフィング、クライアントIDスプーフィング、MACアドレススプーフィング、アドレス枯渇などのサービス。

DHCPオプション82は、時に転送DHCP要求パケットに特定の情報を挿入するためにDHCPリレーエージェントを有効にしますクライアントDHCPパケットをDHCPサーバーに送信し、サーバーを転送するときにDHCP応答パケットから特定の情報を削除しますDHCPクライアントへのDHCPパケット。DHCPサーバーは、この情報を使用してIPアドレスまたはその他の割り当てを実装できます。ポリシー。具体的には、このオプションは2つのサブオプションを設定することで機能します。

- 回路ID（オプション1）
- リモートID（オプション2）。

Circuit IDサブオプションには、要求が発生した回線に固有の情報が含まれているはずで。リモートIDサブオプションは、回線のリモートホスト側に関連する情報を伝送するように設計されています。

スイッチの回路IDの定義は4バイトの長さで、形式は「vlan_id」「module_id」「port_no」です。のパラメータ「vlan_id」は、VLANIDを表す最初の2バイトです。「module_id」のパラメータは、モジュールIDの3番目のバイトです（スタンドアロンスイッチは常に0に等しく、スイッチではスイッチIDを意味します）。「port_no」のパラメータは4番目のバイトであり、ポート番号。

DHCPスヌーピングを有効にした後、スイッチはすべてのDHCPメッセージを監視し、ソフトウェア送信を実装します。ザ・図4-9-44および図4-9-45のDHCPレート制限設定および構成画面が表示されます。

図4-9-44Option82グローバル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
・州	DHCP要求によって追加されたオプション82のoption2（リモートIDオプション）コンテンツを設定します パケット。 ■デフォルトは、デフォルトのVLANMACフォーマットを意味します。 ■ユーザー定義とは、ユーザーが指定したオプション82のリモートIDコンテンツを意味します

ボタン

: クリックして変更を適用します。

図4-9-45Option82グローバル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
・Option82リモートID	現在のoption82リモートIDを表示します

4.9.7.9Option82ポート設定

この関数は、以下を含む受信DHCP要求メッセージのシステムの再送信ポリシーを設定するために使用されます。

option82。

- ドロップメッセージがoption82でいれば、システムは処理せずにそれをドロップすることモード手段。
- キープシステムは、メッセージの元option82セグメントを保持し、それを転送することモード手段
処理するサーバー
- 交換するシステムは、自身の持つ既存のメッセージでオプション82のセグメントを置換するモード手段を
オプション82を選択し、メッセージをサーバーに転送して処理します。

図4-9-46および図4-9-47のOption82ポート設定画面が表示されます。

図4-9-46Option82グローバル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
・ポート	このドロップダウンリストからポートを選択します
・有効にする	ポートでoption82機能を有効または無効にします
・信頼できないものを許可する	このドロップダウンリストからモードを選択します。次のモードを使用できます。 ■ドロップ ■維持する ■交換

ボタン

：クリックして変更を適用します。

図4-9-47Option82グローバル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
・ポート	論理ポートのスイッチポート番号
・有効にする	現在のステータスを表示する
・信頼できないものを許可する	現在の信頼できないモードを表示する

4.9.7.10Option82回路ID設定

option82の作成方法を設定すると、ユーザーは自分でcircuit-idサブオプションのパラメーターを定義できます。Option82 Circuit-ID

[図4-9-48](#)および[図4-9-49](#)の設定画面が表示されます。

図4-9-48Option82ポート回路-ID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
•ポート	このドロップダウンリストからポートを選択します
•VLAN	この特定のVLANのIDを示します
•回路ID	DHCP要求パケットによって追加されたオプション82のoption1（回路ID）の内容を設定します

ボタン

: クリックして変更を適用します。

図4-9-49Option82ポート回路-ID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
•ポート	現在のポートを表示する
•VLAN	現在のVLANを表示する
•回路ID	現在の回路IDを表示します

4.9.8動的ARP検査

動的ARP検査（DAI）は安全な機能です。ホストまたはデバイスに対していくつかのタイプの攻撃を開始できます
ARPキャッシュを「ポイズニング」することによってレイヤー2ネットワークに接続されます。この機能は、このような攻撃をブロックするために使用されます。有効なARPのみ
要求と応答はDUTを通過できます。このページでは、ARP検査関連の設定を提供します。

ダイナミックARPは、DHCPスヌーピングデータベースに基づく信頼できないARPパケットを防止します。

4.9.8.1グローバル設定

図4-9-50および図4-9-51のDAI設定および情報画面が表示されます。

図4-9-50DAI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
• DAI	グローバルダイナミックARPインスペクションを有効にするか、グローバルARPインスペクションを無効にします
ボタン	: クリックして変更を適用します。

図4-9-51DAI情報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
• DAI	現在のDAIステータスを表示します

4.9.8.2VLAN設定

図4-9-52および図4-9-53のDAI/VLAN設定画面が表示されます。

図4-9-52DAIVLAN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
・VLANID	この特定のVLANのIDを示します
状態	指定されたVLANで動的ARP検査を有効にします オプション： ■有効にする ■無効にする

ボタン

：クリックして変更を適用します。

図4-9-53DAIVLAN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
・VLANリスト	現在のVLANリストを表示する
・ステータス	現在のステータスを表示する

4.9.8.3ポート設定

スイッチポートをDAIの信頼できるまたは信頼できないチェックモードとして構成します。図4-9-54および図のDAIポート設定画面4-9-55が表示されます。

図4-9-54DAIポート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
•ポート	このドロップダウンリストからポートを選択します
•タイプ	どのポートでARP検査を有効にするかを指定します。両方のグローバルモードの場合のみ 特定のポートでポートモードが有効になっている場合、これでARP検査が有効になります 与えられたポート。 デフォルト：すべてのインターフェースは信頼されていません。
• Src-MacChk	イーサネットヘッダーの送信元MACアドレスをチェックするために有効または無効にします ARP本体の送信者MACアドレスに対して。このチェックはに実行されます ARP要求と応答の両方。有効にすると、MACが異なるパケット アドレスは無効として分類され、削除されます。
• Dst-MacChk	イーサネットヘッダーの宛先MACアドレスをチェックするために有効または無効にします ARP本体のターゲットMACアドレスに対して。このチェックはARPに対して実行されます 反応。有効にすると、異なるMACアドレスを持つパケットが分類されます 無効として削除されます。
• IPChk	有効または無効にして、ARPの送信元IPアドレスと宛先IPアドレスを確認します パケット。オールゼロ、オールワン、またはマルチキャストIPアドレスは無効と見なされます 対応するパケットは破棄されます。
• IP許可ゼロ	すべてゼロのIPアドレスをチェックするために有効または無効にします。

ボタン

: クリックして変更を適用します。

図4-9-55DAIポート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
•ポート	論理ポートのスイッチポート番号
•タイプ	現在のポートタイプを表示します
• Src-MacChk	現在のSrc-MacChkステータスを表示します
• Dst-MacChk	現在のDst-MacChkステータスを表示します
• IPChk	現在のIPChkステータスを表示します
• IP許可ゼロ	現在のIP許可ゼロステータスを表示します

4.9.8.4統計

スイッチポートをDAIの信頼できるまたは信頼できないチェックモードとして構成します。[図4-9-56](#)のDAIポート設定画面が表示されます。

図4-9-56DAIポート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
--------	----

・ポート	論理ポートのスイッチポート番号
・転送	転送された電流を表示します
ソースMAC障害	現在のソースMAC障害を表示します
・宛先MACの障害	現在のソースMAC障害を表示します
・SIP検証の失敗	現在のSIP検証の失敗を表示します
・DIP検証の失敗	現在のDIP検証の失敗を表示します
・IP-MACの不一致	現在のIP-MAC不一致の失敗を表示します
失敗	

ボタン

：クリックして統計をクリアします。

：クリックして統計を更新します。

4.9.8.5レート制限

図4-9-57および図4-9-58のARPレート制限設定および設定画面が表示されます。

図4-9-57ARPレート制限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
・ポート	このドロップダウンリストからポートを選択します
・州	デフォルトを設定するか、ユーザー定義
・レート制限（pps）	ポートポリサのレート制限を設定します。デフォルト値は「無制限」です。

ボタン

：クリックして変更を適用します。

図4-9-58ARPレート制限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
•ポート	論理ポートのスイッチポート番号
•レート制限（pps）	現在のレート制限を表示します

266

4.9.9IPソースガード

IP Source Guardは、DHCPに基づいてトラフィックをフィルタリングすることにより、信頼できないポートをスヌーピングするDHCPのIPトラフィックを制限するために使用される安全な機能です。DHCPスヌーピングテーブルまたは手動で構成されたIPソースバインディング。ホストがしようとしたときにIPスプーフィング攻撃を防ぐのに役立ちます別のホストのIPアドレスを偽装して使用します。

パケットを受信した後、ポートはパケットの主要な属性（IPアドレス、MACアドレス、VLANタグなど）を検索します。

IPソースガードのバインディングエントリ。一致するエントリがある場合、ポートはパケットを転送します。それ以外の場合、ポートはパケットを破棄します。

IPソースガードは、次のタイプのバインディングエントリに基づいてパケットをフィルタリングします。

- IPポートバインディングエントリ
- MACポートバインディングエントリ
- IP-MACポートバインディングエントリ

4.9.9.1ポート設定

IP Source Guardは、DHCPに基づいてトラフィックをフィルタリングすることにより、信頼できないポートをスヌーピングするDHCPのIPトラフィックを制限するために使用される安全な機能です。DHCPスヌーピングテーブルまたは手動で構成されたIPソースバインディング。ホストがしようとしたときにIPスプーフィング攻撃を防ぐのに役立ちます別のホストのIPアドレスを偽装して使用します。

図4-9-60および図4-9-61の[IPソースガードポートの設定と情報]画面が表示されます。

図4-9-60IPソースガードポート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
・ポート	このドロップダウンリストからポートを選択します
・ステータス	IPソースガードを有効または無効にします
・ソースを確認する	インバウンドトラフィックベースのIPアドレスまたはIPアドレスをフィルタリングするようにスイッチを構成し、Macアドレス。 <div>■なし管理対象スイッチのIPソースガードフィルタリングを無効にします。</div> <div>■IPがバインドに保存されているIPアドレスに基づいてフィルタリングトラフィックを有効にします</div> <div>テーブル。</div> <div>■IPおよびMACIPアドレスに基づくトラフィックフィルタリングを有効にし、</div> <div>バインディングテーブルに保存されている対応するMACアドレス。</div>
・最大バインディングエントリ	このポートで保護できるIPソースガードの最大数

ボタン

: クリックして変更を適用します。

図4-9-61IPソースガードポート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
・ポート	論理ポートのスイッチポート番号
・ステータス	現在のステータスを表示する
・ソースを確認する	現在の検証ソースを表示します
・最大バインディングエントリ	現在の最大バインディングエントリを表示します
・現在のバインディングエントリ	現在のバインディングエントリを表示します

4.9.9.2バインディングテーブル

図4-9-62および図4-9-63のIPSourceGuard静的バインディングエントリおよびテーブルステータス画面が表示されます。

図4-9-62IPソースガードの静的バインディングエントリ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
・ポート	このドロップダウンリストからポートを選択します
・VLANID	この特定のVLANのIDを示します
・MACアドレス	MACアドレスのソーシングが許可されています
・IPアドレス	ソーシングIPアドレスが許可されます

ボタン

: クリックして認証リストを追加

図4-9-63IPソースガードバインディングテーブルのステータス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
・ポート	現在のポートを表示する
・VLANID	現在のVLANを表示する
・MACアドレス	現在のMACアドレスを表示します
・IPアドレス	現在のIPアドレスを表示する
・タイプ	現在のエントリタイプを表示します
・リース時間	現在のリース時間を表示する
・アクション	クリック IPソースガードバインディングテーブルのステータスエントリを削除するには

4.9.10ポートセキュリティ

このページでは、ポートセキュリティ制限制御システムとポート設定を構成できます。制限制御により、特定のポートのユーザー数。ユーザーは、MACアドレスとVLANIDによって識別されます。ポートで制限制御が有効になっている場合、limitは、ポートの最大ユーザー数を指定します。この数を超えると、アクションが実行されます。アクションは1つにすることができます以下に説明するように4つの異なるの。

制限制御モジュールは、ポートセキュリティモジュールがMACを管理している間、下位層モジュールを利用するモジュールの1つです。ポートで学習したアドレス。

Limit Control構成は、system-widとport-widの2つのセクションで構成されています。IPソースガードの静的バインディングエントリ [図4-9-64](#)および[図4-9-65](#)の[テーブルステータス]画面が表示されます。

図4-9-64ポートセキュリティ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
•ポート	このドロップダウンリストからポートを選択します
•セキュリティ	ポートセキュリティを有効または無効にします
• MacL2エントリ	<p>このポートで保護できるMACアドレスの最大数。の場合制限を超えると、対応するアクションが実行されます。</p> <p>スイッチは、すべてのポートからのMACアドレスの総数で「生まれる」</p> <p>ポートセキュリティが有効なポートで新しいMACアドレスが検出されるたびに描画します。</p> <p>すべてのポートが同じプールから取得されるため、構成済みのポートが発生する可能性があります</p> <p>残りのポートがすでにすべてを使用している場合、最大値を付与することはできません</p> <p>利用可能なMACアドレス。</p>
•アクション	<p>制限に達した場合、スイッチは次のいずれかのアクションを実行できます。</p> <p>■転送：ポートで制限MACアドレスを超えて許可しないでください。</p> <p>それ以上のアクションはありません。</p> <p>■シャットダウン：ポートにLimit + 1 MACアドレスが表示されている場合は、シャットダウンします。</p> <p>ポート。これは、保護されたすべてのMACアドレスがから削除されることを意味します</p> <p>ポート、および新しいものは学習されません。リンクが物理的に切断されている場合でも</p>

(ケーブルを外して) ポートに再接続すると、ポートはシャットダウンしたままにします。ポートを再度開くには、次の3つの方法があります。

1) ポートまたはスイッチの制限制御を無効にしてから再度有効にします。

- 2) [再開]ボタンをクリックします。
- 破壊：ポートに制限+ 1のMACアドレスが表示されると、トリガーされます。
- 新しいMACを学習せず、パッケージをドロップしないアクション。

ボタン

: クリックして変更を適用します。

図4-9-65ポートセキュリティ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
・ポート名	論理ポートのスイッチポート番号
・状態を有効にする	ポートごとの現在のセキュリティステータスを表示します
・L2エントリ番号	現在のL2エントリ番号を表示します
・アクション	現在のアクションを表示する

4.9.11 DoS

DoSは、インターネットに対する単純ですが効果的な破壊的攻撃であるサービス拒否の略です。DoSの下サーバー攻撃者のデータパケットの処理が停止しないため、攻撃は通常のユーザーデータパケットをドロップし、拒否につながります。サービスが悪化すると、サーバーの機密データが漏洩する可能性があります。

