

D-Link DGS-1210/GE シリーズ
Layer2 Web Smart Switch

ユーザマニュアル





安全にお使いいただくために



ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意












必ずお守りください






本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

 警告	この表示を無視し、まちがった使いかたをすると、火災や感電などにより人身事故になるおそれがあります。
 注意	この表示を無視し、まちがった使いかたをすると、傷害または物損損害が発生するおそれがあります。





記号の意味  してはいけない「禁止」内容です。  必ず実行していただく「指示」の内容です。

警告

-  **分解・改造をしない**
機器が故障したり、異物が混入すると、やけどや火災の原因となります。
分解禁止
-  **落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない**
故障の原因につながります。
-  **発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない**
感電、火災の原因になります。
使用を止めて、ケーブル/コード類を抜いて、煙が出なくなつてから販売店に修理をご依頼してください。
-  **ぬれた手でさわらない**
感電のおそれがあります。
ぬれ手禁止
-  **水をかけたり、ぬらしたりしない**
内部に水が入ると、火災、感電、または故障のおそれがあります。
水ぬれ禁止
-  **油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない**
火災、感電、または故障のおそれがあります。
-  **内部に金属物や燃えやすいものを入れない**
火災、感電、または故障のおそれがあります。
-  **表示以外の電圧で使用しない**
火災、感電、または故障のおそれがあります。
-  **たこ足配線禁止**
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。
-  **設置、移動のときは電源プラグを抜く**
火災、感電、または故障のおそれがあります。
-  **雷鳴が聞こえたら、ケーブル/コード類にはさわらない**
感電のおそれがあります。

-  **ケーブル/コード類や端子を破損させない**
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル/コードや端子の破損の原因となり、火災、感電、または故障につながります。
-  **正しい電源ケーブル、コンセントを使用する**
火災、感電、または故障の原因となります。
-  **乳幼児の手の届く場所では使わない**
やけど、ケガ、または感電の原因になります。
-  **次のような場所では保管、使用をしない**
禁止
 - ・直射日光のあたる場所
 - ・高温になる場所
 - ・動作環境範囲外
-  **光源をのぞかない**
禁止
光ファイバケーブルの断面、コネクタ、および製品のコネクタをのぞきますと強力な光源により目を損傷するおそれがあります。

注意

-  **静電気注意**
コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。
-  **コードを持って抜かない**
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。
-  **振動が発生する場所では使用しない**
接触不良や動作不良の原因となります。
-  **付属品の使用は取扱説明書にしたがう**
禁止
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因となります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- 保守マーク表示を守ってください。また、ドキュメント類に説明されている以外の方法でのご使用はやめてください。三角形の中に稲妻マークがついたカバー類をあげたり外したりすると、感電の危険性を招きます。筐体の内部は、訓練を受けた保守技術員が取り扱うようにしてください。
- 以下のような状況に陥った場合は、電源ケーブルをコンセントから抜いて、部品の交換をするかサービス会社に連絡してください。
 - 電源ケーブル、延長ケーブル、またはプラグが破損した。
 - 製品の中に異物が入った。
 - 製品に水がかかった。
 - 製品が落下した、または損傷を受けた。
 - 操作方法に従って運用しているのに正しく動作しない。
- 本製品をラジエータや熱源の近くに置かないでください。また冷却用通気孔を塞がないようにしてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。万一製品が濡れてしまった場合は、トラブルシューティングガイドの該当する文をお読みになるか、サービス会社に連絡してください。
- 本システムの開口部に物を差し込まないでください。内部コンポーネントのショートによる火事や感電を引き起こすことがあります。
- 本製品と一緒にその他のデバイスを使用する場合は、弊社の認定を受けたデバイスを使用してください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 電気定格ラベル標記と合致したタイプの外部電源を使用してください。正しい外部電源タイプがわからない場合は、サービス会社、あるいはお近くの電力会社にお問い合わせください。
- システムの損傷を防ぐために、電源装置の電圧選択スイッチ（装備されている場合のみ）がご利用の地域の設定と合致しているか確認してください。
 - 東日本では 100V/50Hz、西日本では 100V/60Hz
- また、付属するデバイスが、ご使用になる地域の電気定格に合致しているか確認してください。
- 付属の電源ケーブルのみを使用してください。
- 感電を防止するために、本システムと周辺装置の電源ケーブルは、正しく接地された電気コンセントに接続してください。このケーブルには、正しく接地されるように、3ピンプラグが取り付けられています。アダプタプラグを使用したり、ケーブルから接地ピンを取り外したりしないでください。延長コードを使用する必要がある場合は、正しく接地されたプラグがついている3線式コードを使用してください。
- 延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは電源分岐回路の定格アンペア限界の8割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動からシステムコンポーネントを保護するには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたりつまずいたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルやプラグを改造しないでください。設置場所の変更をする場合は、資格を持った電気技術者または電力会社にお問い合わせください。国または地方自治体の配線規則に必ず従ってください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
 - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
 - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
 - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いてください。
- 製品の移動は気をつけて行ってください。キャストやスタビライザがしっかりと装着されているか確認してください。急停止や、凹凸面上の移動は避けてください。

ラック搭載型製品に関する一般的な注意事項

ラックの安定性および安全性に関する以下の注意事項を遵守してください。また、システムおよびラックに付随する、ラック設置マニュアル中の注意事項や手順についてもよくお読みください。

警告 前面および側面のスタビライザを装着せずに、システムをラックに搭載すると、ラックが倒れ、人身事故を引き起こす場合があります。ラックにシステムを搭載する前には、必ずスタビライザを装着してください。

警告 接地用伝導体を壊したり、接地用伝導体を適切に取り付けずに装置を操作しないでください。適切な接地ができるかわからない場合、電気保安協会または電気工事士にお問い合わせください。

警告 システムのシャーシは、ラックキャビネットのフレームにしっかり接地される必要があります。接地ケーブルを接続してから、システムに電源を接続してください。電源および安全用接地配線が完了したら、資格を持つ電気検査技師が検査する必要があります。安全用接地ケーブルを配線しなかったり、接続されていない場合、エネルギーハザードが起こります。

- システムとは、ラックに搭載されるコンポーネントを指しています。コンポーネントはシステムや各種周辺デバイスや付属するハードウェアも含みます。
- ラックにシステム/コンポーネントを搭載した後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは1つのみとしてください。2つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。
- ラックに装置を搭載する前に、スタビライザがしっかりとラックに固定されているか、床面まで到達しているか、ラック全体の重量がすべて床にかかるようになっているかをよく確認してください。ラックに搭載する前に、シングルラックには前面および側面のスタビライザを、複数結合型のラックには前面用スタビライザを装着してください。
- ラックへの装置の搭載は、常に下から上へ、また最も重いものから行ってください。
- ラックからコンポーネントを引き出す際には、ラックが水平で、安定しているかどうか確認してから行ってください。
- コンポーネントレール解除ラッチを押して、ラックから、またはラックへコンポーネントをスライドさせる際は、指をスライドレールに挟まないよう、気をつけて行ってください。
- ラックに電源を供給する AC 電源分岐回路に過剰な負荷をかけないでください。ラックの合計負荷が、分岐回路の定格の 80 パーセントを超えないようにしてください。
- ラック内部のコンポーネントに適切な空気流があることを確認してください。
- ラック内の他のシステムを保守する際には、システムやコンポーネントを踏みつけたり、その上に立ったりしないでください。

注意 資格を持つ電気工事士が、DC 電源への接続と接地を行う必要があります。すべての電気配線が、お住まいの地域、および国の電気基準と規制に準拠していることを確認してください。

静電気障害を防止するために

静電気は、システム内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、マイクロプロセッサなどの電子部品に触れる前に、身体から静電気を逃がしてください。シャーシの塗装されていない金属面に定期的に触れることにより、身体の静電気を逃がすことができます。

さらに、静電気放出 (ESD) による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 静電気に敏感なコンポーネントを箱から取り出す時は、コンポーネントをシステムに取り付ける準備が完了するまで、コンポーネントを静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。
2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。
3. 静電気に敏感なコンポーネントの取り扱いには、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

バッテリーの取り扱いについて

警告 不適切なバッテリーの使用により、爆発などの危険性が生じることがあります。バッテリーの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリーの廃棄については、製造者の指示に従って行ってください。

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

本製品には電源ケーブル抜け防止金具が同梱されております。本製品を製品背面の電源コネクタ部分に取り付けます。電源ケーブルを接続して金具に固定すると、ケーブルの抜けを防止することができます。

このたびは、弊社製品をお買い上げいただきありがとうございます。

本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。

また、必ず本書、設置マニュアル、および同梱されている製品保証書をよくお読みいただき、内容をご理解いただいた上で、記載事項にしたがってご使用ください。

- 本書および同梱されている製品保証書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 本書および同梱されている製品保証書は大切に保管してください。
- 弊社製品を日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用前にご確認ください。製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。

<http://www.dlink-jp.com/support>

目次

安全にお使いいただくために.....	2
ご使用上の注意.....	3
ラック搭載型製品に関する一般的な注意事項.....	4
静電気障害を防止するために.....	4
バッテリーの取り扱いについて.....	4
電源の異常.....	5
はじめに	9
本マニュアルの対象者.....	10
表記規則について.....	10
第1章 本製品のご利用にあたって	11
スイッチ概要.....	11
サポートする機能.....	12
搭載ポート.....	12
前面パネル.....	13
LED表示.....	13
背面パネル.....	14
ギガビットコンボポート.....	15
第2章 スイッチの設置	16
パッケージの内容.....	16
ネットワーク接続前の準備.....	16
ゴム足の取り付け (19 インチラックに設置しない場合).....	16
19 インチラックへの取り付け.....	17
ブラケットの取り付け.....	17
19 インチラックにスイッチを取り付ける.....	17
電源の投入.....	17
第3章 スイッチの接続	18
エンドノードと接続する.....	18
ハブまたはスイッチと接続する.....	18
バックボーンまたはサーバと接続する.....	19
第4章 SmartConsole Utility による管理	20
SmartConsole Utility のインストール.....	20
SmartConsole Utility の画面構成.....	23
ツールメニュー.....	23
アイコンメニュー.....	24
モニタリスト.....	24
SmartConsole Utility の機能.....	25
デバイスの検出、追加、削除、モニタリング.....	25
デバイスのモニタ (ツールメニュー).....	26
デバイスの設定 (アイコンメニュー).....	29
第5章 Web マネージャによる詳細設定	32
Web ベースの管理について.....	32
Web マネージャへのログイン.....	32
Smart Wizard 設定.....	34
Web マネージャの画面構成.....	36
Web マネージャのメイン画面について.....	36
Web マネージャのメニュー構成.....	37
Web マネージャの初期画面.....	38
Device Information (デバイス情報).....	38
Save メニュー.....	39
Save Configuration (コンフィグレーション保存).....	39
Save Log (ログ保存).....	39
Tools メニュー.....	40
Reset (リセット).....	40
Reset System (システムリセット).....	40
Reboot Device (デバイスの再起動).....	40
Configuration Backup & Restore (コンフィグレーションの保存と復元).....	41
Firmware Backup & Upgrade (ファームウェアの保存と更新).....	42
Smart Wizard メニュー (スマートウィザード).....	42

Online Help メニュー (オンラインヘルプ)	43
Online Support Site (オンラインサポートサイトへの参照)	43
User Guide (ユーザガイドへの参照)	43
System (システム設定)	44
System Settings (スイッチの基本機能の設定)	44
Trap Settings (トラップ設定)	45
Port Settings (ポート設定)	46
SNMP Settings (SNMP 設定)	47
Password Access Control (パスワードアクセス制御)	48
System Log Settings (システムログ設定)	49
Configuration (管理フォルダ)	50
Jumbo Frame (ジャンボフレーム)	50
802.1Q VLAN (802.1Q VLAN 設定)	51
Asymmetric VLAN (非対称 VLAN 設定)	53
802.1Q Management VLAN (802.1Q マネジメント VLAN 設定)	55
Voice VLAN (音声 VLAN)	55
Link Aggregation (リンクアグリゲーション設定)	57
IGMP Snooping (IGMP Snooping 設定)	58
Port Mirroring (ポートミラーリング)	60
Power Saving (省電力設定)	61
Loopback Detection (ループバック検知設定)	61
SNTP Settings (SNTP 設定)	62
Spanning Tree (スパンニングツリー設定)	64
QoS (QoS 機能の設定)	66
Storm Control (ストームコントロール)	66
Bandwidth Control (帯域幅の設定)	67
802.1p/DSCP Priority Settings (802.1p/DSCP プライオリティ設定)	68
Security (セキュリティ機能の設定)	69
Trusted Host (トラストホスト)	69
Safeguard Engine (セーフガードエンジン)	70
Port Security (ポートセキュリティ)	70
802.1X (802.1X 機能の設定)	71
MAC Address Table (MAC アドレステーブル)	72
Monitoring (スイッチのモニタリング)	74
Statistics (統計情報)	74
Cable Diagnostics (ケーブル診断)	75
System Log (システムログ)	76
ACL メニュー (ACL 機能の設定)	77
ACL Configuration Wizard (ACL 設定ウィザード)	77
Access Profile List (アクセスプロファイルリスト)	78
ACL Finder (ACL エントリの検索)	81
PoE メニュー (PoE の設定) (DGS-1210-10P/GE のみ)	82
PoE Port Settings (PoE ポート設定)	82
PoE System Settings (PoE システム設定)	83
Time-Based PoE メニュー (タイムベース PoE の設定)	84
Time Range Settings (タイムレンジ設定)	84
LLDP (LLDP 設定) (DGS-1210-10P/GE のみ)	85
LLDP Global Settings (LLDP グローバル設定)	85
LLDP Remote Port Information (LLDP リモートポート情報)	86
LLDP MED Settings (LLDP MED 設定)	86

第6章 コマンドラインインタフェース	87
接続とログイン	87
Telnet 経由でスイッチに接続する	87
コマンドラインインタフェースにログインする	87
コマンド	87
CLI コマンドについて	87
download	88
upload	88
config ipif system	89
logout	89
ping	89
reboot	90
reset	90
show ipif	90
show switch	91
config account admin password	91
save	91
第7章 スイッチのメンテナンス	92
工場出荷時設定に戻す	92
付録 A ケーブルとコネクタ	93
付録 B ケーブル長	93
付録 C 用語解説	94

はじめに

DES-1210 シリーズユーザマニュアルは、本製品のインストールおよび操作方法を例題と共に記述しています。

第 1 章 本製品のご利用にあたって

- 製品の概要とその機能について説明します。また、前面および背面などの各パネルと LED 表示について説明します。

第 2 章 スイッチの設置

- スイッチの基本的な設置方法について説明します。また、スイッチの電源接続の方法についても紹介します。

第 3 章 スイッチの接続

- スイッチをご使用のイーサネット、またはバックボーンなどに接続する方法についても紹介します。

第 4 章 SmartConsole Utility による管理

- SmartConsole Utility を使用したスイッチのトラップモニタや設定について説明します。

第 5 章 Web マネージャによる詳細設定

- Web ベースの管理機能への接続方法および詳細な設定方法について説明します。

第 6 章 コマンドラインインタフェース (CLI)

- コマンドラインインタフェース (CLI) を使用した基本的な管理、設定方法について説明します。

付録 A ケーブルとコネクタ

- RJ-45 コンセント / コネクタ、ストレート / クロスオーバーケーブルと標準的なピンの配置について説明します。

付録 B ケーブル長

- ケーブルの種類と最大ケーブル長についての情報を示します。

付録 C 用語解説

- 本マニュアルに使用される用語の定義を示します。

本マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、使用にあたっての注意事項について説明します。

警告 警告では、ネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

補足 補足では、特長や技術についての詳細情報について説明します。

参照 参照では、別項目での説明へ誘導します。

表 1 に、本マニュアル中での字体・記号についての表記規則を表します。

表 1 字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に " (13 ページ) をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	(switch-prompt)#
courier 太字	コマンド、ユーザによるコマンドライン入力。	show network
<i>courier 斜体</i>	コマンドパラメータ (可変または固定)。	value
< >	可変パラメータ。< > にあたる箇所に値または文字を入力します。	<value>
[]	任意の固定パラメータ。	[value]
[< >]	任意の可変パラメータ。	[<value>]
{ }	{ } 内の選択肢から 1 つ選択して入力するパラメータ。	{choice1 choice2}
(垂直線)	相互排他的なパラメータ。	choice1 choice2
{ { }	任意のパラメータで、指定する場合はどちらかを選択します。	{ {choice1 choice2}

第1章 本製品のご利用にあたって

- スイッチ概要
- サポートする機能
- 搭載ポート
- 前面パネル
- 背面パネル
- ギガビットコンボポート

スイッチ概要

DGS-1210/GE シリーズは、低コストで高信頼性に加え、プラグアンドプレイの簡便さも兼ね備えている中小規模（SMB）ネットワーク用スイッチです。すべてのモデルは、見やすい前面パネルの診断用 LED を搭載するメタルケースに収納されており、100BASE-TX/1000BASE-T/SFP コンボポート、ネットワークセキュリティ、Asymmetric VLAN、QoS などの多様な管理機能を搭載しています。

PoE 機能

DGS-1210-10P/GE は、IEEE 802.3af 規格および IEEE 802.3at ドラフトに準拠しており、ネットワークにおいてネットワークケーブルを経由した電力供給を行う機能を提供しています。本製品では 8 個の 10BASE-T/100BASE-TX/1000BASE-T イーサネットポートが選択可能で、接続した無線アクセスポイント、IP 電話およびその他の PoE 対応デバイスに最大 15.4W または 30W の電力を供給することができます。これにより高い壁面や天井、AC 電源など設置が困難な場所にも配置することができます。

D-Link グリーンテクノロジー

D-Link グリーン製品は、高性能で環境に優しい製品を提供します。本シリーズは、デバイスが未接続のポートの節電、接続しているイーサネットケーブルに応じた電力使用量の調整など、エネルギー消費を削減する D-Link グリーンテクノロジーによる数多くのイノベーションが盛り込まれています。また、PoE モデルの DGS-1210-10P/GE は、ポートごとに電力供給時間の範囲を指定し、必要なポートの電源を切ることで稼働時間を削減するタイムベース PoE 機能を提供しています。

レイヤ 2 機能

本スイッチは、IGMP Snooping、ポートミラーリング、スパンニングツリー、リンクアグリゲーションおよびループバック検知などの L2 機能を搭載しており、性能とネットワークの柔軟性を強化しています。

Asymmetric VLAN と QoS

スイッチは、ネットワークセキュリティと性能を強化するため、トラフィックに優先順位を付加することによってタグ付けする 802.1Q VLAN 標準をサポートしています。また、802.1p プライオリティキューをサポートしており、ネットワークでストリーミングマルチメディアや VoIP などの帯域幅に敏感なアプリケーションを実行することができます。これらの機能により、スイッチはネットワークで VLAN と 802.1p トラフィックと共通とされることなく動作します。自動音声 VLAN は、通常のトラフィックと分けるために IP 電話から、より高い優先度を持つ VLAN に自動的に音声トラフィックを置きます。Asymmetric LAN はサーバやゲートウェイデバイスなどの共有リソースのより効率的な使用のために本スイッチに実装されています。

ネットワークセキュリティ

セーフガードエンジン機能は、ウイルス攻撃により引き起こされるトラフィックのフラッドからスイッチを保護します。スタティック MAC アドレス設定機能は、ネットワークへのアクセスを制限します。また、IEEE 802.1X ポートベース認証をサポートしており、ネットワークを外部の RADIUS サーバと共に設定することができます。ACL 機能は不要な IP/MAC のトラフィックの対応する強力なツールです。ストームコントロールにより、異常なトラフィックによるフラッドからネットワークを保護します。ポートセキュリティはネットワークデバイスの統合を維持するためにシンプルですが、便利な認証方式です。

多様な管理

ギガビット Web スマートスイッチは、管理者がリモートからネットワークをポートレベルでコントロール可能な直感的な SmartConsole Utility または Web ベース管理インターフェースを使用して、成長中のビジネスに簡便な管理を提供します。SmartConsole Utility は、ユーザのローカル PC に接続する同じ L2 ネットワークセグメントにおける複数の D-Link Web スマートスイッチを検出します。本ユーティリティの場合、ユーザは PC の IP アドレスを変更せずに、スマートスイッチの簡単な初期設定が可能です。また、ユーザのローカルな PC に接続する同じ L2 ネットワークセグメントのスイッチを画面に表示します。ここでは、大規模なスイッチ構成の設定やパスワード変更、ファームウェア更新などの検出したデバイスの基本設定が可能です。

ユーザは Telnet を使用してスイッチへ接続することもできます。IP アドレスの変更、工場出荷時設定へのリセット、再起動およびファームウェアの更新などの基本的なタスクはコマンドライン (CLI) を使用することができます。

さらに、スイッチステータスに関する情報のために、実装されている MIB ブラウザを使用してスイッチへのポーリングや異常なイベントのトラップ送信が可能です。MIB をサポートすることで SNMP 環境における管理のためにサードパーティのデバイスと本スイッチを統合化することができます。本スイッチはまた「D-View 6.0」に対応したプラグインモジュールを実装しており、視覚的なインターフェースによる効果的な操作、管理が可能です。

注意 D-Link 独自開発の SNMP 管理ソフトウェア、D-View は、D-Link のホームページ (<http://dlink-jp.com>) からソフトウェアとマニュアルのダウンロードが可能です。

サポートする機能

- IEEE 802.3 10BASE-T 準拠
- IEEE 802.3u 100BASE-TX 準拠
- IEEE 802.3ab 1000BASE-T 準拠
- IEEE 802.3z 1000BASE-LX/SX/LH 準拠
- IEEE 802.3x 全二重モードフローコントロール
- IEEE 802.1X ポートベース認証
- IEEE 802.1p Class of Service
- IEEE 802.1Q VLAN
- IEEE 802.1D スパニングツリー、IEEE 802.1w ラピッドスパニングツリー
- IEEE 802.3ad Link Aggregation
- IEEE 802.3af Power over Ethernet (DGS-1210-10P/GE のみ)
- ブロードキャストストーム制御
- ポート入出力速度制御
- アドレステーブル: デバイス毎最大 8K MAC アドレス
- パケットバッファ: 最大 512K バイト (DGS-1210-10P/GE、DGS-1210-16/GE、DGS-1210-24/GE)、最大 1M バイト (DGS-1210-48/GE)
- SNMP
- マネジメント VLAN、Asymmetric VLAN、自動音声 VLAN
- アクセスコントロールリスト (ACL)
- スタティック MAC アドレス設定
- D-Link セーフガードエンジン機能
- IGMP Snooping
- TFTP クライアント、DHCP クライアント、SNTP クライアント
- ケーブル診断機能
- タイムベース PoE (DGS-1210-10P/GE のみ)
- LLDP/LLDP-MED (DGS-1210-10P/GE のみ)
- Web ブラウザまたは SmartConsole Utility 経由の簡単設定
- Web ブラウザによるファームウェアのバックアップ/アップロード/システムの再起動
- ハードウェアおよび Web ブラウザによるコンフィギュレーションのリセット
- コマンドラインインタフェース (CLI)
- 以下の MIB のサポート
 - RFC 1213 MIB II
 - Bridge MIB (RFC1493)
 - SNMP v2 MIB (RFC1907)
 - MIB Traps Convention (RFC1215)
 - Interface Group MIB (RFC2233)
 - Power-Ethernet-MIB (RFC3621) (DGS-1210-10P/GE のみ)
 - LLDP-MIB (DGS-1210-10P/GE のみ)
 - プライベート MIB

搭載ポート

DGS-1210/GE シリーズスイッチは以下のポートを搭載しています。

DGS-1210-10P/GE

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 10
- SFP コンボポート x 2

DGS-1210-16/GE

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 16
- SFP コンボポート x 4

DGS-1210-24/GE

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 24
- SFP コンボポート x 4

DGS-1210-48/GE

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 48
- SFP コンボポート x 4

前面パネル

前面パネルには、Power、リセットボタン、オプションモジュール用の SFP ポート、ポートの Link/Act の状態を表示する LED を搭載しています。DGS-1210-10P/GE には Link/Act/State と PoE モードの切り替えを行う「Mode」ボタンが配置されています。「LED 表示」(13 ページ) の項で詳細の動作について説明します。また、リセットボタンを押下すると、すべての設定を工場出荷時の状態にリセットします。



図 1-1 DGS-1210-10P/GE の前面パネル図

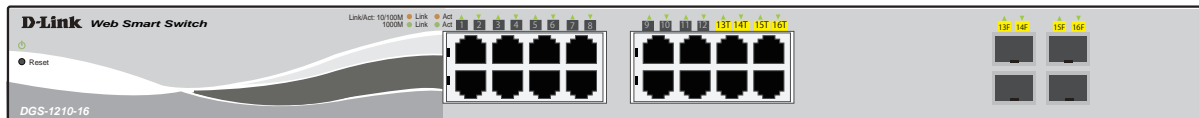


図 1-2 DGS-1210-16/GE の前面パネル図

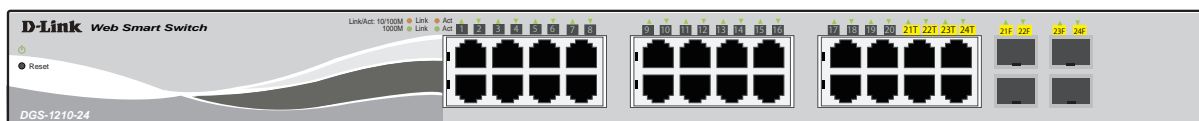


図 1-3 DGS-1210-24/GE の前面パネル図



図 1-4 DGS-1210-48/GE の前面パネル図

注意 SFP コンボポートは、対応する 1000BASE-T ポートと同時に使用することはできません。同時に使用すると SFP ポートが優先となり、1000BASE-T ポートは使用不可能となります。

LED 表示

Power、オプションモジュール用の SFP ポート、ポートの Link/Act の状態を表示する LED を搭載しています。DGS-1210-10P/GE は PoE の状態を示す LED を、DGS-1210-48/GE はファンの状態を表示する LED を搭載しています。

DGS-1210-10P/GE

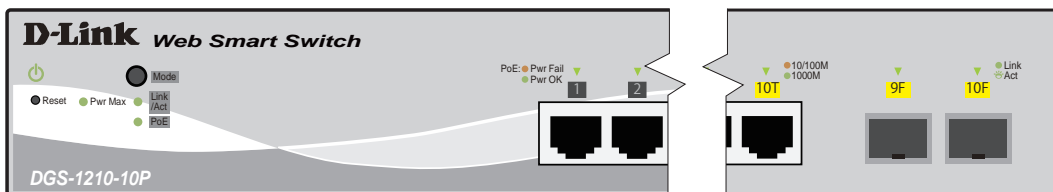


図 1-5 DGS-1210-10P/GE の前面パネルの LED 配置図

DGS-1210-16/GE

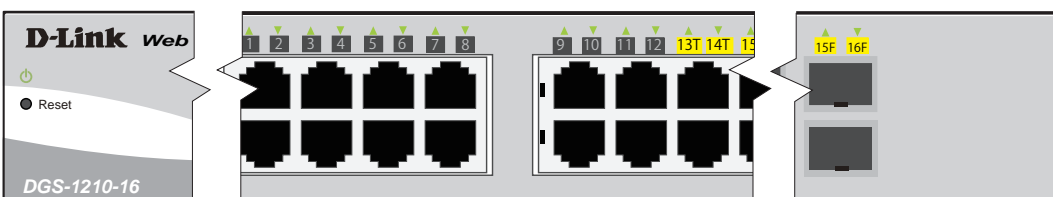


図 1-6 DGS-1210-16/GE の前面パネルの LED 配置図

DGS-1210-24/GE

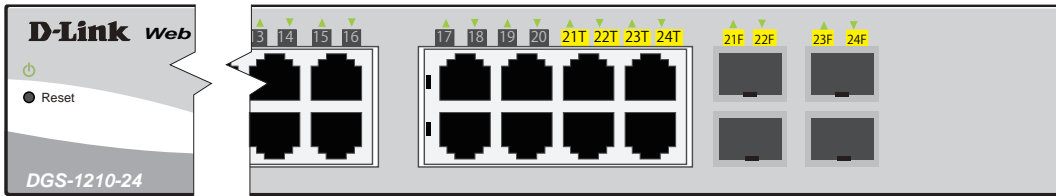


図 1-7 DGS-1210-24/GE の前面パネルの LED 配置図

DGS-1210-48/GE

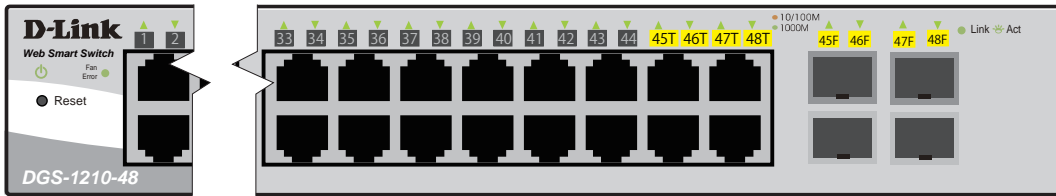


図 1-8 DGS-1210-48/GE の前面パネル LED 配置図

以下の表にスイッチの LED の状態が意味するスイッチの状態を示します。

LED	状態	色	内容
Power	点灯	緑	電源が供給され正常に動作しています。
	消灯	—	電源コード未接続、または電源不良などの原因で電源が供給されていません。
ポート LED	点灯	緑	1000Mbps でリンクが確立しています。
	点灯	橙	10/100Mbps でリンクが確立しています。
	点滅	緑 / 橙	データを送受信しています。
	消灯	—	リンクが確立していません。
PoE (DGS-1210-10P/GE のみ)			
Power Max	点灯	赤	設定した供給可能電力 (初期値では 78W) に到達しました。
	消灯	—	設定した供給可能電力 (初期値では 78W) に到達していません。PoE 受電機器に給電可能です。
PoE (DGS-1210-48/GE のみ)			
Fan Err	点灯	橙	ファンに異常が発生しました。
	消灯	—	ファンは正常に動作しています。

背面パネル

背面パネルには電源コネクタがあります。電源コネクタは標準の電源ケーブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 ~ 240VAC 内の電圧に調整されます。



図 1-9 DGS-1210-10P/GE の背面パネル図



図 1-10 DGS-1210-16/GE、DGS-1210-24/GE、DGS-1210-48/GE の背面パネル図

ギガビットコンボポート

DGS-1210/GE シリーズスイッチは、スイッチの前面パネルにギガビットイーサネット・コンボポートを装備しています。これらのポートは 1000BASE-T ポートと SFP ポート (オプション) の兼用ポートです。以下にスイッチに SFP ポートモジュールを挿入した図を示します。

注意 これらの前面パネルモジュールは同時に使用できませんが、SFP ポートモジュール挿入時は 1000BASE-T ポートとしての使用はできません。SFP ポートが優先されます。

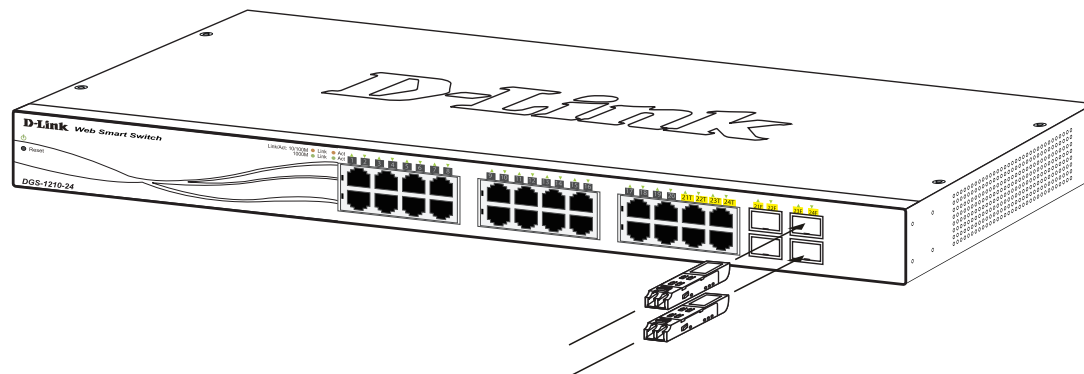


図 1-11 スイッチに光トランシーバを取り付ける

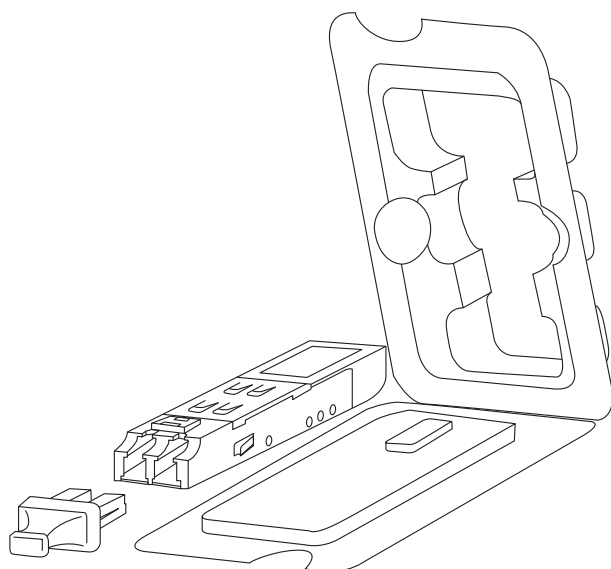


図 1-12 SFP モジュール図

第2章 スwitchの設置

- パッケージの内容
- ネットワーク接続前の準備
- ゴム足の取り付け (19 インチラックに設置しない場合)
- 19 インチラックへの取り付け
- 電源の投入

パッケージの内容

ご購入いただいたスイッチの梱包箱を開け、同梱物を注意して取り出してください。以下のものが同梱されています。

- ・ 本体 x 1
- ・ AC 電源ケーブル x 1
- ・ 電源ケーブル抜け防止金具 x 1
- ・ ラックマウントキット 1 式 (ブラケット 2 枚、ネジ)
- ・ ゴム足 (貼り付けタイプ) x 4
- ・ CD-ROM
- ・ クイックインストールガイド
- ・ 製品保証書

万一、不足しているものや損傷を受けているものがありましたら、交換のために弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