セキュリティ機能とは、DoSなどの攻撃からサーバーを保護するためのプロトコルチェックなどのアプリケーションを指します。ザ・プロトコルチェックにより、ユーザーは指定された条件に基づいて一致したパケットをドロップできます。セキュリティ機能はいくつかを提供しますの線形転送パフォーマンスに影響を与えずに、DoS攻撃に対するシンプルで効果的な保護

スイッチ。

4.9.11.1グローバルDoS設定

図4-9-66および図4-9-67のグローバルDoS設定および情報画面が表示されます。

図4-9-66グローバルDoS設定のスクリーンショット

273

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
• DMAC = SMAC	DMAC = SMACによるDoSチェックモードの有効化または無効化
• 土地	土地によるDoSチェックモードの有効化または無効化
• UDPBlat	UDPblatによるDoSチェックモードを有効または無効にします
• TCPBlat	TCPblatによるDoSチェックモードの有効化または無効化
• POD	PODによるDoSチェックモードを有効または無効にします
• IPv6最小フラグメント	IPv6分フラグメントによるDoSチェックモードの有効化または無効化
• ICMPフラグメント	ICMPフラグメントによるDoSチェックモードの有効化または無効化
• IPv4Pingの最大サイズ	IPv4pingの最大サイズによるDoSチェックモードの有効化または無効化

• IPv6Pingの最大サイズ	IPv6pingの最大サイズでDoSチェックモードを有効または無効にします
• Pingの最大サイズ設定	pingの最大サイズを設定します
• スマーフ攻撃	Smurf攻撃によるDoSチェックモードの有効化または無効化
• TCP最小Hdrサイズ	TCP minhdrサイズによるDoSチェックモードの有効化または無効化
• TCP-SYN (SPORT < 1024)	TCP-synによるDoSチェックモードの有効化または無効化 (sport <1024)
• ヌルスキャン攻撃	ヌルスキャン攻撃によるDoSチェックモードの有効化または無効化
• X-Masスキャン攻撃	クリスマススキャン攻撃によるDoSチェックモードの有効化または無効化
• TCPSYN-FIN攻撃	TCPSyn-fin攻撃によるDoSチェックモードの有効化または無効化
• TCPSYN-RST攻撃	TCPSyn-rst攻撃によるDoSチェックモードの有効化または無効化
• TCPフラグメント (オフセット = 1)	TCPフラグメントによるDoSチェックモードの有効化または無効化 (オフセット= 1)

ボタン

: クリックして変更を適用します。

図4-9-67DoS情報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
• DMAC = SMAC	現在のDMAC = SMACステータスを表示します
• ランドアタッチ	現在の土地接続ステータスを表示します
• UDPIBlat	現在のUDPIBlatステータスを表示します
• TCPBlat	現在のTCPBlatステータスを表示します
• POD	現在のPODステータスを表示します
• IPv6最小フラグメント	現在のIPv6分のフラグメントステータスを表示します
• ICMPフラグメント	現在のICMPフラグメントステータスを表示します
• IPv4Pingの最大サイズ	現在のIPv4pingの最大サイズステータスを表示します
• IPv6Pingの最大サイズ	現在のIPv6pingの最大サイズステータスを表示します
• スマーフ攻撃	現在のsmurf攻撃ステータスを表示します
• TCP最小ヘッダー長	現在のTCP最小ヘッダー長を表示します
• TCP-SYN (SPORT <1024)	現在のTCPSynステータスを表示します
• スルスキャン攻撃	現在のスルスキャン攻撃ステータスを表示します
• X-Masスキャン攻撃	現在のクリスマススキャン攻撃ステータスを表示します
• TCPSYN-FIN攻撃	現在のTCPシンフィン攻撃ステータスを表示します
• TCPSYN-RST攻撃	現在のTCPシンスト攻撃ステータスを表示します
• TCPフラグメント (オフセット= 1)	TCPフラグメント (オフセット= 1) のステータスを表示します

4.9.11.2DoSポート設定

図4-9-68および図4-9-69のDoSポート設定およびステータス画面が表示されます。

図4-9-68ポートセキュリティ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
• ポート選択	このドロップダウンリストからポートを選択します。
• DoS保護	ポートごとのDoS保護を有効または無効にします。

ボタン

：クリックして変更を適用します。

図4-9-68ポートセキュリティ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
・ポート	論理ポートのスイッチポート番号
・DoS保護	現在のDoS保護を表示する

4.9.12ストームコントロール

スイッチのストーム制御は、このページで構成されます。

不明なユニキャストストームレート制御、不明なマルチキャストストームレート制御、およびブロードキャストストームレート制御があります。

これらは、フラッドイングされたフレーム、つまり（VLAN ID、DMAC）ペアがMACアドレステーブルに存在しないフレームにのみ影響します。

4.9.12.1グローバル設定

図4-9-69および図4-9-70のストーム制御グローバル設定および情報画面が表示されます。

図4-9-69ストームコントロールのグローバル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
・ユニット	ストーム制御率の測定単位を「pps」または「bps」として制御します。ザ・デフォルト値は「bps」です。
・前文とIFG	除外または含まれるフレーム間ギャップを設定します

ボタン

：クリックして変更を適用します。

図4-9-70 ストームコントロールのグローバル情報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
・ユニット	現在の単位を表示する
・前文とIFG	現在のプリアンブルとIFGを表示します

4.9.12.2ポート設定

スイッチのストーム制御は、このページで構成されます。ストームレート制御には3つのタイプがあります。

- ブロードキャストストームレート制御
- 不明なユニキャストストームレート制御
- 不明なマルチキャストストームレート制御

構成は、不明なユニキャスト、不明なマルチキャスト、またはブロードキャストトラフィックの許容パケットレートを示します。
スイッチ。図4-9-71および図4-9-72のストーム制御設定画面が表示されます。

図4-9-71 ストームコントロール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
・ポート	このドロップダウンリストからポートを選択します。
・ポートステート	特定のストームタイプのストーム制御ステータスを有効または無効にします。
・アクション	ポートでストーム制御がオーバーレートのときに実行されるアクションを設定します。有効値はShutdownまたはDropです。
・「有効」と入力します	特定の行の設定は、ここにリストされているフレームタイプに適用されます。 <ul style="list-style-type: none">■ 放送■ 不明なユニキャスト■ 不明なマルチキャスト
・レート (kbps / pps)	ストームコントロールのレートを設定します。デフォルト値は「10,000」です。

ボタン

: クリックして変更を適用

図4-9-72 ストームコントロール情報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
・ポート	論理ポートのスイッチポート番号
・ポートステート	現在のポート状態を表示します
・ブロードキャスト (Kbps / pps)	現在のブロードキャストストーム制御率を表示します
・不明なマルチキャスト (Kbps / pps)	現在の不明なマルチキャストストーム制御レートを表示します
・不明なユニキャスト (Kbps / pps)	現在の不明なユニキャストストーム制御率を表示します
・アクション	現在のアクションを表示する

4.10 ACL

ACLは、**アクセス制御リスト**の頭字語です。これはACEのリストテーブルであり、個々を指定するアクセス制御エントリが含まれています。

プロセスやプログラムなどの特定のトラフィックオブジェクトに対して許可または拒否されたユーザーまたはグループ。アクセス可能な各トラフィックオブジェクト ACLの識別子が含まれています。特権は、特定のトラフィックオブジェクトのアクセス権があるかどうかを決定します。

ACLの実装は、たとえば、さまざまな状況でACEが優先される場合、非常に複雑になる可能性があります。ネットワーキングでは、

ACLは、ホストまたはサーバーで使用可能なサービスポートまたはネットワークサービスのリストを参照し、それぞれにホストのリストまたはサービスの使用を許可または拒否されたサーバー。ACLは通常、インバウンドトラフィックを制御するように設定できます。このコンテキストでは、それらはファイアウォールに似ています。

ACEは、**Access ControlEntry**の頭字語です。特定のACEIDに関連付けられたアクセス許可について説明します。

3つのACEフレームタイプ（イーサネットタイプ、ARP、およびIPv4）と2つのACEアクション（許可および拒否）があります。ACEも個々のアプリケーションで使用できる多くの詳細で異なるパラメータオプションが含まれています。

ACLページには、次の主要トピックへのリンクが含まれています。

■	MACベースのACL	構成MACベースのACL設定
■	MACベースのACE	MACベースのACE（アクセス制御エントリ）設定の追加/編集/削除
■	IPv4ベースのACL	構成IPv4ベースのACL設定
■	IPv4ベースのACE	IPv4ベースのACE（アクセス制御エントリ）設定の追加/編集/削除
■	IPv6ベースのACL	構成IPv6ベースのACL設定
■	IPv6ベースのACE	IPv6ベースのACE（アクセス制御エントリ）設定の追加/編集/削除
■	ACLバインディング	各スイッチポートのACLパラメータ（ACE）を設定します。

4.10.1MACベースのACL

このページには、さまざまなACLユーザーによるACLステータスが表示されます。各行は、定義されているACEを示しています。特定の場合は競合ですハードウェアの制限により、ACEはハードウェアに適用されません。図4-10-1および図4-10-2のMACベースのACL画面現れる。

図4-10-1MACベースのACL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
• ACL名	名前付きMACベースのACLリストを作成する

■ ACL表

図4-10-2ACLテーブル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
• 削除	クリック ACL名エントリを削除するには

4.10.2MACベースのACE

ACEはいくつかのパラメータで構成されています。使用するフレームタイプに応じて、さまざまなパラメータオプションが表示されます
選択されました。図4-10-3および図4-10-4のMACベースのACE画面が表示されます。

図4-10-3MACベースのACE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
• ACL名	このドロップダウンリストからACL名を選択します
•シーケンス	ACLシーケンスを設定します
•アクション	ACEの転送アクションを示します。 ■許可：ACEに一致するフレームが転送および学習される場合があります。 ■拒否：ACEに一致するフレームはドロップされます。 ■シャットダウン：ACEのポートシャットダウンは無効になっています。
• DAMAC	このACEの宛先MACフィルタを指定します。 ■任意：DAMACフィルターが指定されていません。

	■ユーザー定義：特定の宛先MACアドレスをでフィルタリングする場合 このACE、この値を選択します。DAMAC値を入力するためのフィールドが表示されます。
• DAMAC値	DA MACフィルターで「ユーザー定義」を選択すると、特定の情報を入力できます 宛先MACアドレス。有効な形式は「xx-xx-xx-xx-xx-xx」です。そのフレーム このACEにヒットすると、このDAMAC値と一致します。
• DAMACマスク	送信側ハードウェアに応じて、フレームがアクションにヒットできるかどうかを指定します

	アドレスフィールド（SHA）の設定。 ■ 0：SHAはDA MACアドレスと等しくないARPフレーム。 ■ 1：SHAは、DA MACアドレスと等しいARPフレーム。
• SAMAC	このACEの送信元MACフィルタを指定します。 ■ 任意：SAMACフィルターが指定されていません。 ■ ユーザー定義：これで特定の送信元MACアドレスをフィルタリングする場合 ACE、この値を選択してください。SAMAC値を入力するためのフィールドが表示されます。
• SAMAC値	SA MACフィルターで「ユーザー定義」を選択すると、特定の情報を入力できます 送信元MACアドレス。有効な形式は「xx-xx-xx-xx-xx」です。ヒットするフレーム このACEはこのSAMAC値と一致します。
• SAMACマスク	送信側ハードウェアに応じて、フレームがアクションにヒットできるかどうかを指定します アドレスフィールド（SHA）の設定。 ■ 0：SHAはSA MACアドレスと等しくないARPフレーム。 ■ 1：SHAはSA MACアドレスと等しいARPフレーム。
• VLANID	この特定のVLANのIDを示します
• 802.1p	802.1p値を含めるか除外する
• 802.1p値	802.1p値を設定します
• 802.1pマスク	■ 0：フレームは、802.1p値に等しくない場合。 ■ 1：フレームは、802.1p値に等しいです。
• EtherType（範囲： 0x05DD – 0xFFFF）	特定のEtherType値を入力できます。許容範囲は0x05DDから 0xFFFF。このACEにヒットするフレームは、このEtherType値と一致します。
ボタン	
	：クリックしてACEリストを追加します。

図4-10-4MACベースのACEテーブル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
• ACL名	現在のACL名を表示します
• シーケンス	現在のシーケンスを表示する
• アクション	現在のアクションを表示する
• 宛先MACアドレス	現在の宛先MACアドレスを表示します
• 宛先MACアドレス マスク	現在の宛先MACアドレスマスクを表示します
• 送信元MACアドレス	現在の送信元MACアドレスを表示します

•送信元MACアドレスマスクは、現在の送信元MACアドレスマスクを表示します	
•VLANID	現在のVLANIDを表示します
•802.1p	現在の802.1p値を表示します
•802.1pマスク	現在の802.1pマスクを表示する
•Etherstype	現在のイーサネットタイプを表示します
•変更	
	クリック MACベースのACLパラメータを編集するには
	クリック MACベースのACLエントリを削除するには

4.10.3IPv4ベースのACL

このページには、さまざまなACLユーザーによるACLステータスが表示されます。各行は、定義されているACEを示しています。特定の場合は競合ですハードウェアの制限により、ACEはハードウェアに適用されません。図4-10-5および図4-10-6のIPv4ベースのACL画面現れる。

図4-10-5IPv4ベースのACL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
• ACL名	名前付きIPv4ベースのACLリストを作成する

ボタン

: クリックしてACL名リストを追加します。

図4-10-6ACLテーブル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	
•削除	クリック	ACL名のエントリを削除します。

4.10.4IPv4ベースのACE

ACEはいくつかのパラメータで構成されています。使用するフレームタイプに応じて、さまざまなパラメータオプションが表示されます
選択されました。 [図4-10-7](#)および [図4-10-8](#)のIPv4ベースのACE画面が表示されます。

図4-10-7IPベースのACEスクリーンショット

286

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
• ACL名	このドロップダウンリストからACL名を選択します。
• シーケンス	ACLシーケンスを設定します。
• アクション	ACEの転送アクションを示します。 ■許可：ACEに一致するフレームが転送および学習される場合があります。 ■拒否：ACEに一致するフレームはドロップされます。 ■シャットダウン：ACEのポートシャットダウンは無効になっています。
• プロトコル	このACEのプロトコルフィルタを指定します。 ■Any（IP）：プロトコルフィルタが指定されていません。 ■リストから選択：このACEで特定のプロトコルをフィルタリングする場合は、この値を入力し、このドロップダウンリストからプロトコルを選択します。 ■一致するプロトコルID：このACEで特定のプロトコルをフィルタリングする場合は、この値を選択し、現在のプロトコルIDを設定します。
• 送信元IPアドレス	このACEの送信元IPアドレスフィルタを指定します。 ■任意：送信元IPアドレスフィルタが指定されていません。 ■ユーザー定義：このACEで特定の送信元IPアドレスをフィルタリングする場合は、この値を選択してください。送信元IPアドレス値を入力するためのフィールドが表示されます。
• 送信元IPアドレス 値	送信元IPアドレスフィルタで「ユーザー定義」を選択すると、次のように入力できます。 特定の送信元IPアドレス。有効な形式は「xxx.xxx.xxx.xxx」です。そのフレーム このACEにヒットすると、この送信元IPアドレス値と一致します。
• ソースIPワイルドカード マスク	ソースIPフィルタに「ユーザー定義」を選択すると、特定のIPフィルタを入力できます ドット付き10進表記のSIPマスク。
• 宛先IPアドレス	このACEの宛先IPアドレスフィルタを指定します。 ■任意：宛先IPアドレスフィルタが指定されていません。