ネットワーク接続前の準備

スイッチの設置場所が性能に大きな影響を与えます。以下のガイドラインに従って本製品を設置してください。

- ・ スイッチは、しっかりとした水平面で耐荷重性のある場所に設置してください。
- ・ スイッチの上に重いものを置かないでください。
- ・ 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- ・ 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- ・ 本スイッチの周辺で熱の放出と十分な換気ができることを確認してください。換気のためには少なくとも製品の前後 16cm 以上の空間を保つようにしてください。
- ・ スイッチは動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- ・ スイッチは強い電磁場が発生するような場所 (モータの周囲など) や、振動、ほこり、および直射日光を避けて設置してください。
- ・ スイッチを水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム製の足はスイッチのクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

ゴム足の取り付け (19 インチラックに設置しない場合)

机や棚の上に設置する場合は、まずスイッチに同梱されていたゴム製足をスイッチの裏面の四隅に取り付けます。スイッチの周囲に十分な通気確保するようにしてください。

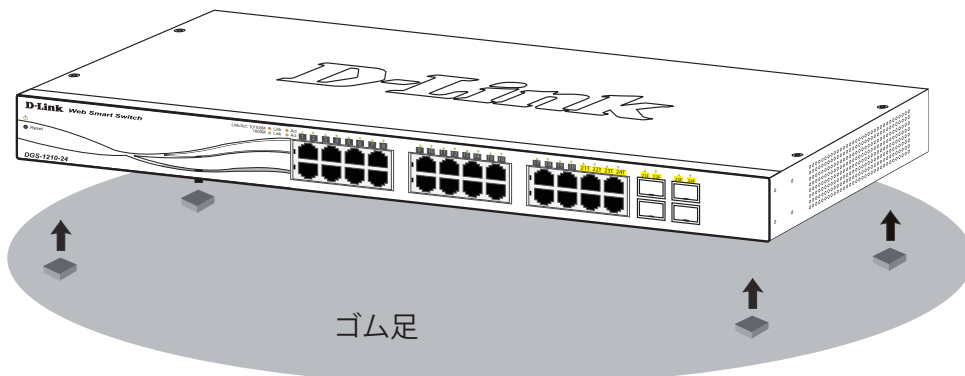


図 2-1 机や棚の上に設置する場合の準備

19 インチラックへの取り付け

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

ブラケットの取り付け

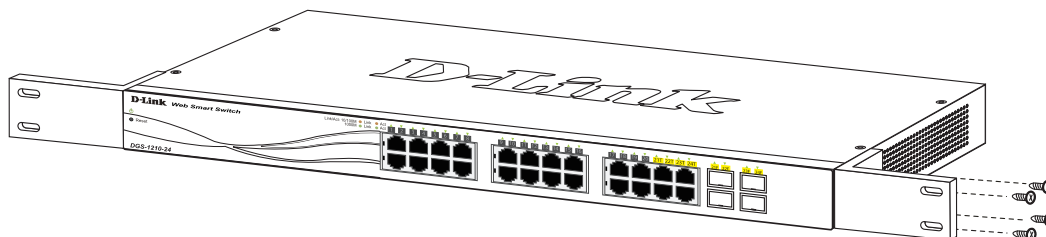


図 2-2 スイッチへのブラケットの取り付け

ラックマウントキットに付属のネジを使用して、本スイッチにブラケットを取り付けます。完全にブラケットが固定されていることを確認し、本スイッチを以下の通り標準の 19 インチラックに固定します。

19 インチラックにスイッチを取り付ける

警告 前面、側面にスタビライザを取り付けずに製品を設置すると、ラックが転倒し、場合によっては人身事故を引き起こすことがあります。そのため、ラック内に製品を取り付ける前に必ずスタビライザを取り付けてください。ラックにシステム/コンポーネントを取り付けた後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つだけとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。

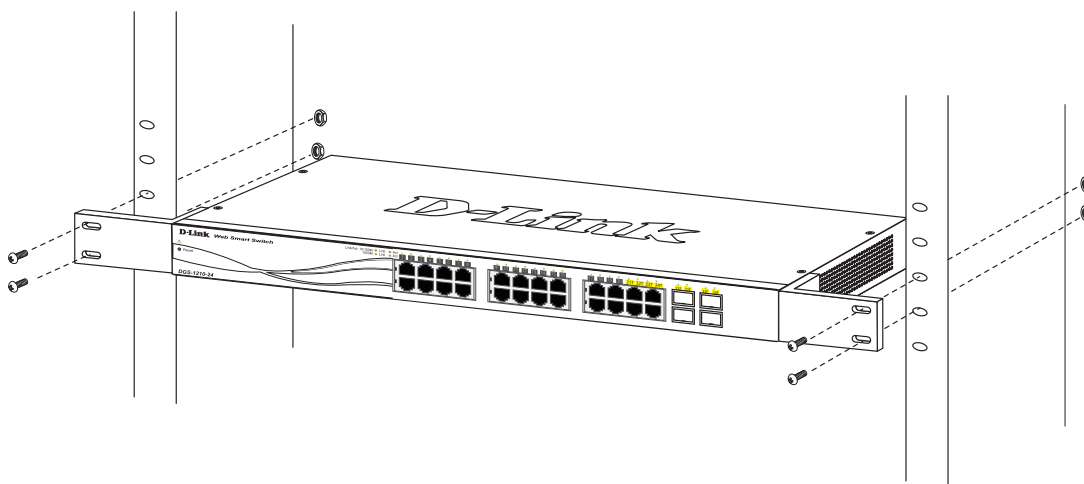


図 2-3 スイッチのラックへの設置

電源の投入

1. 電源ケーブルを本スイッチの電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。
2. 本スイッチに電源が供給されると、Power LED が点灯します。

第3章 スイッチの接続

- エンドノードと接続する
- ハブまたはスイッチと接続する
- バックボーンまたはサーバと接続する

注意 すべてのポートは Auto MDI/MDI-X 接続をサポートしています。

エンドノードと接続する

本スイッチの 10BASE-T/100BASE-TX//1000BASE-T ポートとエンドノードをカテゴリ 3、4、5 の UTP/STP ケーブルを使用して接続します。エンドノードとは、RJ-45 コネクタ対応 10/100Mbps または 1000Mbps ネットワークインタフェースカードを装備した PC やルータを指しています。エンドノードとスイッチ間にはカテゴリ 3、4、または 5 の UTP ケーブルで接続できます。エンドノードへの接続はスイッチ上のすべてのポートから行えます。

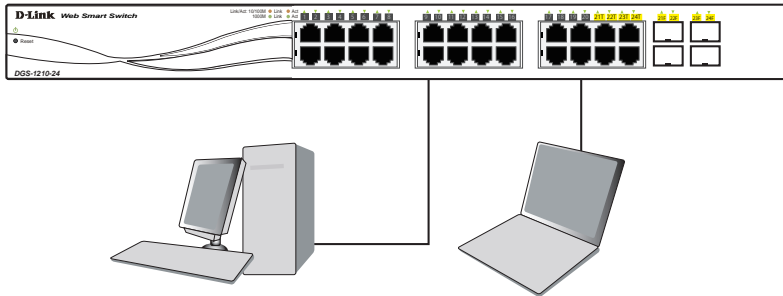


図 3-1 エンドノードと接続した図

エンドノードと正しくリンクが確立すると本スイッチの各ポートの Link/Act LED は緑または橙に点灯します。データの送受信中は点滅します。

ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

- ・ カテゴリ 3 以上の UTP ケーブル：10BASE-T ハブまたはスイッチと接続する。
- ・ カテゴリ 5 以上の UTP ケーブル：100BASE-TX ハブまたはスイッチと接続する。
- ・ エンハンストカテゴリ 5 以上の UTP ケーブル：1000BASE-T スイッチと接続する。PoE 給電に使用する。(DGS-1210-10P/GE のみ)

ケーブル仕様については「[付録 A ケーブルとコネクタ](#)」(93 ページ) を参照してください。

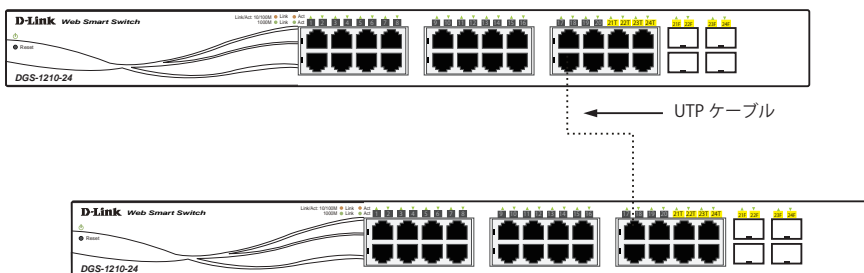


図 3-2 ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

2つの SFP ポートは、ネットワークバックボーンやサーバとのアップリンク接続に適しています。ギガポートは 10/100/1000Mbps の速度を提供し、SFP ポートは、全二重モード時において 100Mbps または 1000Mbps の速度を提供します。

ギガビットイーサネットポートとの接続はポートのタイプによって光ファイバケーブルまたはエンハンスドカテゴリ 5 ケーブルを使用します。正しくリンクが確立すると Link LED が点灯します。

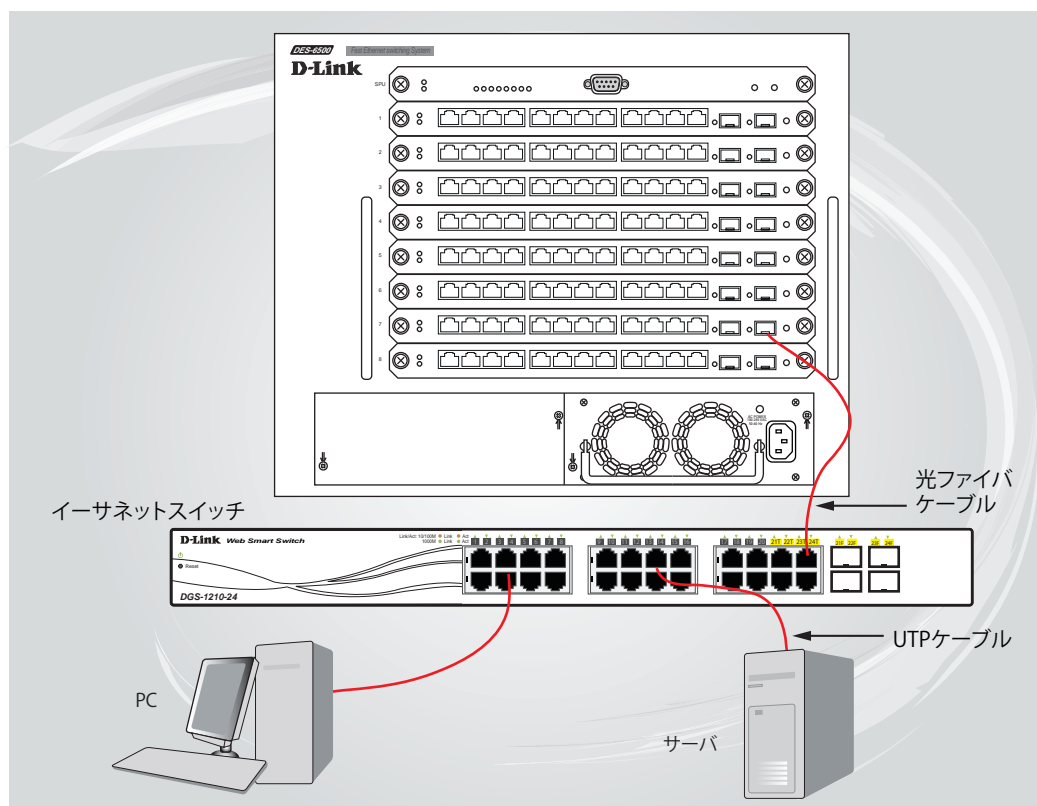


図 3-3 サーバ、PC、スイッチスタックとのアップリンク接続図

第4章 SmartConsole Utility による管理

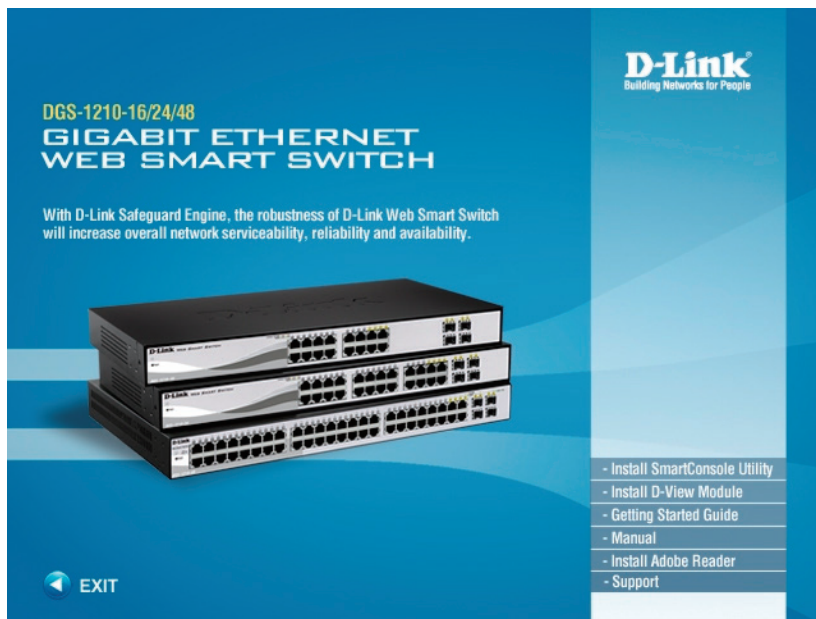
- SmartConsole Utility のインストール
- SmartConsole Utility の画面構成
- SmartConsole Utility の機能

本製品添付の「SmartConsole Utility」ですべての Web 管理スイッチを簡単に検出し、IP アドレスの割り当て、パスワードの変更、および新しいファームウェアの更新を行うことができます。

SmartConsole Utility のインストール

SmartConsole Utility を使用すると、ネットワークに接続したワークステーションから、複数の D-Link Web スマートスイッチの監視や設定を行うことが可能になります。以下の手順に従って SmartConsole Utility のインストールを行ってください。

1. 製品に付属の CD-ROM を管理用 PC の CD-ROM ドライブに挿入します。自動的に起動し、製品に応じて以下のような起動画面が表示されます。



補足

起動画面が表示されない場合は、Windows の「スタート」-「マイコンピュータ」の順にクリックし、「マイコンピュータ」画面で以下のアイコンをダブルクリックします。



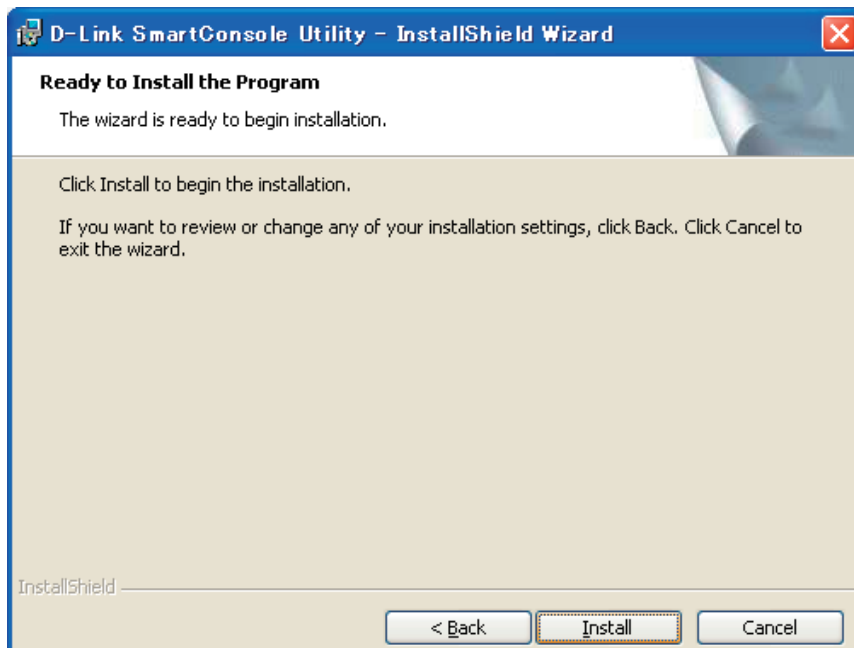
2. 「Install SmartConsole Utility」メニューをクリックすると、以下の画面が表示されます。



3. 「Install」 ボタンをクリックすると、InstallShield ウィザードが開始されます。「Next」 ボタンをクリックします。



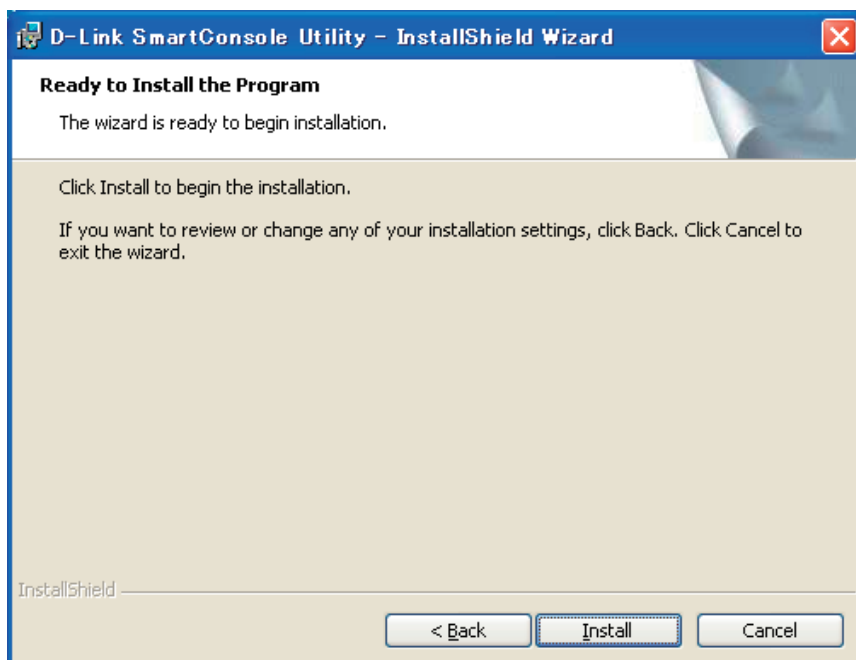
4. プログラムのインストール先を指定します。



プログラムのインストール先を変更する場合は、「Change」 ボタンをクリックし、フォルダを指定します。

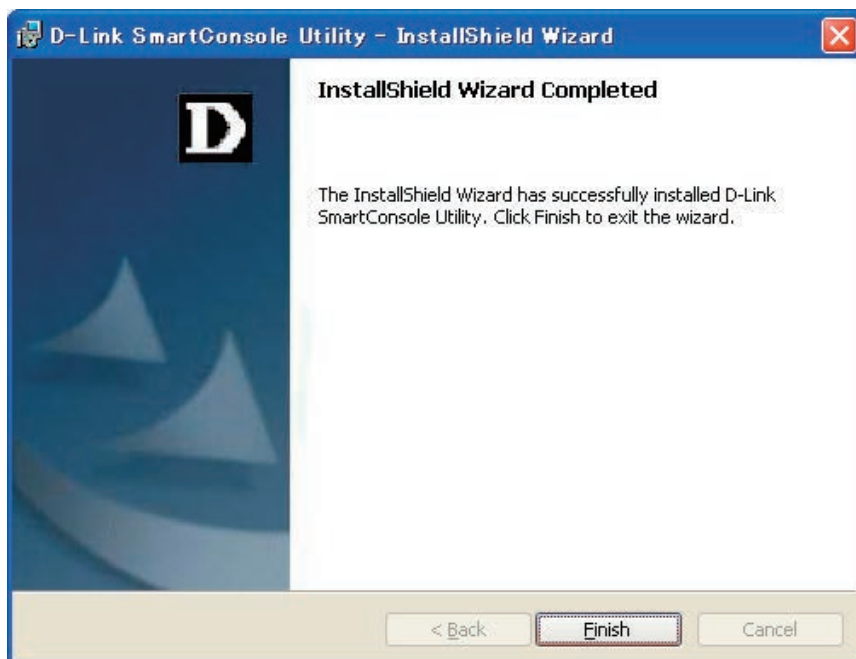
「Next」 ボタンをクリックします。

5. 以下の画面が表示されます。



「Install」 ボタンをクリックすると、インストールが開始し、インストール中のダイアログが表示されます。

6. インストールが終了するとインストールの完了画面が表示されます。



「Finish」 ボタンをクリックしてインストールを完了します。また、CD-ROM の起動画面は「EXIT」をクリックして終了します。

7. Windows デスクトップアイコン  をダブルクリックします。または、「スタート」メニューの「すべてのプログラム」から「D-Link SmartConsole Utility」の「D-Link SmartConsole Utility」を選択して SmartConsole Utility を起動します。

SmartConsole Utility の画面構成

SmartConsole Utility の画面は、ツールメニュー、アイコンメニューおよびモニタリストに分かれています。

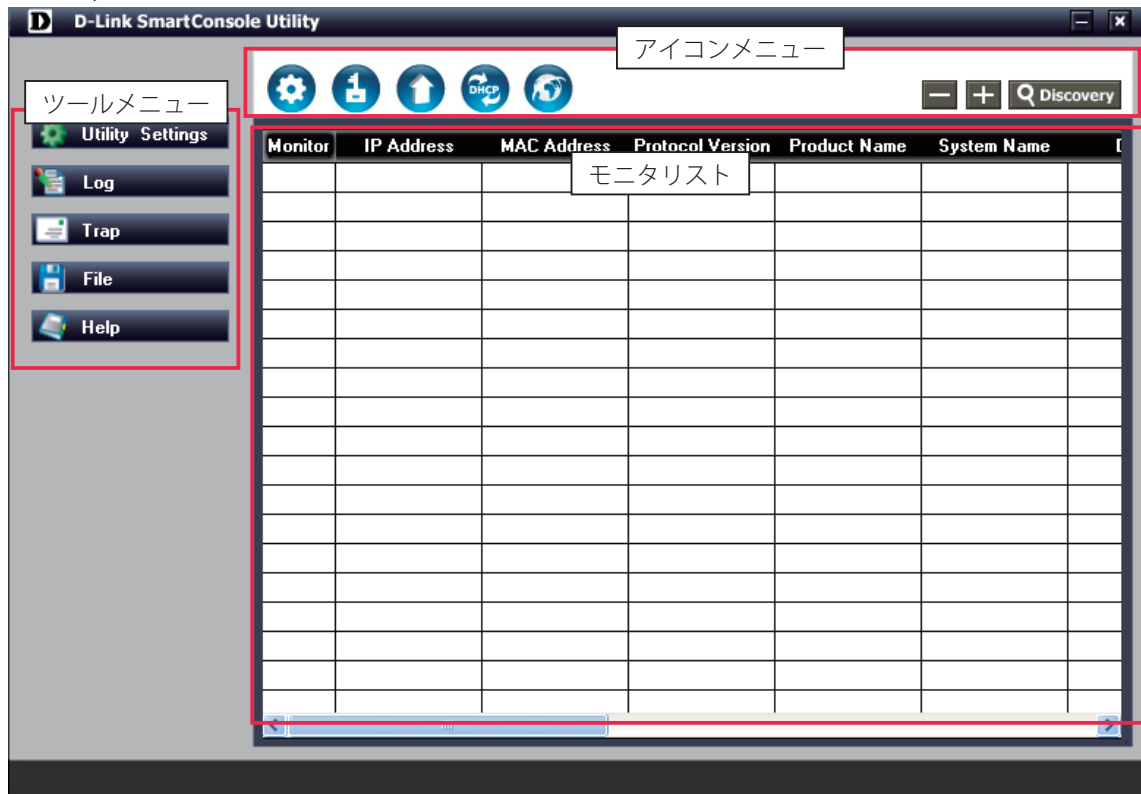







図 4-1 SmartConsole Utility 画面構成









ツールメニュー

SmartConsole Utility のツールメニューには以下の「Utility Settings」、「Log」、「Trap」、「File」および「Help」の 5 つのメニューがあります。

項目	説明
 Utility Settings	デバイスのモニタデータを更新する間隔または Web スマートスイッチの検出を行い、表示を更新する間隔を指定します。
 Log	ログの参照またはクリアをします。
 Trap	トラップの参照またはクリアをします。
 File	<ul style="list-style-type: none"> Monitor Save - モニタリストの現在の設定を初期設定として保存し、次回ユーティリティを起動した場合に自動的にモニタリストに加えてモニタを行います。 Monitor Save As - モニタリストの現在の設定をファイルに保存します。 Monitor Load - 「Monitor Save As」で保存したファイルを選択し、モニタリストに設定します。
 Help	ユーティリティのバージョンを表示します。


アイコンメニュー

SmartConsole Utility のアイコンメニューは以下の通りです。

項目	説明
 Device Settings	デバイスの設定を変更します。
 Device Password Manager	デバイスのパスワードを変更します。
 Multi Firmware Upgrade	複数のデバイスのファームウェアを更新します。
 DHCP Refresh	DHCP サーバに IP アドレスの割り当てを要求します。
 Web Access	Web ベースのユーティリティにアクセスします。
 Delete the selected Items	選択デバイスをモニタリストから削除します。
 Add the new Item	指定スイッチをモニタリストに追加します。
 Discovery	ネットワーク上の Web スマートスイッチを検出し、モニタリストに表示します。

モニタリスト

モニタリストの項目は以下の通りです。

項目	説明
Monitor	<input type="checkbox"/> アイコン - ユーティリティが検出済みのデバイスです。 <input checked="" type="checkbox"/> アイコン - モニタを行うデバイスをチェックすると、デバイスからトラップとログのデータを収集します。デバイスを設定する場合は、チェックを外します。  アイコン - 検出されたデバイスに接続できません。デバイスの電源またはケーブルを確認する必要があります。
IP Address	デバイスの現在の IP アドレス。
MAC Address	デバイスの MAC アドレス。
Protocol Version	ユーティリティプロトコルのバージョン。
Product Name	デバイスの製品名。
System Name	デバイスのシステム名。
DHCP	ネットワークのブートプロセス中に DHCP サーバから IP アドレスのリースを取得する機能の有効 (Enable) / 無効 (Disable)。
Location	デバイスの位置する場所。
Trap IP	トラップ送信先 IP アドレス。
Subnet Mask	デバイスのサブネットマスク。
Gateway	デバイスのゲートウェイ。
Group Interval	スイッチがモニタリストに検出される間隔 (秒)。
Firmware version	管理するデバイスのファームウェアバージョンを表示します。
LLDP	スイッチの LLDP (Link Layer Discovery Protocol) について表示します。
SNMP	スイッチの SNMP について表示します。

デバイスのモニタリング

リスト上のデバイスの「Monitor」をチェックすると、モニタの対象となります。また、トラップを受信してデバイスの状態を確認することもできます。デバイスの設定をする場合は、対象デバイスの「Monitor」のチェックを外します。

各設定項目は以下の通りです。

項目	説明
Monitor	<input type="checkbox"/> アイコン - ユーティリティが検出済みのデバイスです。 <input checked="" type="checkbox"/> アイコン - モニタを行うデバイスをチェックすると、デバイスからトラップとログのデータを収集します。デバイスを設定する場合は、チェックを外します。 <input type="checkbox"/> アイコン - 検出されたデバイスに接続できません。デバイスの電源またはケーブルを確認する必要があります。
IP Address	デバイスの現在の IP アドレス。
MAC Address	デバイスの MAC アドレス。
Protocol Version	ユーティリティプロトコルのバージョン。
Product Name	デバイスの製品名。
System Name	デバイスのシステム名。
DHCP	ネットワークのブートプロセス中に DHCP サーバから IP アドレスのリースを取得する機能の有効 (Enable) / 無効 (Disable)。
Location	デバイスの位置する場所。
Trap IP	トラップ送信先ホスト IP アドレス。
Subnet Mask	デバイスのサブネットマスク。
Gateway	デバイスのゲートウェイ。
Group Interval	スイッチがモニタリストに検出される間隔 (秒)。
Firmware version	管理するデバイスのファームウェアバージョンを表示します。
LLDP	スイッチの LLDP (Link Layer Discovery Protocol) について表示します。
SNMP	スイッチの SNMP について表示します。


注意 デバイスが赤く表示された場合、ファームウェアのアップグレードが必要です。

注意 LLDP 機能は、DGS-1210-10P/GE モデルでのみ提供しています。その他のモデルでは空白となります。

デバイスのモニタ (ツールメニュー)

Utility Settings

デバイスのモニタデータの更新間隔またはスマートスイッチの検出間隔を指定します。

ツールメニューから  Utility Settings アイコンを選択し、以下の画面を表示します。

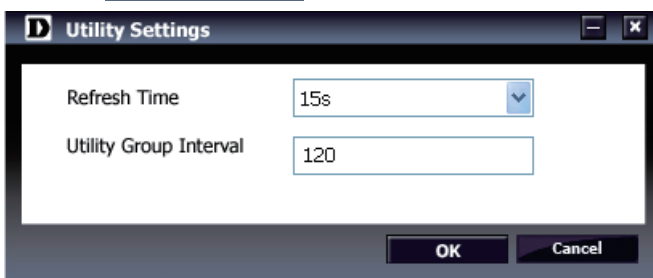


図 4-5 Utility Settings ダイアログ

「Refresh Time」または「Utility Group Interval」欄を入力後、「OK」ボタンをクリックします。

画面には以下の項目があります。

項目	説明
Refresh Time	デバイスのモニタデータを更新する間隔を指定します。15 秒、30 秒、1 分、2 分、5 分から選択します。
Utility Group Interval	Web スマートスイッチの検出を行い、モニタリストの表示を更新する間隔 (秒) を指定します。

注意 「Utility Group Interval」に 0 を指定する場合、IGMP Snooping 機能を必ず無効にしてください。無効にしないと、Web スマートスイッチは検出されません。

Log

ログの参照またはクリアをします。

ツールメニューから  Log アイコンを選択し、以下の画面を表示します。



図 4-6 Log ダイアログ

画面には以下の項目があります。

項目	説明
Date	ログを受信した日を表示します。
Time	ログを受信した時刻を表示します。
IP	ログが発生した IP アドレスを表示します。
Status	ログメッセージの内容を表示します。
System Name	デバイスのシステム名。
View Log	SmartConsole Utility とデバイス上で発生したイベントを表示します。
Clear Log	すべてのログをクリアします。

「OK」 ボタンをクリックし、画面を終了します。

Trap

トラップの参照またはクリアをします。

ツールメニューから  Trap アイコンを選択し、以下の画面を表示します。

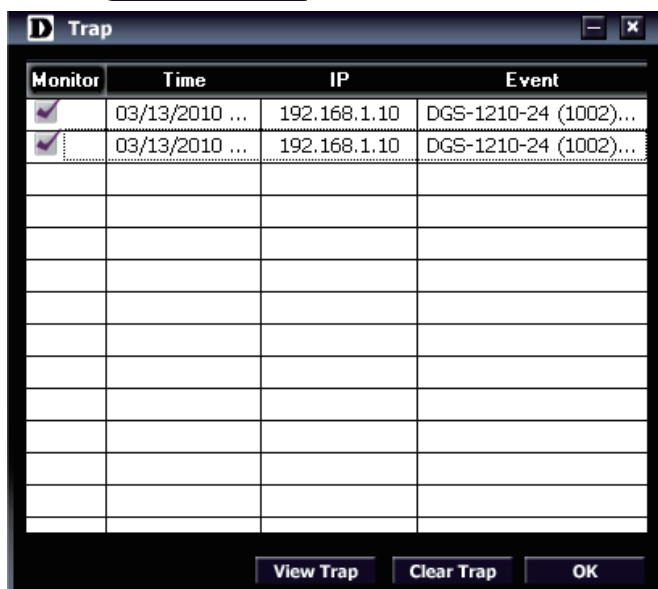


図 4-7 Trap ダイアログ



Smart Console Utilityによる管理

画面には以下の項目があります。

項目	説明
Date	トラップを受信した日を表示します。
Time	トラップを受信した時刻を表示します。
IP	トラップが発生した IP アドレスを表示します。
Event	トラップメッセージの内容を表示します。
View Trap	SmartConsole Utility とデバイス上で発生したトラップを表示します。
Clear Trap	すべてのトラップをクリアします。

「OK」 ボタンをクリックし、画面を終了します。

ユーティリティから新しいトラップを受信するとトラップアイコンが以下の通り変わります。

アイコン	説明
 Trap	新しいトラップはありません。
 Trap	新しいトラップを受信しました。

注意 トラップ情報を受信するためには、Web ブラウザの「Trap Setting」メニューでトラップホストの IP アドレスとトラップイベントを設定する必要があります。「[Trap Settings \(トラップ設定\)](#)」(45 ページ) を参照してください。

File

現在のモニタリストの保存または保存ファイルのリストアをします。

ツールメニューから  File アイコンを選択し、さらに以下のメニューから選択します。

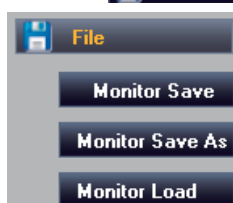


図 4-8 File メニュー

項目	説明
Monitor Save	モニタリストの現在の設定を初期設定として保存し、次回ユーティリティを起動した場合に自動的にモニタリストに加えてモニタを行います。
Monitor Save As	モニタリストの現在の設定をファイルに保存します。
Monitor Load	「Monitor Save As」で保存したファイルを選択し、モニタリストに設定します。

Help

ユーティリティのバージョンを表示します。

ツールメニューから「Help」を選択し、以下の画面を表示します。

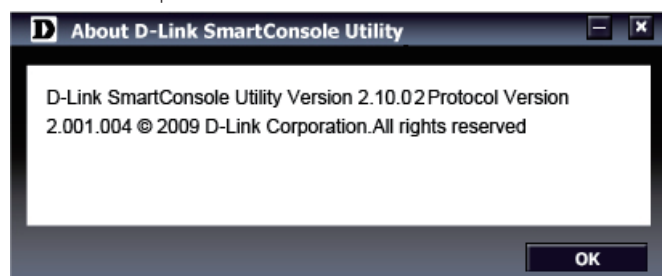



図 4-9 Help ダイアログ

「OK」 ボタンをクリックし、本ダイアログを終了します。

デバイスの設定 (アイコンメニュー)

Device Settings (デバイス設定)

デバイスの設定を変更します。

モニタリストで変更を行うデバイスの「Monitor」のチェックを外してデバイスを選択し、アイコンメニューから  アイコンをクリックすると「Device Settings」ダイアログが表示されます。

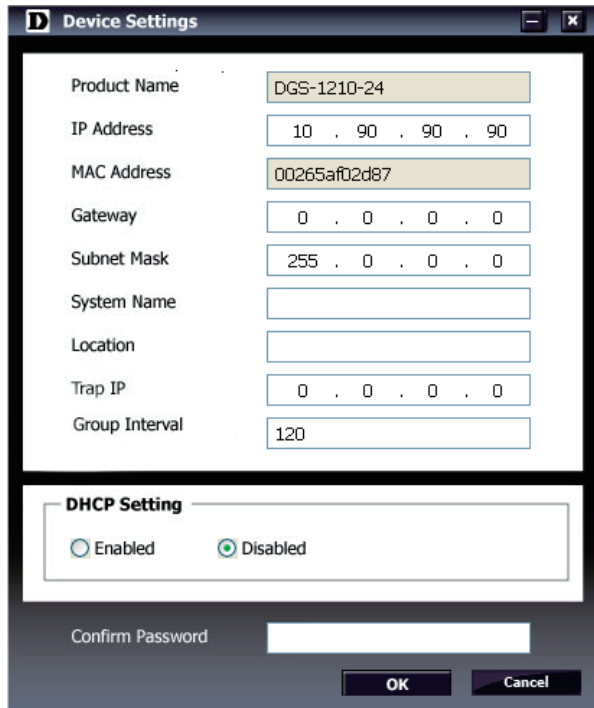


図 4-10 Device Settings 画面

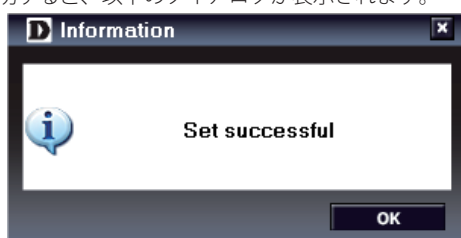
変更を行うデータを入力後、「Confirm Password」に現在のパスワードを入力し、「OK」ボタンをクリックします。

注意 パスワードの初期値は「admin」です。

各設定項目は以下の通りです。

項目	説明
Product Name	デバイスの製品名。
IP Address	デバイスの IP アドレス。
MAC Address	デバイスの MAC アドレス。
Gateway	ゲートウェイの IP アドレス。
Subnet Mask	デバイスのサブネットマスク。
System Name	デバイスのシステム名。
Location	デバイスの場所。
Trap IP	トラップ送信先 IP アドレス。
Group Interval	デバイスのグループインターバル。
DHCP Setting	DHCP サーバからの IP アドレス取得の有無。初期値は「Disabled」(取得しない)です。
Confirm Password	デバイスのパスワード。

設定に成功すると、以下のダイアログが表示されます。



「OK」ボタンをクリックします。

Device Password Manager (パスワード変更)

デバイスのパスワードを変更します。


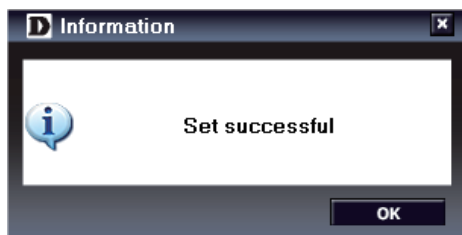
モニタリストで変更を行うデバイスの「Monitor」のチェックを外してデバイスを選択し、アイコンメニューから  アイコンをクリックすると「Device Password Manager」画面が表示されます。



図 4-11 Device Password Manager 画面


パスワードを変更するためには、「Old Password」に現在のパスワードを、「New Password」および「Confirm Password」に新しいパスワードを入力して「OK」ボタンをクリックします。

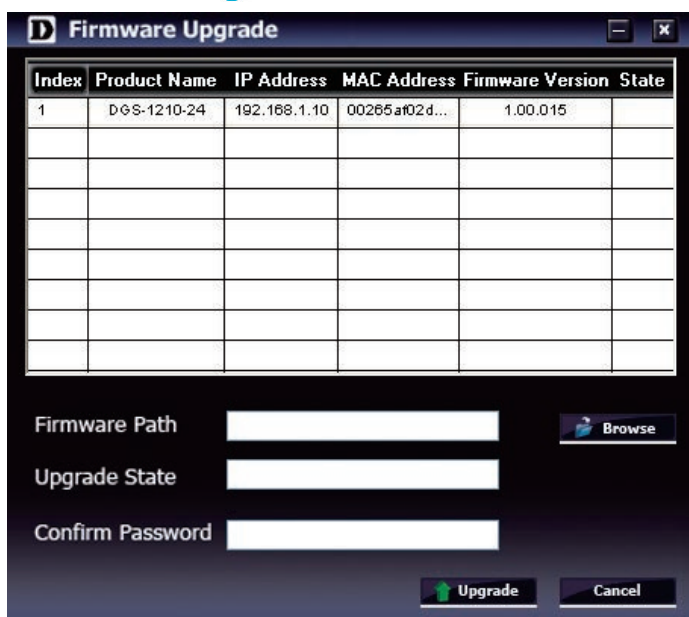
設定に成功すると、以下のダイアログが表示されます。



「OK」ボタンをクリックします。

Multi Firmware Upgrade (ファームウェアの更新)

デバイスリスト内の同じ機種種のファームウェアを更新します。モニタリストで更新を行うデバイスの「Monitor」のチェックを外してデバイスを選択します。アイコンメニューから  アイコンをクリックすると「Firmware Upgrade」画面が表示されます。

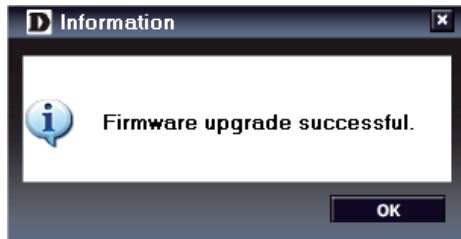


Index	Product Name	IP Address	MAC Address	Firmware Version	State
1	DGS-1210-24	192.168.1.10	00265a102d...	1.00.015	

図 4-12 Multi Firmware Upgrade 画面

「Firmware Path」にファームウェアの保存先へのパスを指定後、「Confirm Password」に現在のパスワードを入力し「Upgrade」ボタンをクリックします。

「Upgrade State」に更新状態が表示されます。更新が完了すると以下のダイアログが表示されます。



「OK」ボタンをクリックします。

注意 ファームウェアの更新が終了するまでPCの接続の切断、電源コードの取り外しは行わないでください。ファームウェアの更新が完了していない場合、スイッチが破損する可能性があります。

DHCP Refresh (DHCP リフレッシュ)

Web スマートスイッチは DHCP サーバに IP アドレスの割り当てを要求します。本機能は、デバイスの DHCP 機能が有効な場合に動作します。



「Device Settings」の「DHCP Setting」で、事前に機能を「Enabled」(有効)にします。モニタリストでリフレッシュを行うデバイスの「Monitor」のチェックを外してデバイスを選択します。モニタリストからデバイスを選択し、アイコンメニューから  アイコンをクリックすると「DHCP Refresh」画面が表示されます。



図 4-13 DHCP Refresh ダイアログ

「Device Password」に現在のパスワードを入力し「OK」ボタンをクリックします。

Web Access (Web ブラウザへの接続)

モニタリストからデバイスを選択し、アイコンメニューから  アイコンをクリックすると、Web ベースのユーティリティにアクセスできます。Web ベースのユーティリティへの接続については「[Web マネージャへのログイン](#)」(32 ページ)を参照してください。

第5章 Web マネージャによる詳細設定

- Web ベースの管理について
- Web マネージャへのログイン
- Smart Wizard 設定
- Web マネージャの画面構成
- Web マネージャのメニュー構成
- Web マネージャの初期画面について
- Save メニュー
- Tools メニュー
- Smart Wizard メニュー (スマートウィザード)
- Online Help (オンラインヘルプ)
- System (システム設定)
- Configuration (管理フォルダ)
- QoS (QoS 機能の設定)
- Security (セキュリティ機能の設定)
- Monitoring (スイッチのモニタリング)
- ACL (ACL 機能の設定)

Web ベースの管理について

本スイッチのすべてのソフトウェア機能は、実装されている Web ベース (HTML) インタフェース経由で管理、設定およびモニタできます。標準的なブラウザを使用してネットワーク上のリモートステーションから本スイッチを管理できます。ブラウザが普遍的なアクセスツールの役割をし、HTTP プロトコルを使用してスイッチと直接通信することが可能です。

Web マネージャへのログイン

スイッチに詳細設定を行うためには、はじめにコンピュータでブラウザを起動し、本スイッチに定義した IP アドレスを入力します。ブラウザのアドレスバーに以下のように URL を入力します。

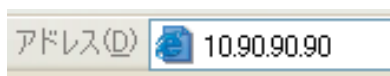


図 5-1 URL の入力

注意 工場出荷時設定では IP アドレス「10.90.90.90」、サブネットマスク「255.0.0.0」が設定されています。端末側の IP インタフェースを本スイッチに合わせるか、本スイッチを端末側の IP インタフェースに合わせてください。例えば Web スマートスイッチの初期値の IP アドレスが 192.168.1.1 であれば、管理 PC のアドレスは 192.168.1.x (x は 2 ~ 254 の間の整数)、サブネットマスクは 255.255.255.0 である必要があります。

参照 Web ベースのユーティリティには SmartConsole Utility 経由でアクセスすることも可能です。詳細については「[第4章 SmartConsole Utility による管理](#)」(20 ページ)を参照してください。

以下のユーザ認証画面が表示されます。



図 5-2 パスワード入力用画面

「Password」に「admin」(初期値)を入力して「OK」ボタンをクリックし、Web ベースユーザインタフェースに接続します。パスワードを既に設定している場合は、設定したパスワードを入力します。

以下のウィザード画面が表示されます。



図 5-3 Wizard 画面

ここでは、ウィザードの各タブにより、本製品のパスワード、基本的な SNMP 設定および IP アドレスなどのシステム設定を行います。ウィザードを使用して設定する場合は、次の「Smart Wizard 設定」を参照してください。ウィザードを使用しない場合は、「Exit」ボタンをクリックします。「Don't show Smart Wizard next time」をチェックすると、次回からウィザード画面は表示されなくなります。

以下の Web マネージャのメイン画面が表示されます。

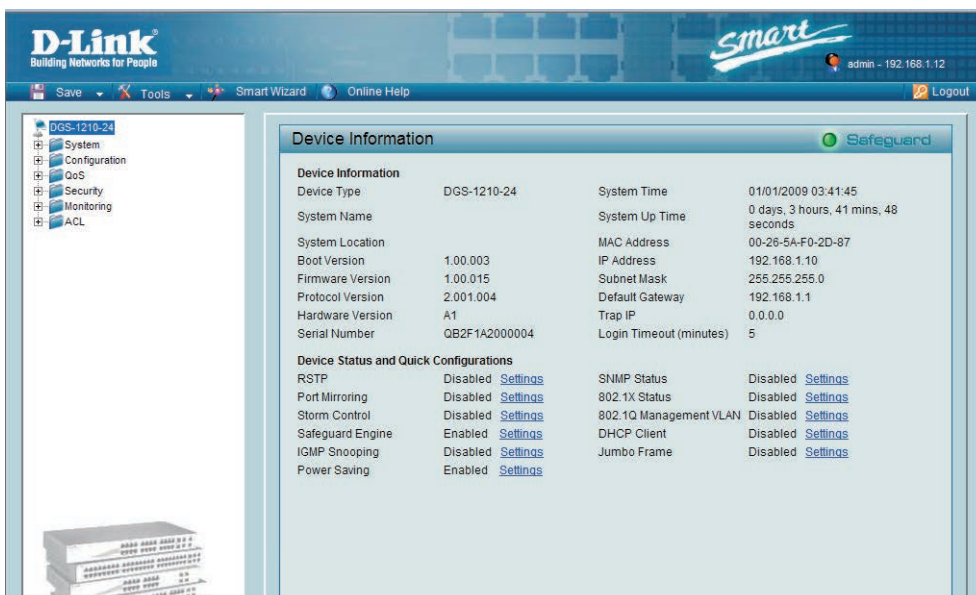


図 5-4 Web マネージャメイン画面

Smart Wizard 設定

Web ベースのマネジメントユーティリティを利用する前に、「Smart Wizard」で基本的な機能を設定します。

1. Web マネージャメイン画面の「Smart Wizard」メニューをクリックしてウィザードを開始します。変更しない場合は、「Exit」ボタンをクリックしてウィザードを終了し、Web インタフェースに移ります。
2. 「Password Settings」タブでデバイスのログインパスワードを変更します。

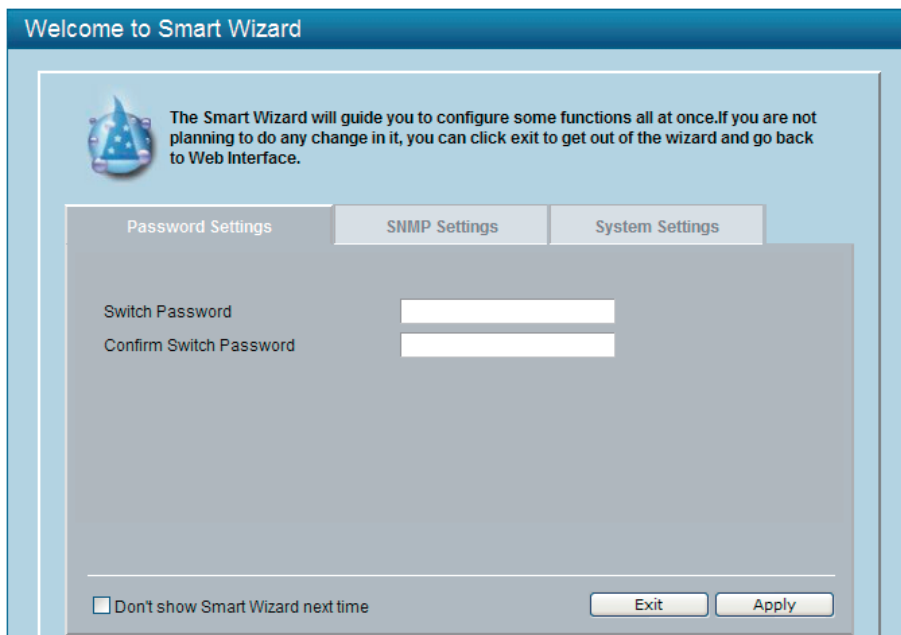


図 5-5 パスワード設定画面

「Switch Password」欄に新しいパスワードを入力し、「Confirm Switch Password」欄に確認のため再度同じパスワードを入力して「Apply」ボタンをクリックするとパスワードが変更されます。

3. 「SNMP Settings」タブで SNMP 機能を有効 / 無効、SNMP コミュニティ名の設定を行います。

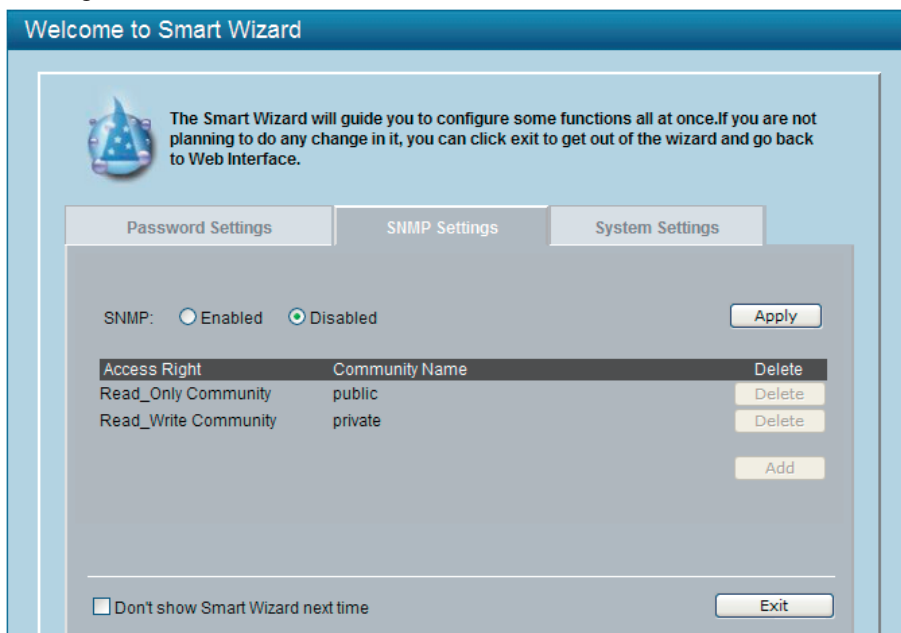


図 5-6 SNMP 設定画面

初期設定では SNMP 機能は「Disabled」（無効）です。「Enabled」（有効）をチェックしてコミュニティの設定を行い、「Apply」ボタンをクリックして設定を適用します。

項目	説明
Read_Only Community	MIB オブジェクトの読み取り権限が許可されているコミュニティ名を入力します。初期値は「public」です。
Read_Write Community	MIB オブジェクトの読み取りと書き込みの権限を与えられているコミュニティ名を入力します。初期値は「private」です。

注意 SNMP 機能の詳細については、「[SNMP Settings \(SNMP 設定\)](#)」(47 ページ)を参照してください。

4. 「System Settings」タブで、IP アドレスなど本製品のシステム設定を行います。

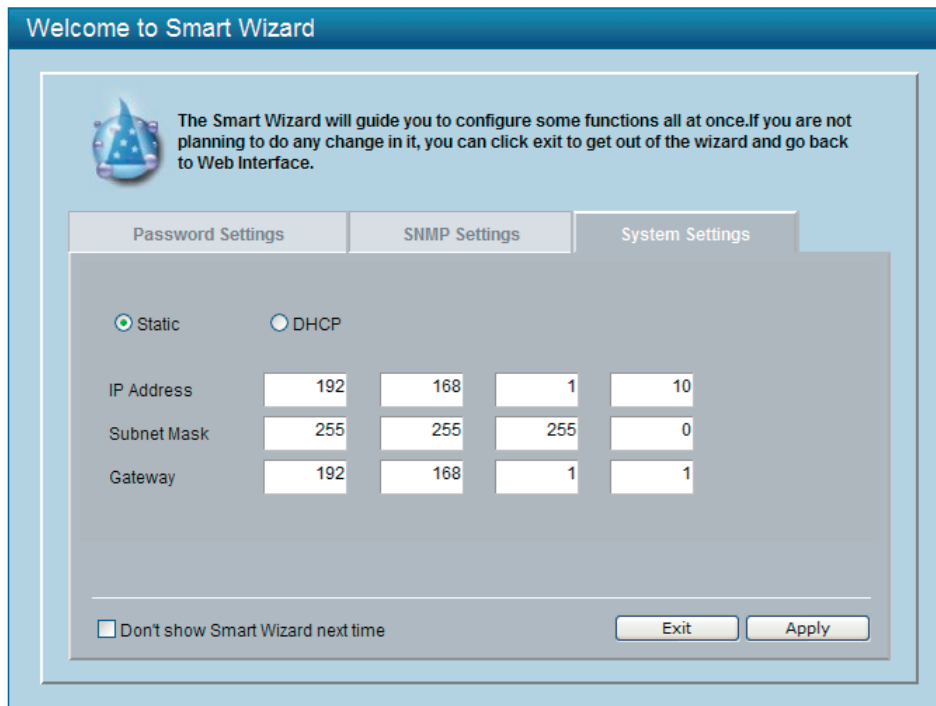


図 5-7 システム設定画面

IP アドレスを取得するモードを「Static」(固定設定)または「DHCP」(自動取得)から選択します。「Static」を選択した場合は、続く「IP Address」(IP アドレス)、「SubnetMask」(サブネットマスク)、および「Gateway」(ゲートウェイアドレス)を手動で変更します。「Apply」ボタンをクリックして設定を適用します。

IP 設定を変更した場合、続いて以下の確認画面が表示されます。



図 5-8 IP アドレス変更の確認画面

「OK」ボタンをクリックすると新しい Web マネージャが開始します。

参照 Web マネージャメイン画面から **System > System Settings** の順にメニューをクリックして、さらに詳細な設定を行うことができます。詳しくは「[System \(システム設定\)](#)」(44 ページ)を参照してください。

注意 スイッチの IP アドレスを変更すると、インターネット接続が切断します。Web ブラウザに正しい IP アドレスを入力して、必ずで使用するコンピュータをスイッチと同じサブネットに設定してください。詳細については、「[Web マネージャへのログイン](#)」(32 ページ)を参照してください。

5. Web ベースマネジメントユーティリティの確認を行います。Smart Wizard の「Exit」ボタンをクリックすると以下の画面が表示されます。

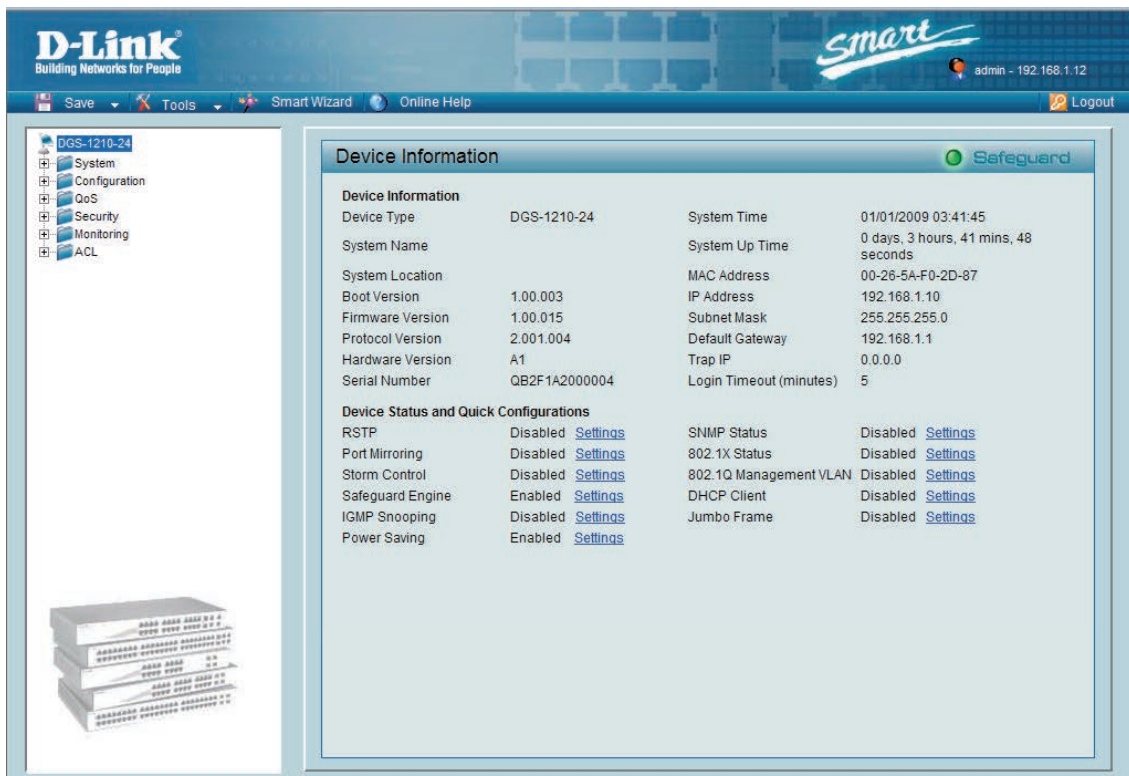


図 5-9 Web ベース管理ユーティリティの確認画面

Web マネージャの画面構成

Web マネージャでスイッチの設定または管理画面にアクセスしたり、パフォーマンス状況やシステム状況を参照できます。ログインに成功すると、デバイスの状態表示を行う画面が開きます。画面右上の角にユーザ名（初期値では「admin」）とスイッチの IP アドレスが表示されます。その下にはセッション終了時に使用する「Logout」ボタンがあります。

Web マネージャのメイン画面について

Web マネージャのメイン画面は 3 つのエリアで構成されています。

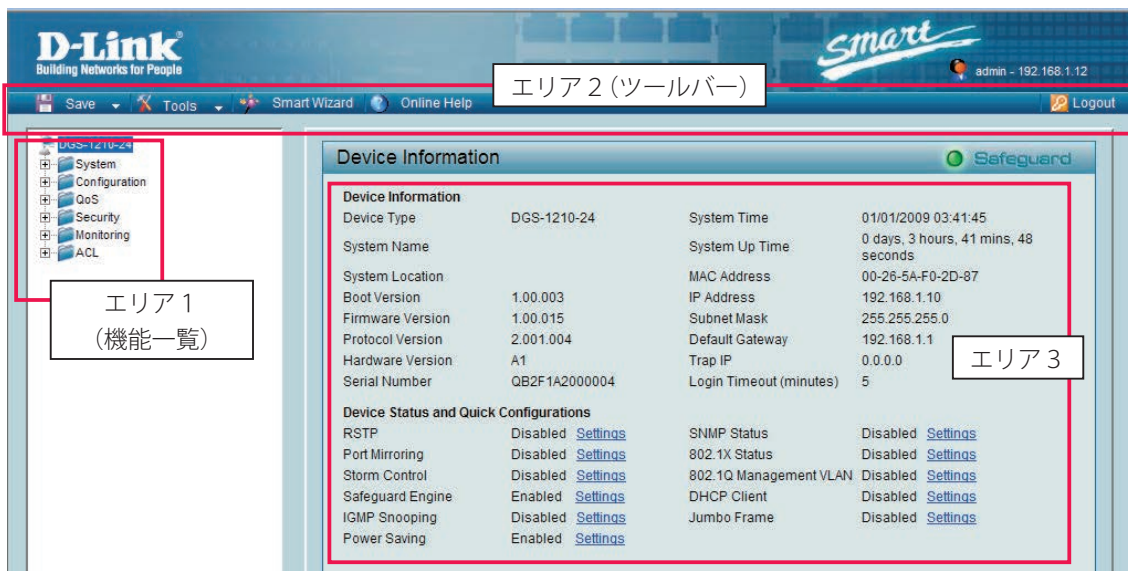


図 5-10 初期画面

注意 ハードウェアリミテーションによりユーザートラフィック、もしくは装置の高負荷時には WebGUI の表示が遅延または表示できない場合、Ping に応答できない場合があります。

エリア	機能
エリア 1 (機能一覧)	表示するメニューまたは画面を選択します。メニューアイコンを開いて、ハイパーリンクしたメニューボタンの表示やサブメニューを表示します。D-Link のロゴをクリックすると D-Link のホームページに接続します。
エリア 2 (ツールバー)	スイッチの再起動、設定 / ファームウェアのバックアップ、設定の初期化を行う「Tools」メニュー、スイッチの基本的な設定を行う「Smart Wizard」メニューがあります。
エリア 3	選択したスイッチ情報の表示と設定データの入力を行えます。

Web マネージャのメニュー構成

Web マネージャで設定可能な機能は以下の通りです。スイッチのすべての設定オプションは画面左側の機能フォルダの各項目をクリックして、設定画面にアクセスします。ここでは各オプションに関する機能や設定の詳細を説明します。

メインメニュー	サブメニュー	説明
ツールバー		
Save	Save Configuration	スイッチにコンフィグレーションの設定を保存します。
	Save Log	ログエントリをローカルドライブに保存します。「Backup Log」をクリックし保存先のパスを設定します。ログはテキストファイル形式で保存され、閲覧、編集が可能です。
Tools	Reset	スイッチのリセットを行います。IP アドレス以外の設定が初期値にリセットされます。
	Reset System	スイッチの完全リセットを行います。全ての設定値が初期値にリセットされ、再起動します。
	Reboot Device	システムを再起動します。
	Configuration Backup & Restore	コンフィグレーションをファイルに保存し、またはスイッチへ復元します。復元方法は「HTTP」「TFTP」から選択します。
	Firmware Backup & Upload	ファームウェアのバックアップとアップロードを行います。「HTTP」「TFTP」から選択します。
Smart Wizard		「Smart Wizard」画面へ移動します。「Smart Wizard」で設定をする場合に使用します。
Online Help		<p>「Online Help」により 2 種類のオンラインヘルプを使用することができます。</p> <ul style="list-style-type: none"> • Online Support - アップデートファイルのダウンロードなど、リソースの取得について D-Link の Web サイトを案内します。 • User Guide - 機能の特性や設定方法について参照します。
機能一覧		
System	System Settings	スイッチの IP 情報およびシステム情報の設定を行います。
	Trap Settings	Web スマートスイッチのイベントモニタのためにトラップの設定を行います。
	Port Settings	ポートの設定と状態モニタを行います。
	SNMP Settings	SNMP の設定を行います。
	Password Access Control	パスワードの設定を行います。
	System Log Settings	システムログの範囲、記録方法、有効 / 無効について設定します。
Configuration	Jumbo Frame	ジャンボフレームを有効にします。
	802.1Q VLAN	802.1Q VLAN の設定、および Asymmetric VLAN の設定を行います。
	802.1Q Management VLAN	スイッチの設定した VLAN に変更します。
	Voice VLAN	音声 VLAN 機能を設定します。
	Link Aggregation	Link Aggregation 機能を設定します。
	IGMP Snooping	IGMP Snooping 機能を設定します。
	Port Mirroring	ポートミラーリングの設定を行います。
	Power Saving	省電力モードを有効にします。
	Loopback Detection	ループ検知機能を設定します。
	SNTP Settings	時刻、タイムゾーンの設定をします。
	Spanning Tree	802.1D スパニングツリーの設定を行います。
QoS	Storm Control	Storm Control (パケット制御) の設定を行います。
	Bandwidth Control	帯域幅の設定を行います。
	802.1p/DSCP Priority Settings	QoS プライオリティレベルの設定を行います。
Security	Trusted Host	トラストホストを設定します。
	Safeguard Engine	セーフガードエンジン機能を設定します。
	Port Security	ポートセキュリティの設定を行います。
	802.1X	802.1X 認証の設定をします。
	MAC Address Table	スタティック / ダイナミック MAC アドレステーブルの設定をします。
Monitoring	Statistics	ポートのパケットカウント統計情報を表示します。
	Cable Diagnostics	スイッチに接続しているケーブルの診断をします。
	System Log	システムログを表示します。
ACL	ACL Configuration Wizard	ACL 設定ウィザード (ACL Configuration Wizard) で ACL の設定を行います。
	ACL Profile List	ACL プロファイルリストを表示、編集します。
	ACL Finder	ACL エントリを検索します。
PoE	PoE Port Settings	PoE の有効 / 無効などポートにおける PoE 機能の設定を行います。
	PoE System Settings	PoE ステータスを表示します。
Time-Based PoE	Time Range Settings	タイムベース PoE を設定します。
LLDP	LLDP Global Settings	LLDP のグローバル設定を行います。
	LLDP Remote Port Information	LLDP リモートポート情報を表示します。
	LLDP MED Settings	指定ポートに対して PSE TLV タイプを有効にします。

Web マネージャの初期画面

Web マネージャが表示された場合、または画面左側部「機能一覧」の機種名が選択されている場合、メイン画面には「Device Information」(デバイス情報)が表示されます。本画面から現在のデバイスの状態を確認し、設定の変更を行います。

Device Information (デバイス情報)

ファームウェア情報、ハードウェア情報や IP アドレスなどスイッチについて重要な情報が表示されます。

Device Information			
Device Information			
Device Type	DGS-1210-24	System Time	01/01/2009 01:31:57
System Name		System Up Time	0 days, 1 hours, 32 mins, 1 seconds
System Location		MAC Address	00-26-5A-F0-2D-87
Boot Version	1.00.003	IP Address	192.168.1.10
Firmware Version	1.00.015	Subnet Mask	255.255.255.0
Protocol Version	2.001.004	Default Gateway	192.168.1.1
Hardware Version	A1	Trap IP	0.0.0.0
Serial Number	QB2F1A2000004	Login Timeout (minutes)	5
Device Status and Quick Configurations			
RSTP	Disabled Settings	SNMP Status	Disabled Settings
Port Mirroring	Disabled Settings	802.1X Status	Disabled Settings
Storm Control	Disabled Settings	802.1Q Management VLAN	Disabled Settings
Safeguard Engine	Enabled Settings	DHCP Client	Disabled Settings
IGMP Snooping	Disabled Settings	Jumbo Frame	Disabled Settings
Power Saving	Enabled Settings		

図 5-11 Device Information 画面

「Device Status and Quick Configurations」の項目は、現在のステータスを確認してから直接設定を変更することができます。以下の項目について本画面から設定が可能です。

機能	設定方法
Device Information	
Device Type	工場にて定義した機種名と型式を表示します。
System Name	ユーザが定義したシステム名を表示します。
System Location	システムが現在動作している場所を表示します。
Boot Version	デバイスのブートバージョンを表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
Protocol Version	デバイスのプロトコルバージョンを表示します。
Hardware Version	デバイスのハードウェアバージョンを表示します。
Serial Number	デバイスのシリアル番号を表示します。
System Time	システムの日付を表示します。日/月/年/時刻で表示します。
System Up Time	最後のデバイスリセットからの経過時間を表示します。日、時、分、秒の形式で表示します。 例: 41days, 2 hours, 22 mins, 5 seconds
MAC Address	デバイスに割り当てられた MAC アドレスを表示します。
IP Address	デバイスに割り当てられた IP アドレスを表示します。
Subnet Mask	デバイスに割り当てられたサブネットマスクを表示します。
Default Gateway	デバイスに割り当てられたデフォルトゲートウェイを表示します。
Trap IP	トラップを受信するホストの IP アドレスを表示します。
Login Timeout (minutes)	ユーザが何もしなかった場合にデバイスがタイムアウトするまでの時間を表示します。

機能	設定方法
Device Status and Quick Configurations	
RSTP	「Settings」をクリックすると Configuration > Spanning Tree > STP Global Settings にリンクします。 初期値は「Disabled/ 無効」です。
Port Mirroring	「Settings」をクリックすると Configuration > Port Mirroring にリンクします。初期値は「Disabled/ 無効」です。
Storm Control	「Settings」をクリックすると Configuration > QoS > Storm Control にリンクします。初期値は「Disabled/ 無効」です。
Safeguard Engine	「Settings」をクリックすると Security > Safeguard Engine にリンクします。 初期値は「Enabled/ 有効」です。
IGMP Snooping	「Settings」をクリックすると Configuration > IGMP Snooping にリンクします。初期値は「Disabled/ 無効」です。
Power Saving	「Settings」をクリックすると Configuration > Power Saving にリンクします。初期値は「Enabled/ 有効」です。
SNMP Status	「Settings」をクリックすると System > SNMP Setting にリンクします。初期値は「Disabled/ 無効」です。
802.1X Status	「Settings」をクリックすると Security > 802.1X > 802.1X Settings にリンクします。 初期値は「Disabled/ 無効」です。
802.1Q Management VLAN	「Settings」をクリックすると Configuration > 802.1Q Management VLAN にリンクします。 初期値は「Disabled/ 無効」です。
DHCP Client	「Settings」をクリックすると System > System Settings にリンクします。初期値は「Disabled/ 無効」です。
Jumbo Frame	「Settings」をクリックすると System > Jumbo Frame にリンクします。初期値は「Disabled/ 無効」です。