		<p>■ ユーザー定義：これで特定の宛先IPアドレスをフィルタリングする場合 ACE、この値を選択してください。送信元IPアドレス値を入力するためのフィールド が表示されます。</p>
・宛先IPアドレス	値	<p>宛先IPアドレスフィルターに「ユーザー定義」を選択すると、次のことができます。</p> <p>特定の宛先IPアドレスを入力します。有効な形式は「xxx.xxx.xxx.xxx」です。A このACEにヒットするフレームは、この宛先IPアドレス値と一致します。</p>
・宛先IP	ワイルドカードマスク	<p>宛先IPフィルターに「ユーザー定義」を選択すると、次のように入力できます。</p> <p>ドット付き10進表記の特定のDIPマスク。</p>
・送信元ポート		<p>このACEの送信元ポートを指定します。</p> <p>■ 任意：特定の送信元ポートが指定されていません（送信元ポートのステータスは「ドントケア」です）。</p> <p>■ シングル：このACEで特定の送信元ポートをフィルタリングする場合は、次のことができます。</p> <p>特定の送信元ポート値を入力します。送信元ポート値を入力するためのフィールド が表示されます。許容範囲はからです0に65535。このACEに当たるフレーム</p>
		<p>この送信元ポート値と一致します。</p> <p>■ 範囲：このACEで特定の送信元ポート範囲をフィルタリングする場合は、 特定の送信元ポート範囲の値を入力できます。送信元ポートを入力するためのフィールド 値が表示されます。許容範囲はからです0に65535。これに当たるフレーム ACEはこの送信元ポート値と一致します。</p>
・宛先ポート		<p>このACEの宛先ポートを指定します。</p> <p>■ 任意：特定の宛先ポートが指定されていません（宛先ポートのステータスは 「ドントケア」）。</p> <p>■ シングル：このACEで特定の宛先ポートをフィルタリングする場合は、次のことができます。</p> <p>特定の宛先ポート値を入力します。宛先ポートを入力するためのフィールド 値が表示されます。許容範囲はからです0に65535。これに当たるフレーム ACEはこの宛先ポート値と一致します。</p> <p>■ 範囲：このACEで特定の宛先ポート範囲をフィルタリングする場合は、 特定の宛先ポート範囲の値を入力できます。入力するためのフィールド 宛先ポート値が表示されます。</p>
・TCPフラグ	UGR	<p>このためのTCP「緊急ポインタフィールド重要」（URG）値を指定します エース。</p> <p>■ 設定：URGフィールドが設定されているTCPフレームは一致できる必要があります このエントリ。</p> <p>■ 設定解除：URGフィールドがセットされたTCPフレームのことができるようにはなりません このエントリに一致します。</p> <p>■ は気にしない：任意の値が（「ドント・ケア」）を許可されています。</p>
	ACK	<p>このためのTCP「Acknowledgementfieldimportant」（ACK）値を指定します エース。</p> <p>■ 設定：ACKフィールドが設定されているTCPフレームは一致できる必要があります このエントリ。</p> <p>■ 設定解除：ACKフィールドがセットされたTCPフレームのことができるようにはなりません このエントリに一致します。</p> <p>■ は気にしない：任意の値が（「ドント・ケア」）を許可されています。</p>
	PSH	<p>このACEのTCP「プッシュ機能」（PSH）値を指定します。</p> <p>■ 設定：PSHフィールドが設定されているTCPフレームは一致できる必要があります</p>

このエントリ。
■設定解除：PSHフィールドがセットされたTCPフレームのことができるようにはなりません
 このエントリに一致します。
■は気にしない：任意の値が（「ドント・ケア」）を許可されています。
 RST **■このACEのTCP「接続のリセット」（RST）値を指定します。**
セット：RSTフィールドが設定されているTCPフレームは一致する必要があります
 このエントリ。
■設定解除：RSTフィールドがセットされたTCPフレームのことができるようにはなりません
 このエントリに一致します。

288

■は気にしない：任意の値が（「ドント・ケア」）を許可されています。
 SYN このためのTCP「シーケンス番号の同期」（SYN）値を指定します
 エース。
■設定：SYNフィールドが設定されているTCPフレームは一致する必要があります
 このエントリ。
■設定解除：SYNフィールドがセットされたTCPフレームのことができるようにはなりません
 このエントリに一致します。
■は気にしない：任意の値が（「ドント・ケア」）を許可されています。
 フィン このACEのTCP「送信者からのデータはもうありません」（FIN）値を指定します。
■設定：FINフィールドが設定されているTCPフレームは一致する必要があります
 このエントリ。
■設定解除：FINフィールドがセットされているTCPフレームのことができるようにはなりません
 このエントリに一致します。
■は気にしない：任意の値が（「ドント・ケア」）を許可されています。

・サービスの種類

このACEのサービスの種類を指定します。
■任意：特定のタイプのサービスが指定されていません（宛先ポートのステータスは「ドントケア」）。
■DSCP：あなたはこのACEを持つ特定のDSCPをフィルタリングする場合は、あなたが入力することができます
 特定のDSCP値。DSCP値を入力するためのフィールドが表示されます。許可された
 範囲はある0に63。このACEにヒットするフレームは、このDSCP値と一致します。
■IP Recedence：あなたは、このACEを特定のIP recedenceをフィルタリングしたい場合は、
 特定のIP後退値を入力できます。IP後退を入力するためのフィールド
 値が表示されます。許容範囲はある0に7。このACEに当たるフレーム
 このIP後退値と一致します。

・ICMP

このACEのICMPを指定します。
■任意：特定のICMPが指定されていません（宛先ポートのステータスは「ドントケア」です）。
■リスト：このACEで特定のリストをフィルタリングする場合は、特定のリストを選択できます
 リスト値。
■プロトコルID：このACEで特定のプロトコルIDフィルターをフィルター処理する場合は、
 特定のプロトコルID値を入力できます。プロトコルID値を入力するためのフィールド
 が表示されます。許容範囲はからです0に255。このACEに当たるフレーム
 このプロトコルID値と一致します。

・ICMPコード

このACEのICMPコードフィルタを指定します。
■任意：ICMPコードフィルターが指定されていません（ICMPコードフィルターのステータスは「ドントケア」）。
■ユーザー定義：これを使用して特定のICMPコードフィルターをフィルター処理する場合

ACE、特定のICMPコード値を入力できます。入力するためのフィールド
ICMPコード値が表示されます。許容範囲はからです0に255。A

このACEにヒットするフレームは、このICMPコード値と一致します。

ボタン

: クリックしてACEリストを追加します。

図4-10-8IPv4ベースのACEテーブル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
• ACL名	現在のACL名を表示します
• シーケンス	現在のシーケンスを表示する
• アクション	現在のアクションを表示する
• プロトコル	現在のプロトコルを表示する
• 送信元IPアドレス	現在の送信元IPアドレスを表示します
• 送信元IPアドレス ワイルドカードマスク	現在の送信元IPアドレスのワイルドカードマスクを表示します
• 宛先IPアドレス現在の宛先IPアドレスを表示します	
• 宛先IPアドレス ワイルドカードマスク	現在の宛先IPアドレスのワイルドカードマスクを表示します
• 送信元ポート範囲	現在の送信元ポート範囲を表示します
• 宛先ポート 範囲	現在の宛先ポート範囲を表示します
• フラグセット	現在設定されているフラグを表示します
• DSCP	現在のDSCPを表示する
• IPの優先順位	現在のIP優先順位を表示する
• ICMPタイプ	現在のICMPタイプを表示します
• ICMPコード	現在のICMPコードを表示する
• 変更	クリック IPv4ベースのACLパラメータを編集するには
	クリック IPv4ベースのACLエントリを削除するには

4.10.5IPv6ベースのACL

このページには、さまざまなACLユーザーによるACLステータスが表示されます。各行は、定義されているACEを示しています。特定の場合は競合ですハードウェアの制限により、ACEはハードウェアに適用されません。図4-10-9および図4-10-10のIPv6ベースのACL画面現れる。

図4-10-9IPv6ベースのACL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
• ACL名	名前付きIPv6ベースのACLリストを作成する

ボタン

: クリックしてACL名リストを追加します。

図4-10-10ACLテーブル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
• 削除	クリック ACL名エントリを削除するには

4.10.6IPv6ベースのACE

ACEはいくつかのパラメータで構成されています。使用するフレームタイプに応じて、さまざまなパラメータオプションが表示されます
選択されました。図4-10-11および図4-10-12のIPv6ベースのACE画面が表示されます。

図4-10-11IPv6ベースのACE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
• ACL名	このドロップダウンリストからACL名を選択します
• シーケンス	ACLシーケンスを設定します

・アクション	<p>ACEの転送アクションを示します</p> <p>■許可：ACEに一致するフレームが転送および学習される場合があります。</p> <p>■拒否：ACEに一致するフレームはドロップされます。</p> <p>■シャットダウン：ACEのポートシャットダウンは無効になっています。</p>
・プロトコル	<p>このACEのプロトコルフィルタを指定します</p> <p>■任意（IP）：プロトコルフィルタが指定されていません。</p> <p>■リストから選択：このACEで特定のプロトコルをフィルタリングする場合は、この値を入力し、このドロップダウンリストからプロトコルを選択します。</p>
・送信元IPアドレス	<p>このACEの送信元IPアドレスフィルタを指定します</p> <p>■任意：送信元IPアドレスフィルタが指定されていません。</p> <p>■ユーザー定義：このACEで特定の送信元IPアドレスをフィルタリングする場合は、この値を選択してください。送信元IPアドレス値を入力するためのフィールドが表示されます。</p>
・送信元IPアドレス 値	<p>送信元IPアドレスフィルタで「ユーザー定義」を選択すると、次のように入力できます。</p> <p>特定の送信元IPアドレス。有効な形式は「xxxx：xxxx：xxxx：xxxx：」です。</p> <p>xxxx：xxxx：xxxx：xxxx "。このACEにヒットするフレームは、この送信元IPアドレスと一致します</p> <p>値。</p>
・ソースIPプレフィックス 長さ	<p>ソースIPフィルタに「ユーザー定義」を選択すると、特定のIPフィルタを入力できます</p> <p>ドット付き10進表記のSIPプレフィックス長。</p>
・宛先IPアドレス	<p>このACEの宛先IPアドレスフィルタを指定します。</p> <p>■任意：宛先IPアドレスフィルタが指定されていません。</p> <p>■ユーザー定義：これで特定の宛先IPアドレスをフィルタリングする場合</p> <p>ACE、この値を選択してください。送信元IPアドレス値を入力するためのフィールド</p> <p>が表示されます。</p>
・宛先IPアドレス 値	<p>宛先IPアドレスフィルタに「ユーザー定義」を選択すると、次のことができます。</p> <p>特定の宛先IPアドレスを入力します。有効な形式は「xxxx：xxxx：xxxx：xxxx：」です。</p> <p>xxxx：xxxx：xxxx：xxxx "。このACEにヒットするフレームは、この宛先IPと一致します</p> <p>アドレス値。</p>
・宛先IPプレフィックス 長さ	<p>宛先IPフィルタに「ユーザー定義」を選択すると、次のように入力できます。</p> <p>ドット付き10進表記の特定のDIPプレフィックス長。</p>
・送信元ポート	<p>このACEの送信元ポートを指定します。</p> <p>■任意：特定の送信元ポートが指定されていません（送信元ポートのステータスは「ドントケア」です）。</p> <p>■シングル：このACEで特定の送信元ポートをフィルタリングする場合は、次のことができます。</p> <p>特定の送信元ポート値を入力します。送信元ポート値を入力するためのフィールド</p> <p>が表示されます。許容範囲はからです0に65535。このACEに当たるフレーム</p>

・宛先ポート	<p>この送信元ポート値と一致します。</p> <p>■範囲：このACEで特定の送信元ポート範囲をフィルタリングする場合は、</p> <p>特定の送信元ポート範囲の値を入力できます。送信元ポートを入力するためのフィールド</p> <p>値が表示されます。許容範囲はからです0に65535。これに当たるフレーム</p> <p>ACEはこの送信元ポート値と一致します。</p> <p>このACEの宛先ポートを指定します。</p> <p>■任意：特定の宛先ポートが指定されていません（宛先ポートのステータスは「ドントケア」）。</p> <p>■シングル：このACEで特定の宛先ポートをフィルタリングする場合は、次のことができます。</p> <p>特定の宛先ポート値を入力します。宛先ポートを入力するためのフィールド</p>
--------	--

値が表示されます。許容範囲はからです0に65535。これに当たるフレーム

ACEはこの宛先ポート値と一致します。

■ **範囲**：このACEで特定の宛先ポート範囲をフィルタリングする場合は、
特定の宛先ポート範囲の値を入力できます。入力するためのフィールド
宛先ポート値が表示されます。

•TCPフラグ

UGR このためのTCP「緊急ポインタフィールド重要」（URG）値を指定します
エース。
■ **設定**：URGフィールドが設定されているTCPフレームは一致できる必要があります
このエントリ。
■ **設定解除**：URGフィールドがセットされたTCPフレームのことができるようにはなりません
このエントリに一致します。
■ **は気にしない**：任意の値が（「ドント・ケア」）を許可されています。
ACK このためのTCP「Acknowledgementfieldimportant」（ACK）値を指定します
エース。
■ **設定**：ACKフィールドが設定されているTCPフレームは一致できる必要があります
このエントリ。
■ **設定解除**：ACKフィールドがセットされたTCPフレームのことができるようにはなりません
このエントリに一致します。
■ **は気にしない**：任意の値が（「ドント・ケア」）を許可されています。
PSH このACEのTCP「ブッシュ機能」（PSH）値を指定します。
■ **設定**：PSHフィールドが設定されているTCPフレームは一致できる必要があります
このエントリ。
■ **設定解除**：PSHフィールドがセットされたTCPフレームのことができるようにはなりません
このエントリに一致します。
■ **は気にしない**：任意の値が（「ドント・ケア」）を許可されています。
RST このACEのTCP「接続のリセット」（RST）値を指定します。
■ **設定**：RSTフィールドが設定されているTCPフレームは一致できる必要があります
このエントリ。
■ **設定解除**：RSTフィールドがセットされたTCPフレームのことができるようにはなりません
このエントリに一致します。