Save メニュー

コンフィグレーション、ログなどを保存します。

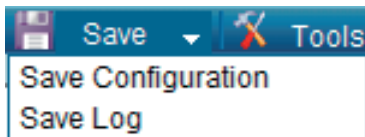


図 5-12 Save メニュー

Save Configuration (コンフィグレーション保存)

設定したコンフィグレーションをファイルにて保存します。

Save > Save Configuration の順にメニューをクリックし、以下の画面を表示します。

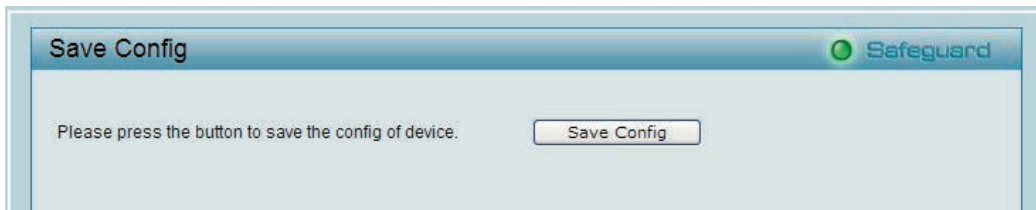


図 5-13 Save Configuration 画面

「Save Config」ボタンをクリックします。

警告 「Save Config」ボタンをクリックしたあと、30 秒間以上経過するまで電源を切らないでください。
30 秒以上経過する前に電源を切ると、設定が正しく保存されないか、設定が工場出荷時状態に戻ります。

Save Log (ログ保存)

ログをファイルに保存します。

Save > Save Log の順にメニューをクリックし、以下の画面を表示します。

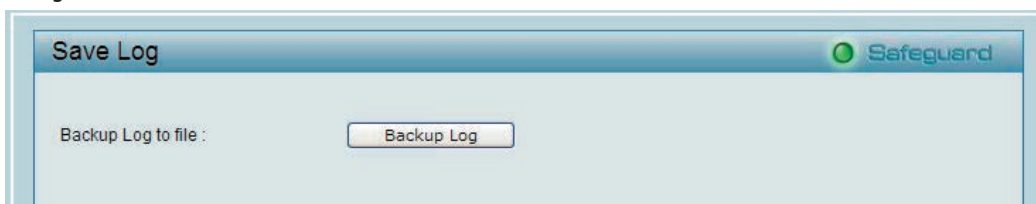


図 5-14 Save Log 画面

「Backup Log」ボタンをクリックします。

Tools メニュー

リセット、システムリセット、コンフィグレーションのバックアップとリストア、ファームウェアのバックアップとアップグレード、システムの再起動などのシステムに関する機能を提供します。

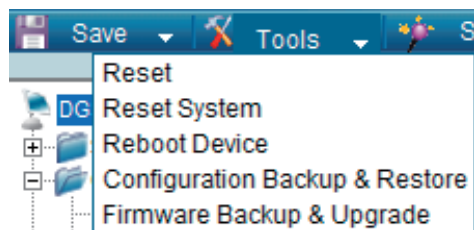


図 5-15 Tools メニュー

Reset (リセット)

スイッチのリセットを行います。IP アドレスを除くすべてのコンフィグレーションは工場出荷時設定にリセットされます。

Tools > Reset の順にメニューをクリックし、以下の画面を表示します。

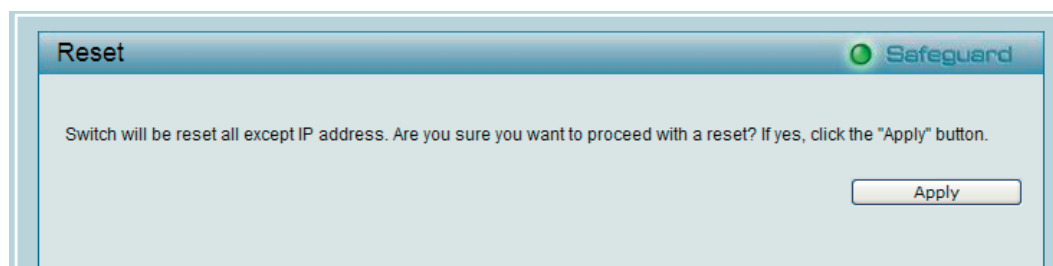


図 5-16 Reset 画面

「Apply」ボタンをクリックします。

Reset System (システムリセット)

スイッチのリセット / 再起動を行います。すべてのコンフィグレーションは工場出荷時設定にリセットされ、その後システムが再起動します。

Tools > Reset System の順にメニューをクリックし、以下の画面を表示します。

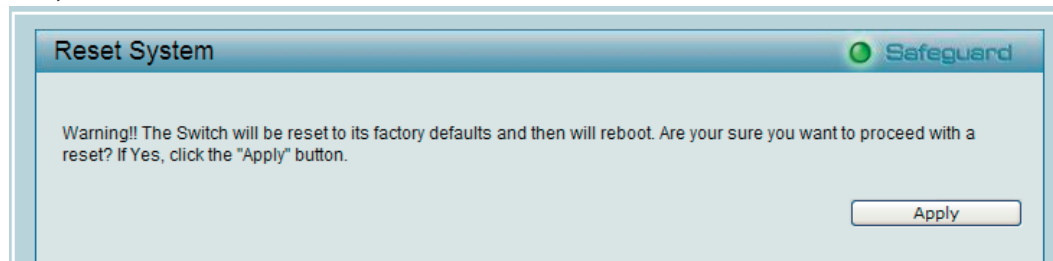


図 5-17 Reset System 画面

「Apply」ボタンをクリックします。

Reboot Device (デバイスの再起動)

スイッチの再起動を行います。保存していない設定は失われます。

Tools > Reboot Device の順にメニューをクリックし、以下の画面を表示します。

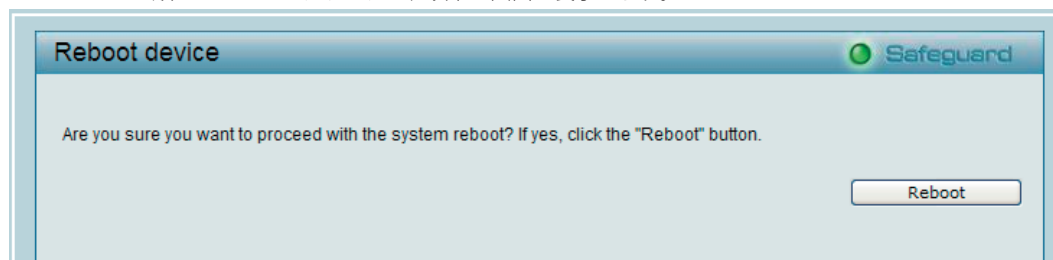


図 5-18 Reboot device 画面

「Reboot」ボタンをクリックします。

Configuration Backup & Restore (コンフィグレーションの保存と復元)

現在のコンフィグレーション (パスワードは除く) をファイルに保存します。必要時にこの保存ファイルを使用した復元も可能です。方法は「HTTP」または「TFTP」から選択可能です。

Tools > Configuration Backup & Restore の順にメニューをクリックし、以下の画面を表示します。

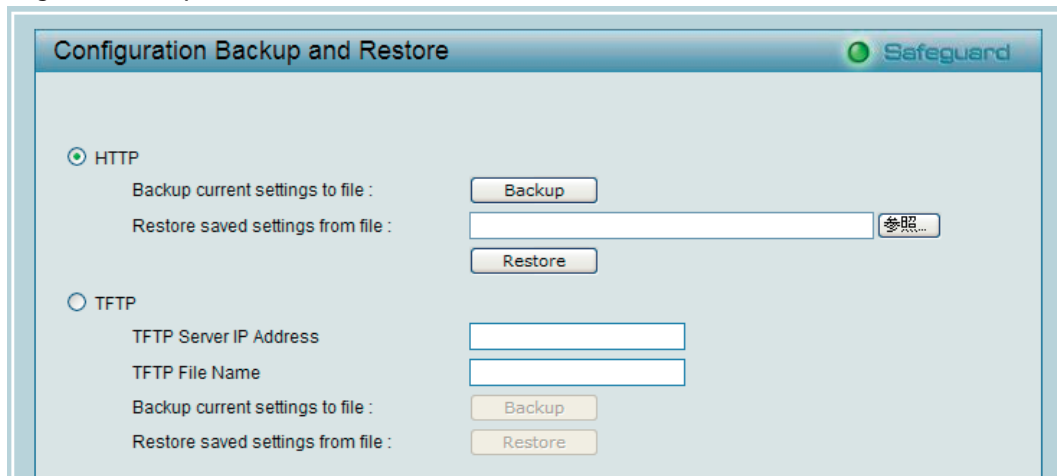


図 5-19 Configuration Backup and Restore 画面

プロトコル	説明
HTTP	<p>HTTP を使用してコンフィグレーションファイルの保存と復元を行います。</p> <p>保存方法</p> <ul style="list-style-type: none"> 「Backup」ボタンをクリックし、現在のコンフィグレーションをローカルデスクに保存します。 <p>復元方法</p> <ul style="list-style-type: none"> 「Restore saved settings from file:」でコンフィグレーションファイルのパスを入力するか、「参照」ボタンをクリックし、保存したコンフィグレーションファイルを参照します。 保存済みのコンフィグレーションファイルを指定後に「Restore」をクリックし、設定の復元を開始します。
TFTP	<p>TFTP を使用してコンフィグレーションファイルの保存と復元を行います。</p> <p>対応する TFTP サーバのパスを「TFTP Server IP Address」に入力し、「TFTP File Name」にファイル名を入力します。</p> <p>保存方法</p> <ul style="list-style-type: none"> 「Backup」ボタンをクリックし、現在のコンフィグレーションを指定した TFTP サーバに保存します。 <p>復元方法</p> <ul style="list-style-type: none"> 「Restore」ボタンをクリックし、TFTP サーバから設定の復元を開始します。

注意 コンフィグレーションを復元するためにはスイッチの再起動が必要です。また、コンフィグレーションを復元すると、現在のすべての設定が失われます。

Firmware Backup & Upgrade (ファームウェアの保存と更新)

ファームウェアをバックアップとして保存します。また保存されたファームウェアファイルを使用しスイッチを更新します。方法は「HTTP」または「TFTP」から選択可能です。

Tools > Firmware Backup & Upgrade の順にメニューをクリックし、以下の画面を表示します。

図 5-20 Firmware Backup and Upgrade 画面

プロトコル	説明
HTTP	<p>HTTP を使用してファームウェアの保存と更新を行います。</p> <p>保存方法</p> <ul style="list-style-type: none"> 「Backup」をクリックし、現在のファームウェアをローカルデスクに保存します。 <p>更新方法</p> <ul style="list-style-type: none"> 「Upgrade firmware from file :」でファームウェアファイルのパスを入力するか、「参照」ボタンをクリックし、ファームウェアファイルを参照します。 ファイルを指定後に「Upgrade」ボタンをクリックし、更新を開始します。
TFTP	<p>「TFTP」を使用してファームウェアの保存と更新を行います。</p> <p>対応する TFTP サーバのパスを「TFTP Server IP Address」に入力し、「TFTP File Name」にファイル名を入力します。</p> <p>保存方法</p> <ul style="list-style-type: none"> 「Backup」をクリックし、現在のファームウェアを指定した TFTP サーバに保存します。 <p>更新方法</p> <ul style="list-style-type: none"> 「Upgrade」をクリックし、TFTP サーバからスイッチの更新を開始します。

注意 ファイルの更新が完全に終了する前に PC との接続を切断したり、電源コードを外したりしないでください。ファームウェアの更新が終了しないと、スイッチが破損する可能性があります。

Smart Wizard メニュー (スマートウィザード)

「Smart Wizard」をクリックして、「Smart Wizard」画面へ移動します。「Smart Wizard」で設定をします。詳しくは「[Smart Wizard 設定](#)」(34 ページ)を参照してください。

Online Help メニュー (オンラインヘルプ)

オンラインヘルプには2通りのサポート方法があります。本項目ではファームウェアファイルなどのオンライン上のリソースを提供する D-Link のオンラインサポートサイトか、設定方法についてのユーザガイドを参照します。

Online Support Site (オンラインサポートサイトへの参照)



図 5-21 Online Support Site 選択画面

「Apply」ボタンをクリックすると、D-Link のオンラインサポートサイトを表示します。ここで製品名を指定し、必要なリソースを検索します。

User Guide (ユーザガイドへの参照)

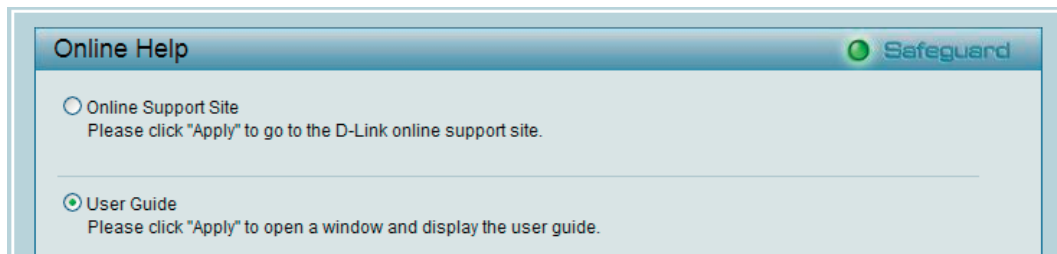


図 5-22 User Guide 選択画面

「Apply」ボタンをクリックします。以下の画面を表示します。



図 5-23 User Guide 画面

System (システム設定)

以下は、System のサブメニューの説明です。

サブメニュー	説明	参照ページ
System Settings	スイッチの IP 情報およびシステム情報の設定を行います。	44 ページ
Trap Settings	Web スマートスイッチのイベントモニタのためにトラップの設定を行います。	45 ページ
Port Settings	ポートの設定と状態モニタを行います。	46 ページ
SNMP Settings	SNMP の設定を行います。	47 ページ
Password Access Control	パスワードの設定を行います。	48 ページ
System Log Settings	システムログの範囲、記録方法、有効 / 無効について設定します。	49 ページ

System Settings (スイッチの基本機能の設定)

スイッチの IP 情報およびシステム情報の設定を行います。

System > System Settings の順にメニューをクリックし、以下の画面を表示します。

図 5-24 System Settings 画面

画面には以下の項目があります。

項目	説明
IP Information	
スイッチが IP アドレスを取得するためにはスタティックと DHCP (Dynamic Host Configuration Protocol) の 2 つの方法があります。	
Static/DHCP	IP アドレスを取得するモードを選択します。 <ul style="list-style-type: none"> Static - 本スイッチの IP アドレス、サブネットマスクおよびデフォルトゲートウェイを固定設定します。本モードを選択した場合には、「IP Address」、「Subnet Mask」および「Gateway」を入力します。(初期値) DHCP - DHCP サーバは、DHCP プロトコルを使用して IP アドレス、サブネットマスクおよびデフォルトゲートウェイが自動的に割り当てられます。スイッチは初期設定や登録済みの設定を使用する前に、まず DHCP サーバに IP アドレス、ネットマスク、デフォルトゲートウェイの割り当てを要求します。
IP Address	固定設定する IP アドレス。
Subnet Mask	上記 IP アドレスのサブネットマスク。
Gateway	上記 IP アドレスのゲートウェイ。

項目	説明
System Information	
「System Name」と「System Location」を登録すると、SmartConsole Utility の使用時に LAN 上の他の Web スマートデバイスから特定のデバイスを認識しやすくなります。	
System Name	ネットワーク上で、この名前でスイッチを識別します。
System Location	ネットワーク上のスイッチの場所を入力します。
Login Timeout (3-30 minutes)	セキュリティ対策の一環として、Web ベースユーティリティ上でアクションが行われないアイドル時間制限の設定するものです。指定した時間が経過すると、再びユーティリティを使用する際には再ログインが要求されます。
Group Interval (120-1225 seconds)	正しいデータの保持のために、スイッチからの IGMP v1 のレポートパケットを SmartConsole Utility に定期的送信します。本項目は、SmartConsole Utility が IGMP プロトコルを使用するスイッチを検出する間隔です。 <ul style="list-style-type: none"> 0 - Group Interval は無効となります。 120-1225 - 指定間隔で IGMP v1 レポートパケットを送信します。

「Apply」 ボタンをクリックし、設定を有効にします。

Trap Settings (トラップ設定)

トラップの設定を行い、SmartConsole Utility から Web スマートスイッチのイベントのモニタを行います。

System > Trap Settings for SmartConsole の順にメニューをクリックし、以下の画面を表示します。

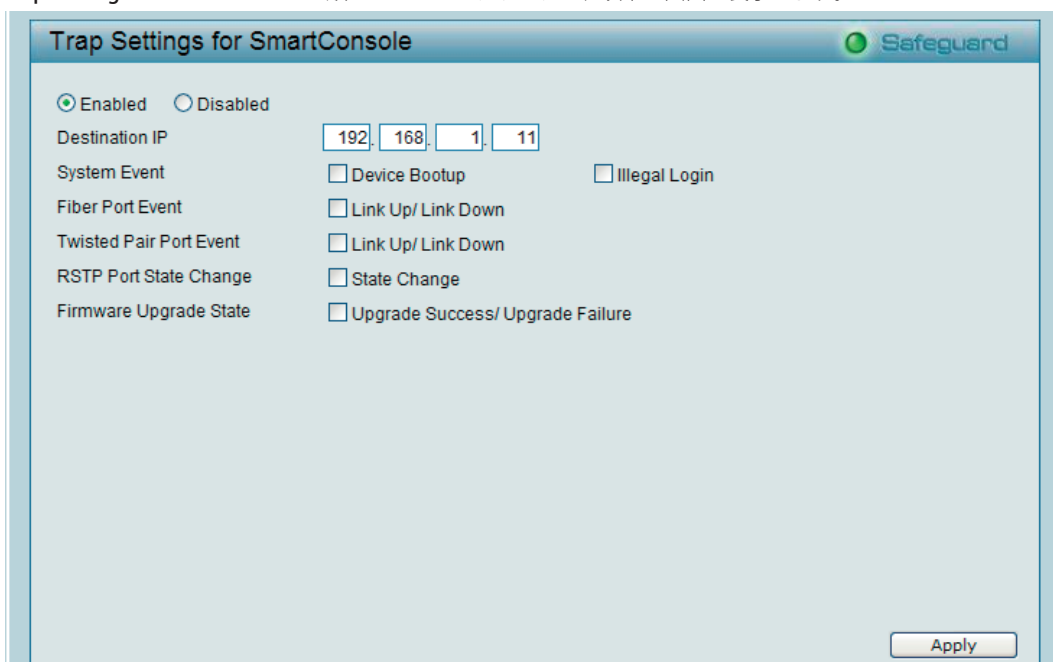


図 5-25 Trap Settings for SmartConsole 画面 (DGS-1210-16/GE、DGS-1210-24/GE、DGS-1210-48/GE)

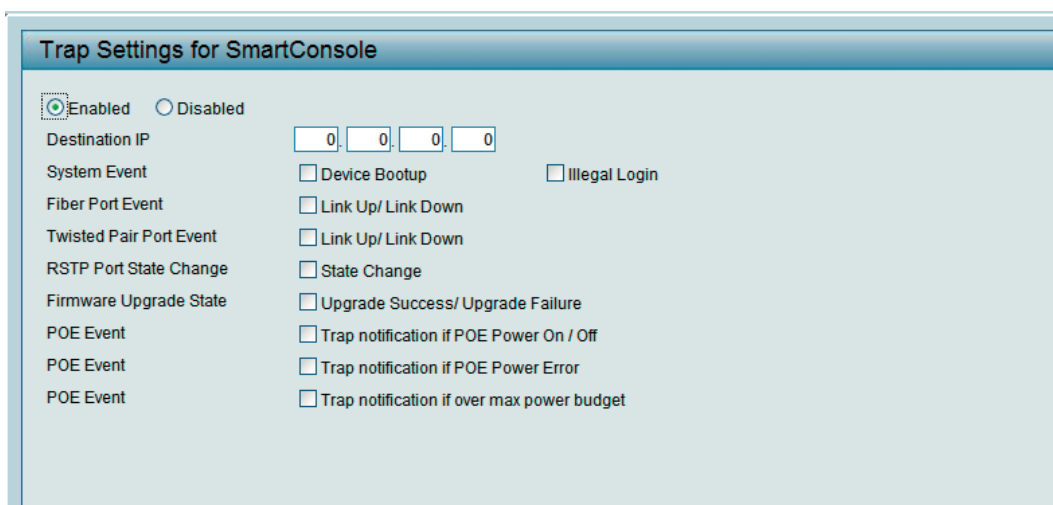


図 5-26 Trap Settings for SmartConsole 画面 (DGS-1210-10P/GE)

トラップ設定の初期値は「Disabled」(無効)です。トラップ設定を「Enabled」(有効)とし、「Destination IP」にトラップ情報を受信する管理 PC の IP アドレスを指定します。

イベント設定項目は以下の通りです。

項目	説明
System Event	システムのトラップ情報をモニタします。 <ul style="list-style-type: none"> • Device Bootup - システムの起動時に再起動情報（トラップ）を通知します。 • Illegal Login - 不正なパスワードによるログインイベントと操作が行われたコンピュータの IP アドレスを通知され、記録されます。
Fiber Port Events	光ファイバポートの状態をモニタします。 <ul style="list-style-type: none"> • Link Up/Link Down - 光ファイバ接続情報を通知します。
Twisted pair Port Events	RJ-45 ポートの状態をモニタします。 <ul style="list-style-type: none"> • Link Up/Link Down - RJ-45 接続情報を通知します。
RSTP Port State Change	<ul style="list-style-type: none"> • State Change - RSTP ポートの状態、変更をモニタします。
Firmware Upgrade State	アップグレードの状態についてモニタします。 <ul style="list-style-type: none"> • Upgrade Success (成功) / Upgrade Failure (失敗)
POE EVENT	<ul style="list-style-type: none"> • Trap notification if POE Power On / Off - PoE ポートの電力供給に関する情報。 • Trap notification if POE Power Error - PoE 電力供給エラーに関する情報。 • Trap notification if over max power budget - 供給可能電力超過に関する情報。

設定を変更する際は「Apply」ボタンをクリックし、設定内容を適用してください。

Port Settings (ポート設定)

すべてのポートの状態モニタと最適なコンフィグレーションのための調整を行います。

System > Port Settings の順にメニューをクリックし、以下の画面を表示します。

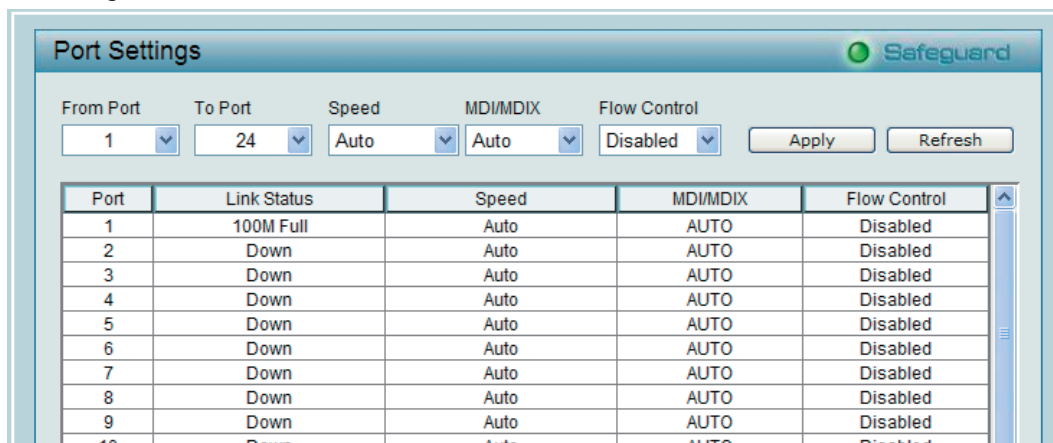


図 5-27 Port Settings 画面

「From Port」 / 「To Port」 でポートの範囲を指定し、「Speed」、「MDI/MDIX」および「Flow Control」欄を指定して「Apply」ボタンをクリックします。最新のリンク状態と優先度を確認するには「Refresh」ボタンをクリックします。

以下の項目を使用して設定を行います。

項目	説明
From Port/To Port	設定を行うポートまたはポート範囲を指定します。
Speed	ギガ光ファイバ接続は「Auto」または「Disable」を指定します。RJ-45 ポートは固定設定（「1000M Full」、「100M Full」、「100M Half」、「10M Full」、「10M Half」）、「Auto」または「Disable」を指定します。100M 光ファイバ接続では「100 M Full」、「Auto」または「Disable」を指定します。初期値は「Auto」です。 注意 接続ケーブルのメディアタイプを変更した場合、適切なポート速度の設定を行ってください。
MDI/MDIX	MDI/MDIX 機能を設定します。「Auto」「MDI」「MDIX」から選択します。通常の接続の場合は「MDIX」を選択します。スイッチがクロスケーブルを使用せずに他のスイッチやハブに接続する場合、「MDI」ポートとして設定します。「Auto MDI/MDIX」はポートや接続の状態に合わせて、自動的に「MDI」「MDIX」を選択します。初期値は「Auto」です。
Flow Control	トラフィックの混雑を軽減する機能を設定します。初期値は「Disabled」（無効）
Link Status	接続の速度や duplex モードを表示します。ポートが未接続の場合、「Down」と表示されます。

補足

1G モジュール使用時、SFP ポートのプライオリティは RJ-45 ポートよりも高くなります。100M モジュールの場合は、RJ-45 ポートが SFP ポートより優先されます。

SNMP Settings (SNMP 設定)

SNMP (Simple Network Management Protocol) は、OSI 参照モデルの第7層 (アプリケーション層) のプロトコルで、ネットワークデバイスの管理や監視を行います。ネットワーク管理デバイスは、SNMP を利用してゲートウェイ、ルータ、およびその他ネットワークデバイスの設定状態の確認や変更をします。また、SNMP を利用してスイッチやスイッチ群、またはネットワークに対し、正常な動作を行うためのシステム設定、パフォーマンスの監視、潜在する問題の検出を行います。

SNMP をサポートする管理デバイスは、スイッチ上で動作する SNMP エージェントと呼ばれるソフトウェアを実装しています。SNMP エージェントが管理する定義された変数 (管理オブジェクト) により、デバイスの管理を行います。これらのオブジェクトは MIB (Management Information Base) 内に定義され、デバイス上の SNMP エージェントにより管理される情報表示の基準を (管理側のデバイスに) 伝えます。SNMP では、MIB の仕様とネットワークを経由してこれらの情報にアクセスするために使用するプロトコルのフォーマットを定義しています。

本スイッチは、SNMP バージョン 1 (SNMP v1) に対応し、ユーザ認証はパスワードの役割を持つコミュニティ設定を使用しています。リモートユーザの SNMP アプリケーションとスイッチの SNMP は同じコミュニティ名を持つ必要があります。認証が行われていない SNMP パケットを受信した場合、そのパケットは無視 (廃棄) されます。

トラップは、スイッチ上で発生したイベントを、ネットワーク管理者に警告するためのメッセージです。イベントには、再起動 (誰かが誤ってスイッチの電源を切ってしまった) などの重大なものから、ポートの状態変化を知らせる軽微なものまで幅広い種類があります。スイッチはトラップを生成してトラップ受信者 (ネットワーク管理者など) に送信します。

System > SNMP Settings の順にメニューをクリックし、以下の画面を表示します。

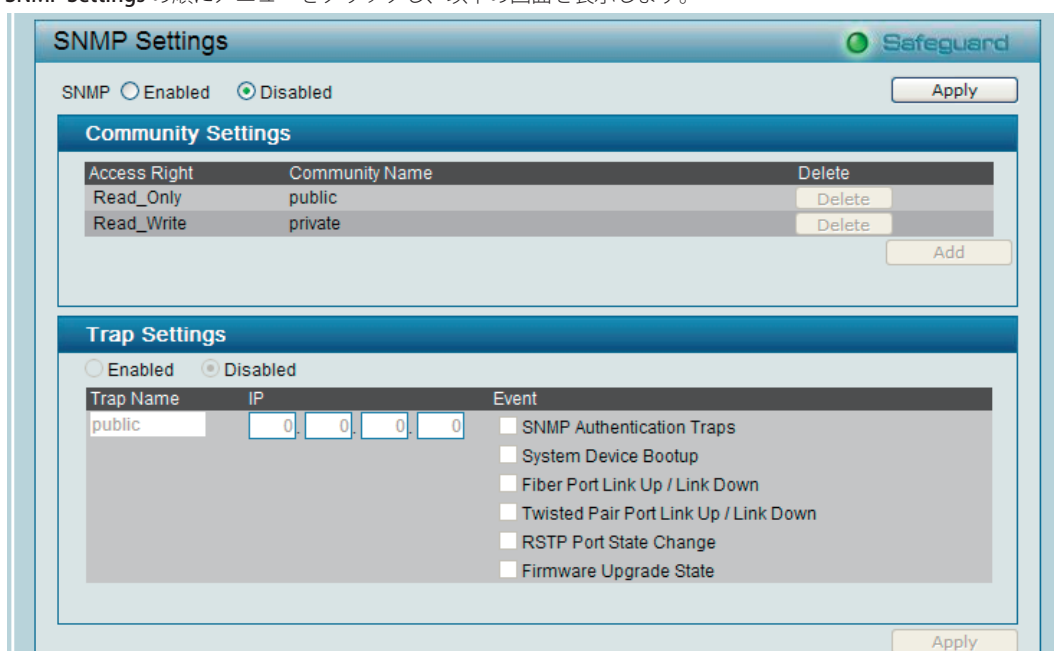


図 5-28 SNMP Settings 画面 (DGS-1210-16/GE、DGS-1210-24/GE、DGS-1210-48/GE)

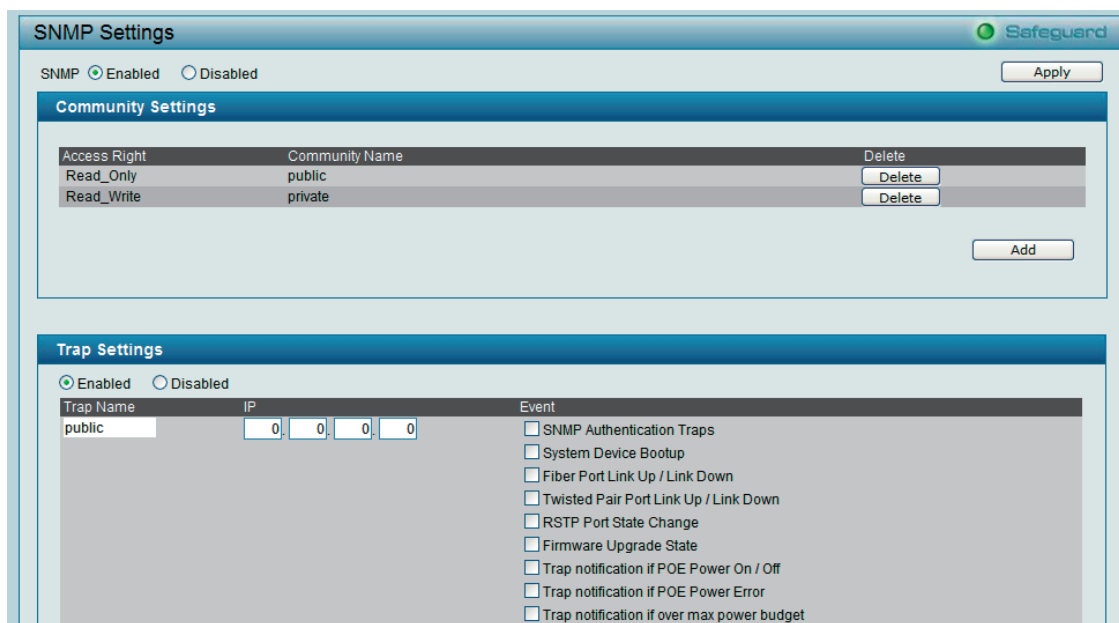


図 5-29 SNMP Settings 画面 (DGS-1210-10P/GE)

コミュニティ名を登録するためには、はじめに SNMP の「Enabled」(有効) を選択し、「Apply」ボタンをクリックします。

Webマネージャによる詳細設定

以下の項目を使用して設定を行います。

項目	説明
Community Settings	
SNMP v1 の管理アクセスに使用するスイッチのコミュニティ名を指定します。	
Read_Only	権限のある管理ステーションによる MIB オブジェクトの読み出しが可能。初期値は「public」です。
Read_Write	権限のある管理ステーションによる MIB オブジェクトの読み出しと変更が可能。初期値は「private」です。
Trap Settings	
Enabled / Disabled	トラップを「Enabled」(有効)または「Disabled」(無効)にします。
Trap Name	トラップ名を指定します。いずれかのコミュニティ名である必要があります。
IP	管理対象のデバイスの IP アドレスを入力します。
Event	トラップするイベントを選択します。 <ul style="list-style-type: none">• SNMP Authentication Traps (SNMP 認証)• System Device Bootup (デバイスの起動)• Fiber Link Up / Link Down (ファイバリンクアップ / ダウン)• Twisted Pair Link Up / Link Down (ツイストペアリンクアップ / ダウン)• RSTP Port State Change (RSTP ポートの状態変更)• Firmware Upgrade State (ファームウェアアップグレード)• Trap notification if POE Power On / Off (POE 電源オン / オフ) *• Trap notification if POE Power Error (PoE 電源エラー) *• Trap notification if over max power budget (供給可能電力超過) *

* DGS-1210-10P/GE のみ

トラップの設定方法

1. 「Trap Settings」セクションの「Enabled」を選択し、「Trap Name」にトラップ名を入力します。
2. 管理対象のデバイスの IP アドレスを入力し、トラップ対象のイベントを選択します。
3. 「Apply」ボタンをクリックし、設定を有効にします。

注意 トラップ名はコミュニティ名から選択される必要があります。

Password Access Control (パスワードアクセス制御)

パスワードの設定は、Web スマートスイッチの安全な運用のために管理者にとって必要です。

System > Password Access Control の順にメニューをクリックし、以下の画面を表示します。

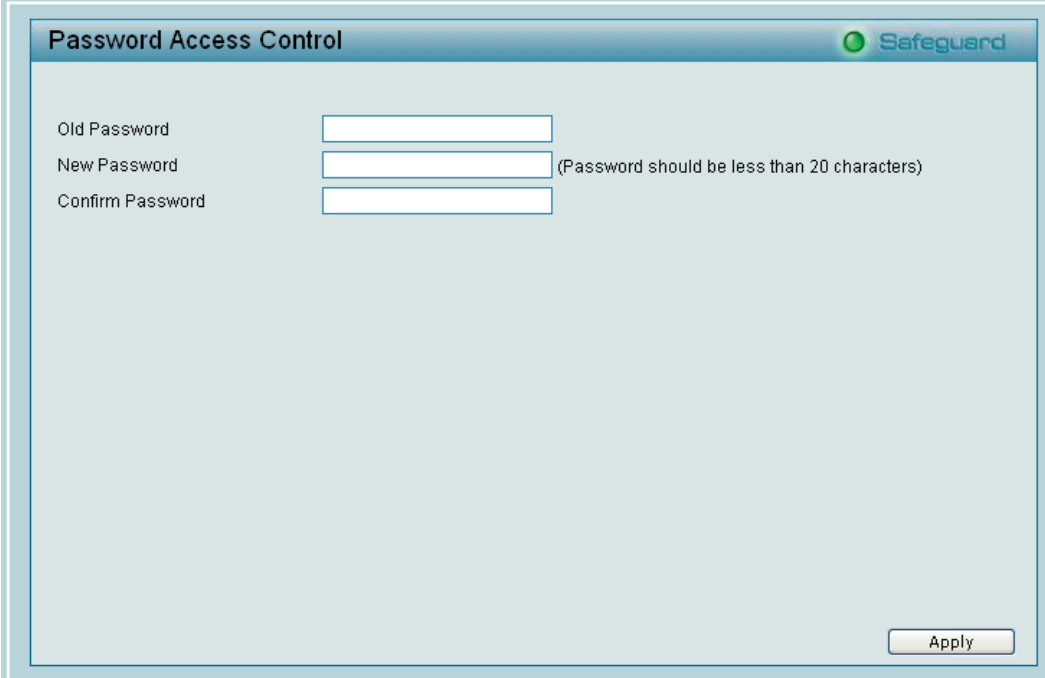


図 5-30 Password Access Control 画面

「Old Password」に現在のパスワード、「New Password」と「Confirm Password」に新しいパスワード(半角英数字 20 文字以内)を入力した後、「Apply」ボタンをクリックし、設定を有効にします。

System Log Settings (システムログ設定)

システムログは情報メッセージやエラー報告など、発生するイベントの管理、記録を行います。「Severity」でイベントの重大性を設定することにより、メッセージを送信する対象のイベントが決まります。「System Log」で「Enabled」をクリックすると、関連する項目の設定が可能になります。「Apply」をクリックして変更を適用します。

System > System Log Settings の順にメニューをクリックし、以下の画面を表示します。

図 5-31 System Log Configuration 画面

以下の項目を使用して設定を行います。

項目	説明
System Log	システムログの出力を「Enabled」(有効) または「Disabled」(無効) にします。
Server IP Address	システムログサーバの IP アドレスを入力します。
UDP Port (1-65535)	ログが送信される UDP ポートを指定します。設定可能範囲は「1-65535」です。初期値は「514」です。
Time Stamp	「Enable」を選択すると、ログメッセージに時刻情報を設定します。
Severity	サーバに警告メッセージを送る必要のあるイベントの重要性を設定します。重要レベルは 3 種類あります。一度重要性が選択されると選択した重要性以上のレベルは全て選択されたこととなります。 <ul style="list-style-type: none"> Warning - 高いレベルの警告になります。デバイスは機能していますが、操作上の問題が発生しています。 Informational - デバイス情報を提供します。 All - 全てのレベルのシステムログが表示されます。
Facility	リモートサーバへのシステムログに送信登録をします。Local 0 ~ Local 7 までの 8 つまで登録が可能です。1 つの登録で 1 つのサーバのみ対応いたします。

Configuration（管理フォルダ）

以下は、Configuration のサブメニューの説明です。

サブメニュー	説明	参照ページ
Jumbo Frame	ジャンボフレームを有効にします。	50 ページ
802.1Q VLAN	802.1Q VLAN の設定を行います。	51 ページ
Asymmetric VLAN	Asymmetric VLAN の設定を行います。	53 ページ
802.1Q Management VLAN	スイッチの設定した VLAN に変更します。	55 ページ
Voice VLAN	音声 VLAN 機能を設定します。	55 ページ
Link Aggregation	Link Aggregation 機能を設定します。	57 ページ
IGMP Snooping	IGMP Snooping 機能を設定します。	58 ページ
Port Mirroring	ポートミラーリングの設定を行います。	60 ページ
Power Saving	省電力モードを有効にします。	61 ページ
Loopback Detection	ループ検知機能を設定します。	61 ページ
SNTP Settings	時刻、タイムゾーンの設定をします。	62 ページ
Spanning Tree	802.1D スパニングツリーの設定を行います。	64 ページ

Jumbo Frame（ジャンボフレーム）

D-Link ギガビット Web スマートスイッチシリーズは、最大 10,000 バイトまでのジャンボフレーム（1536 バイトの標準イーサネットフレームより大きいサイズのフレーム）をサポートしています。

Configuration > Jumbo Frame の順にメニューをクリックして以下の画面を表示します。



図 5-32 Jumbo Frame Configuration 画面 - 初期設定

初期設定は「Disabled」（無効）です。「Enabled」を選択後、「Apply」ボタンをクリックしてジャンボフレームを有効にします。

802.1Q VLAN (802.1Q VLAN 設定)

VLAN とはポートをグループ化したもので、VLAN 内では実際のネットワーク内での場所にとらわれず、あたかも同じエリア内に位置しているかのような通信を可能とします。

VLAN は、例えば部署別（開発研究（R&D）またはマーケティングなど）や、使用用途別（E-mail など）、あるいはマルチキャストグループ別（ビデオ会議などのマルチメディアアプリケーション）などの単位で簡単に編成することができます。VLAN の再編成を行う際にも、ユーザは物理的な接続を変更しないで新しい VLAN に参加することが可能であり、ネットワーク管理の簡素化が実現できます。

「IEEE 802.1Q VLAN Configuration」画面は、VID を管理する目的で使用します。初期値では VID は「01」で、すべてのポートが Untag（タグなし）ポートです。

Configuration > 802.1Q VLAN の順にメニューをクリックして以下の画面を表示します。

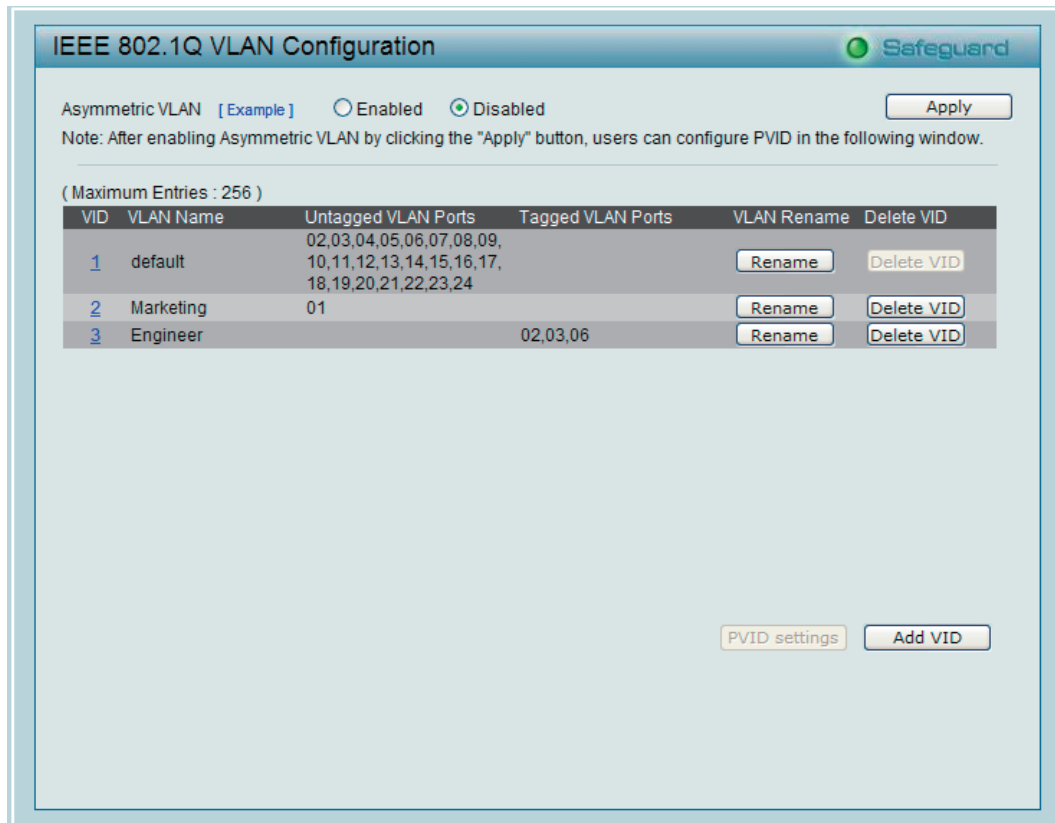


図 5-33 IEEE 802.1Q VLAN Configuration 画面 - 初期設定

以下の項目を使用して設定を行います。

項目	説明
Rename	VLAN グループ名を変更する場合にクリックします。
Delete VID	VLAN グループを削除する場合にクリックします。
Add VID	新しい VID グループを作成し、ポートに「Untag」（タグなし）、「Tag」（タグ付き）、「Not Member」（グループに所属しない）として 1-10 を割り当てます。1 つのポートは 1 つの VID でタグなしとなります。

「Add VID」ボタンをクリックし、以下の画面を表示します。VLAN 名は、Accounting、Marketing などのようにグループの特性に合わせて変更できます。

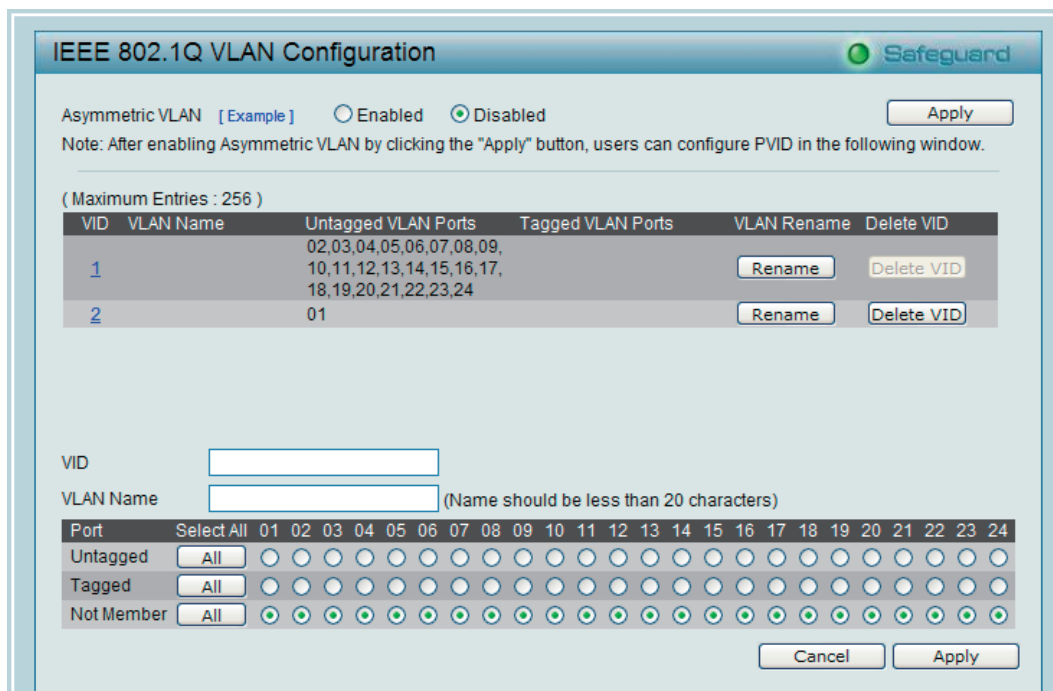


図 5-34 IEEE 802.1Q VLAN Configuration 画面 - Add VID

ポートは1つのVIDにだけ「Untag」(タグなし)となります。設定項目を入力後、「Apply」ボタンをクリックしてVIDグループを保存します。以下の通り、リストに追加されます。

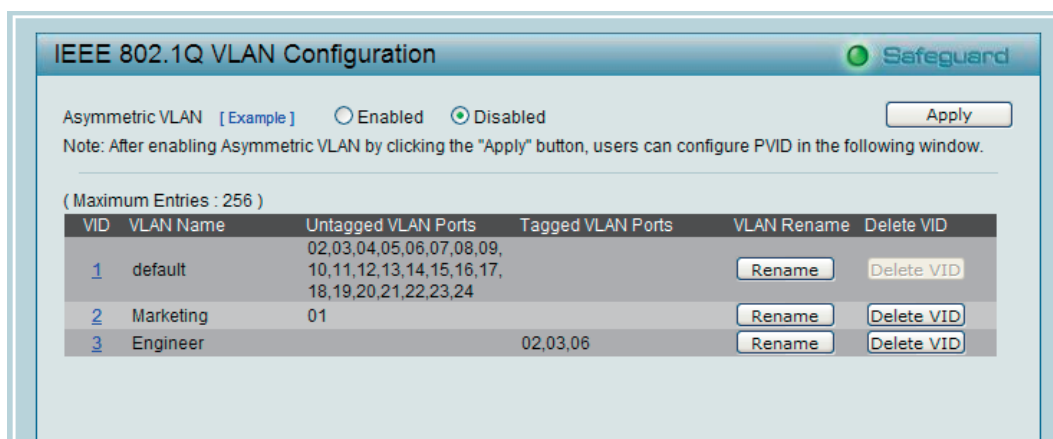


図 5-35 IEEE 802.1Q VLAN Configuration 画面 - VID 例

設定を編集する場合は、編集する「VID」のリンクをクリックし、以下の画面を表示します。

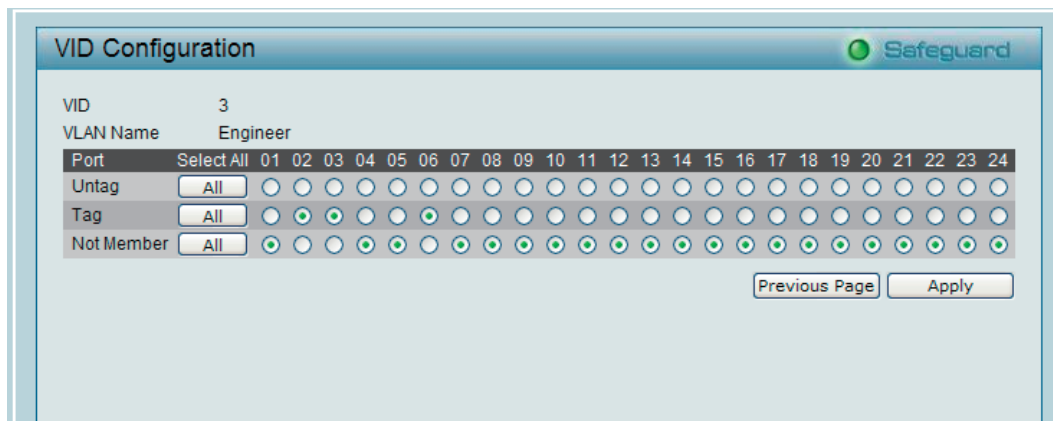


図 5-36 IEEE 802.1Q VLAN Configuration 画面 - VID 割り当て

「IEEE 802.1Q VLAN Configuration」画面に戻るには、「Previous Page」ボタンをクリックします。

Asymmetric VLAN (非対称 VLAN 設定)

Asymmetric VLAN 設定は、それぞれ違った VLAN 内の機器に共有 VLAN 内でサーバやファイアウォールなどのリソースを共有させる機能です。設定は以下の手順となります。

1. Asymmetric VLAN 機能の有効化
2. 共有 VLAN と VLAN アクセスの作成
3. VLAN アクセスの PVID の設定

「Asymmetric VLAN」レイヤ 3 ルーティングができない小規模のネットワーク、またはプリンタなどタグ付き VLAN をサポートしないデバイスの共有において有効です。以下は「Asymmetric VLAN」の基本的な一例です。共有する VLAN にサーバやファイアウォールが存在し、各 PC がそれぞれ違う VLAN におかれています。各 PC が違う VLAN により隔離されているため、相互の通信はできませんが、サーバやファイアウォールへのアクセスは可能です。

「Asymmetric VLAN」の設定の例として下記のようなものがあります。

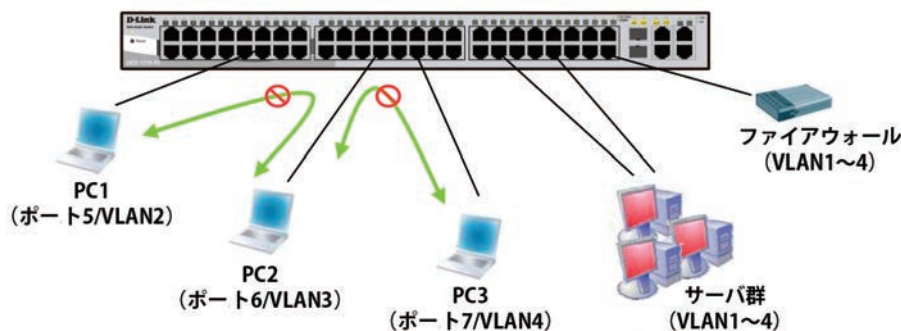


図 5-37 Asymmetric VLAN の例

1. Configuration > 802.1Q VLAN の順にメニューをクリックして以下の画面を表示します。

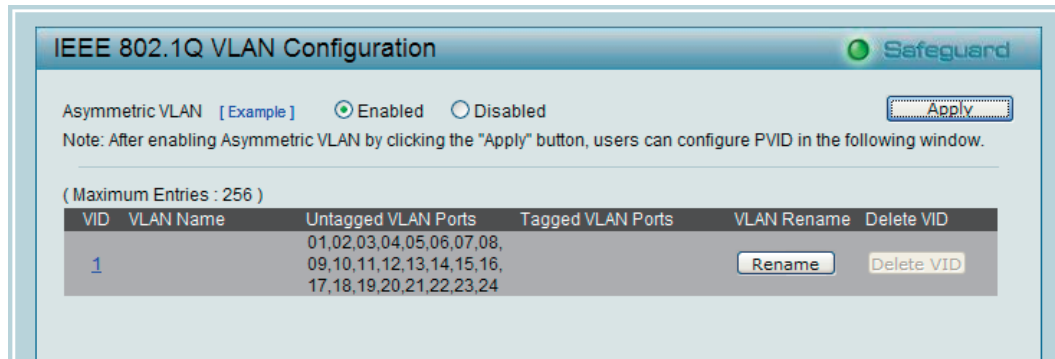


図 5-38 IEEE 802.1Q VLAN Configuration 画面 - Asymmetric VLAN の有効化

「Asymmetric VLAN」を「Enabled」にして「Apply」をクリックしてください。重複する VLAN は本機能をリセットしないと使用することができません。

2. 続いて VLAN の設定をします。共有 VLAN (VLAN1)、アクセス VLAN (VLAN 2-4) の設定を行います。この場合、規定の VLAN は共有 VLAN になります。VLAN ネットワーク上の共有ポートは下記の例に従い設定してください。

- ・ ポート 15-18 はサーバへの接続
- ・ ポート 20 はファイアウォールへの接続

これらの共有ポート群はすべての VLAN に接続されることになります。ポート 15-18、20 は既に VLAN1 に所属し変更する必要はありません。VLAN 2 は 15-18、20 ポート (共有 VLAN ポート) を含んだ形で設定され、その他のポートは他の VLAN から隔離されます。VLAN 3 と 4 はやはり上記ポート (2、3、4) は認識するものの他のポート (6、7) からは隔離されます。この結果 3 つの VLAN が共有ポート (15-18、20) と接続して他のポートを介して、それぞれとの接続はできないよう隔離された状態が出来上がります。

VLAN 設定の一例

- ・ VLAN 1: 規定 VLAN、全ポートタグなしを含む
- ・ VLAN 2: タグなしポート 5、15、18、20 がメンバポート
- ・ VLAN 3: タグなし 6、15、18、20 がメンバポート
- ・ VLAN 4: タグなし 7、15、18、20 がメンバポート

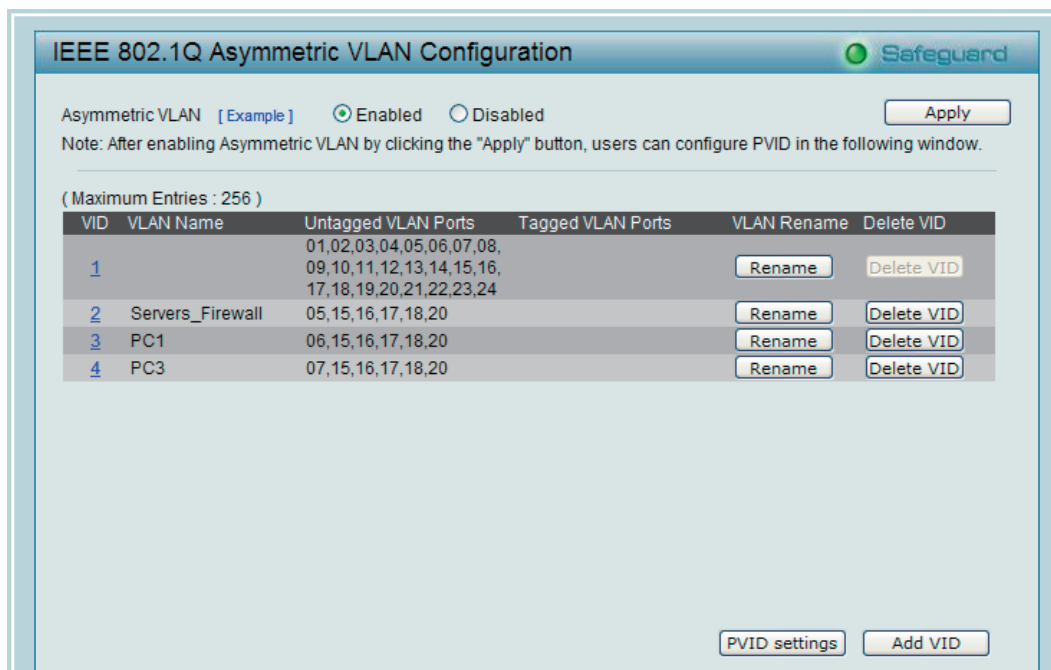


図 5-39 IEEE 802.1Q VLAN Asymmetric Configuration 画面 - VLAN の追加

- VLAN 設定項目の下記にある「PVID settings」を設定します。そして共有ポートを「PVID 1」と設定して、その他の隔離されているポートを「PVID 2、3、または 4」と設定する必要があります。「PVID」の設定の目的はタグなしパケットの送受信が正しく行われているのか確認するためです。

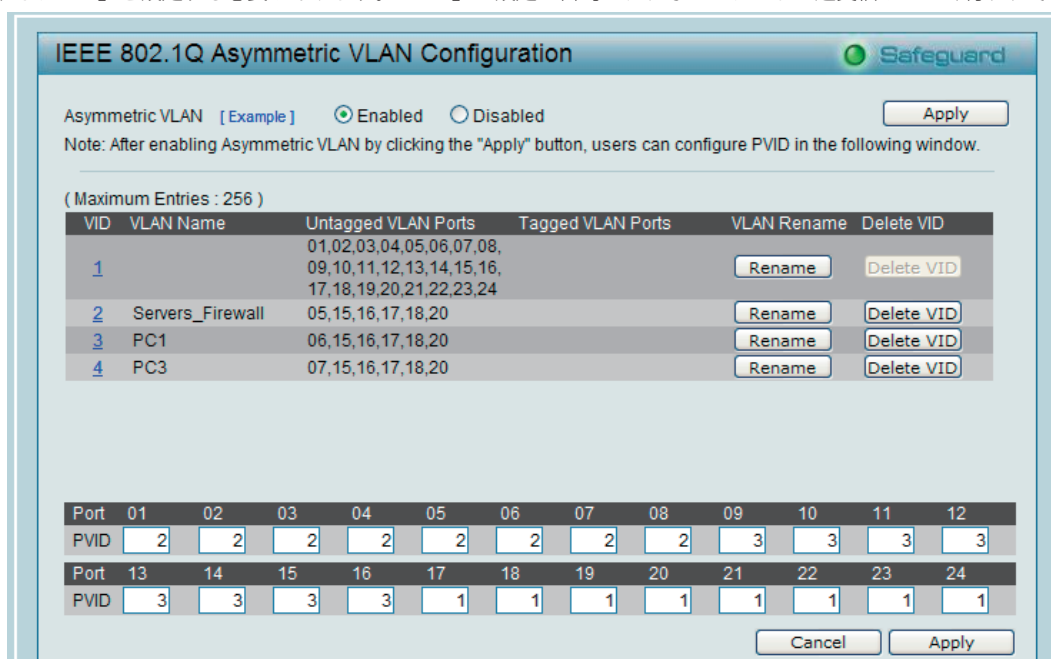


図 5-40 IEEE 802.1Q Asymmetric VLAN Configuration - PVID settings 画面

上記設定後ユーザは「PVID1」に設定された共有ポートを介してネットワークのリソースへのアクセスができるようになり、VLAN2, 3, 4も同様のアクセスは可能になります。しかし VLAN 2, 3 や 4 などはそれぞれの情報を共有することはできません。「Example」をクリックして大規模なネットワークでの「Asymmetric VLAN」の一例を確認します。

注意 「Asymmetric VLAN」が有効の場合、IGMP Snooping、Management VLAN および MAC Address Table が初期値に戻ります。

802.1Q Management VLAN (802.1Q マネジメント VLAN 設定)

スイッチの権限をデフォルト VLAN から設定した VLAN に変更することができます。これによりネットワーク全体をより柔軟に管理することができます。

Configuration > 802.1Q Management VLAN の順にメニューをクリックし、以下の画面を表示します。

図 5-41 IEEE 802.1Q Management VLAN Configuration 画面

初期値では VLAN の管理は無効です。本機能を有効にすると、すべての既存の VLAN をマネジメント VLAN として選択することができます。「Management VLAN」で「Enabled」(有効)を選択し、対応する「VID」を指定します。「Apply」ボタンをクリックして VLAN 管理を有効にします。

Voice VLAN (音声 VLAN)

音声 VLAN は、VoIP サービスを強化するために IP 電話から割り当てられた VLAN まで自動的に音声トラフィックの送信を行う機能です。高い優先度と個別の VLAN を使用することで、VoIP トラフィックの品質とセキュリティを保証します。音声 VLAN 機能は、対応するポート下のタグなしパケットに音声 VLAN タグを挿入するだけです。VLAN タグを持つ VoIP パケットが来ると、音声 VLAN 機能はオリジナルの VLAN タグを置き換えません。

Voice VLAN Settings (音声 VLAN 設定)

Configuration > Voice VLAN > Voice VLAN Settings の順にメニューをクリックし、以下の画面を表示します。

Port	Auto Detection	Status
1	Disabled	None
2	Disabled	None
3	Disabled	None
4	Disabled	None
5	Disabled	None
6	Disabled	None
7	Disabled	None
8	Disabled	None

図 5-42 Voice Vlan Settings 画面

Webマネージャによる詳細設定

以下の項目を使用して設定を行います。

項目	説明
Voice VLAN State	プルダウンメニューを使用して、本機能を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は無効です。本設定を有効にすると「Voice VLAN Global Setting」の設定が可能になります。
VLAN ID	選択をして音声 VLAN の VLAN ID を入力します。音声トラフィックを行う VLAN の ID を設定します。事前に「802.1Q VLAN」ページにて VLAN を作成して、音声 VLAN として割り当てる必要があります。「802.1Q VLAN」で設定されたメンバポートが、音声 VLAN のスタティックメンバポートになります。自動的に音声 VLAN にポートを追加する場合、「Auto Detection」機能を有効にします。
Priority	音声 VLAN の優先度 (Highest、High、Medium、Low) を設定します。
Aging Time	ポートが自動 VLAN の一部の場合、音声 VLAN からポートを削除するまでの時間を設定します。最後の音声機器がトラフィックを送信しなくなり、音声機器の MAC アドレスが期限切れになると、音声 VLAN タイマは開始されます。ポートは音声 VLAN タイマの時間切れの後、音声 VLAN から削除されます。選択可能範囲は「1-120」時間です。初期値は「1」時間です。
From Port / To Port	ポート範囲を指定します。
Auto Detection	ポートを自動的に音声 VLAN の一部として設定する機能です。受信パケットの MAC アドレスが設定した OUI アドレスと一致した場合、ポートは自動的に音声 VLAN の一部であると認識されます。初期値は「Disabled」(無効) です。

注意 Voice VLAN 機能は、他の機能 (QoS を含む) より優先順位が高くなっています。そのため、音声トラフィックは QoS 機能には影響されずに Voice VLAN 機能設定に従って処理されます。

Voice VLAN OUI Settings (音声 VLAN OUI 設定)

ここでは、ユーザ定義の音声トラフィックの OUI を設定します。Organizationally Unique Identifier (OUI) は、MAC アドレスの最初の 3 バイトです。この識別子は、ベンダ、生産者、または他の組織を識別します。

Configuration > Voice VLAN > Voice VLAN OUI Settings の順にメニューをクリックし、以下の画面を表示します。

図 5-43 Voice Vlan OUI Settings 画面

いくつかの定義済みの OUI があり、ユーザが個人的な OUI を設定する場合にはこれらの事前に定義された OUI を避ける必要があります。以下は、定義済みの音声トラフィックの OUI です。

設定済み OUI と対応ベンダー一覧

OUI	供給元	簡略名
00:E0:BB	3COM	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

以下の項目を使用して、設定します。

項目	説明
Default OUI	既存の OUI 値を入力します。「3COM」「Cisco」「Veritel」「Pingtel」「Siemens」「NEC/Philips」「Huawei3COM」「Avaya」があります。
User defined OUI	手で音声 OUI の定義を作成します。作成可能な OUI の数は 10 です。手で設定された OUI が選択されている場合、ACL ルールが 1 つ使用され、設定するともう 1 つ ACL ルールが使用されます。システムは ACL プロファイル (Profile ID:51) を全ての音声 VLAN ルールのために生成します。

OUI を選択して「Add」ボタンをクリックし、設定内容を完了します。

Link Aggregation (リンクアグリゲーション設定)

Port Trunkings (ポートトランキング設定)

トランキング機能は複数のポートを束ねて1つの広帯域のデータパイプラインとして利用する機能です。5個 (DGS-1210-10P/GE) または8個 (DGS-1210-16/GE、DGS-1210-24/GE、DGS-1210-48/GE) のトランキンググループまで作成でき、最大8ポートのトランキングが可能です。

Configuration > Link Aggregation > Port Trunkings の順にメニューをクリックし、以下の画面を表示します。

Port Trunking Safeguard

Link Aggregation State: Enabled Disabled Apply

Edit Trunking Information

ID: Type: Apply

Port	1	2	3	4	5	6	7	8	9	10	11	12
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: maximum 8 ports in static group and 8 ports in LACP group.