■ **は気にしない**：任意の値が（「ドント・ケア」）を許可されています。
SYN このためのTCP「シーケンス番号の同期」（SYN）値を指定します
エース。
■ **設定**：SYNフィールドが設定されているTCPフレームは一致できる必要があります
このエントリ。
■ **設定解除**：SYNフィールドがセットされたTCPフレームのことができるようにはなりません
このエントリに一致します。
■ **は気にしない**：任意の値が（「ドント・ケア」）を許可されています。
フィン このACEのTCP「送信者からのデータはもうありません」（FIN）値を指定します。
■ **設定**：FINフィールドが設定されているTCPフレームは一致できる必要があります
このエントリ。
■ **設定解除**：FINフィールドがセットされているTCPフレームのことができるようにはなりません
このエントリに一致します。
■ **は気にしない**：任意の値が（「ドント・ケア」）を許可されています。
このACEのサービスの種類を指定します。

•サービスの種類

	<p>■ 任意：特定のタイプのサービスが指定されていません（宛先ポートのステータスは「ドントケア」）。</p> <p>■ DSCP：あなたはこのACEを持つ特定のDSCPをフィルタリングする場合は、あなたが入力することができます特定のDSCP値。DSCP値を入力するためのフィールドが表示されます。許可された範囲はある0に63。このACEにヒットするフレームは、このDSCP値と一致します。</p> <p>■ IP Recedence：あなたは、このACEを特定のIP recedenceをフィルタリングしたい場合は、特定のIP後退値を入力できます。IP後退を入力するためのフィールド値が表示されます。許容範囲はある0に7。このACEに当たるフレームこのIP後退値と一致します。</p>
• ICMP	<p>このACEのICMPを指定します。</p> <p>■ 任意：特定のICMPが指定されていません（宛先ポートのステータスは「ドントケア」です）。</p> <p>■ リスト：このACEで特定のリストをフィルタリングする場合は、特定のリストを選択できますリスト値。</p> <p>■ プロトコルID：このACEで特定のプロトコルIDフィルターをフィルター処理する場合は、特定のプロトコルID値を入力できます。プロトコルID値を入力するためのフィールドが表示されます。許容範囲はからです0に255。このACEに当たるフレームこのプロトコルID値と一致します。</p>
• ICMPコード	<p>このACEのICMPコードフィルタを指定します。</p> <p>■ 任意：ICMPコードフィルターが指定されていません（ICMPコードフィルターのステータスは「ドントケア」です）。</p> <p>■ ユーザー定義：このACEで特定のICMPコードフィルターをフィルタリングする場合は、特定のICMPコード値を入力できます。ICMPコードを入力するためのフィールド値が表示されます。許容範囲はからです0に255。これに当たるフレームACEはこのICMPコード値と一致します。</p>

295

ボタン

：クリックしてACEリストを追加

図4-10-12IPv6ベースのACEテーブル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
• ACL名	現在のACL名を表示します
• シーケンス	現在のシーケンスを表示する
• アクション	現在のアクションを表示する
• プロトコル	現在のプロトコルを表示する
• 送信元IPアドレス	現在の送信元IPアドレスを表示します

•送信元IPアドレス ワイルドカードマスク	現在の送信元IPアドレスのワイルドカードマスクを表示します
•宛先IPアドレス	現在の宛先IPアドレスを表示します
•宛先IPアドレス ワイルドカードマスク	現在の宛先IPアドレスのワイルドカードマスクを表示します
•送信元ポート範囲	現在の送信元ポート範囲を表示します
•宛先ポート 範囲	現在の宛先ポート範囲を表示します
•フラグセット	現在設定されているフラグを表示します
• DSCP	現在のDSCPを表示する
• IPの優先順位	現在のIP優先順位を表示する
• ICMPタイプ	現在のICMPタイプを表示します
• ICMPコード	現在のICMPコードを表示する
•変更	
	クリック IPv6ベースのACLパラメータを編集します。
	クリック IPv6ベースのACLエントリを削除します。

4.10.7ACLバインディング

このページでは、ポリシーコンテンツを適切なACLにバインドできます。図4-10-13および図のACLポリシー画面4-10-14が表示されます。

図4-10-13ACLバインディン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
•バインディングポート	このドロップダウンリストからポートを選択します
• ACL選択	このドロップダウンリストからACLリストを選択します

ボタン

：クリックして変更を適用します。

図4-10-14ACLバインディングテーブル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
•ポート	論理ポートのスイッチポート番号
• MACACL	現在のMACACLを表示する
• IPv4ACL	現在のIPv4ACLを表示する
• IPv6ACL	現在のIPv6ACLを表示する
•変更	
	クリック ACLバインディングテーブルパラメータを編集するには
	クリック ACLバインディングエントリを削除するには

4.11MACアドレステーブル

フレームの切り替えは、フレームに含まれるDMACアドレスに基づいています。マネージドスイッチは、マップするテーブルを作成します
フレームがどのポートに行くべきかを知るためのスイッチポートへのMACアドレス（フレーム内のDMACアドレスに基づく）。

このテーブルには、静的エントリと動的エントリの両方が含まれています。静的エントリは、次の場合にネットワーク管理者によって構成されます。
管理者は、DMACアドレスとスイッチポートの間で固定マッピングを実行したいと考えています。

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）も含まれています。
SMACアドレスは、これらの動的MACアドレスで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。動的
設定可能な後に対応するSMACアドレスを持つフレームが見られない場合、エントリはMACテーブルから削除されます
年齢時間。

4.11.1 静的MAC設定

MACテーブルの静的エントリをこのテーブルに示します。MACテーブルは、最初にVLAN IDでソートされ、次にMACアドレスでソートされます。
図4-11-1および図4-11-2の静的MAC設定画面が表示されます。

図4-11-1スタティックMAC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	このインターフェイスに関連付けられている物理アドレス
• VLAN	このドロップダウンリストからVLANを選択します
• ポート	このドロップダウンリストからポートを選択します

ボタン

：クリックして新しい静的MACアドレスを追加します。

図4-11-2StaticsMAC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
• いいえ。	エントリー数です

• MACアドレス	エントリのMACアドレス
• VLAN	エントリのVLANID
• ポート	現在のポートを表示する
• 削除	クリック 静的MACステータスエントリを削除するには

4.11.2MACフィルタリング

MACアドレスをフィルタリングすることにより、スイッチは設定されたMACアドレスを簡単にフィルタリングし、安全性の低下を減らすことができます。静的MAC
[図4-11-3](#)および[図4-11-4](#)の設定画面が表示されます。

図4-11-3MACフィルタリング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	このインターフェイスに関連付けられている物理アドレス
• VLAN（1～4096）	この特定のVLANのIDを示します

ボタン

：クリックして、新しいMACフィルタリング設定を追加します。

図4-11-4StaticsMAC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
• いいえ。	エントリー数です
• MACアドレス	エントリのMACアドレス
• VLAN	エントリのVLANID
• 削除	クリック 静的MACステータスエントリを削除します。

4.11.3動的アドレス設定

デフォルトでは、動的エントリは300秒後にMACテーブルから削除されます。動的アドレス設定/ステータス画面
中図4-11-5および図4-11-6表示されます。

図4-11-5動的アドレス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
・エージングタイム	学習したエントリが破棄されるまでの時間 範囲：10～630秒。 デフォルト：300秒

ボタン

：クリックして変更を適用します。

図4-11-6動的アドレス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
・エージングタイム	現在のエージングタイムを表示します

4.11.4動的学習

動的MACテーブル

動的学習MACテーブルはこのページに表示されます。MACテーブルは、最初にVLAN IDでソートされ、次にMACアドレスでソートされます。ザ・

図4-11-6および図4-11-7の動的学習画面が表示されます。

図4-11-6動的に学習した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
・ポート	このドロップダウンリストからポートを選択します
・VLAN	このドロップダウンリストからVLANを選択します
・MACアドレス	このインターフェイスに関連付けられている物理アドレス

ボタン

：「MACアドレスから開始」および「VLAN」入力フィールドから表示されているテーブルを更新します

：すべての動的エントリをフラッシュします

図4-11-7MACアドレス情報のスクリーンショット

オブジェクト	説明
・MACアドレス	エントリのMACアドレス
・VLAN	エントリのVLANID

・タイプ	エントリが静的エントリか動的エントリかを示します
・ポート	エントリのメンバーであるポート

ボタン

: クリックすると、動的MACアドレスが静的MACアドレスに追加されます。

4.12 LLDP

4.12.1リンク層検出プロトコル

Link Layer Discovery Protocol（LLDP）は、ローカルブロードキャスト上の隣接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。ドメイン。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。アドバタイズ情報は、IEEE 802.1ab標準に準拠したTypeLength Value（TLV）形式で表され、詳細を含めることができます。

デバイスの識別、機能、構成設定など。LLDPは、情報を保存および維持する方法も定義します

検出した隣接ネットワークノードについて収集しました。

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) は、管理を目的としたLLDPの拡張機能です。

Voice overIP電話やネットワークスイッチなどのエンドポイントデバイス。LLDP-MED TLVは、次のような情報をアドバタイズします。

ネットワークポリシー、電源、インベントリ、およびデバイスの場所の詳細。LLDPおよびLLDP-MED情報はSNMPで使用できます

トラブルシューティングを簡素化し、ネットワーク管理を強化し、正確なネットワークトポロジを維持するためのアプリケーション。

4.12.2LLDPグローバル設定

このページでは、ユーザーは現在のLLDPポート設定を検査および構成できます。LLDPグローバル設定および構成画面

中図4-12-1および図4-12-2表示されます。

図4-12-1グローバル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
•有効にする	LLDP機能をグローバルに有効または無効にします
•LLDP PDUを無効にする アクション	LLDP PDU無効化アクションを設定します。「フィルタリング」、「ブリッジング」、「フラッディング」を含めます。 ■フィルタリング ：すべてのLLDP PDUを破棄します。 ■ブリッジング ：同じVLANでLLDP PDUを送信します。 ■フラッディング ：すべてのポートにLLDP PDUを送信します。
•送信間隔	スイッチは定期的にLLDPフレームをネイバーに送信して、最新のネットワーク検出情報。各LLDP間の間隔 フレームは、 送信間隔 の値によって決定されます。有効な値は次のとおりです 5〜32768秒に制限されています。 デフォルト：30秒 この属性は、次のルールに準拠する必要があります。 (送信間隔*ホールドタイム乗数) ≤65536、および送信間隔 >= (4 *遅延間隔)
•ホールドタイム乗数	各LLDPフレームには、情報の長さに関する情報が含まれています。 LLDPフレームは有効と見なされます。LLDP情報の有効期間はに設定されています ホールドタイムに送信間隔 秒を掛けたもの。有効な値は次のとおりです 2〜10回に制限されています。
•再初期化の遅延	ポートが無効になると、LLDPが無効になるか、スイッチがLLDPで再起動されます。 シャットダウンフレームが隣接ユニットに送信され、LLDPがそのことを通知します 情報はもう有効ではありません。 TxReinit は秒数を制御します シャットダウンフレームと新しいLLDP初期化の間。有効な値は次のとおりです 1〜10秒に制限されています。
•送信遅延	一部の構成（IPアドレスなど）が変更された場合、新しいLLDPフレームは 送信されますが、LLDPフレーム間の時間は常に少なくとも 送信遅延 秒の値。 送信遅延 は、1/4を超えることはできません 送信間隔 の値。有効な値は1〜8192秒に制限されています。 この属性は、次のルールに準拠する必要があります。 (4 *遅延間隔) ≤送信間隔
•LLDP-MEDファストスタート 繰り返しカウント	中に送信するLLDP MED Fast Start LLDP PDUの量を設定します LLDP-MEDファストスタートメカニズムのアクティブ化プロセス。

秒単位のTTLは、次のルールに基づいています。

(送信間隔*ホールドタイム乗数) ≤65536。
したがって、デフォルトのTTLは4 * 30 = 120秒です。

ポートが無効になると、LLDPが無効になるか、スイッチがLLDPで再起動されます。
シャットダウンフレームが隣接ユニットに送信され、LLDPがそのことを通知します
情報はもう有効ではありません。**TxReinit**は秒数を制御します
シャットダウンフレームと新しいLLDP初期化の間。有効な値は次のとおりです
1〜10秒に制限されています。

一部の構成（IPアドレスなど）が変更された場合、新しいLLDPフレームは
送信されますが、LLDPフレーム間の時間は常に少なくとも
送信遅延秒の値。**送信遅延**は、1/4を超えることはできません
送信間隔の値。有効な値は1〜8192秒に制限されています。

この属性は、次のルールに準拠する必要があります。

(4 *遅延間隔) ≤送信間隔

中に送信するLLDP MED Fast Start LLDP PDUの量を設定します
LLDP-MEDファストスタートメカニズムのアクティブ化プロセス。

範囲：1～10/ケット。
デフォルト：3/ケット

MED Fast Start Count/パラメーターはタイマーの一部であり、
LLDP-MED FastStartメカニズムがポートに対してアクティブです。LLDP-MED FastStartは
LLDPのタイムリーな起動に不可欠であり、したがって迅速な可用性に不可欠です
緊急通報サービスの。

ボタン

：クリックして変更を適用します。

図4-12-2LLDPグローバル構成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
• LLDPの有効化	現在のLLDPステータスを表示します
• LLDP PDUを無効にする	現在のLLDP PDU無効化アクションを表示します
アクション	
•送信間隔	現在の送信間隔を表示します
•ホールドタイム乗数	現在のホールドタイム乗数を表示します
•再初期化の遅延	現在の再初期化遅延を表示します
•送信遅延	現在の送信遅延を表示します
• LLDP-MEDファストスタート	現在のLLDP-MED Fast Start Repeat Countを表示します
繰り返しカウント	

4.12.3LLDPポート設定

LLDPポート設定を使用して、メッセージがあるかどうかなど、個々のインターフェイスのメッセージ属性を指定します。
送信、受信、または送信と受信の両方。図4-12-3のLLDPポート設定およびステータス画面と
図4-12-4が表示されます。

図4-12-3LLDPポートの構成とオプションのTLV選択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
・ポート選択	このドロップダウンリストからポートを選択します
・州	LLDPプロトコルデータのLLDPメッセージ送信および受信モードを有効にします 単位。オプション：