Trunking list

ID	Type	Ports
01	Static	5, 6, 7, 8
02	Static	9, 10, 11, 12
03	LACP	13, 14, 15, 16
04	Disable	
05	Disable	
06	Disable	
07	Disable	
08	Disable	

図 5-44 Port Trunking 画面

項目	説明
Link Aggregation State	本機能を「Enabled」(有効) / 「Disabled」(無効) にします。
Type	トランキンググループの種類を設定します。 <ul style="list-style-type: none"> Disabled - トランキンググループ内のすべてのメンバを削除します。 Static - 手でリンクアグリゲーションの設定をします。 LACP - ポートトランキンググループのリンクを自動的に検出します。

「Apply」ボタンをクリックし、設定内容を有効にします。

注意 トランクグループの所属ポートは同一の VLAN グループに所属している必要があります。

LACP Port Settings (LACP ポート設定)

スイッチにポートトランキンググループを作成します。LACP 制御フレームを送受信時のポートごとの動作を設定します。

Configuration > Link Aggregation > LACP Port Settings の順にメニューをクリックし、以下の画面を表示します。

LACP Port Settings Safeguard

Link Aggregation Port Configuration

From Port: To Port: Port Priority(0~65535): Activity: Timeout: Apply

Port	Port Priority	Activity	Timeout
01	128	Active	Long (90 sec)
02	128	Active	Long (90 sec)
03	128	Active	Long (90 sec)
04	128	Active	Long (90 sec)
05	128	Active	Long (90 sec)
06	128	Active	Long (90 sec)
07	128	Active	Long (90 sec)
08	128	Active	Long (90 sec)
09	128	Active	Long (90 sec)
10	128	Active	Long (90 sec)

図 5-45 LACP Port Settings 画面

項目	説明
From Port/To Port	設定の対象となるポートの最初と最後の番号を設定します。
Port Priority(0-65535)	ポートの LACP 優先度を表示します。初期値は「128」です。
Activity	<ul style="list-style-type: none"> Active - Active ポートは LACP 制御フレームの処理と送信を行います。これにより LACP 準拠のデバイス同士はネゴシエーションとリンクの集約を行い、グループは必要に応じて動的に変更されます。グループへのポート追加、または削除などのグループの変更を行うためには、少なくともどちらかのデバイスで LACP ポートを「Active」に設定する必要があります。また、両方のデバイスは LACP をサポートしている必要があります。 Passive - Passive ポートは自分から LACP 制御フレームの送信を行いません。リンクするポートグループがネゴシエーションを行い、動的にグループの変更を行うためには、コネクションのどちらか一端がアクティブな LACP ポートである必要があります。(初期値)
Timeout	LACP の時間設定を行います。 <ul style="list-style-type: none"> Short (3 Sec) - LACP の中断まで 3 秒です。 Long (90 Sec) - LACP の中断まで 90 秒です。

「Apply」ボタンをクリックし、設定内容を有効にします。

IGMP Snooping (IGMP Snooping 設定)

IGMP (Internet Group Management Protocol) Snooping 機能を利用すると、Web スマートスイッチは各フレームのレイヤ 2 MAC ヘッダの内容を確認し、高度なマルチキャストフォワーディングを行うようになります。

IGMP Snooping 機能では LAN 上に散乱したトラフィックの削減に貢献します。本機能をグローバルに有効にすると、Web スマートスイッチはマルチキャストトラフィックを、そのマルチキャストグループのメンバのみに転送します。

IGMP は IP マルチキャストパケットの変更やルーティングを行うものではない点に注意が必要です。サブネットワークを越えて IP マルチキャストパケットを送信するには、マルチキャストルーティングプロトコルが必要になります。

Configuration > IGMP Snooping の順にメニューをクリックし、以下の画面を表示します。

図 5-46 IGMP Snooping Configuration 画面

IGMP Snooping 機能の初期設定は無効です。IGMP Snooping をグローバルに有効にするには、「Enabled」を選択して「Apply」ボタンをクリックします。

さらに以下の IGMP 項目の設定を行います。

項目	説明
Host Timeout (130-153025sec)	学習されたホストポートエントリが削除されるまでの時間。学習された各ホストポートに対し、「HostPortPurgeInterval」に使用する「PortPurgeTimer」が起動されます。本タイムはそのポートにてホストからの Report メッセージが受信される度に開始されます。「HostPortPurgeInterval」の間に Report メッセージが受信されない場合、そのホストエントリはマルチキャストグループから除外されます。初期値は 260 (秒) です。
Robustness Variable (2-255)	本値は予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい値を指定します。本値には 0 と 1 を指定しないでください。初期値は 2 (秒) です。
Query Interval (60-600 sec)	General Query の送信間隔。クエリインターバルの値を調整することで、送信する IGMP メッセージの数を増減できます。大きい値を指定すると IGMP クエリの送信頻度は低くなります。初期値は 125 (秒) です。
Router Timeout (60-600sec)	学習されたルータポートエントリが削除されるまでの時間。学習された各ルータポートに対し、「RouterPortPurgeInterval」に使用する「RouterPortPurgeTimer」が起動されます。本タイムはそのポートから Router control メッセージが受信される度に開始されます。「RouterPortPurgeInterval」の間に Router control メッセージが受信されない場合、そのルータポートエントリは除外されます。初期値は 260 (秒) です。
Last Member Query Interval (1-25sec)	Leave Group メッセージを受け取った時に送信する Group-Specific Membership Query の Max Response Time フィールドに設定する値 (Last Member Query Interval)。また、同 Query の送信間隔でもあります。本値はネットワークでの「Leave Latency」を変更する目的でも使用できます。小さい値を設定するとグループの最後のメンバの不在を検知する時間が短く設定されます。初期値は 1 (秒) です。
Max Response Time (10-25sec)	IGMP Response report を送信するまでの最大時間 (秒) です。本値を調整すると「Leave Latency」(最後のホストがグループを抜けた瞬間から、ルーティングプロトコルがメンバが存在していないことに気付くまでの時間差) に影響を与えます。またサブネット上の IGMP トラフィックの頻度を制御することも可能です。初期値は 10 (秒) です。
Querier State	IGMP クエリを送信して、マルチキャストクライアントのステータスをチェックします。初期値は「Disabled」(無効) です。

特定の VLAN に対して IGMP Snooping を有効にするためには、「The VLAN Setting of IGMP snooping」セクションの該当 VLAN の「State」を「Enabled」とし、「Router Port Setting」の下の「Edit」ボタンをクリックして以下の画面を表示します。

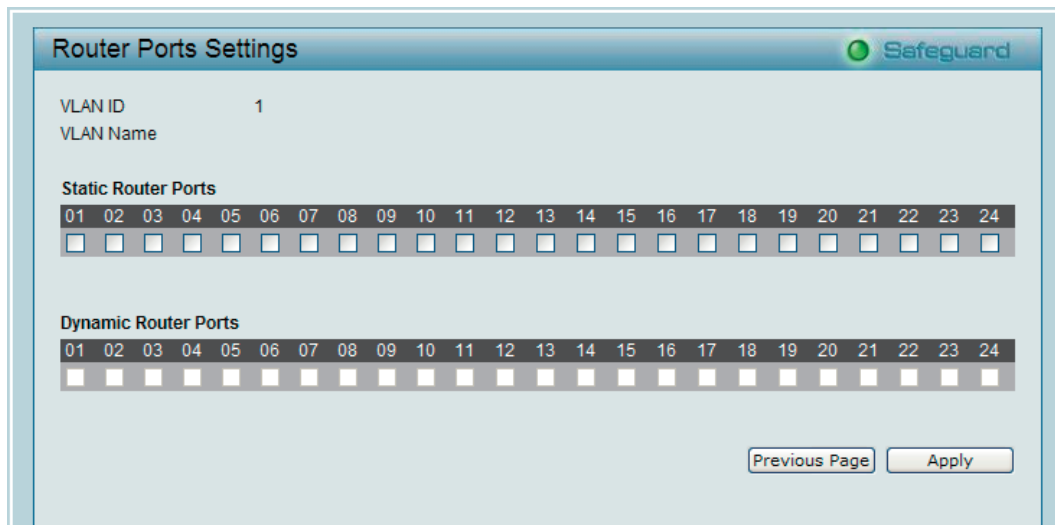


図 5-47 Router Ports Settings 画面

IGMP Snooping を適用するポートを選択後、「Apply」ボタンをクリックし、設定を有効にします。

ルータポートとして「Static Router Ports」に手動で設定します。「Dynamic Router Ports」に設定すると、Query コントロールメッセージを受信した場合にスイッチが自動的に設定します。

「IGMP Snooping Configuration」画面に戻るには、「Previous Page」ボタンをクリックします。

指定 VLAN のマルチキャストエントリテーブルを確認するには、「IGMP Snooping Configuration」画面で「View」ボタンをクリックして以下の画面を表示します。

Group ID	VLAN ID	VLAN Name	Multicast Group	Multicast MAC address	Port Members
001	1	default	239.255.255.100	01-00-5e-7f-ff-64	11

図 5-48 Multicast Entry Table 画面

Port Mirroring (ポートミラーリング)

ポートミラーリングとは、スイッチのあるポートに入出力するパケットのコピーを、他のポートに送信して、そこでパケットを監視することにより、ネットワークトラフィックのモニタリングを行う方法です。本機能によりネットワーク管理者は効率よくネットワークパフォーマンスを監視できるようになります。

Configuration > Port Mirroring の順にメニューをクリックし、以下の画面を表示します。

図 5-49 Port Mirroring Configuration 画面

ソースポートの設定項目は以下の通りです。

項目	説明
Port Mirroring	ポートミラーリング機能を「Enabled」(有効)または「Disabled」(無効)にします。
Target Port	ターゲットポートを選択します。
TX	ソースポートが送信したデータをコピーしてターゲットポートに送信します。「All」ボタンをクリックすると、すべてのポートを対象とします。
RX	ソースポートが受信したデータをコピーしてターゲットポートに送信します。「All」ボタンをクリックすると、すべてのポートを対象とします。
Both	ソースポートが送信したデータと受信したデータの両方をターゲットポートに送信します。「All」ボタンをクリックすると、すべてのポートを対象とします。
None	ポートミラーリングを行いません。「All」ボタンをクリックすると、すべてのポートを対象から外します。

「Apply」ボタンをクリックし、設定を有効にします。

Power Saving (省電力設定)

Power Saving モード機能は、RJ-45 ポートがリンクダウンしている場合、または接続デバイスの電源が入っていない場合に、自動的に電力の消費量を削減します。使用されているケーブルが短い（20メートル以内）場合にも、電力消費が削減されます。電力消費を削減することにより発生熱量が少なくなり、結果として製品寿命が延び運用コストの削減を見込むことができます。

Configuration > Power Saving の順にメニューをクリックし、以下の画面を表示します。

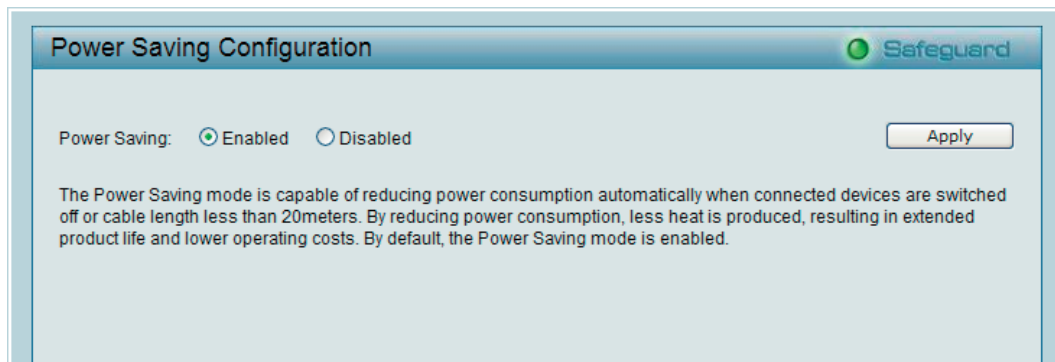


図 5-50 Power Saving Configuration 画面

「Enabled」を選択し、「Apply」ボタンをクリックし、省電力モードを有効にします。初期値は、「Enabled」です。

Loopback Detection (ループバック検知設定)

ループバック検知機能は、ネットワーク内にスパンニングツリー (STP) が有効ではない時に、ハブやアンマネージドスイッチなどの特定のポートによって生成されるループを検出するために使用されます。本機能は、スイッチのポートを自動的にシャットダウンし管理者にログを送信します。「Loopback Detection Recover Time」がタイムアウトになると、ループバック検知ポートは開放されます。ループバック検知機能はポート範囲に実行されます。プルダウンメニューを使用し、機能を「Enabled」(有効) / 「Disabled」(無効) にします。

Configuration > Loopback Detection の順にメニューをクリックし、以下の画面を表示します。

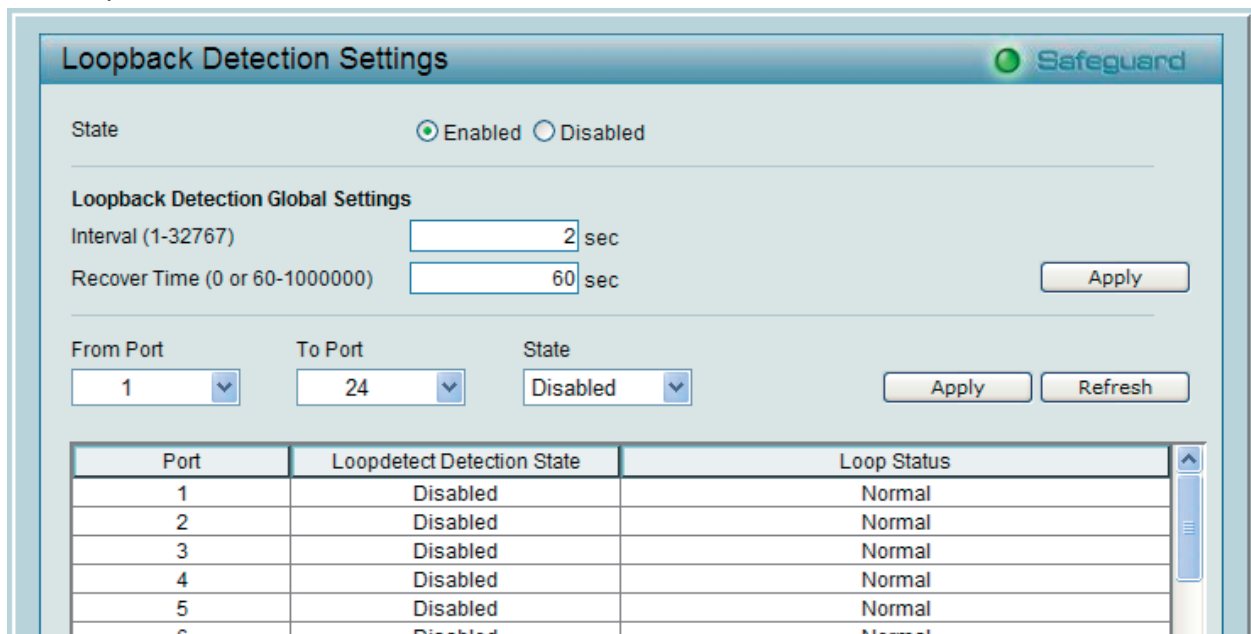


図 5-51 Loopback Detection Settings 画面

項目	説明
State (ラジオボタン)	ループバック検知機能を「Enabled」(有効)または「Disabled」(無効)にします。初期値は「Disabled」です。
Interval (1-32767)	ループ検知間隔を設定します。(1-32767 秒)
Recover Time (0 or 60-1000000)	ループバックが検知された場合にリカバリする時間 (秒) を指定します。指定時間に到達すると、スイッチはループバックをチェックします。0 または 60-1000000 (秒) に設定します。0 を指定すると、Loopdetect Recover Time は無効になります。初期値は 60 (秒) です。
From Port	プルダウンメニューで開始ポートを選択します。
To Port	プルダウンメニューで終了ポートを選択します。
State (プルダウンメニュー)	「Enabled」(有効) または 「Disabled」(無効) を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SNTP Settings (SNTP 設定)

SNTP (Simple Network Time Protocol) は、コンピュータのクロックにスイッチを同期させるために使用されます。SNTP 設定には「Time Settings」と「Time Zone Settings」メニューがあります。

Time Settings (時刻設定)

スイッチに時刻を設定します。

Configuration > SNTP Settings > Time Settings の順にクリックし、以下の画面を表示します。

図 5-52 Time Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Clock Source	システム時刻を設定するタイムソースを設定します。 <ul style="list-style-type: none"> SNTP - システム時刻を SNTP サーバから受信するように設定します。 Local - システム時刻をデバイスに対して直接設定します。
Current Time	現在の時間を表示します。
SNTP Server Configuration	
SNTP First Server	システム時刻を受け取るプライマリ SNTP サーバの IP アドレスを設定します。
SNTP Second Server	システム時刻を受け取るセカンダリ SNTP サーバの IP アドレスを設定します。
SNTP Poll Interval In Seconds (30-99999)	SNTP サーバにユニキャストによる問い合わせを行う間隔 (30-99999 秒) を設定します。
Manually Set Current Time/ Set time from PC	
	<ul style="list-style-type: none"> Manually Set Current Time - 手動で時刻の設定をします。 Set time from PC - PC の時刻設定を同期させます。
Date (DD/MM/YYYY)	現在のシステム日付を設定します。項目のフォーマットは日 / 月 / 年です。
Time (HH:MM:SS)	現在のシステム時刻を時 : 分 : 秒 (24 時間制) で設定します。例えば午後 9 時であれば 21:00:00 と指定します。

「Apply」 ボタンをクリックし、デバイスに SNTP 設定を適用します。

TimeZone Settings (タイムゾーン設定)

以下の画面では、SNTP 用のタイムゾーンとサマータイム (Daylight Saving Time) の設定を行います。

Configuration > SNTP Settings > TimeZone Settings の順にメニューをクリックし、以下の設定画面を表示します。

図 5-53 TimeZone Settings 画面

以下に、画面の各項目を示します。

項目	説明
Daylight Saving Time State	デバイスに設定するサマータイムの種類を設定します。 <ul style="list-style-type: none"> Disabled - サマータイムを無効にします。(初期値) Annual - サマータイムを日付指定で有効にします。このオプションでは開始と終了の日付を設定する必要があります。
Daylight Saving Time Offset In Minutes	プルダウンメニューを使用して、サマータイムによる調整時間を 30、60、90、120 分から選択します。
Time Zone Offset: from GMT In +/- HH:MM	プルダウンメニューを使用して、GMT (グリニッジ標準時) からのオフセット時間を選択します。
DST Annual Settings	
Annual モードを使用すると、DST(サマータイム)設定を指定した詳細な期日で自動的に調整できるようになります。例: DST を 4 月 3 日から開始し、10 月 14 日を終了と設定します。	
From: Month	DST が開始する月を指定します。(毎年)
From: Day	DST が開始する日を指定します。(毎年)
From: Time In HH MM	DST が開始する時間を指定します。(毎年)
To: Month	DST が終了する月を指定します。(毎年)
To: Day	DST が終了する日を指定します。(毎年)
To: Time In HH MM	DST が終了する時間を指定します。(毎年)

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Spanning Tree (スパンニングツリー設定)

本スイッチは2つのバージョンのスパンニングツリーを搭載しています。1つは802.1W「Rapid Spanning Tree Protocol」(RSTP)、もう1つは802.1D「Spanning Tree Protocol」(STP)です。RSTPは802.1D STP対応のレガシー機器にも対応可能ですが、この場合のRSTPの利点は失われます。

RSTPは、IEEE 802.1D STPの改良版で、STPを使用する上での制限を克服する目的で開発されました。そのため、RSTPの基本的な機能や用語の多くはSTPと同じであり、設定パラメータの多くがRSTPでも同じように使用されます。

RSTPはブロードキャストストームを引き起こすおそれのあるネットワークループを防止するために、スイッチ、ブリッジまたはルータ間のバックアップリンクとして実装されます。物理リンクがループを形成し、冗長が発生している時、1つのパスのみがフレームの送信に使用されます。そのリンクに障害が発生すると、STPによりもう一方のリンクが自動的にアクティブになります。

スパンニングツリー機能を有効にするとスイッチはBPDUパケットとそれに付随するHelloパケットをリッスンします。BPDU Helloパケットは受信しない相手にも送信されます。それによりブリッジ間の各リンクはリンクの状態を感知します。最終的にはこの違いにより障害が発生したリンクの検出が速やかに行われ、迅速なトポロジの再構成へと繋がります。802.1Dの欠点は、隣接ブリッジからの迅速なフィードバックが行われなことです。

STP Global Settings (スパンニングツリーグローバル設定)

Configuration > Spanning Tree > STP Global Settings の順にメニューをクリックし、以下の画面を表示します。

図 5-54 802.1D Spanning Tree Configuration 画面

STPの設定を行うには、「RSTP Status」で「Enabled」を選択し、以下の設定項目を指定します。

項目	説明
STP Version	「RSTP」「STP Compatible」から選択します。初期値は「RSTP」です。
Bridge Priority (0-61410 secs)	パケット送信を行う優先度 (0-61410) を示します。値が小さいほど優先度は高くなります。初期値は 32768 です。
Tx Hold Count (1-10)	各送信間隔に送信される「Hello Packet」の最大数を設定します。値の範囲は 1-10 で初期値は 6 です。
Maximum Age (6-40 secs)	本設定項目は古い情報がネットワーク内の冗長パスを永遠に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。この値は、ルートブリッジにより設定され、スイッチと他の Bridged LAN (ブリッジで相互接続された LAN) 内のデバイスが持っているスパンニングツリー設定値が矛盾していないかを確認します。本値が経過した時にルートブリッジからのBPDUパケットを受信していないと、スイッチは自分でBPDUパケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40 (秒) の範囲から値を指定します。初期値は 20 (秒) です。
Hello Time (1-10 sec)	ルートデバイスにより、スイッチが機能している旨を通知するために送信されるコンフィグレーションメッセージの送信間隔を指定します。初期値は 2 (秒) です。「Max Age」の値は「Hello Time」より大きい必要があります。
Forward Delay (4-30 secs)	ルートデバイスが状態を変更するまでの最大待ち時間。初期値は 15 (秒) です。
Root Bridge	ルートブリッジの MAC アドレスを表示します。
Root Cost	ルートブリッジのルートコストを表示します。
Root Maximum Age	ルートブリッジの「Maximum Age」を表示します。
Root Forward Delay	ルートブリッジの「Forward Delay」を表示します。
Root Port	ルートポートを表示します。

「Apply」ボタンをクリックし、設定を有効にします。「Refresh」ボタンをクリックすると、画面が更新されます。

STP Port Settings (スパンニングツリーポート設定)

スイッチレベルでのスパンニングツリー設定のほかに、ポートをグループ分けして、各ポートグループに対してスパンニングツリーの設定を行うことも可能です。

STP グループは、スイッチレベルでの設定に使用したパラメータのほかに、ポートプライオリティとポートコストを使用します。STP グループのスパンニングツリーは、スイッチレベルのスパンニングツリーと同様の働きをしますが、ルートブリッジの概念はルートポートに置き換えられて考えることができます。グループ内のルートポートは、ポートプライオリティとポートコストに基づいて選出され、ネットワークとグループを接続する役割を果たします。スイッチレベルの場合と同様に、冗長リンクはブロックされます。

スイッチレベルの STP は、スイッチ間 (または同様のネットワークデバイス) の冗長リンクをブロックし、ポートレベルの STP は STP グループ内の冗長リンクをブロックします。STP グループと VLAN グループを関連付けて定義することをお勧めします。

Configuration > Spanning Tree > STP Port Settings の順にメニューをクリックし、以下の画面を表示します。

Port	State	Priority	External Cost	Edge	P2P	Restricted Role	Restricted TCN	Port State
01	Enable	128	AUTO/20000	Auto	Auto	False	False	Blocking
02	Enable	128	AUTO/20000	Auto	Auto	False	False	Blocking
03	Enable	128	AUTO/200000	Auto	Auto	False	False	Forwarding
04	Enable	128	AUTO/20000	Auto	Auto	False	False	Blocking
05	Enable	128	AUTO/19900	Auto	Auto	False	False	Blocking
06	Enable	128	AUTO/19900	Auto	Auto	False	False	Blocking
07	Enable	128	AUTO/19900	Auto	Auto	False	False	Blocking

図 5-55 STP Port Settings 画面

ポートごとに 802.1D STP を設定します。

項目	説明
From Port/To Port	設定を適用するポートおよびポート範囲を指定します。
State	ポートの STP を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。
External Cost (1-2000000000; 0 = AUTO)	設定対象のポートに対し、パケット送信のためのコストを表すメトリックを定義します。ポートコストには、自動設定、または手動でメトリック値を指定できます。初期値は 0 (自動) です。 <ul style="list-style-type: none"> 0-0 を指定すると、指定したポートに対して、最適なパケット送信速度を自動的に設定します。 デフォルトポートコスト: 100Mbps ポートの場合は 200000、ギガビットポートの場合は 20000。 1-200000000 の範囲から指定 - 小さい数字を指定すると、パケット送出ポートとして選出される確率が上がります。
Migrate	RSTP モードで動作中に、「Enabled」を選択すると、選択されたポートは RSTP BPDU を送信します。
Edge	<ul style="list-style-type: none"> True - 選択されたポートはエッジポートとして指定されます。エッジポートはループを発生しませんが、トポロジの変更によってループ発生の可能性が生じると、エッジポートはエッジポートとしての資格を失います。エッジポートは通常 BPDU パケットを受信しませんが、BPDU パケットを受信すると、そのポートはエッジポートの資格を失います。 False - そのポートにエッジポートの資格がないことを示しています。 AUTO - ポートが自動的にエッジポートステータスを持つかどうかを示します。
Priority	各ポートのプライオリティ (0-240) を指定します。初期値は 128 です。低い数字ほど、ポートがルートポートとして選択される可能性が高くなります。
P2P	<ul style="list-style-type: none"> True - 選択ポートは P2P ポートとして指定されます。P2P ポートはエッジポートと似ていますが、P2P ポートは全二重モードでのみ稼動する点で異なります。RSTP の特長として、エッジポート同様、P2P ポートは迅速に Forwarding 状態に遷移します。 False - そのポートに P2P ポートの資格がないことを示しています。(初期値) Auto - ポートはいつでも可能な時に (True を指定した時と同様に) P2P ポートとして稼動します。ポートの資格を失う時 (例えば、半二重モードを指定された時など)、自動的に False を指定した時と同様になります。
Restricted Role	「True」「False」からパケットの「Restricted Role」を選択します。「True」に設定した場合、ポートはルートポートとして識別されません。初期値は「False」です。
Restricted TCN	「True」「False」からパケットの「Restricted TCN」を選択します。Topology Change Notification (TCN) はブリッジがルートポートにトポロジの変更を送信する BPDU です。「True」に設定すると、受信した TCN を他のポートへ伝搬することを停止します。初期値は「False」です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。「Refresh」ボタンをクリックすると、画面が更新されます。

QoS（QoS機能の設定）

以下は、QoSのサブメニューの説明です。

サブメニュー	説明	参照ページ
Storm Control	Storm Control (パケット制御) の設定を行います。	66 ページ
Bandwidth Control	帯域幅の設定を行います。	67 ページ
802.1p/DSCP Priority Settings	QoS プライオリティレベルの設定を行います。	68 ページ

Storm Control (ストームコントロール)

ストームコントロール機能は、ブロードキャスト、マルチキャスト、不正なユニキャストパケットを制限する機能です。一度パケットストームが検出されると、ストームがおさまるまでスイッチはパケットの廃棄を継続します。

QoS > Storm Control の順にメニューをクリックして、以下の画面を表示します。

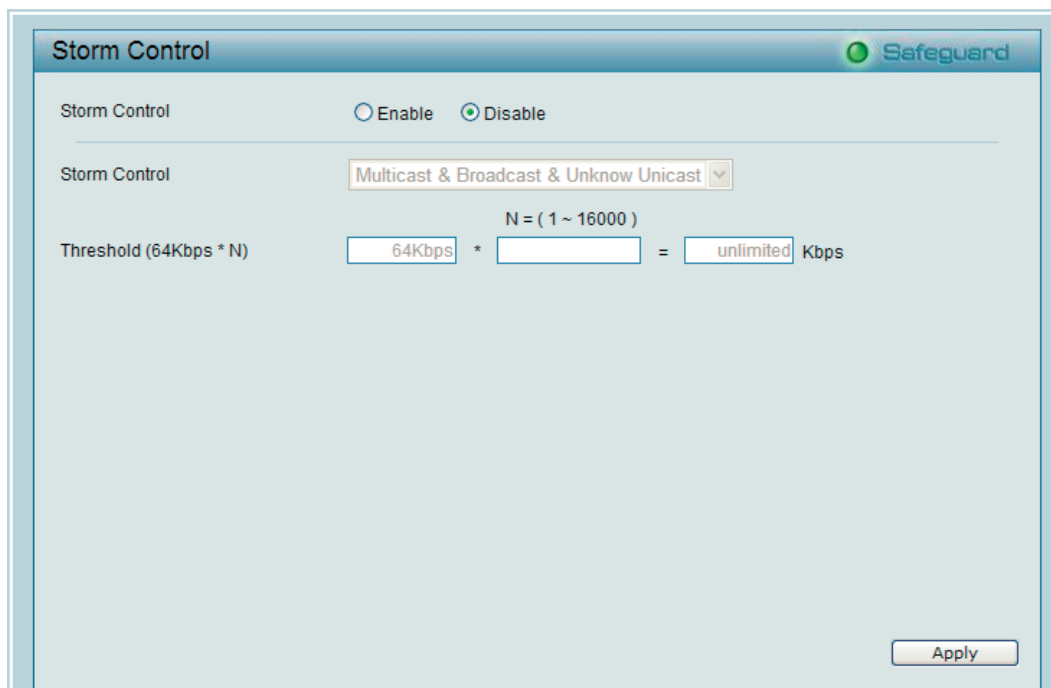


図 5-56 Storm Control 画面

「Storm Control」を「Enable」にして、以下の項目を設定します。

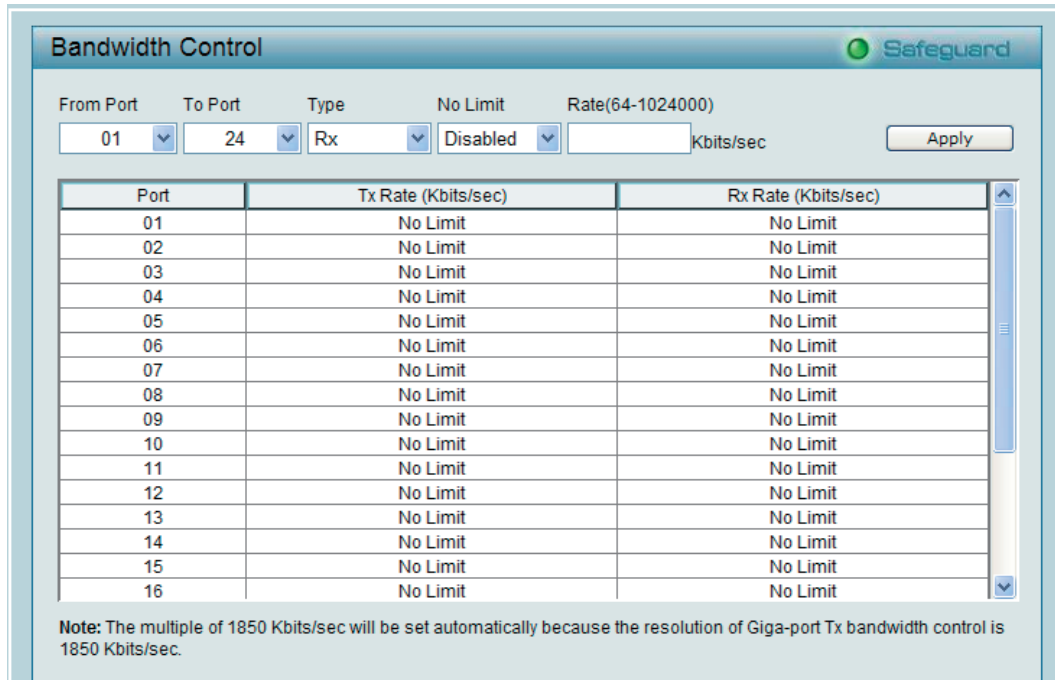
項目	説明
Storm Control	適用するストームの種類を選択します。「Broadcast Only」「Multicast & Broadcast」「Multicast & Broadcast & Unknown Unicast」から選択します。
Threshold (64Kbps * N)	ストームコントロールが有効の場合（初期値では無効）、しきい値は毎秒 64 - 1,024,000 Kbit で設定可能です。「N」に数値を設定して 64Kbps との倍数を指定します。「N」は 1 から 16000 で設定可能です。

「Apply」ボタンをクリックし、設定を適用します。

Bandwidth Control (帯域幅の設定)

帯域制御の設定を行うことにより、すべての選択ポートに対して、送信と受信のデータレートを制限することができます。

ポートの帯域制御の設定を行うには、**QoS > Bandwidth Control** の順にメニューをクリックし、以下の画面を表示します。



Port	Tx Rate (Kbits/sec)	Rx Rate (Kbits/sec)
01	No Limit	No Limit
02	No Limit	No Limit
03	No Limit	No Limit
04	No Limit	No Limit
05	No Limit	No Limit
06	No Limit	No Limit
07	No Limit	No Limit
08	No Limit	No Limit
09	No Limit	No Limit
10	No Limit	No Limit
11	No Limit	No Limit
12	No Limit	No Limit
13	No Limit	No Limit
14	No Limit	No Limit
15	No Limit	No Limit
16	No Limit	No Limit

Note: The multiple of 1850 Kbits/sec will be set automatically because the resolution of Giga-port Tx bandwidth control is 1850 Kbits/sec.

図 5-57 Bandwidth Control 画面

以下の項目を設定または表示できます。

項目	説明
From Port	帯域幅設定を表示するポートグループの最初の番号を設定します。
To Port	帯域幅設定を表示するポートグループの最後の番号を設定します。
Type	Rx (受信)、Tx (送信) および Both (両方) から選択します。帯域上限を受信、送信、送受信の両方のいずれに適用するのかが設定します。
No Limit	ポートに対する帯域制限を設定します。 <ul style="list-style-type: none"> Enabled - ポートで帯域制限を行いません。 Disabled - ポートで帯域制限を行います。(初期値)
Rate (64-1024000)	指定したポートでのデータ速度の上限値 (Kbit/秒)。値は 64 から 1024000 の間の 64 の倍数を入力します。

「Apply」ボタンをクリックし、選択ポートの帯域制御を設定します。設定の結果は、画面下部のテーブルに表示されます。

802.1p/DSCP Priority Settings (802.1p/DSCP プライオリティ設定)

QoSはIEEE 802.1p標準で規定される技術で、これによりネットワーク管理者は、VoIP(Voice-over Internet Protocol)、Web閲覧用アプリケーション、ファイルサーバアプリケーション、およびビデオ会議などのような広帯域を必要とする、またはより高い優先順位を持つ重要なサービスのために、帯域を確保することができます。帯域幅が広く重要度が低いトラフィックを制限することで、帯域を確保することが可能です。

以下の図は、それぞれのポートにおけるQoS優先順位のステータスを表示しており、優先順位が高いほどそのポートからのトラフィックがスイッチにおいて優先されることを示しています。タグ付けされていないパケットに関しては、スイッチはユーザの設定に従って優先順位を割り当てます。

各ポートのQoSプライオリティレベルの設定および表示を行います。タグなしパケットが入力された場合、本スイッチは各ポートに設定された優先度のタグを付加して送信します。

QoS > 802.1p/DSCP Priority Settings の順にメニューをクリックし、以下の画面を表示します。

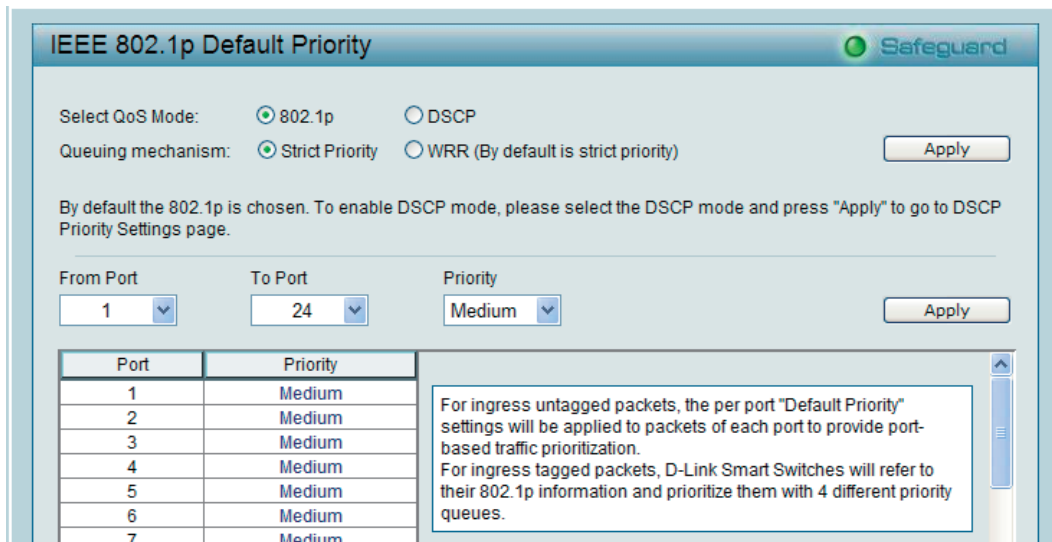


図 5-58 IEEE 802.1p Default Priority 画面

「Select QoS Mode」で「DSCP」に設定して、「Apply」ボタンをクリックすると、画面は以下のように変更されます。

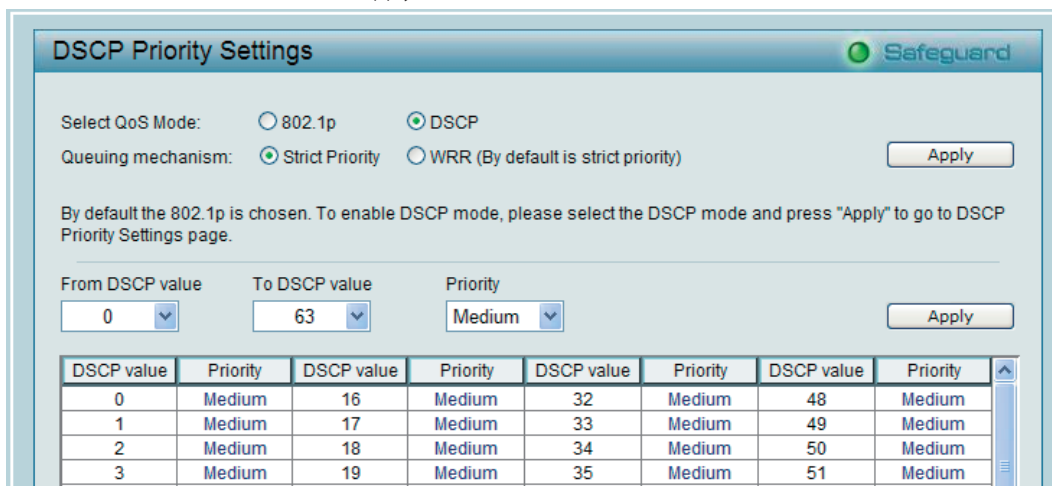


図 5-59 DSCP Priority Settings 画面

以下の項目を設定または表示できます。

項目	説明
Select QoS Mode	スマートスイッチで優先させるトラフィックを選択します。 ・ 802.1p - VLAN タグの 802.1p プライオリティベースとします。 ・ DSCP - IP ヘッダの DSCP プライオリティベースとします。
Queuing mechanism	・ Strict Priority - パケットへのプロセスが最優先となります。(初期値) ・ WRR - Weighted Round-Robin はパケットのプロセスがそれぞれのプライオリティに従って決まります。プライオリティのレベルが限界に達した時、パケットに残りがあったとしてもシステムはパケットへのプロセスを次のレベルに移行してしまいます。システムのパケットのレベルは最高で「8」、高が「4」、中が「2」、低が「1」となっています。
Priority	802.1p QoS モード (Highest、High、Medium、Low) を選択します。初期値は「Medium」です。

各ポートにデフォルトプライオリティを設定する場合は、「From Port」 / 「To Port」でポートを選択します。QoS モードが「DSCP」の場合は、「From DSCP value」 / 「To DSCP value」を使用して、グローバルなデフォルトプライオリティを設定します。

Security（セキュリティ機能の設定）

以下は、Securityのサブメニューの説明です。

サブメニュー	説明	参照ページ
Trusted Host	トラストホストを設定します。	69 ページ
Safeguard Engine	セーブガードエンジン機能を設定します。	70 ページ
Port Security	ポートセキュリティの設定を行います。	70 ページ
802.1X	802.1X 認証の設定をします。	71 ページ
MAC Address Table	スタティック/ダイナミック MAC アドレステーブルの設定をします。	72 ページ

Trusted Host（トラストホスト）

トラストホスト機能を使用して、リモートステーションからスイッチを管理します。以下の図のように、IP アドレス /IP マスクを定義したホストを最大 10 つまで登録することができ、Web マネージャまたは Telnet セッションを使用してスイッチを管理することができます。

トラストホストの追加

1. Security > Trusted Host の順にメニューをクリックし、以下の画面を表示します。

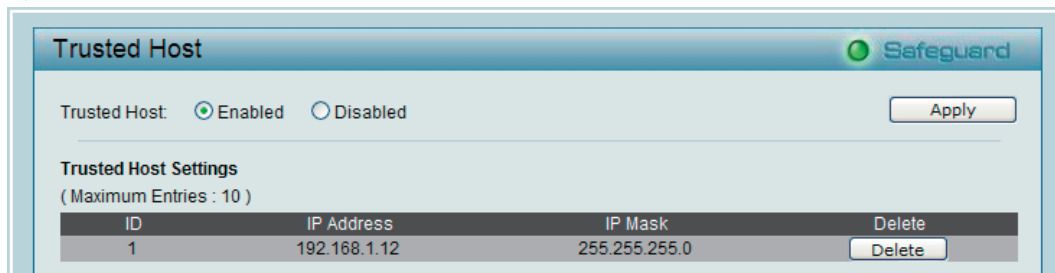


図 5-60 Trusted Host 画面 - Disabled

「Trusted Host」で「Enabled」を選択し、「Apply」ボタンをクリックして以下の画面を表示します。

2. 「Add Host」ボタンをクリックして以下の画面を表示します。

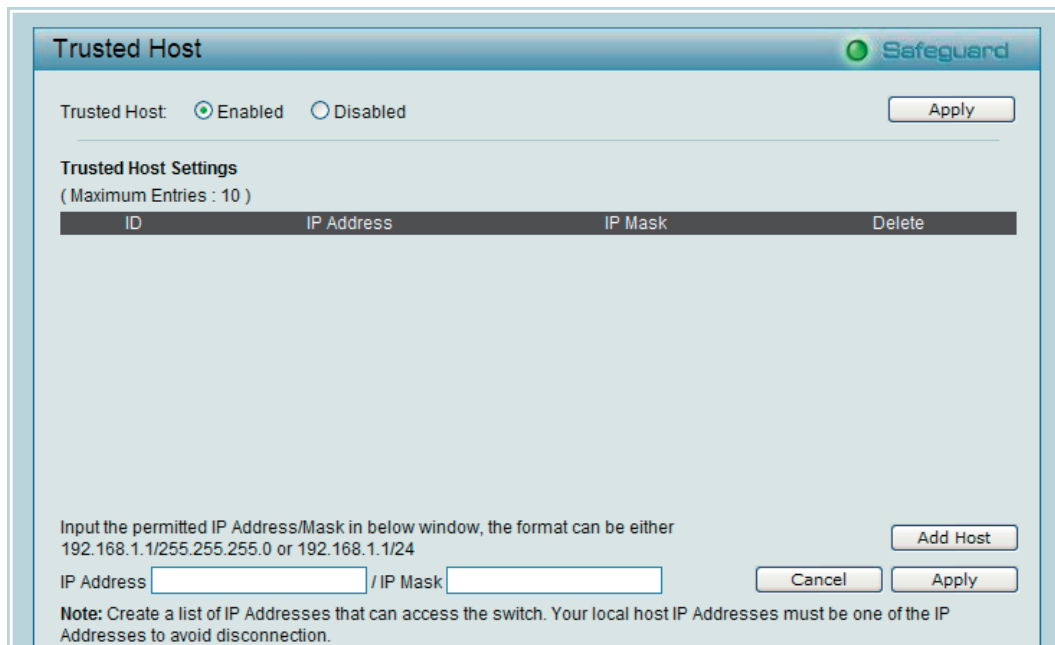


図 5-61 Trusted Host 画面

「IP Address」に IP アドレスと「IP Mask」に IP マスクを入力し、「Apply」ボタンをクリックします。

異なる IP マスク設定ごとに IP アドレスまたは IP アドレス範囲を入力することが可能です。入力形式は、192.168.1.1/255.255.255.0 または 192.168.0.1/24 です。入力可能な IP 範囲の例は以下の通りです。

IP アドレス	IP マスク	許可される IP の範囲
192.168.0.1	255.255.255.0	192.168.0.1~192.168.0.255
172.17.5.215	255.0.0.0	172.0.0.1~172.255.255.255

IP アドレスを削除する場合は、「Delete」ボタンをクリックします。

Safeguard Engine (セーフガードエンジン)

セーフガードエンジン機能は、パケットフラディングによるスイッチのCPUへの影響を自動的に抑制します。本機能は、悪意のあるウイルスやワームによる攻撃がWebスマートスイッチの動作に影響を与えないように保護を行います。本機能は初期値で有効です。

Security > Safeguard Engine の順にメニューをクリックし、以下の画面を表示します。

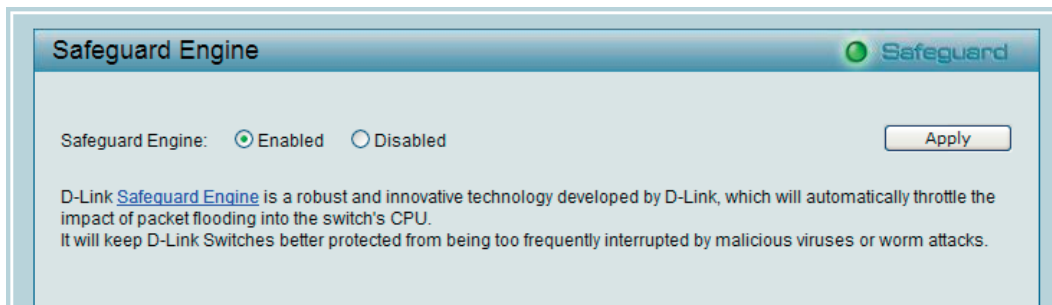


図 5-62 Safeguard Engine 画面

「Enabled」(有効) または「Disabled」(無効) を選択後、「Apply」ボタンをクリックし、設定を有効にします。

Port Security (ポートセキュリティ)

ポートセキュリティは、ポートのロックを行う前にソース MAC アドレスを認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。

ポートやポート範囲を指定して、ダイナミックな MAC アドレス学習をロックすることにより、MAC アドレスフォワーディングテーブルへ、新しいソース MAC アドレスが追加されないよう設定することができます。

Security > Port Security の順にメニューをクリックし、以下の画面を表示します。

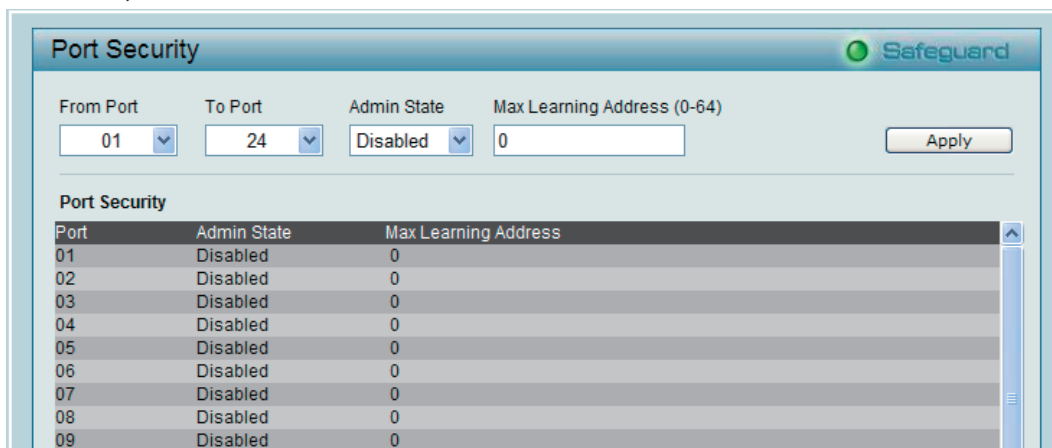


図 5-63 Port Security 画面

以下の項目を設定または表示できます。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
Admin State	ポートのロックを「Enabled」(有効) または「Disabled」(無効) にします。
Max Learning Address (80-64)	ポートが学習できる最大の MAC アドレス数を指定します。0 は MAC アドレスを学習しません。

ポート範囲を選択後、「Admin State」のプルダウンメニューで「Enabled」を選択し、「Apply」ボタンをクリックするとポートをロックできます。

802.1X (802.1X 機能の設定)

ネットワークスイッチを利用することにより、クライアント PC は接続するだけで、簡単にリソースへアクセスできるようになります。しかし、このような自動コンフィグレーション機能は、不正なユーザが簡単に侵入して重要なデータへのアクセスを行う危険性があります。

IEEE 802.1X はネットワークへのアクセス制御に関するセキュリティ標準規格で、特に Wi-Fi 無線ネットワークにおけるユーザ認証仕様として知られています。IEEE 802.1X では、ユーザの認証が完了するまでネットワークポートを切断状態にします。スイッチは EAPOL (Extensible Authentication Protocol over LANs) と呼ばれるプロトコルを使用し、ユーザとの間でユーザ名などのクライアント認証データを交換し、それをリモートの RADIUS 認証サーバに転送してアクセスのための認証を受けます。RADIUS サーバから送信される EAP パケットにも使用する認証方法が格納されています。クライアントは認証方法を拒否し、クライアントのソフトウェアと RADIUS サーバのコンフィグレーションに応じた他の認証方法を要求することができます。認証結果に応じて、そのポートをユーザに開放するか、ユーザのネットワークへのアクセスを拒否するかを決定します。

管理者は RADIUS サーバを利用したユーザリストの収集、記録を行うことで、ネットワーク管理を簡素化できます。

802.1X Settings (802.1X 設定)

Security > 802.1X > 802.1X Settings の順にメニューをクリックし、以下の画面を表示します。

図 5-64 802.1X Settings 画面

802.1X 機能は初期値では無効です。セキュリティに EAP を使用する場合は、はじめに「Enabled」を選択して「802.1X Global Settings」セクションの RADIUS サーバなどの認証情報を入力します。

項目	説明
802.1X Global Settings	
Radius Server IP	RADIUS サーバの IP アドレスを指定します。
Key	RADIUS サーバのキーに照合するパスワードを入力します (マスク表示されます)。
Confirm Key	確認のためにキーを再入力します。
TxPeriod (1-65535 sec)	スイッチがクライアントからの EAP-request/identity フレームへの応答を待つ時間 (秒)。本時間経過後に Request の再送信を行います。初期値は 24 (秒) です。
ReAuthEnabled	クライアントの周期的な再認証を「Enabled」有効または「Disabled」(無効) にします。802.1X 機能が有効の場合、本機能も初期値で「Enabled」です。
QuietPeriod (0-65535 sec)	クライアントとの間での認証が失敗した後の該当インタフェースでの非認証状態 (認証処理を行わない状態) の保持時間 (秒)。初期値は 80 (秒) です。
SuppTimeout (1-65535 sec)	スイッチからクライアントに送出する EAP-request に対してのクライアントからの応答待ち時間。この間に応答がない場合は EAP-request を再送信します。初期値は 12 (秒) です。
ServerTimeout (1-65535 sec)	スイッチがクライアントからの応答を待つ時間。この間に応答がない場合は認証サーバに応答を再送信します。初期値は 16 (秒) です。
MaxReq (1-10)	SuppTimeout 値を超えた際にスイッチが EAP-request パケットをクライアントに送出する最大回数です。再送回数が本値を超えた場合、認証失敗と判定されます。初期値は 5 回です。
ReAuthPeriod (1-4294967295 sec)	認証成功後、クライアントの再認証を行う周期です。クライアントの周期的な再認証 (ReAuthEnabled) が有効とされた場合のみ使用されます。初期値は 3600 (秒) です。

項目	説明
802.1X Port Access Control	
From Port / To Port	制御するポート範囲を指定します。
Control	<p>ポートの認証状態を制御します。</p> <ul style="list-style-type: none"> Force Authorized - 802.1X を無効にし、認証情報の交換を要求せずにポートを Authorized 状態にします。この時ポートではクライアントの 802.1X ベースの認証を行うことなく、通常のトラフィックの送受信が可能になります。 Force Unauthorized - 対象ポートは Unauthorized 状態を貫き、すべてのクライアントからの認証要求を無視します。スイッチはインタフェースを通したクライアントの認証サービスを行いません。 Auto - 802.1X を有効にし、Unauthorized 状態を開始し、ポートにおいて EAPOL フレームのみの送受信を許可します。認証プロセスは、ポートのリンク状態が Down から Up に遷移した時、または EAPOL-start フレームが受信された時に開始されます。スイッチはクライアントの ID を要求し、クライアントと認証サーバとの間で認証メッセージの中継を開始します。(初期値)

「Apply」ボタンをクリックし、設定を有効にします。

MAC Address Table (MAC アドレステーブル)

Static MAC (スタティック MAC)

ここでは 2 つの異なる機能を提供しています。上の欄では、ポートがアップリンクスイッチ (DHCP サーバ等) に接続していない場合に MAC アドレスの自動学習を行わないように設定できます。初期値は「Off」(自動学習は有効)です。

Security > MAC Address Table > Static MAC の順にメニューをクリックし、以下の画面を表示します。

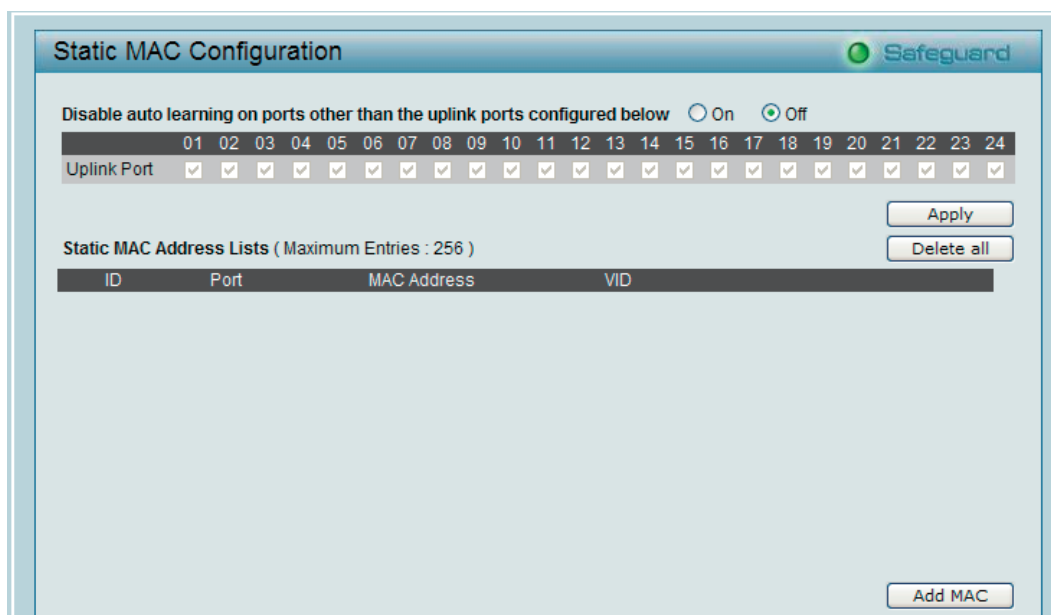


図 5-65 Static MAC Configuration 画面

指定アップリンクポートに対して MAC 自動学習機能を無効にするため、はじめに「On」を選択し、自動学習を無効にするポートを選択して「Apply」ボタンをクリックします。「Static MAC Address Lists」には接続する MAC アドレスと VID が表示されます。

新しい MAC アドレスエントリを追加するためには、「Add MAC」ボタンをクリックし、以下の画面を表示します。

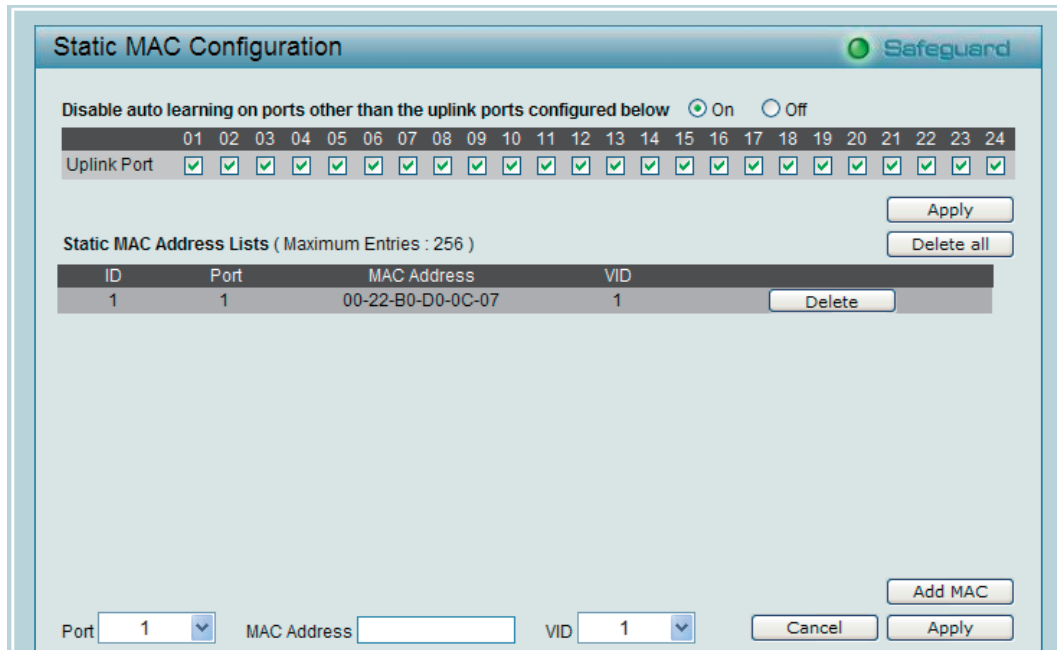


図 5-66 Static MAC Configuration 画面 - Add MAC

「Port」（ポート番号）を選択し、「MAC Address」（MAC アドレス）と「VID」を入力して「Apply」ボタンをクリックします。

エントリを削除する場合は、「Delete」ボタンをクリックします。

学習した MAC アドレスを Dynamic Forwarding Table からコピーすることも可能です。（Security > MAC Address Table > Dynamic Forwarding Table の順にクリックして詳細を参照してください。）

Auto Learning 機能を無効にしてスタティック MAC アドレスを指定すると、スイッチは不法な MAC アドレスからのトラフィックを送信しなくなるため、ハッカーなどの潜在的な脅威からネットワークを保護します。

Dynamic Forwarding Table（ダイナミックフォワーディングテーブル）

本リストには、スイッチの各ポートを通過するパケットの送信元 MAC アドレスを表示します。

Security > MAC Address Table > Dynamic Forwarding Table の順にメニューをクリックし、以下の画面を表示します。

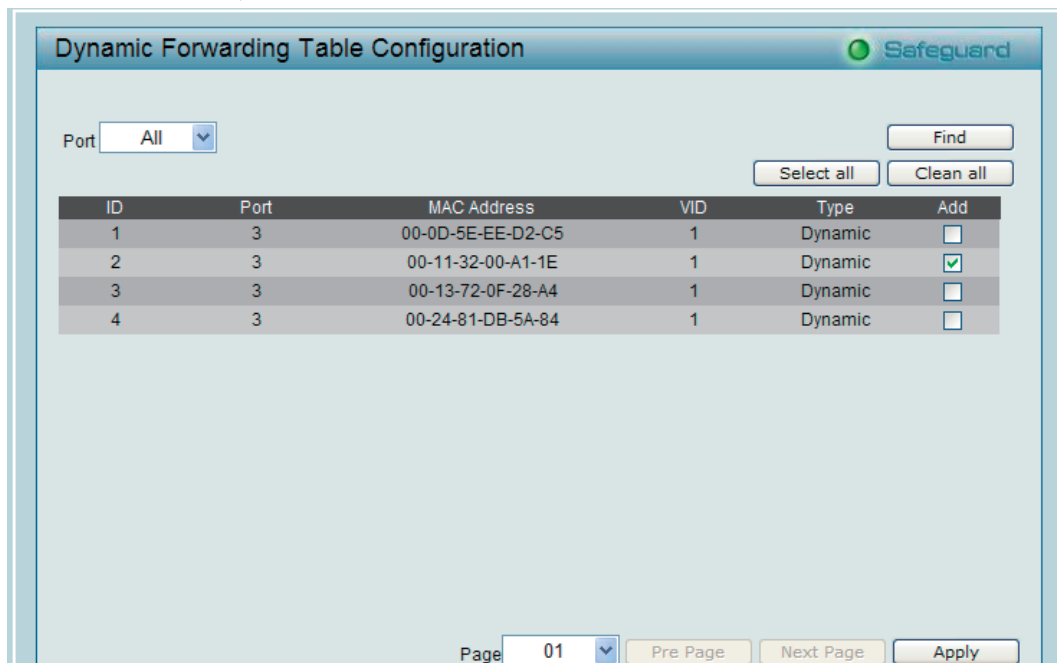


図 5-67 Dynamic Forwarding Table Configuration 画面

特定の MAC アドレスをスタティック MAC アドレスリストに追加するためには、該当するエントリの「Add」チェックボックスをクリックします。「Apply」ボタンをクリックし、設定を有効にします。

Monitoring (スイッチのモニタリング)

以下は、Monitoring のサブメニューの説明です。

サブメニュー	説明	参照ページ
Statistics	ポートの packets カウント統計情報を表示します。	74 ページ
Cable Diagnostics	スイッチに接続しているケーブルの診断をします。	75 ページ
System Log	システムログを表示します。	76 ページ

Statistics (統計情報)

各ポートの packets カウント統計情報を表示します。

Monitoring > Statistics の順にメニューをクリックし、以下の画面を表示します。

Port	TxOK	RxOK	TxError	RxError
1	0	0	0	0
2	0	0	0	0
3	687	586	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0

図 5-68 Statistics 画面

以下の項目を設定および表示します。

設定項目	説明
Refresh All	収集された統計情報を更新して表示します。
Clear All Counters	カウンタをリセットします。
TxOK	正常に送信されたパケット数。
RxOK	正常に受信されたパケット数。
TxError	エラーが発生した送信パケット数。
RxError	エラーが発生した受信パケット数。

各ポートについての詳細な統計情報を表示するためには、ポート番号のリンクをクリックし、以下の画面を表示します。

TX		RX	
OutOctets	422061	InOctets	82684
OutUcastPkts	735	InUcastPkts	606
OutNUcastPkts	3	InNUcastPkts	25
OutErrors	0	InDiscards	0
LateCollisions	0	InErrors	0
ExcessiveCollisions	0	FCSErrors	0
InternalMacTransmitErrors	0	FrameTooLongs	0
		InternalMacReceiveErrors	0

図 5-69 Port Statistic 画面

以下の項目を設定および表示します。

設定項目	説明
Refresh	収集された情報を更新して表示します。
Clear Counter	表示内容をリセットします。
Previous Page	メインページに戻ります。

Cable Diagnostics (ケーブル診断)

スイッチに接続しているケーブルをテストします。イーサネットケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。

Monitoring > Cable Diagnostics の順にメニューをクリックし、以下の画面を表示します。

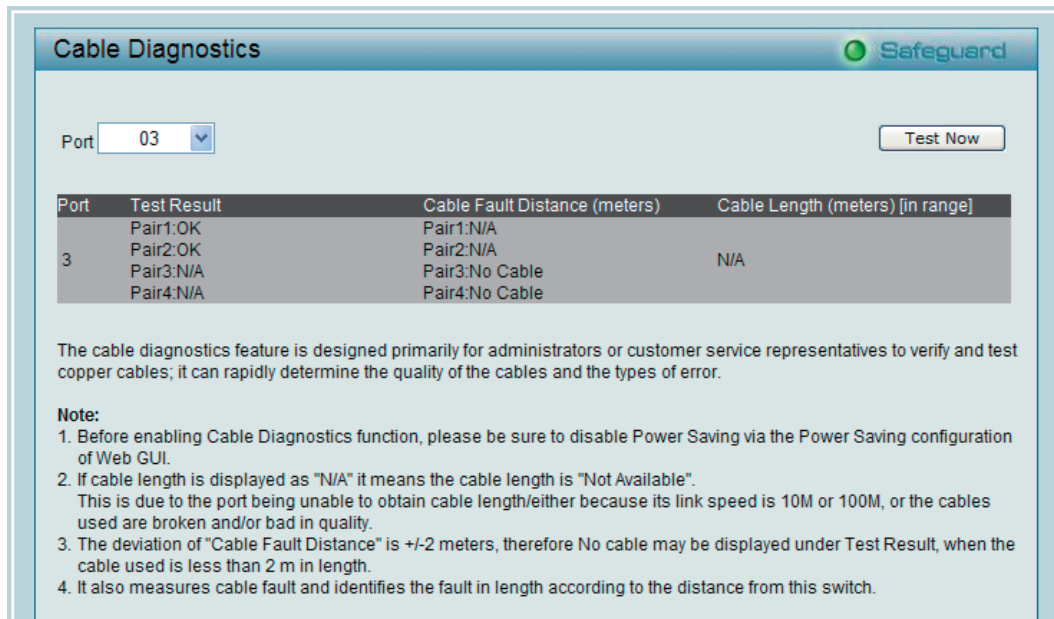


図 5-70 Cable Diagnostic 画面

ポートを選択し、「Test Now」ボタンをクリックして診断を行います。テーブルに結果が表示されます。

以下の項目を設定および表示します。

設定項目	説明
Test Result	ケーブル診断の結果を説明します。以下のテスト結果が表示されます。 <ul style="list-style-type: none"> OK - ケーブルに問題がありません。 エラーの場合、以下の可能性があります。 <ul style="list-style-type: none"> Open in Cable - UTP ケーブルが断線しているか、あるいはただ単に接続が外れていることを示します。 Short in Cable - UTP ケーブルがどこかでショートしていることを示します。 Test Failed - ケーブル診断中に他のエラーが発生したことを示します。再度同じポートを選択して診断を行ってください。
Cable Fault Distance (meters)	スイッチポートからケーブル故障点までの距離を示しますが、ケーブルが 2 メートル未満の場合は「No Cable」と表示されます。
Cable Length (meter)	診断結果でケーブルが「OK」の場合、ケーブルの全長を示します。ケーブルの長さは以下の 4 つに分類されます。50 メートル未満、50 ～ 80 メートル、80 ～ 100 メートル、100 メートル以上。

注意 ケーブル長の検出機能をサポートしているのはギガビットポートのみです。

注意 ケーブル診断機能を使用する時は、事前に省電力機能を無効にしてください。

System Log (システムログ)

Web マネージャでは、デバイスの起動、ポートの動作方法、ユーザのログインした時間、セッションがタイムアウトした時間などのシステム情報を含むスイッチのヒストリログを表示します。

Monitoring > System Log の順にメニューをクリックし、ヒストリログの表示を行います。

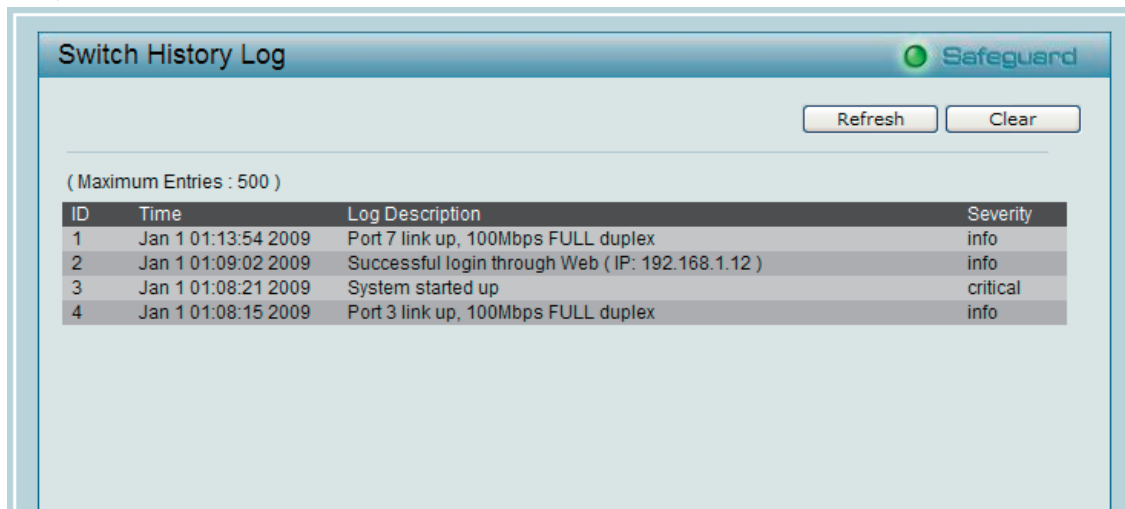


図 5-71 System Log 画面

以下の項目が表示されます。

項目	説明
ID	記録されたシステムログエントリの番号です。最大数は 500 です。
Time	スイッチに発生したイベントの日時を表示します。
Log Description	ヒストリログエントリを発生させたイベントに関する説明を表示します。
Severity	ヒストリログエントリの重要性レベルを表示します。

「Refresh」をクリックし表示ページを更新します。「Clear」をクリックすると全てのログエントリが消去されます。

ACL メニュー (ACL 機能の設定)

以下は、ACL のサブメニューの説明です。

サブメニュー	説明	参照ページ
ACL Configuration Wizard	ACL 設定ウィザード (ACL Configuration Wizard) で ACL の設定を行います。	77 ページ
Access Profile List	アクセスプロファイルリストを表示、編集します。	78 ページ
ACL Finder	ACL エントリを検索します。	81 ページ

ACL Configuration Wizard (ACL 設定ウィザード)

アクセスコントロールリスト (ACL) により、パケットヘッダの中の情報に従ってスイッチがパケット送信を決定するための基準を設定できるようになります。この基準は MAC アドレスや IP アドレスをベースに設定することができます。

ACL 設定ウィザードは、アクセスプロファイルと ACL ルールの新規作成を行います。ACL ウィザードは自動的にアクセスルールとプロファイルを作成します。本製品が使用できるプロファイルは最大 50 個、それに適用するルールは合計 240 個です。

ACL > ACL Configuration Wizard の順にメニューをクリックし、以下の画面を表示します。



図 5-72 ACL Configuration Wizard 画面

本画面には以下の項目があります。

項目	説明
From / To	プルダウンメニューを使用して、「MAC Address」、「IPv4 Address」または「Any」を選択し、対応するアドレスを指定します。 <ul style="list-style-type: none"> Any - 送信元の種類に関わらず ACL を適用します。 MAC Address - MAC アドレスから送信されたパケットを対象に ACL を適用します。 IPv4 Address - IPv4 アドレスから送信されたパケットを対象に ACL を適用します。
Service Type	<ul style="list-style-type: none"> Any - サービスの種類に関わらず全てのパケットに ACL を適用します。 EtherType - フィルタするパケットのイーサネットタイプ指定します。 ICMP All - すべての ICMP パケットに ACL を適用します。 IGMP - IGMP メッセージの種類により IGMP パケットがフィルタされます。 TCP All - 全てのパケットに ACL が適用されます。 TCP Source Port - TCP 送信ポートからのパケットを照合します。 TCP Destination Port - TCP 宛先ポートからのパケットを照合します。 UDP All - 全ての UDP パケットに ACL が適用されます。 UDP Source Port - UDP 送信ポートからのパケットを照合します。 UDP Destination Port - UDP 宛先ポートからのパケットを照合します。
Action	<ul style="list-style-type: none"> Permit - スイッチはアクセスプロファイルに一致するパケットの送信を、以下の欄で設定する追加のルールに従って行います。 Deny - スイッチはアクセスプロファイルに一致するパケットの送信を行いません。
Ports	適用するポート範囲を設定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 ACL ルールに矛盾がある場合、ルール ID が小さい方が優先されます。