	<div><div><div></div><div>Txのみ</div></div><div><div></div><div>Rxのみ</div></div><div><div></div><div>TxRx</div></div><div><div></div><div>無効</div></div></div>
・ポート選択	このドロップダウンリストからポートを選択します
・オプションのTLV選択	アドバタイズされたメッセージのTLVフィールドに含まれる情報を構成します。 <div><div>■システム名：チェックすると、「システム名」がLLDPに含まれます 送信された情報。</div><div>■ポートの説明：チェックすると、「ポートの説明」はに含まれます LLDP情報が送信されました。</div><div>■システムの説明：チェックすると、「システムの説明」は次のようになります。 送信されるLLDP情報に含まれます。</div><div>■システム機能：チェックすると、「システム機能」が含まれます 送信されるLLDP情報で。</div><div>■802.3 MAC-PHY："802.3 MAC-PHYが"に含まれているチェックボックスをオンにします LLDP情報が送信されました。</div><div>■802.3リンクアグリゲーション：チェックすると、「802.3リンクアグリゲーションが」 送信されるLLDP情報に含まれます。</div><div>■802.3最大フレームサイズ：「802.3最大を確認 「フレームサイズ」は、送信されるLLDP情報に含まれています。</div><div>■管理アドレス：チェックすると、「管理アドレス」は 送信されるLLDP情報に含まれます。</div><div>■802.1 PVID：チェックする"802.1 PVIDは、" LLDPに含まれています 送信された情報。</div></div>

ボタン

：クリックして変更を適用

図4-12-4LLDPポート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
・ポート	論理ポートのスイッチポート番号
・州	現在のLLDPステータスを表示します
・選択されたオプション	現在選択されているオプションのTLVを表示します
TLV	

図4-12-5および図4-12-6のVLAN名TLVVLAN選択およびLLDPポートVLANTLVステータス画面が表示されます。

図4-12-5VLAN名TLV選択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
・ポート選択	このドロップダウンリストからポートを選択します。
・VLAN選択	このドロップダウンリストからVLANを選択します。

ボタン

: クリックして変更を適用します。

図4-12-6LLDPポートVLANTLV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
・ポート	論理ポートのスイッチポート番号
・選択されたVLAN	現在選択されているVLANを表示する

4.12.4LLDPローカルデバイス

LLDPローカルデバイス情報画面を使用して、MACアドレス、シャーシID、スイッチなどのスイッチに関する情報を表示します。
管理IPアドレス、およびポート情報。図4-12-7の[ローカルデバイスの概要]画面と[ポートステータス]画面および
図4-12-8が表示されます。

図4-12-7ローカルデバイスの概要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
・シャーシIDサブタイプ	現在のシャーシIDサブタイプを表示します
・シャーシID	現在のシャーシIDを表示します
・システム名	現在のシステム名を表示する
・システムの説明	現在のシステムの説明を表示する
・サポートされている機能現在サポートされている機能	を表示します
・有効な機能	有効になっている現在の機能を表示する
・ポートIDサブタイプ	現在のポートIDサブタイプを表示します

図4-12-8ポート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
・インターフェース	論理ポートのスイッチポート番号。
・LLDPステータス	現在のLLDPステータスを表示します
・LLDPMEDステータス	現在のLLDPMEDステータスを表示します

4.12.5LLDP削除デバイス

このページには、すべてのLLDP削除デバイスのステータスの概要が表示されます。表示されるテーブルには、各ポートの行が含まれています。
LLDPネイバーが検出されました。図4-12-9の[LLDPデバイスの削除]画面が表示されます。

図4-12-9LLDPリモートデバ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
・ローカルポート	現在のローカルポートを表示する
・シャーシIDサブタイプ	現在のシャーシIDサブタイプを表示します
・シャーシID	シャーシIDは、ネイバーのLLDPフレームのIDです。
・ポートIDサブタイプ	現在のポートIDサブタイプを表示します
・ポートID	リモートポートIDは、隣接ポートのIDです。
・システム名	システム名は、ネイバーユニットによってアドバタイズされた名前です。
・存続時間	現在の存続時間を表示します

ボタン

：クリックしてLLDP削除デバイスエントリを削除します。

：クリックしてLLDP削除デバイスを更新します。

4.12.6MEDネットワークポリシー

ネットワークポリシー検出により、VLAN構成との不一致の問題を効率的に検出および診断できます。

関連付けられたレイヤー2およびレイヤー3属性を使用して、そのポート上の特定のプロトコルアプリケーションのセットに適用します。不適切

ネットワークポリシーの構成はVoIP環境で非常に重要な問題であり、音声品質が低下することがよくあります。

またはサービスの喪失。

ポリシーは、インタラクティブなど、特定の「リアルタイム」ネットワークポリシー要件を持つアプリケーションでの使用のみを目的としています。

音声および/またはビデオサービス。

アダプタ化されるネットワークポリシー属性は次のとおりです。

- 1.レイヤー2VLAN ID (IEEE 802.1Q-2003)
- 2.レイヤ2優先度値 (IEEE 802.1D-2004)
- 3.レイヤー3Diffservコードポイント (DSCP) 値 (IETF RFC 2474)

このネットワークポリシーは潜在的にアダプタ化され、特定のポートでサポートされているアプリケーションタイプの複数のセットに関連付けられています。

具体的に対処されるアプリケーションの種類は次のとおりです。

- 1.声
- 2.ゲストボイス
- 3.ソフトフォンボイス
- 4.ビデオ会議
- 5.ストリーミングビデオ
- 6.制御/シグナリング (上記のメディアタイプに対して個別のネットワークポリシーを条件付きでサポートします)

大規模なネットワークでは、組織全体で複数のVoIPポリシーがサポートされ、アプリケーションタイプごとに異なるポリシーがサポートされる場合があります。

LLDP-MEDを使用すると、ポートごとに複数のポリシーをアダプタ化でき、それぞれが異なるアプリケーションタイプに対応します。異なるポート


同じネットワーク接続デバイス上で、認証されたユーザーIDに基づいて、異なるポリシーのセットをアダプタ化する場合があります。

ポート構成。

LLDP-MEDは、ネットワーク接続デバイスとの間以外のリンクで実行することを目的としていないことに注意してください。

エンドポイント、したがって、集約されたリンクで頻繁に実行される多数のネットワークポリシーをアダプタ化する必要はありません

LANの内部。

音声自動モードの設定、ネットワークポリシーの設定とでLLDP MEDネットワークポリシー表画面

[4-12-10](#)および [4-12-11](#)が表示されます。

図4-12-10音声自動モードの設定とネットワークポリシー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
• LLDPMEDポリシー	音声アプリケーションモードのLLDPMEDポリシーを設定します
音声アプリケーション	
• ネットワークポリシー	このドロップダウンリストからネットワークポリシー番号を選択します
数	
• アプリケーションタイプ	アプリケーションタイプの使用目的：
	<p>音声-専用IPテレフォニーハンドセットおよび他の同様のアプライアンスで使用するため</p> <p>インタラクティブ音声サービスのサポート。これらのデバイスは通常、展開を容易にし、セキュリティを強化するための個別のVLANデータアプリケーション。</p> <p>音声シグナリング-異なるポリシーを必要とするネットワークボロジで使用するため</p> <p>音声メディアよりも音声シグナリング。このアプリケーションタイプは、Voiceでアダプタイズされたものと同じネットワークポリシーがすべて適用される場合、アダプタイズされますアプリケーションポリシー。</p> <p>ゲストボイス-ゲスト用に個別の「限定機能セット」音声サービスをサポート</p> <p>独自のIPテレフォニーハンドセットおよび他の同様のものを使用するユーザーおよび訪問者</p> <p>インタラクティブ音声サービスをサポートするアプライアンス。</p> <p>ゲスト音声シグナリング-異なるものを必要とするネットワークボロジで使用するため</p> <p>ゲスト音声メディアよりもゲスト音声シグナリングのポリシー。この</p> <p>同じネットワークポリシーがすべて適用される場合は、アプリケーションタイプをアダプタイズしないでください。</p> <p>ゲストボイスアプリケーションポリシーでアダプタイズされたもの。</p>

ソフトフォン音声-一般的なデータ中心のソフトフォンアプリケーションで使用するため

PCやラップトップなどのデバイス。このクラスのエンドポイントは頻繁にあるとしても複数のVLANをサポートし、通常は「タグなし」を使用するように構成されます

VLANまたは単一の「タグ付き」データ固有VLAN。ネットワークポリシーが定義されている場合

「タグなし」VLAN（下記のタグ付きフラグを参照）で使用する場合は、L2優先度

フィールドは無視され、DSCP値のみが関連性を持ちます。

ビデオ会議-専用のビデオ会議機器および

リアルタイムのインタラクティブなビデオ/オーディオサービスをサポートする他の同様のアプライアンス。

アプリストリーミングビデオ-ブロードキャストまたはマルチキャストベースのビデオコンテンツで使用するため

ストリーミングビデオサービスをサポートする配信およびその他の同様のアプリケーション

特定のネットワークポリシー処理が必要です。TCPに依存するビデオアプリケーション

	<p>バッファリングを使用することは、このアプリケーションタイプの使用目的ではありません。</p> <p>ビデオシグナリング 個別のポリシーを必要とするネットワークポロジで使用するため</p> <p>ビデオメディアよりもビデオシグナリング。このアプリケーションタイプは、</p> <p>ビデオで宣伝されているものと同じネットワークポリシーがすべて適用される場合は宣伝されます</p> <p>会議アプリケーションポリシー。</p>
• VLANID	IEEE 802.1Q-2003で定義されているポートのVLAN識別子（VID）
• タグ	<p>タグ 指定されたアプリケーション・タイプが使用されているかどうかを示すには「タグ付けし」または「タグなし」VLAN。</p> <p>タグなしは、デバイスがタグなしフレーム形式を使用していることを示します。</p> <p>IEEE802.1Q-2003で定義されているタグヘッダーは含まれていません。これで</p> <p>この場合、VLAN IDとレイヤ2優先度フィールドの両方が無視され、</p> <p>DSCP値には関連性があります。</p> <p>タグ付きは、デバイスがIEEE802.1Qタグ付きフレーム形式を使用していることを示します。</p> <p>また、VLANIDとレイヤー2の優先順位の値の両方が使用されていること</p> <p>DSCP値として。タグ付けされた形式には、</p> <p>タグヘッダー。タグ付きフレーム形式には、優先タグ付きフレームも含まれます。</p> <p>IEEE802.1Q-2003で定義されています。</p>
• L2優先度	<p>L2優先度は、指定されたアプリケーションタイプに使用されるレイヤー2優先度です。L2</p> <p>優先度は、IEEEで定義されているように、8つの優先度レベル（0から7）のいずれかを指定できます。</p> <p>802.1D-2004。値0は、で定義されているデフォルトの優先度の使用を表します。</p> <p>IEEE802.1D-2004。</p>
• DSCP	<p>指定されたDiffServノードの動作を提供するために使用されるDSCP値</p> <p>IETF RFC2474で定義されているアプリケーションタイプ。DSCPには64のいずれかが含まれる場合があります</p> <p>コードポイント値（0から63）。値0は、デフォルトの使用を表します</p> <p>RFC2475で定義されているDSCP値。</p>

ボタン

: クリックして変更を適用します。

図4-12-11LLDPMEDネットワークポリシーテーブル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
• ネットワークポリシー	現在のネットワークポリシー番号を表示します

数	
・アプリケーション	現在のアプリケーションを表示する
・VLANID	現在のVLANIDを表示します
・VLANタグ	現在のVLANタグのステータスを表示します
・L2優先度	現在のL2優先度を表示します
・DSCP値	現在のDSCP値を表示します

ボタン

: クリックして、LLDPMEDネットワークポリシーテーブルエントリを削除します。

4.12.7MEDポート設定

図4-12-12および図4-12-13のPortLLDPMED構成/ポート設定テーブル画面が表示されます。

図4-12-12ポートLLDPMED構成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
・ポート選択	このドロップダウンリストからポートを選択します
・MEDの有効化	MED構成を有効または無効にします
・MEDオプションのTVL	アドバタイズされたMEDTLVフィールドに含まれる情報を設定します メッセージ。 -ネットワークポリシー-このオプションはネットワークポリシー構成をアドバタイズします VLAN構成の検出と診断を支援する情報 ポートの不一致。不適切なネットワークポリシー構成は、しばしば

音声品質の低下または完全なサービスの中断。

-location -このオプションは、位置識別の詳細をアドバタイズします。

-インベントリ-このオプションは、インベントリに役立つデバイスの詳細をアドバタイズします
メーカー、モデル、ソフトウェアバージョンなどの管理
適切な情報。

• MEDネットワークポリシー このドロップダウンリストからMEDネットワークポリシーを選択します

ボタン

：クリックして変更を適用します。

図4-12-13ポートLLDPMED構成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
•インターフェース	論理ポートのスイッチポート番号
•LLDPMEDステータス	現在のLLDPMEDステータスを表示します
•アクティブ	現在のアクティブステータスを表示します
•アプリケーション	現在のアプリケーションを表示する
•場所	現在地を表示する
•在庫	現在の在庫を表示する

図4-12-14および図4-12-15のMEDロケーション設定およびLLDPMEDポートロケーションテーブル画面が表示されます。

図4-12-14ポートLLDPMED構成のスクリーンショット

318

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	このドロップダウンリストからポートを選択します
•ロケーション座標	このエントリが属する場所の座標を識別する文字列
•ロケーションシビック住所	このエントリが属する場所の市民の住所を識別する文字列
•場所ESCELIN	このエントリが属する場所ESCELINを識別する文字列

ボタン

: クリックして変更を適用します。

図4-12-15LLDPMEDポートロケーションテーブル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
--------	----

•ポート	論理ポートのスイッチポート番号
•コーディネート	現在の座標を表示します
•市民の住所	現在の市民の住所を表示する
•ESCELIN	現在のESCELINを表示する

4.12.8LLDPの過負荷

図4-12-16のLLDPポートオーバーロード画面が表示されます。

図4-12-16LLDPポートの過負荷テーブル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
•インターフェース	論理ポートのスイッチポート番号
•合計（バイト）	通常パケットで送信されるLLDP情報の合計バイト数
•送信するために残された（バイト）	パケットでLLDP情報を送信することもできる使用可能なバイトの総数
•ステータス	TLVのステータスを示します
•必須のTLV	TLVの必須グループが送信されたか過負荷になったかを表示します
•MED機能	機能パケットが送信されたか、過負荷になったかを表示します
•MEDの場所	ロケーションパケットが送信されたか過負荷になったかを表示します
•MEDネットワークポリシー	ネットワークポリシーパケットが送信されたか過負荷になっているかを表示します
•MED拡張パワー	MDIパケットを介した拡張電力が送信されたか過負荷になったかを表示します

・オプションのTLV	MDIバケットを介してLLDPMED拡張電力が送信された場合、または送信された場合 過負荷
・MEDインベントリ	TLVの必須グループが送信されたか過負荷になったかを表示します
・802.1TLV	802.1TLVが送信されたか過負荷になっているかを表示します

4.12.9LLDP統計

[LLDPデバイス統計]画面を使用して、スイッチに接続されているLLDP対応デバイスおよびLLDPの一般的な統計を確認します
すべてのローカルインターフェイスで送受信されるプロトコルメッセージ。図4-12-17のLLDPグローバルおよびポート統計画面
そして図は4-12-18表示されます。

図4-12-17LLDPグローバル統計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
・挿入	スイッチの再起動後に追加された新しいエントリの数を示します。 \
・削除	スイッチの再起動後に削除された新しいエントリの数を示します。 \
・ドロップ	エントリテーブルがいっぱいになったためにドロップされたLLDPフレームの数を示します。 \
・エイジアウト	Time-To-Liveの有効期限が切れたために削除されたエントリの数を示します。 \

ボタン

：クリックして統計をクリアします

：クリックして統計を更新します

図4-12-18LLDPポート統計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
•ポート	LLDPフレームが受信または送信されるポート
•TXフレーム-合計	ポートで送信されたLLDPフレームの数
•RXフレーム-合計	ポートで受信されたLLDPフレームの数
•RXフレーム-破棄	LLDPフレームがポートで受信され、スイッチの内部テーブルがいっぱいになった場合、LLDPフレームがカウントされ、破棄されます。この状況は「多すぎる」として知られています LLDP標準の「Neighbors」。LLDPフレームにはテーブルに新しいエントリが必要です シャーシIDまたはリモートポートIDがまだテーブルに含まれていない場合。 特定のポートがリンクダウンすると、LLDPのエントリがテーブルから削除されます。 シャットダウンフレームを受信したとき、またはエントリが期限切れになったとき。
•RXフレーム-エラー	ある種のエラーを含む受信LLDPフレームの数。
•RXTLV -破棄	各LLDPフレームには、TLVと呼ばれる複数の情報を含めることができます。 （TLVは「TypeLengthValue」の略です）。TLVの形式が正しくない場合は、カウントされ、廃棄されました。
•RXTLV - 認識されない	整形形式のTLVの数ですが、タイプ値が不明です
•RXエイジャウト-合計	受け取った組織的なTLVの数

4.13 診断

このセクションでは、トラブルシューティングのための物理層およびIP層のネットワーク診断ツールを提供します。診断ツールはネットワークマネージャーがポイントツーポイントとより良いサービスの顧客の間の問題を迅速に診断できるように設計されています。

[診断]メニュー項目を使用して、マネージドスイッチの基本的な管理の詳細を表示および構成します。システムの下で

システム情報を構成および表示するために、以下のトピックが提供されています。

このセクションには、次の項目があります。

- ケーブル診断
- pingテスト
- IPv6Pingテスト
- トレースルート

4.13.1 ケーブル診断

Cable Diagnosticsは、銅線ケーブルでテストを実行します。これらの機能には、ケーブルの長さを識別し、動作条件、およびCat5ツイストペアケーブルで発生する可能性のあるさまざまな一般的な障害を特定します。あるかもしれませんが次の2つのステータス：

- 1000Base-Tモードのツイストペアインターフェイスでリンクが確立されている場合、ケーブル診断はリンクまたはデータ転送の中断。
- リンクが100Base-TXまたは10Base-Tで確立されている場合、ケーブル診断により、診断中にリンクがドロップされます。走っている。

診断が終了すると、リンクが再確立されます。また、以下の機能が利用できます。

- ケーブルペア間の結合。
- ケーブルペア終端
- ケーブル長

ケーブル診断は、15～100メートルの長さのケーブルに対してのみ正確です。

図4-13-1銅線テスト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
・ポート	このドロップダウンリストからポートを選択します
ボタン	
	: クリックして診断を実行します

図4-13-2テスト結果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
・ポート	ケーブル診断を要求しているポート
・チャンネルA～D	現在のチャンネルステータスを表示します
・ケーブル長A～D	現在のケーブル長を表示します
・結果	テスト結果を表示する

4.13.2 Ping

pingとIPv6pingを使用すると、ICMP PING/パケットを発行して、IP接続の問題のトラブルシューティングを行うことができます。マネージドスイッチ ICMP/パケットを送信し、応答を受信するとシーケンス番号とラウンドトリップ時間が表示されます。

4.13.3pingテスト

このページでは、ICMP PING/パケットを発行して、IP接続の問題をトラブルシューティングできます。

「適用」を押すと、ICMP/パケットが送信され、シーケンス番号とラウンドトリップ時間が表示されます。

返信の受信。すべてのパケットへの応答が受信されるまで、またはタイムアウトが発生するまで、ページは自動的に更新されます。ザ・

[図4-13-3のICMPping画面が表示されます。](#)

図4-13-3ICMPPing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
• IPアドレス	宛先IPアドレス
• カウント	送信するエコー要求の数
• 間隔（秒単位）	各ICMPパケットの送信間隔
• サイズ（バイト単位）	ICMPパケットのペイロードサイズ。値の範囲は8バイトから5120バイトです。
• pingの結果	現在のping結果を表示します。

ボタン

：クリックしてICMPパケットを送信します。

ターゲットIPアドレスがスイッチの同じネットワークサブネット内にあることを確認してください。そうでない場合は、設定する必要があります。
正しいゲートウェイIPアドレス。

4.13.4 IPv6Pingテスト

このページでは、ICMPv6 PINGパケットを発行して、IPv6接続の問題のトラブルシューティングを行うことができます。
「適用」を押すと、5つのICMPv6パケットが送信され、シーケンス番号とラウンドトリップ時間が表示されます。
返信の受信。すべてのパケットへの応答が受信されるまで、またはタイムアウトが発生するまで、ページは自動的に更新されます。ザ・
図4-13-4のICMPv6Ping画面が表示されます。

図4-13-4ICMPv6Ping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
• IPアドレス	宛先IPv6アドレス
• カウント	送信するエコー要求の数
• 間隔（秒単位）	各ICMPパケットの送信間隔
• サイズ（バイト単位）	ICMPパケットのペイロードサイズ。値の範囲は8バイトから5120バイトです
• pingの結果	現在のping結果を表示します

ボタン

：クリックしてICMPv6パケットを送信します

4.13.5トレースルーター

Traceroute機能は、データパケットが送信元デバイスから宛先に移動するゲートウェイをテストするためのものです。
デバイスなので、ネットワークのアクセス可能性を確認し、ネットワーク障害を特定します。

Traceroute関数の実行手順は、次の要素で構成されます。まず、TTLが1のデータパケットが宛先アドレスに送信されます。
最初のホップはICMPエラーメッセージを返し、このパケットを送信できないことを通知します（TTLタイムアウトのため）、TTL付きのデータパケット
2時に送信されます。また、送信ホップはTTLタイムアウトリターンである可能性がありますが、データパケットが送信されるまで手順は続行されます。
先。これらの手順は、ICMP TTLタイムアウトメッセージを返したすべての送信元アドレスを記録するためのものです。
IPデータパケットが宛先に到達するために移動したパス。図4-13-5のTraceRouteSetting画面が表示されます。

図4-13-5 トレースルート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
・IPアドレス	宛先IPアドレス
・マックスホップ	traceroute機能で許可される最大ゲートウェイ数
・ルート結果のトレース	現在のトレースルートの結果を表示します

ボタン

：クリックしてICMPv6パケットを送信します

4.14 RMON

RMONは、標準SNMPの最も重要な拡張です。RMONはMIB定義のセットであり、標準を定義するために使用されます

ネットワーク監視機能とインターフェース、SNMP管理端末とリモート間の通信を可能にします

モニター。RMONは、サブネット内のアクションを監視するための非常に効率的な方法を提供します。

RMONのMIDは10グループで構成されています。スイッチは、最も頻繁に使用されるグループ1、2、3、および9をサポートします。

- **統計**：エージェントによって監視されている各サブネットの基本的な使用状況とエラーの統計を維持します。
- **履歴**：Statisticsから入手できる定期的な統計サンプルを記録します。
- **アラーム**：管理コンソールのユーザーが、サンプル間隔とアラートしきい値に任意のカウントまたは整数を設定できるようにします。
RMONエージェントレコード。
- **イベント**：RMONエージェントによって生成されたすべてのイベントのリスト。

アラームは、イベントの実装によって異なります。統計と履歴には、現在または履歴のサブネット統計が表示されます。警報

およびイベントは、ネットワーク内の整数データの変更を監視する方法を提供し、異常なイベントに対していくつかのアラートを提供します
(トラップを送信するか、ログに記録します)。

4.14.1 RMON統計

このページには、特定のRMON統計エントリの詳細が表示されます。図4-14-1のRMONStatistics画面が表示されます。

図4-14-1：RMON統計の詳細のスクリーンショット

328

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	このドロップダウンリストからポートを選択します
・ドロップイベント	パケットが原因でブロープによってドロップされたイベントの総数 財源不足
・オクテット	で受信されたデータのオクテットの総数（不良パケットのデータを含む） ネットワーク
・パケット	パケットの総数（不良パケット、ブロードキャストパケット、および マルチキャストパケット）を受信しました
・ブロードキャストパケット	ブロードキャストに向けられた、受信された正常なパケットの総数。 住所
・マルチキャストパケット	マルチキャストに送信された、受信した正常なパケットの総数 住所
・CRC/アライメントエラー	長さのある受信パケットの総数（フレーミングビットを除く、 ただし、64～1518オクテットのFCSオクテットを含む）
・アンダーサイズパケット	64オクテット未満の受信パケットの総数
・特大パケット	1518オクテットより長い受信パケットの総数
・フラグメント	無効なCRCで受信されたサイズが64オクテット未満のフレームの数
・ジャバー	サイズが64オクテットを超え、無効な状態で受信されたフレームの数 CRC
・衝突	このイーサネットセグメントでの衝突の総数の最良の見積もり。
・64バイトフレーム	64オクテットであった受信パケット（不良パケットを含む）の総数 長さで
・65～127バイトフレーム	受信したパケット（不良パケットを含む）の総数 長さ65～127オクテット
・128～255バイトフレーム	受信したパケット（不良パケットを含む）の総数 長さ128～255オクテット
・256～511バイトフレーム	受信したパケット（不良パケットを含む）の総数

	長さ256～511オクテット
・512～1023バイトフレーム受信したパケット（不良パケットを含む）の総数。	
	長さ512から1023オクテット
・1024～1518バイトフレーム	受信したパケット（不良パケットを含む）の総数
	長さ1024～1518オクテット

ボタン

: クリックしてRMON統計をクリアします

4.14.2RMONイベント

このページでRMONイベントテーブルを設定します。図4-14-2および図4-14-3のRMONイベント画面が表示されます。

図4-14-2：RMONイベント構成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
・インデックスを選択します	このドロップダウンリストからインデックスを選択して、新しいインデックスを作成するか、インデックスを変更します
・インデックス	エントリのインデックスを示します。範囲は1～65535です。
・タイプ	イベントの通知を示します。可能なタイプは次のとおりです。 ■なし：フレーミングを含む、インターフェースで受信されたオクテットの総数。 文字。 ■ログ：ユニキャストパケットの数は、上位層のプロトコルに配信されました。 ■SNMP -Trap：に配信されたブロードキャストおよびマルチキャストパケットの数 上位層プロトコル。 ■ログとトラップ：さらに破棄されるインバウンドパケットの数 パケットは正常です。
・コミュニティ	トラップが送信されるときにコミュニティを指定します。文字列の長さは0～127です。 デフォルトは「public」です。
・所有者	このイベントの所有者を示します。文字列の長さは0～127で、デフォルトは null文字列
・説明	このイベントの説明を示します。文字列の長さは0～127で、デフォルトは

ボタン

: クリックして変更を適用します。

図4-14-3 : RMONイベント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
・インデックス	現在のイベントインデックスを表示する
・イベントタイプ	現在のイベントタイプを表示します
・コミュニティ	SNMPトラップの現在のコミュニティを表示する
・説明	現在のイベントの説明を表示する
・最終送信時刻	現在の最終送信時刻を表示します
・所有者	現在のイベント所有者を表示する
・アクション	クリック RMONイベントエントリを削除するには

4.14.3RMONイベントログ

このページでは、RMONイベントログの概要を説明します。図4-14-4のRMONイベントログテーブル画面が表示されます。

図4-14-4 : RMONイベントログテーブル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
・インデックスを選択します	このドロップダウンリストからインデックスを選択します
・インデックス	ログエントリのインデックスを示します
・ログ時間	イベントログ時間を示します
・説明	イベントの説明を示します

4.14.4RMONアラーム

このページでRMONアラームテーブルを設定します。図4-14-5および図4-14-6のRMONアラーム画面が表示されます。

図4-14-5：RMONアラームテーブル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
・インデックスを選択します	このドロップダウンリストからインデックスを選択して、新しいインデックスを作成するか、インデックスを変更します
・インデックス	アラームエントリのインデックスを示します
・サンプルポート	このドロップダウンリストからポートを選択します
・サンプル変数	サンプリングされる特定の変数を示します。可能な変数は次のとおりです。 <div><div>■ DropEvents</div>: パケットが原因廃棄されたイベントの総数 リソースの不足に。 <div>■ オクテット</div>: 受信および送信された（良好および不良）バイト数。 FCSを含みますが、フレーミングビットは除外します。 <div>■ パケット</div>: 受信したフレーム（不良、ブロードキャスト、マルチキャスト）の総数 送信されます。 <div>■ BroadcastPkts</div>: 良いフレームの総数であったことを受け ブロードキャストアドレスに送信されます。これにはマルチキャストが含まれないことに注意してください パケット。 <div>■ MulticastPkts</div>: 指示された受信された良好なフレームの総数</div>

このマルチキャストアドレスに。

■ **CRCAlignErrors** : CRC /アライメントエラー (FCSまたはアラインメントの数エラー)。

■ **UnderSizePkts** : 未満64以上であった受信フレームの総数
オクテット長 (フレーミングビットを除くが、FCSオクテットを含む) であり、
そうでなければ整形形式。

■ **OverSizePkts** : より長くした受信フレームの総数
1518オクテット (フレーミングビットを除くが、FCSオクテットを含む)
そうでなければ整形形式。

■ **フラグメント** : 64未満の受信フレームの総数
長さがオクテット (フレーミングビットを除くが、FCSオクテットを含む) であり、
FCSまたはアライメントエラーのいずれか。

■ **ジャバ** : 1518より長い受信フレームの総数
オクテット (フレーミングビットを除くが、FCSオクテットを含む)、および
FCSまたはアライメントエラー。

■ **衝突** : これに関する衝突の総数の最良の推定値
イーサネットセグメント。

■ **Pkts64Octets** : (不良パケットを含む) フレームの総数受信
長さが64オクテットの送信済み (フレーミングビットを除くが
FCSオクテットを含む)。

■ **Pkts64to172Octets** : (不良パケットを含む) フレームの総数
オクテットの数
指定された範囲 (フレーミングビットを除くが、FCSオクテットを含む)。

■ **Pkts158to255Octets** : (不良パケットを含む) フレームの総数
オクテットの数
指定された範囲 (フレーミングビットを除くが、FCSオクテットを含む)。

■ **Pkts256to511Octets** : (不良パケットを含む) フレームの総数
オクテットの数
指定された範囲 (フレーミングビットを除くが、FCSオクテットを含む)。

■ **Pkts512to1023Octets** : (不良パケットを含む) フレームの総数
オクテットの数
指定された範囲 (フレーミングビットを除くが、FCSオクテットを含む)。

■ **Pkts1024to1518Octets** : (不良パケットを含む) フレームの総数
オクテットの数
指定された範囲 (フレーミングビットを除くが、FCSオクテットを含む)。

・サンプル間隔

サンプル間隔 (1~2147483647)

・サンプルタイプ

選択した変数をサンプリングし、値を計算する方法
しきい値と比較すると、可能なサンプルタイプは次のとおりです。
■ **絶対** : サンプルを直接取得します (デフォルト)。

■ **デルタ** : サンプル間の差を計算します。

・上昇しきい値

上昇しきい値 (0~2147483647)

・立ち下がりがしきい値

下降しきい値 (0~2147483647)

・ライジングイベント	上昇しきい値を超えたときに発生するイベント
・落下イベント	下降しきい値を超えたときに発生するイベント
・所有者	アラームの所有者を指定します

ボタン

：クリックして変更を適用します。

図4-14-6：RMONアラーム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	
・インデックス	アラーム制御エントリのインデックスを示します	
・サンプルポート	現在のサンプルポートを表示する	
・サンプル変数	現在のサンプル変数を表示します	
・サンプル間隔	現在の間隔を表示する	
・サンプルタイプ	現在のサンプルタイプを表示する	
・上昇しきい値	現在の上昇しきい値を表示します	
・立ち下がりがしきい値	現在の下降しきい値を表示します	
・ライジングイベント	現在の上昇イベントを表示します	
・落下イベント	現在の落下イベントを表示します	
・所有者	現在の所有者を表示する	
・アクション	クリック	RMONアラームエントリを削除するには

4.14.5RMONの履歴

このページでRMON履歴テーブルを構成します。図4-14-7および図4-14-8のRMON履歴画面が表示されます。

図4-14-7：RMON履歴テーブル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
・インデックスを選択します	このドロップダウンリストからインデックスを選択して、新しいインデックスを作成するか、インデックスを変更します
・インデックス	履歴エントリのインデックスを示します
・サンプルポート	このドロップダウンリストからポートを選択します
・バケットが要求されました	に保存されているこの履歴コントロールエントリに関連付けられている最大データエントリを示します RMON。範囲は1～50で、デフォルト値は50です。
・間隔	履歴統計データをサンプリングする間隔を秒単位で示します。ザ・ 範囲は1～3600で、デフォルト値は1800秒です。
・所有者	履歴の所有者を指定します

ボタン

：クリックして変更を適用します。

図4-14-8：RMON履歴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
・インデックス	現在のインデックスを表示する
・データソース	現在のデータソースを表示する
・バケットが要求されました	要求された現在のバケットを表示する
・間隔	現在の間隔を表示する
・所有者	現在の所有者を表示する
・アクション	クリック RMON履歴エントリを削除します。

4.14.6RMON履歴ログ

このページでは、RMON履歴エントリの詳細を提供します。図4-14-9の画面が表示されます。

図4-14-9：RMON履歴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
履歴インデックス	このドロップダウンリストから履歴インデックスを選択します

ボタン

：クリックして変更を適用します。

4.15 Power over Ethernet

GS-4210 PoEスイッチシリーズは、電力集中制御IP電話システム、IPカメラシステム、およびAPグループを簡単に構築できます。企業のために。たとえば、カメラ/ APは、監視のために会社の角を曲がったところに簡単に設置できます。オフィスでワイヤレスローミング環境を要求または構築します。電源ソケットの制限がない場合、GS-4210PoEスイッチシリーズにより、カメラまたはWLANAPのインストールがより簡単かつ効率的になります。

GS-4210PoEスイッチシリーズのPoEパワーバジェットリスト

モデル名	PoEバジェット@ 25℃	PoEバジェット@摂氏50度
GS-4210-8P2T2S	120ワット	100ワット
GS-4210-8P2T2S	240ワット	200ワット
GS-4210-16P4C	220ワット	190ワット
GS-4210-24P4C	220ワット	190ワット
GS-4210-24PL4C	440ワット	380ワット

図4-16-1 : Power overEthernetのステータス

4.15.1 Power overEthernet搭載デバイス

3～5ワット	ボイスオーバーIP電話
	企業はPOEVoIP電話、ATAなどをインストールできます
	UPSが存在する中央エリアのイーサネット/非イーサネットエンドデバイス 無停電電力システムおよび電力制御システム用にインストールされています。
6～12ワット	無線LANアクセスポイント
	美術館、観光スポット、空港、ホテル、キャンパス、工場、 倉庫はどこにでもアクセスポイントを設置できます。
	IP監視
10～12ワット	企業、美術館、キャンパス、病院、銀行はIPをインストールできます
	設置場所の制限のないカメラ。電気技師は必要ありません
	ACソケットを取り付ける。
3～12ワット	PoEスプリッター
	PoEスプリッターは、イーサネットケーブルを介したPoE 56VDCを5 / 12VDCに分割します
	電力出力。電力による制限からデバイスの展開を解放します
3～25ワット	ハイパワーPoEスプリッター
	追加のAC配線と追加のAC配線のコストを排除するコンセントの場所
	インストール時間を短縮します。
3～25ワット	High PoE Splitter
	High PoE Splitterは、イーサネットケーブルを介してPoE 56VDCを次のように分割します。
	24 / 12VDC電源出力。デバイスの展開を制限から解放します
3～25ワット	追加のACのコストを排除する電源コンセントの場所による
	追加のACのコストを排除する電源コンセントの場所による
	配線し、設置時間を短縮します。

ハイパワースピードドーム
この最先端の設計は、さまざまなネットワークに適合するのに十分です。
交通センター、ショッピングモール、鉄道駅などの環境
最も要求の厳しい倉庫、空港、生産施設
屋外監視アプリケーション。ACをインストールするために電気技師は必要ありません
ソケット。

30ワット

PoEポートごとのGS-4210PoEスイッチシリーズは56VDC PoE電力出力をサポートしているため、どうぞ
受電装置（PD）の許容DC電力範囲が56VDCであることを確認してください。そうでなければ、それ
パワードデバイス（PD）を損傷します。

4.15.2システム構成

Power over Ethernetシステムでは、動作電力はLANを介して電源（PSU電源ユニット）から供給されます。
ポートに接続されている**パワードデバイス（PD）**へのインフラストラクチャ。ある条件下では、必要な総出力電力
PDによって、PSUによって提供される最大利用可能電力を超える可能性があります。PSUを備えたシステムはより少ない供給が可能です
システム内のすべてのPoEポートの潜在的な総消費電力よりも電力。の機能を維持するために
ポートの大部分、電源管理が実装されています。

PSUの入力消費電力は、電圧と電流を測定することによって監視されます。入力消費電力は、
システムの総消費電力。電力管理の概念により、すべてのポートをアクティブにし、追加のポートをアクティブにすることができます。
システムの総電力が、追加のPDができない電力レベルよりも低い限り、ポート
この値を超えると、ユーザー定義の優先順位に従って、ポートが非アクティブ化されます。電力バジェットは
次のユーザー定義可能なパラメーターに従って管理されます：最大使用可能電力、ポート優先度、および最大
ポートあたりの許容電力。

予約電力

ポート/ PDが電力を予約する方法と、ポートをシャットダウンするタイミングを構成するには、5つのモードがあります。

■ 分類モード

このモードでは、各ポートは、接続されたPDが属するクラスに応じて、予約する電力量を自動的に決定します。
に、それに応じて電力を予約します。4つの異なるポートクラスが存在し、1つは4、7、15.4、および30.8ワット用です。

クラス	使用法	PDが使用する最大電力の範囲	クラスの説明
0	デフォルト	0.44〜12.95ワット	分類の実装解除
1	オプション	0.44〜3.84ワット	非常に低電力
2	オプション	3.84〜6.49ワット	低電力
3	オプション	6.49〜12.95ワット（または15.4ワット）	ミッドパワー
4	オプション	12.95〜25.50ワット（または30.8ワット）	ハイパワー

表4-16-1：標準のPoEパラメータと比較

1.このモードでは、[最大電力]フィールドは効果がありません。

2.そのクラスレベル0に設計されたPD69008 / PD69012のPoEチップが割り当てられます

分類電力制限モードでは、AFモードで15.4ワット、ATモードで30.8ワット。

ハードウェアに制限があります。

■ 割り当てモード

このモードでは、ユーザーは各ポートが予約できる電力量を割り当てます。それぞれに割り当てられた/予約された電力ポート/ PDは[最大電力]フィールドで指定されます。予約電力の合計が量を超えると、ポートはシャットダウンされます電源が供給できる電力の。

このモードでは、PDがより多くの利用可能な電力を要求した場合、ポートの電源はオンになりません。

4.15.3 Power overEthernet構成

このセクションでは、ユーザーは図4-16-1の画面のように、現在のPoE構成設定を検査および構成できます。が表示されます。

図4-16-1：PoE構成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
•システムPoE管理者	ユーザーがPoE機能を有効または無効にできるようにします。これにより、すべてのPoEポートが
モード	電力を供給するかどうか。
• PoE管理	ポート/ PDが電力を予約する方法を構成するための6つのモードがあります。
モード	いつポートをシャットダウンするか。
	■分類モード：システムは、以下に従ってPDU電力をPDに予約します。
	PoEクラスレベル。
	■消費モード：システムは、PDリアルに従ってPoE電力を提供します
	消費電力。
	■割り当てモード：ユーザーは、各ポートにどのくらいのPoE電力を割り当てることができます
	システムはPoE電力をPDに予約します。
•温度	過熱保護しきい値を設定できます。システムの場合
しきい値	温度が高すぎると、システムはPoEパワーバジェットの合計を下げます
	自動的に。
• PoE温度	PoEチップ温度を表示する

このセクションでは、[図4-16-2](#)に示すように、現在の消費電力のPoE電力使用量を表示します。

図4-16-2：現在の消費電力のスクリーンショット

340

このセクションでは、ユーザが現在のPoEポートの設定を検査し、設定することを可能にするように、[図4-16-3](#)示します。

図4-16-3：Power overEthernet構成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
• PoEモード	PoEモードには3つのモードがあります。 <div><div>■有効：PoE機能を有効にします。</div><div>■無効：PoE機能を無効にします。</div><div>■スケジュール：スケジュールモードでPoE機能を有効にします。</div></div>
•スケジュール	スケジュールされたプロファイルモードを示します。可能なプロファイルは次のとおりです。 <div><div>■プロファイル1</div><div>■プロファイル2</div><div>■プロファイル3</div><div>■プロファイル4</div></div>
• AF / ATモード	ユーザが802.3atまたは802.3af互換モードを選択できるようにします。デフォルト値は802.3atモード。

•優先度

のみ、802.3afモードとして、システムは最大15.4Wを予約します。

Class3レベルをサポートするPD。IEEE 802.3atモードとして、システムは予備30.8ワットCLASS4レベルをサポートしていPDため。

802.3atモードのclass1からclass3レベルまで、同じPoEを予約します

802.3afモードと同様の電力。

優先度は、PoEポートの優先度を表します。電力の優先順位には3つのレベルがあります

Low、High、Criticalという名前。

総消費電力が総電力を超える場合に優先順位が使用されます

予算。この場合、優先度が最も低いポートがオフになり、優先度の高いポートの電力。

•PDクラス

ポートに接続されているPDのクラスを表示します。

分類プロセス。クラス0はPDのデフォルトです。PDはパワードベース

システムが分類モードで動作している場合は、PoEクラスレベルで。PDは指定された最大消費電力に従ってクラス0から4に戻ります

表4-16-1。

•使用電流[mA]

電源が使用されるPDが現在使用しているどのくらいの現在のショーを。

•使用電力[W]

電源が使用されるPDが現在使用しているどのくらいの電力を示しています。

•電力割り当て

ポートのPoE供給ワットを制限できます。ポートあたりの最大値は小さくする必要があります

30.8ワットより。ポートの合計値は、電力予約よりも小さくする必要があります

値。電力過負荷が検出されると、ポートは自動的にシャットダウンし、PDの消費電力が電力制限を下回るまで検出モードで

値

ボタン

: クリックして変更を適用します。

4.15.4PoEスケジュール

このページでは、ユーザーがPoEスケジュールとスケジュールされた電力リサイクルを定義できます。

PoEスケジュール

マネージドPoEスイッチは、IP監視として使用されるだけでなく、あらゆるPoEネットワークの構築にも確実に適用できます。

VoIPと無線LANを含みます。世界的な省エネと環境保護への貢献のトレンドの下で

地球上では、マネージドPoEスイッチは、高ワットの電力を供給する機能に加えて、電源を効果的に制御できます。

「**PoEスケジュール**」機能は、指定された時間内に各PoEポートのPoE給電を有効または無効にするのに役立ちます

間隔とそれはSMBまたはエンタープライズが電力とお金を節約するのを助ける強力な機能です。

定期的な電力リサイクル

マネージドPoEスイッチを使用すると、接続されている各PoEIPカメラを毎週指定された時間に再起動できます。したがって、それ
バッファオーバーフローが原因でIPカメラがクラッシュする可能性を減らします。

図4-16-4の画面が表示されます。

図4-16-4：PoEスケジュールのスクリーンショット

Add New Ruleボタンを押して、PoEスケジュール機能の設定を開始してください。プロファイルにPoEスケジュールを設定してから、PoEポート構成に戻り、ポートごとの「PoEモード」オプションから「スケジュール」モードを選択して、どちらを指定できるようにします。スケジュールプロファイルをPoEポートに適用できます。

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
・プロファイル	スケジュールプロファイルモードを設定します。可能なプロファイルは次のとおりです。 <div>プロファイル1</div> <div>プロファイル2</div> <div>プロファイル3</div> <div>プロファイル4</div>
・平日	ユーザーがPoE機能を定義するための曜日を、その日に有効にすることで設定できるようにします。
・開始時間	PoE機能を有効にすることで、PoE機能の実行時間を設定できます。

・最小開始	ユーザーがPoE機能を有効にすることで何を実行するかを設定できます。
・終了時間	PoE機能を無効にすることで、PoE機能の実行時間を設定できます。
・終了分	ユーザーがPoE機能を無効にすることで、その機能を設定できるようにします。
・再起動の有効化	ユーザーがPoE再起動スケジュールによってPoEポート全体の再起動を有効または無効にできるようにします。 <div>PoEスケジュールとPoE再起動スケジュールをで機能させたい場合は注意してください</div> <div>同時に、この機能を使用してください。再起動のみの機能は使用しないでください。この</div> <div>この機能により、管理者は指定された時間にPoEデバイスを再起動できます。</div>

	管理者にはこの種の要件があります。
・再起動のみ	<p>ユーザーがPoE再起動スケジュールによってPoE機能を再起動できるようにします。次の場合に注意してください</p> <p>管理者がこの機能を有効にすると、PoEスケジュールはプロファイルする時間を設定しません。この機能は、指定された時間にPoEポートをリセットするためのものです。</p>
・リブートアワー	<p>PoEを再起動する時間をユーザーが設定できるようにします。この機能はPoEリブート専用ですスケジュール。</p>
・最小再起動	<p>ユーザーがPoEを再起動する分を設定できるようにします。この機能はPoEリブート専用ですスケジュール。</p>
ボタン	
	<p>：クリックして新しいルールを追加します。</p> <p>：クリックして変更を適用</p> <p>：チェックしてエントリを削除します。</p>

4.15.5PoEアライブチェック構成

GS-4210 PoEスイッチシリーズは、pingアクションを介して接続されたPDのステータスをリアルタイムで監視するように構成できます。一度PD動作を停止し、応答がない場合、PoEスイッチはPoEポートの電源を再起動し、PDを動作に戻します。そうなる信頼性を大幅に向上させ、管理者の管理負担を軽減します。

このページでは、PD AliveCheckを構成する方法について説明します。図4-16-5の画面が表示されます。

図4-15-5：PDアライブチェック構成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
・モード	ユーザーがポートごとのPDアライブチェック機能を有効または無効にできるようにします。 デフォルトでは、すべてのポートが無効になっています。
・PDIPアドレスにpingを実行します	この列を使用すると、ユーザーはシステムがpingを実行するためのPoEデバイスのIPアドレスを設定できます。 PoEデバイス。PDのIPアドレスは同じネットワークに設定する必要があることに注意してください PoEスイッチでセグメント化します。

・インターバル時間（10～300秒）	この列により、ユーザーはシステムがPDにping要求を発行する期間を設定できます。 PDが生きているか死んでいるかを検出するため。 インターバル時間の範囲は10秒から300秒です。
・再試行回数（1～5）	この列を使用すると、ユーザーはシステムがPDへのpingを再試行する回数を設定できます。 たとえば、カウント2を設定した場合、システムがPDへのpingを再試行すると、 PDは継続的に応答せず、PoEポートはリセットされます。
・アクション	PDに応答がない場合に、どのアクションを適用するかをユーザーが設定できるようにします。ザ・ PoEスイッチシリーズは、次の3つのアクションを提供します。 ■ PDリポート：これは、システムが接続されているPoEポートをリセットする手段と PD。 ■ PD再起動してアラーム：これは、システムがPoEポートと問題をリセットする意味 Syslogを介したアラームメッセージ。 ■ アラーム：システムがSyslogを介してアラームメッセージを発行することを意味します。
・再起動時間（30～180秒）	この列では、非常に多くのPoEデバイスの再起動時間を設定できます。 市場に出回っているPoEデバイスの種類であり、再起動時間は異なります。 PD Alive-checkは定義基準ではないため、市場に出回っているPoEデバイス 再起動が完了した情報をPoEスイッチに報告しません。したがって、ユーザーは作成する必要があります

PDが起動を完了するのにかかる時間を確認してから、時間値をこれに設定します
カラム。

システムは、再起動時間に従ってPDを再度チェックします。そうでない場合
正確な起動時間を確認するには、もっと長く設定することをお勧めします。

ボタン

: クリックして変更を適用します。

図4-15-6：PDアライブチェック構成のスクリーンショット

4.16メンテナンス

メンテナンスメニュー項目を使用して、マネージドスイッチの基本構成を表示および構成します。メンテナンス中、
構成をバックアップ、アップグレード、保存、および復元するために、次のトピックが提供されています。このセクションには、次の項目があります。

- 工場出荷時のデフォルト このページでスイッチの構成をリセットできます。
- スイッチの再起動 このページでスイッチを再起動できます。再起動後、スイッチが起動します
通常は。
- バックアップマネージャ スイッチ構成をバックアップできます。
- アップグレードマネージャー スイッチ構成をアップグレードできます。
- デュアルイメージ このページでアクティブまたはバックアップイメージを選択します。

4.16.1工場出荷時のデフォルト

このページでスイッチの構成をリセットできます。IP構成のみが保持されます。新しい構成は
すぐに利用できます。つまり、再起動は必要ありません。図4-15-1の工場出荷時のデフォルト画面が表示されたら、
構成を工場出荷時のデフォルトにリセットします。

図4-15-1工場出荷時のデフォルトのスクリーンショット

「工場出荷時」ボタンを押して再起動すると、システムは次のようにデフォルトのIP設定をロードします。
。 デフォルトの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
- 。他の設定値は無効に戻るか、なしに戻ります。

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するには、ハードウェアリセットボタンを押すこともできます
フロントパネルで約10秒。デバイスを再起動した後。管理WEBにログインできます
192.168.0.xxの同じサブネット内のインターフェイス。

4.16.2スイッチの再起動

[再起動]ページでは、デバイスをリモートの場所から再起動できます。再起動ボタンが押されたら、ユーザーはする必要があります
Webインターフェイスに約60秒間再ログインします。図4-16-2の[スイッチの再起動]画面が表示されたら、クリックして再起動します。
システム。

図4-16-2リブートスイッチのスクリーンショット

4.16.3バックアップマネージャ

この機能により、管理対象スイッチの現在のイメージまたは構成をローカル管理ステーションにバックアップできます。ザ・
図4-16-3のバックアップマネージャ画面が表示されます。

図4-16-3BackupManager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
・バックアップ方法	このドロップダウンリストからバックアップ方法を選択します。
・サーバーIP	TFTPサーバーのIPアドレスを入力します。
・バックアップタイプ	バックアップの種類を選択します。
・画像	アクティブまたはバックアップイメージを選択します。

ボタン

：クリックして、イメージ、構成、またはログをバックアップします。

4.16.4アップグレードマネージャー

この機能により、管理対象スイッチの現在のイメージまたは構成をローカル管理ステーションに再ロードできます。ザ・
図4-16-4のUpgradeManager画面が表示されます。

図4-16-4UpgradeManager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
・アップグレード方法	このドロップダウンリストからアップグレード方法を選択します。
・サーバーIP	TFTPサーバーのIPアドレスを入力します。
・ファイル名	ファームウェアイメージまたは構成の名前。
・アップグレードタイプ	アップグレードタイプを選択します。
・画像	アクティブまたはバックアップイメージを選択します。

ボタン

：クリックしてイメージまたは構成をアップグレードします。

4.16.5デュアルイメージ

このページには、デバイス内のアクティブなファームウェアイメージとバックアップファームウェアイメージに関する情報が表示され、に帰ることができます。
バックアップイメージ。Webページには、アクティブなファームウェアイメージとバックアップファームウェアイメージに関する情報を含む2つのテーブルが表示されます。デュアル
[図4-16-5](#)および[図4-16-6](#)の[イメージの構成と情報]画面が表示されます。

図4-15-5 : デュアルイメージ構成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
・アクティブな画像	アクティブまたはバックアップイメージを選択します

ボタン

: クリックしてアクティブな画像を適用します。

図4-16-6 : デュアルイメージ情報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
・フラッシュパーティション	現在のフラッシュパーティションを表示します
・画像名	現在の画像名を表示する

5.スイッチ操作

5.1アドレステーブル

スイッチはアドレステーブルで実装されます。このアドレステーブルは、多くのエントリで構成されています。各エントリは保存に使用されます。MACアドレス、ポート番号など、ネットワーク上の一部のノードのアドレス情報。この情報は、イーサネットスイッチの学習プロセス。

5.2学習

1つのパケットがいずれかのポートから着信すると、スイッチは送信元アドレス、ポート番号、および関連する他のパケットを記録します。アドレステーブルの情報。この情報は、将来の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。

5.3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イッチングのあるポートから来ると、送信元以外の宛先アドレスもチェックします。アドレス学習。イーサネットスイッチングは、宛先アドレスのアドレステーブルを検索します。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。これらのポートはこのパケットを接続したネットワーク。見つかった場合、宛先アドレスがこのパケットの着信とは異なるポートにある場合、イーサネットスイッチングは、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。アドレステーブル。ただし、宛先アドレスがこのパケッ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、それによってネットワークのスループットと可用性の向上

5.4ストアアンドフォワード

ストアアンドフォワードは、パケット転送技術の一種です。ストアアンドフォワードイーサネットスイッチングは、着信を保存します。内部バッファ内のフレームであり、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、エラーパケットは発生しません。それはネットワークに効率と安定性が必要な場合に最適です。

イーサネットスイッチは、パケットヘッダーから宛先アドレスをスキャンし、着信用に提供されたルーティングテーブルを検索します。必要な場合にのみ、パケットをポートして転送します。早送りにより、スイッチはサーバーを直接接続するのに魅力的です。ネットワークにより、スループットと可用性が向上します。ただし、スイッチは存在をセグメント化するために最も一般的に使用されます。ハブ。ほとんどの場合、全体的なパフォーマンスが向上します。イーサネットスイッチングは、どのイーサネットでも簡単に構成できます。従来のケーブルとアダプターを使用して帯域幅を大幅に拡大するネットワーク環境。

イーサネットスイッチングの学習機能により、各着信および各着信の送信元アドレスと対応するポート番号。発信パケットはルーティングテーブルに保存されます。この情報は、宛先アドレスがであるパケットをフィルタリングするために後で使用されます。送信元アドレスと同じセグメント上。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制限され、全体的な負荷が軽減されます。ネットワーク上。

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、それは再送信率を減らします。
パケット損失は発生しません。

5.5オートネゴシエーション

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。このテクノロジーは、可能な限り最高の帯域幅を自動的に設定します
別のネットワークデバイスとの接続が確立されたとき（通常は電源オンまたはリセット時）。これは、
両方のデバイスが接続されている場合のモードと速度。10BASE-Tデバイスと100BASE-TXデバイスの両方がのポートに接続できます
半二重モードまたは全二重モードのいずれか。

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、オートネゴシエーションなし	10Mbps。
10Mbps、オートネゴシエーション付き	10 / 20Mbps（10BASE-T /全二重）
100Mbps、オートネゴシエーションなし	100Mbps
100Mbps、オートネゴシエーション付き	100 / 200Mbps（100BASE-TX /全二重）

6.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。管理対象スイッチが正しく機能していない場合は、マネージドスイッチは、このマニュアルの指示に従ってセットアップされます。

■リンクLEDが点灯しない

解決：

ケーブル接続を確認し、マネージドスイッチのデュプレックスモードを削除します

■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：

VLAN設定、トラUNK設定、またはポートの有効/無効のステータスを確認してください。

■パフォーマンスが悪い

解決：

管理対象スイッチの全二重ステータスを確認します。管理対象スイッチが全二重に設定されており、パートナーが半分に設定されている場合デュプレックスの場合、パフォーマンスが低下します。ポートの出入り率も確認してください。

■スイッチがネットワークに接続しない理由

解決：

- 1.1。 マネージドスイッチのLNK / ACTLEDを確認します
- 2.2。 マネージドスイッチで別のポートを試してください
- 3.3。 ケーブルが正しく取り付けられていることを確認してください
- 4.4。 ケーブルが正しいタイプであることを確認してください
- 5.5。 電源を切ります。しばらくして、もう一度電源を入れてください

■100BASE-TXポートリンクLEDが点灯しているが、トラフィックが不規則

解決：

接続されているデバイスが全二重に設定されていないことを確認してください。一部のデバイスは、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を変更しますモード。オートネゴシエーションは、このタイプの全二重設定を認識しない場合があります。

■スイッチの電源が入らない

解決：

- 1.1。 AC電源コードが挿入されていないか、故障しています
- 2.2。 AC電源コードが正しく挿入されているか確認してください
- 3.3。 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。AC電源が動作しているかどうかを確認します
スイッチの代わりに別のデバイスを接続します。

- 4.4。 そのデバイスが機能する場合は、次の手順を参照してください。
- 5.5。 そのデバイスが機能しない場合は、AC電源を確認してください

■PoEイーサネットスイッチがネットワークに接続しない理由

解決：

PoEイーサネットスイッチのLNK / ACTLEDを確認します。PoEイーサネットスイッチの別のポートを試してください。ケーブルが

正しく取り付けられ、ケーブルが正しいタイプであることを確認してください。電源を切ります。しばらくしてから、もう一度電源を入れてください。

■ PoEデバイスをPoEイーサネットスイッチに接続すると、電源が入らない

解決：

- 1. PoEイーサネットスイッチ（ポート1からポート8） からもう一方の端までの接続のケーブルタイプを確認してください。ザ・ケーブルは、8線UTP、カテゴリ5以上、100メートル以内のEIA568ケーブルである必要があります。4線のためのケーブル、ショートループまたは100メートルを超えると電源に影響します。
- 2. デバイスがIEEE802.3af /802.3at標準に完全に準拠していることを確認してください。

付録AスイッチのRJ45ピン割り当て

A.1 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。ただし、明示的に禁止されているわけではありません。
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、ストレートケーブルまたはクロスケーブルは必要。スイッチの各ポートは、自動MDI / MDI-X検出をサポートしています。つまり、スイッチを任意の場所に直接接続できます
クロスケーブルを作らないイーサネットデバイス。次の表と図は、標準のRJ45レセプタクルを示しています。
コネクタとそのピン割り当て：

RJ45コネクタのピン割り当て		
連絡先	MDI	MDI-X
	メディア依存インターフェース	メディアに依存 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	使用されていない	
6	Rx- (受信)	Tx- (送信)
7、8	使用されていない	

標準ケーブル、RJ45ピン割り当て

標準のRJ45レセプタクル/コネクタ

標準のUTP / STPケーブルには8本のワイヤーがあり、各ワイヤーは色分けされています。以下にピンの割り当てと色を示します
ストレートケーブルとクロスケーブルの接続：

ストレートケーブル	サイド1	サイド2
-----------	------	------

1	2	3	4	5	6	7	8	サイド1	1=白/オレンジ 2=オレンジ 3=白/緑 4=青 5=白/青 6=緑 7=ホワイト/ブラウン 8=ブラウン	1=白/オレンジ 2=オレンジ 3=白/緑 4=青 5=白/青 6=緑 7=ホワイト/ブラウン 8=ブラウン
1	2	3	4	5	6	7	8	サイド2	サイド1 1=白/オレンジ 2=オレンジ 3=白/緑 4=青 5=白/青 6=緑 7=ホワイト/ブラウン 8=ブラウン	サイド2 1=白/緑 2=緑 3=白/オレンジ 4=青 5=白/青 6=オレンジ 7=ホワイト/ブラウン 8=ブラウン
クロスケーブル								サイド1		
1	2	3	4	5	6	7	8	サイド1	1=白/オレンジ 2=オレンジ 3=白/緑 4=青 5=白/青 6=緑 7=ホワイト/ブラウン 8=ブラウン	1=白/緑 2=緑 3=白/オレンジ 4=青 5=白/青 6=オレンジ 7=ホワイト/ブラウン 8=ブラウン
1	2	3	4	5	6	7	8	サイド2		

図A-1：ストレートケーブルとクロスケーブル

展開する前に、接続されているケーブルが上記の表と同じピン割り当てと色であることを確認してください
ネットワークへのケーブル。