注意 ACL ルールを設定する場合、不適切な ACL ルールは管理アクセス障害を引き起こす可能性があるので注意してください。

Access Profile List (アクセスプロファイルリスト)

アクセスプロファイルを使用することにより、各パケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定することができます。

現在のアクセスプロファイルを表示するには **ACL > Access Profile List** の順にメニューをクリックし、以下の画面を表示します。ここでは、各タイプに1つのアクセスプロファイルが説明のために作成されています。

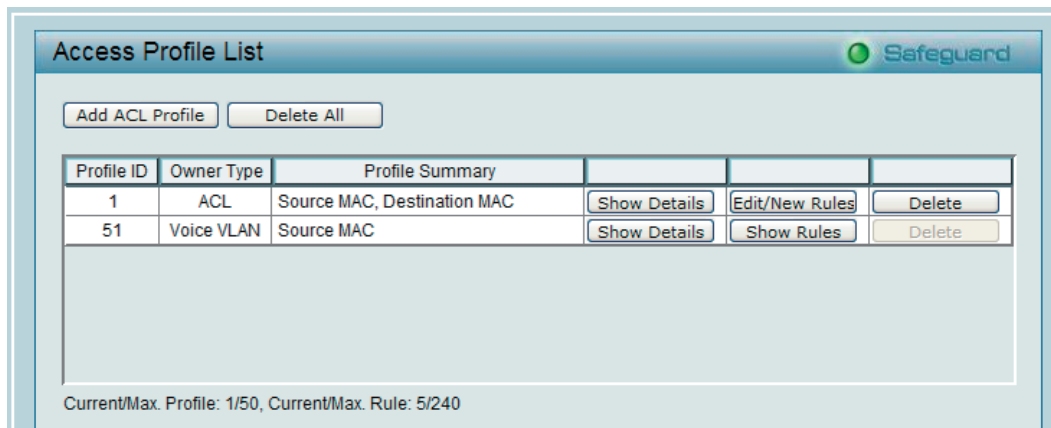


図 5-73 Access Profile List 画面

Access Profile List 画面は以下の内容になります。

項目	説明
Profile ID	プロファイル ID 番号を表示します。設定可能な ID 番号は 1 ~ 50 になります。「51」は音声 VLAN 専用の ID になります。
Owner Type	ACL プロファイルのオーナーの種類（「ACL」または「Voice VLAN」）を表示します。
Profile Summary	プロファイルの概要を表示します。
Show Details	ACL プロファイルの詳細を表示します。詳細内容は ACL テーブルの下部に表示されます。
Show Rules	ACL プロファイルのルールを表示します。
Edit / New Rules	ACL プロファイルのルールを作成 / 編集します。新しいルールを作成する場合は「Access Rule List」を参照してください。
Delete	ACL プロファイルを削除します。

アクセスプロファイルリストにエンTRIESを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

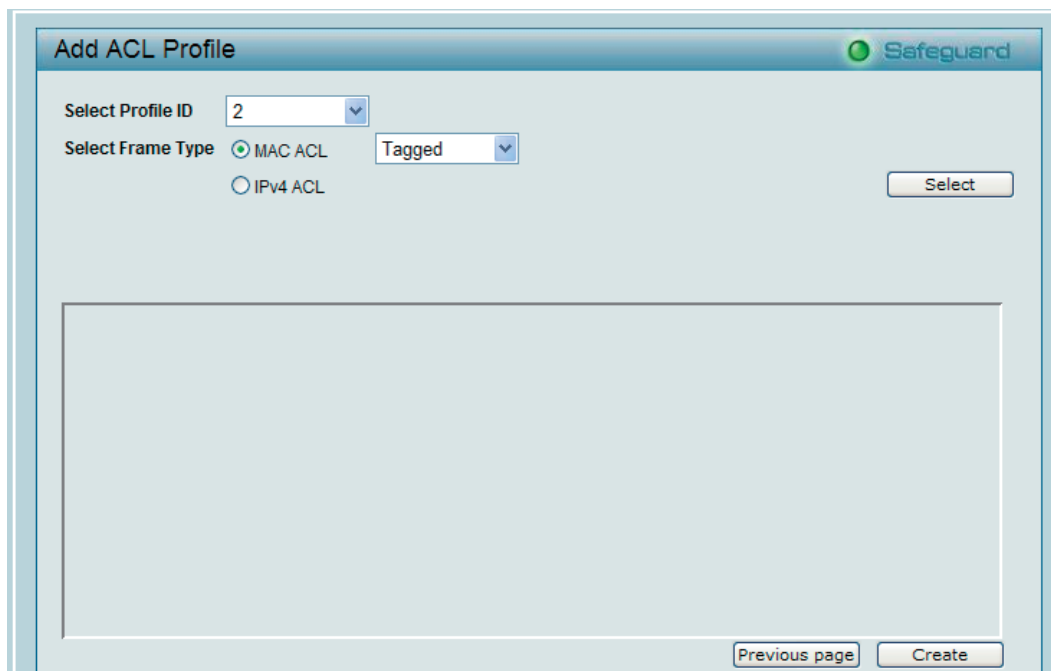


図 5-74 Add ACL Profile - Ethernet ACL 画面

以下の手順でアクセスプロファイルを追加します。

1. 「Select Profile ID」と「Select Frame Type」(「MAC ACL」または「IPv4 ACL」) を選択後、「Untagged/Tagged」(MAC ACL) または「ICMP/IGMP/TCP/UDP」(IPv4 ACL) を選択します。「Select」ボタンをクリックして以下の画面を表示します。

図 5-75 Add ACL Profile 画面

2. ページ下部に表示される関連項目などを選択します。フィルタリングマスクを入力し、「Create」をクリックします。フィルタリングマスクにはチェックする数値を設定します。例えば、「192.168.1.0/24」のネットワークをチェックする場合、IP マスクは「255.255.255.0」として入力します。

図 5-76 Add ACL Profile 画面

3. 「Profile ID」が作成されるとメインの「Access Profile List」ページに戻ります。「Edit/New Rules」ボタンをクリックして、「Access Rule List」ページを表示します。

図 5-77 Access Rule List 画面

以下の項目が表示されます。

項目	説明
Profile ID	プロファイル ID 番号を示します。
Access ID	アクセスルール ID 番号を示します。
Profile Type	プロファイルの種類を示します。
Summary	アクセスルールの概要を表示します。
Action	アクセスルールの動作を示します。

新しいルールを追加するには「Add Rule」ボタンをクリックし、以下の画面を表示します。

図 5-78 Add Access Rule 画面

「Profile Information」セクションでは追加するルールの情報が表示されます。「Profile ID」と他の設定項目が表示されます。

「Rule Details」セクションではアクセスルールの詳細について設定します。以下の項目を設定します。

項目	説明
Access ID	プロファイル設定のための固有の識別番号を指定します。1 から 65535 が指定できます。
Type	ルールの種類を表示します。
VLAN ID	設定済みの VLAN ID を入力します。
Destination MAC Address	宛先 MAC アドレスを指定します。
Source MAC Address	送信元 MAC アドレスを指定します。
802.1P	802.1p プライオリティの値を指定します。
Ether Type	イーサネットタイプ値を設定します。
Destination IP Address	宛先 IP アドレスを指定します。
Source IP Address	送信元 IP アドレスを指定します。
DSCP	DSCP の値を指定します。
IP Protocol	IP 上のプロトコルです。「ICMP」「IGMP」「TCP」「UDP」からなります。
ICMP Type	ICMP パケット種類を指定します。
ICMP Code	ICMP パケットコードを指定します。
IGMP Type	IGMP パケット種類を指定します。
Source Port	TCP/UDP 送信元ポートを指定します。
Destination Port	TCP/UDP 宛先ポートを指定します。
TCP Flag	TCP フラグ値を指定します。チェックすると「Urg」、「Ack」、「Psh」、「Rst」、「Syn」、「Fin」のフラグを設定することができます。それぞれのステータスをさらに選択します。 <ul style="list-style-type: none"> Don't Care - フィルタリングプロセスに影響を与えません。 Set - パケットのフィルタリングを有効にします。 Unset - パケットのフィルタリングを無効にします。
Ports	アクセスルールを適用するスイッチポートを指定します。
Action	<ul style="list-style-type: none"> Permit - アクセスプロファイルに一致したパケットを転送します。 Deny - アクセスプロファイルに一致しないパケットは転送せずに廃棄します。

「Apply」ボタンをクリックし、設定内容を適用します。

注意 スイッチはアクセス ID の小さなルールから接続を開始するので、期待する結果になるように、ID の割り当ては慎重に行ってください。

既存のアクセスルールを編集するにはアクセス ID のハイパーリンクをクリックします。

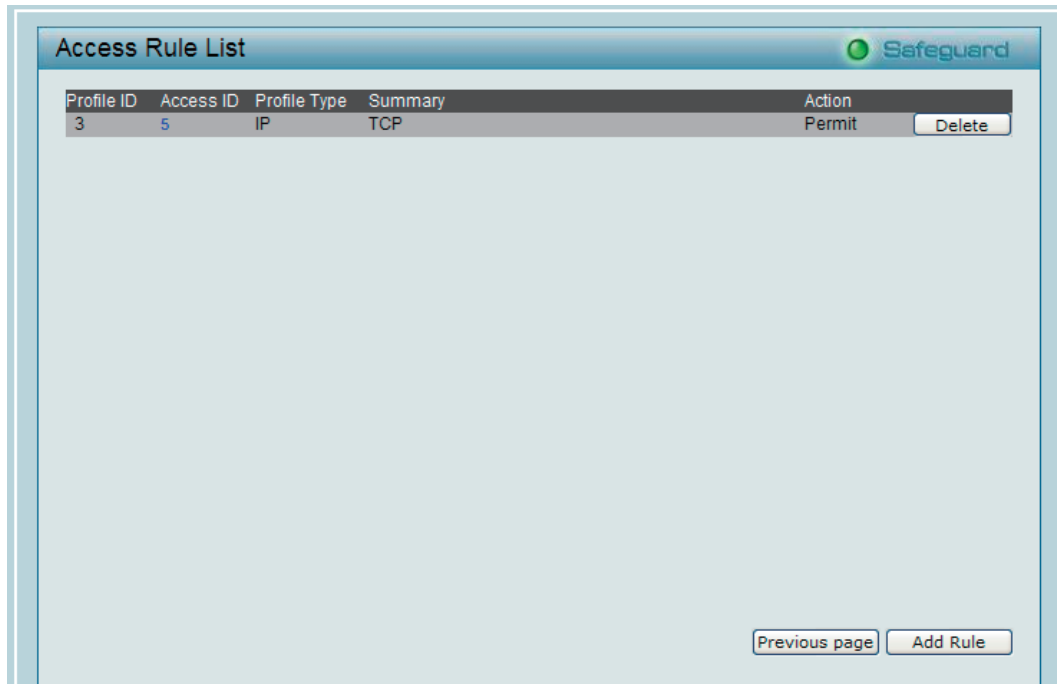


図 5-79 Access Rule List 画面

ACL Finder (ACL エントリの検索)

設定済みの ACL エントリの検索を行います。

ACL > ACL Finder の順にメニューをクリックし、下記画面を表示します。

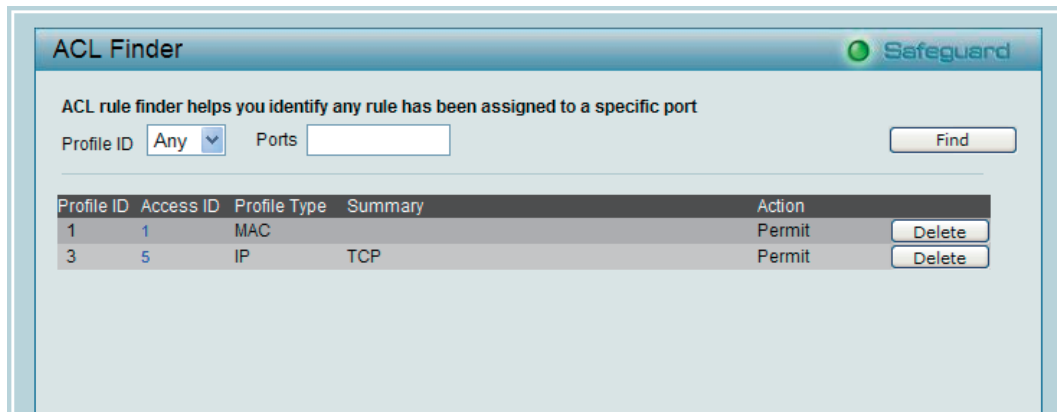


図 5-80 ACL Finder 画面

エントリの検索にはプルダウンメニューからプロファイル ID を入力して表示するポートを選択後、「Find」ボタンをクリックします。テーブル下部にエントリが表示されます。エントリを削除するには「Delete」ボタンをクリックします。

PoE メニュー（PoE の設定）（DGS-1210-10P/GE のみ）

以下は、PoE のサブメニューの説明です。

サブメニュー	説明	参照ページ
PoE Port Settings	PoE の有効 / 無効などポートにおける PoE 機能の設定を行います。	82 ページ
PoE System Settings	PoE ステータスを表示します。	83 ページ

PoE Port Settings（PoE ポート設定）

DGS-1210-10P/GE は、IEEE 802.3af 標準規格で定義される PoE（Power over Ethernet）をサポートします。1-8 番ポートは、カテゴリ 5 またはカテゴリ 3 の UTP イーサネットケーブル経由で受電機器に 54VDC の電力を供給します。DGS-1210-10P/GE は標準の PSE（Power Source over Ethernet）のピン配列 Alternative A に従い、電源出力は 1、2、3、6 番ピンで行われます。

DGS-1210-10P/GE は、弊社の IEEE 802.3af および IEEE 802.3at 準拠製品すべてに給電することができます。また、PoE モードの場合、PoE アダプタ DWL-P50 を経由させることにより、IEEE 802.3af 非対応の弊社無線アクセスポイント、IP カメラおよび IP 電話などの機器にも給電可能です。

IEEE 802.3af は、PSE（給電機器）が以下の電力クラスに応じた給電を行うことを定義しています。

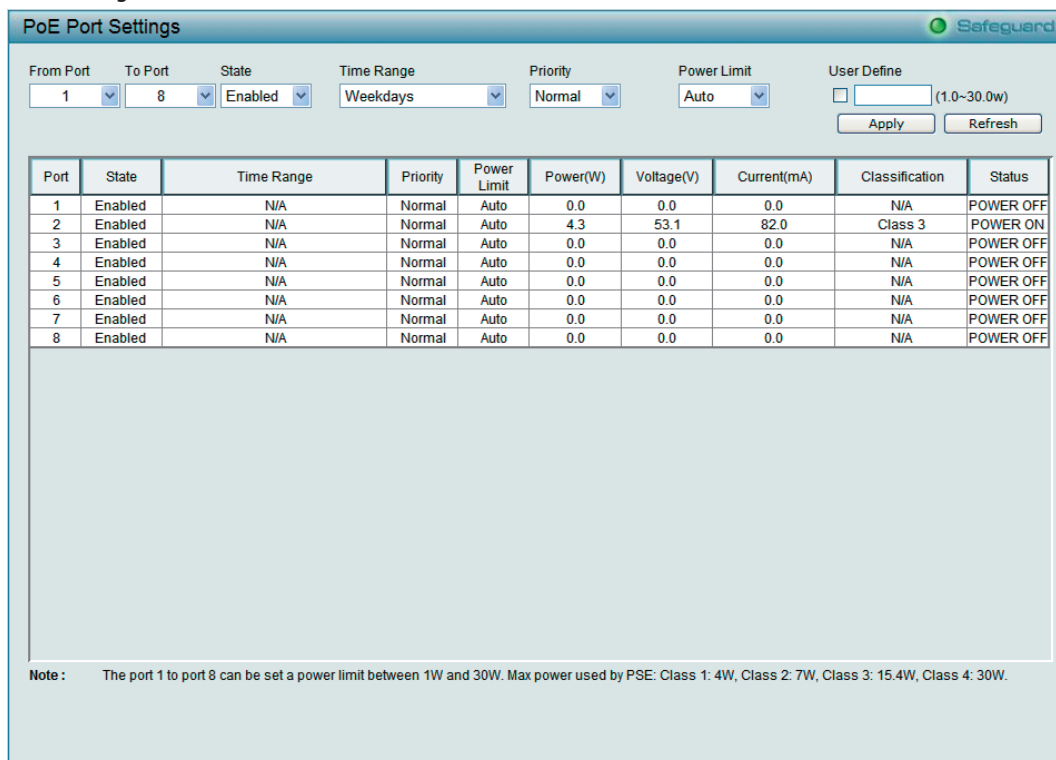
クラス	用途	PSE の最大出力電力
0	初期値	15.4W
1	オプション	4.0W
2	オプション	7.0W
3	オプション	15.4W
4	予約	30W

PoE ポートテーブルには、ポートの PoE 状態（有効 / 無効）、最大電力、電力（W）、電圧（V）、電流（mA）、分類、ポートの状態など PoE の状態が表示されます。「From Port」 / 「To Port」を選択してポートの PoE 機能を制御することができます。本製品は、ポートの電流値が 802.3af モードで 375mA 以上、または pre-802.3at モードで 625mA 以上になると、他のポートはアクティブのまま、自動的にそのポートを無効にします。

注意 電力(W)、電圧(V)、電流(mA)には接続する PD デバイスの電力消費情報が表示されます。情報を更新するためには「Refresh」ボタンをクリックしてください。

PoE ポートの設定を行います。

PoE > PoE Port Settings の順にメニューをクリックし、以下の画面を表示します。



PoE Port Settings Safeguard

From Port: 1 To Port: 8 State: Enabled Time Range: Weekdays Priority: Normal Power Limit: Auto User Define: (1.0-30.0w) Apply Refresh

Port	State	Time Range	Priority	Power Limit	Power(W)	Voltage(V)	Current(mA)	Classification	Status
1	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
2	Enabled	N/A	Normal	Auto	4.3	53.1	82.0	Class 3	POWER ON
3	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
4	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
5	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
6	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
7	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
8	Enabled	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF

Note: The port 1 to port 8 can be set a power limit between 1W and 30W. Max power used by PSE: Class 1: 4W, Class 2: 7W, Class 3: 15.4W, Class 4: 30W.

図 5-81 PoE Port Settings 画面

以下の設定項目を設定します。

設定項目	説明
From Port/ To Port	PoE 機能を設定するポートまたはポート範囲を 1-8 ポートから選択します。
State	「Enabled」(有効) または 「Disabled」(無効) を選択して、指定したポートに PoE 機能を設定します。初期値は「Enabled」です。
Time Range	指定したポートにタイムベース PoE 機能を設定します。初期値は N/A です。タイムレンジ設定で登録した PoE タイムプロファイルを選択します。詳しくは、「 Time Range Settings (タイムレンジ設定) 」(84 ページ) を参照してください。
Priority	指定ポートの電力供給優先順位を「Low」、「Normal」および「High」で指定します。初期値は「Normal」です。
Power limit	接続する PD デバイスに適用する給電量の制限を設定します。本機能により、過負荷発生時にはそのポートの PoE 機能が無効になり、本製品と接続する PD デバイスを保護します。「Class 1」(4W)、「Class 2」(7W)、「Class 3」(15.4W)、「Class 4」(30W) または「Auto」から選択します。「Auto」を指定すると接続デバイスとネゴシエーションを行い IEEE 802.3at に基づいた判断が行われます。
User Define	ボックスをチェックして電力 (1-30W) を入力し、手動でポートの電力の上限値を割り当てます。

「Apply」ボタンをクリックし、設定を有効にします。

注意 電力(W)、電圧(V)、電流(mA)には接続する PD デバイスの電力消費情報が表示されます。情報を更新するためには「Refresh」ボタンをクリックしてください。

PoE System Settings (PoE システム設定)

システム総供給可能電力、総電力、残電力量およびシステム電力供給率を含む PoE ステータスを表示します。本スイッチにグローバルな PoE 設定を行います。

PoE > PoE System Settings の順にメニューをクリックし、以下の画面を表示します。

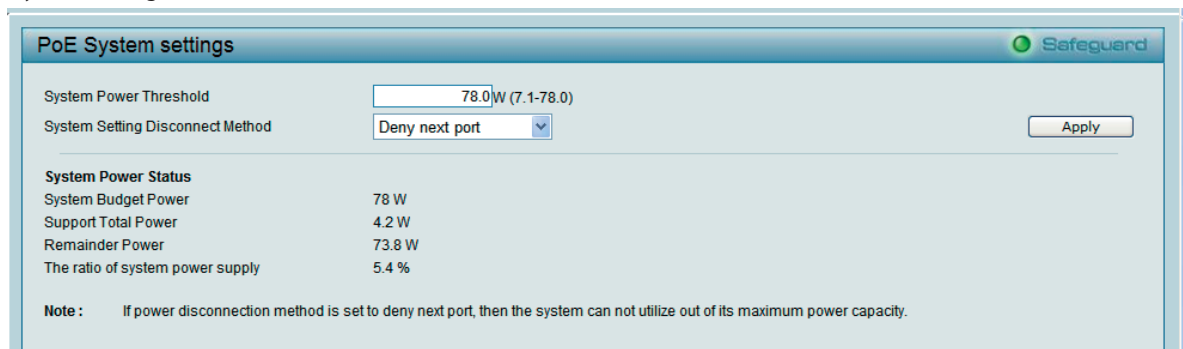


図 5-82 PoE System settings 画面

以下の項目を設定または表示します。

設定項目	説明
System Power Threshold	システムの給電可能電力を手動で入力します。範囲は 7.1-78.0 (W) です。初期値は 78.0 (W) です。
System Setting Disconnection Method	PoE 電力管理モードを設定します。システムの給電可能電力が電力を供給するために十分でない場合、電力管理ポリシーにより優先度の低いポートへの給電を停止します。本製品には 2 つのポリシーがあります。 <ul style="list-style-type: none"> Deny next port - 先にプラグインしたポートの優先度が高く、後でプラグインしたポートの優先度は低くなります。(初期値) Deny low priority port - 「PoE Port Settings」画面で設定したポート優先度設定に適用されます。
System Power Status	
System Budget Power	総供給可能電力を表示します。
Support Total Power	総供給電力を表示します。
Remainder Power	残電力を表示します。
The ratio of system power supply	給電率を表示します。

「Apply」ボタンをクリックし、設定を有効にします。

注意 電力管理ポリシーは、PoE システムが周波数保護モード (0 < 電力残量 <= 7) の時にのみ有効です。

Time-Based PoE メニュー（タイムベース PoE の設定）

Time Range Settings（タイムレンジ設定）

タイムベース PoE を設定します。

PoE 機能に関連付けて使用し、スイッチポートの PoE 機能が有効の場合に曜日ごとに電力供給時間の範囲を決定します。その時間範囲の設定が PoE ポートに適用されます。

Time-Based PoE > Time Range Settings の順にメニューをクリックし、以下の画面を表示します。

図 5-83 Time Range Settings 画面

以下の項目を設定または表示します。

設定項目	説明
Range Name	タイムレンジプロファイル名。
Date	プロファイルを使用する特定の日付があれば、チェックボックスを選択します。「From Day」および「To Day」プルダウンメニューから指定する範囲を選択します。
Hours	「Start Time」および「End Time」のプルダウンメニューから時間範囲を選択します。 注意 「End Time」を「Start Time」より前に設定した場合、「End date」は翌日に設定されます。
Weekdays	チェックボックスを使用して、タイムレンジプロファイルに適用したい曜日をチェックします。「Select All Days」をチェックすると、すべての曜日が選択されます。

「Apply」ボタンをクリックし、設定内容を適用すると、「Time Range Information」テーブルに表示されます。

タイムレンジの編集

「Time Range Information」テーブルで編集する「Range Name」の「Edit」ボタンをクリックし、以下の編集画面を表示します。

図 5-84 Time Range Settings 画面 - 編集

タイムレンジ編集後、「Apply」ボタンをクリックして、設定を適用します。

タイムレンジの削除

「Time Range Information」テーブルで削除する「Range Name」の「Delete」ボタンをクリックします。

LLDP (LLDP 設定) (DGS-1210-10P/GE のみ)

以下は、LLDP のサブメニューの説明です。

サブメニュー	説明	参照ページ
LLDP Global Settings	LLDP のグローバル設定を行います。	85 ページ
LLDP Remote Port Information	LLDP リモートポート情報を表示します。	86 ページ
LLDP MED Settings	指定ポートに対して PSE TLV タイプを有効にします。	86 ページ

LLDP Global Settings (LLDP グローバル設定)

本スイッチは IEEE 802.1AB に準拠した LLDP (Link Layer Discovery Protocol) に準拠しています。本方法では LLDP 対応デバイス同士が隣接する LLDP デバイスに自分自身についての情報を通知し合いお互いを認識します。本スイッチではこれらの情報を MIB (Management Information Base) に保存し、SNMP ユーティリティが各 LLDP デバイスの MIB 情報を取得することでネットワークトポロジを把握します。初期値では LLDP 機能は有効です。

オプションの D-Link Smart WLAN マネージャを使用すると、DGS-1210-10P/GE、DWL-3140AP の中央管理および検出を行うことができます。

LLDP > LLDP Global Settings の順にメニューをクリックし、以下の画面を表示します。

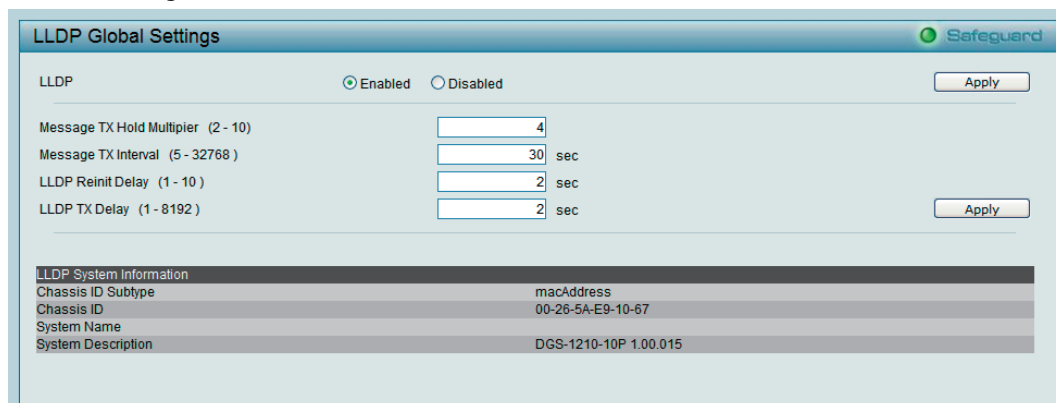


図 5-85 LLDP Global Settings 画面

以下の項目を設定または表示します。

設定項目	説明
LLDP	本機能を有効にすると、スイッチは、LLDP パケットの送受信を開始し、LLDP パケットの処理を行います。LLDP パケットの通知のために、スイッチはポートを通して情報を Neighbor に知らせます。LLDP パケットを受信するためには、スイッチは Neighbor テーブル内の Neighbor から通知された LLDP パケットより情報を学習します。「Apply」ボタンをクリックし、設定内容を適用してください。
Message TX Hold Multiplier (2-10)	LLDPDU 内の実際の TTL 値を計算するのに使用される乗数です。初期値は 4 です。
Message TX Interval (5-32768)	LLDP フレームがこの LLDP エージェントのために送信される間隔を示しています。初期値は 30 (秒) です。
LLDP Reinit Delay (1-10)	admin ステータスが「Disabled」(無効)になってから再初期化が行われるまでの遅延時間を示します。初期値は 2 (秒) です。
LLDP TX Delay (1-8192)	LLDP ローカルシステム MIB において値または状態変更によって開始される連続した LLDP フレーム伝送間の遅延を示しています。txDelay 値は以下の公式によって設定されます。 $1 < \text{txDelay} < (0.25 \times \text{msgTxInterval})$ 初期値は 2 (秒) です。

LLDP Remote Port Information (LLDP リモートポート情報)

「LLDP Remote Port Brief Table」を表示します。追加情報を表示するためには、「Show Normal」をクリックします。

LLDP > LLDP Remote Port Information の順にメニューをクリックし、以下の画面を表示します。



図 5-86 LLDP Remote Port Information 画面

「Port」を「All」または 01-10 から選択後、「Find」ボタンをクリックします。下部のテーブルにエントリが表示されます。

LLDP MED Settings (LLDP MED 設定)

PSE (給電) スイッチは、指定ポートに対して PSE TLV タイプを有効にすることで、LLDP MDI TLV を経由して IEEE 802.3at ドラフト規格準拠の受電装置に高電力 (15.4-30 W) を供給するように指定することができます。本機能により、IEEE 802.3at ドラフト規格準拠の受電装置に対して詳細な電力配分を供給し、効率的な電力管理を実現することができます。

LLDP > LLDP MED Settings の順にメニューをクリックし、以下の画面を表示します。

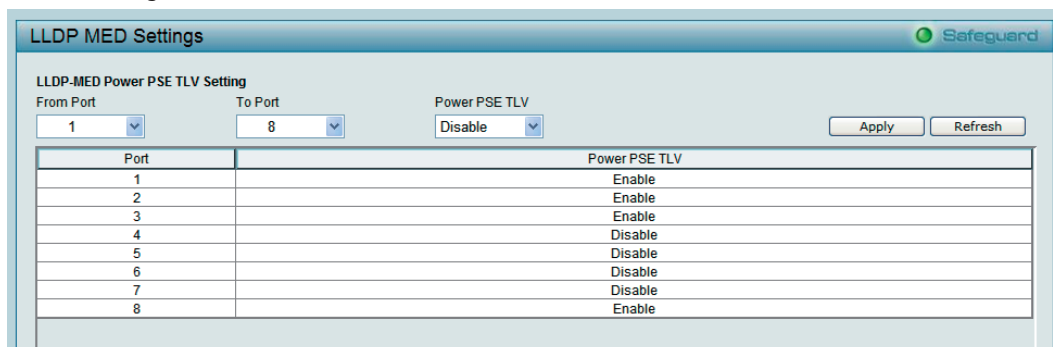


図 5-87 LLDP MED Settings 画面

ポート範囲 (「From Port」および「To Port」) を選択し、「Power PSE TLV」を「Disable」(無効) または「Enable」(有効) を選択後、「Apply」ボタンをクリックして設定を適用します。

第6章 コマンドラインインタフェース

スイッチはコマンドラインインタフェース (CLI) をサポートしており、ネットワーク上で Telnet プロトコルを使用して、基本的な管理やモニタリングを行うことができます。

接続とログイン

Telnet 経由でスイッチに接続する

1. スイッチとコンピュータがネットワークで接続していることを確認します。
2. 接続にはターミナルソフトウェア (例: Windows OS に搭載のハイパーターミナル)、またはコマンドプロンプトを使用して「telnet」コマンドを入力し、スイッチの IP アドレスを続けて入力します。(例: telnet 10.90.90.90)
3. ログインプロンプトが表示されます。

コマンドラインインタフェースにログインする

ユーザ名とパスワードを使ってログインします。ユーザ名とパスワードの初期値は「admin」です。ユーザ名とパスワードは大文字と小文字を区別します。ユーザ名とパスワードの両項目で「Enter」を押します。コマンドプロンプトが以下のように表示されます。

```
DGS-1210-24 login: admin
Password:

DGS-1210-24>
```

ログインタイムアウト時間が過ぎると自動的にログアウトします。ログインタイムアウト時間の初期値は 5 分です。ログインタイムアウト時間の変更は「[System Settings \(スイッチの基本機能の設定\)](#)」(44 ページ) を参照してください。

コマンド

CLI コマンドについて

CLI にはいくつかの有効な機能が存在します。「?」コマンドを入力してコマンドのリストを表示します。

使用例

```
DGS-1210-24> ?
USEREXEC commands :
  config account admin password <passwd>
  config ipif System { ipaddress <ip-address> <subnet-mask> gateway <gw-address>
| dhcp }
  download { firmware_fromTFTP tftp://ip-address/filename | cfg_fromTFTP tftp://
ip-address/filename }
  logout
  ping <ipaddr>
  reboot
  reset config
  save
  show ipif
  show switch
  upload { firmware_toTFTP tftp://ip-address/filename | cfg_toTFTP tftp://ip-
address/filename }
DGS-1210-24>
```

download

目的

TFTP サーバから新しいファームウェアまたはスイッチのコンフィグレーションファイルをダウンロードしてインストールします。

構文

```
download { firmware_fromTFTP tftp://ip-address/filename | cfg_fromTFTP tftp://ip-address/filename }
```

説明

TFTP サーバから新しいファームウェアまたはスイッチのコンフィグレーションファイルをダウンロードします。

パラメータ

パラメータ	説明
firmware_fromTFTP	新しいファームウェアを TFTP サーバからスイッチにダウンロードしてインストールします。 <ul style="list-style-type: none"> tftp://ip-address/ - TFTP サーバの IPv4 アドレスを指定します。 filename - TFTP サーバ上のファームウェアファイルのパスとファイル名を指定します。
cfg_fromTFTP	新しいコンフィグレーションファイルを TFTP サーバからスイッチにダウンロードしてインストールします。 <ul style="list-style-type: none"> tftp://ip-address/ - TFTP サーバの IPv4 アドレスを指定します。 filename - TFTP サーバ上のコンフィグレーションファイルのパスとファイル名を指定します。

使用例

```
DGS-1210-24> download firmware_fromTFTP tftp://192.168.1.12/dgs1210_24_fw.hex

Device will reboot after firmware upgraded successfully

Image Updated Successful
```

upload

目的

スイッチのファームウェアファイル / コンフィグレーションファイルを TFTP サーバにアップロードします。

構文

```
upload { firmware_toTFTP tftp://ip-address/filename | cfg_toTFTP tftp://ip-address/filename }
```

説明

TFTP サーバにコンフィグレーションファイルまたはファームウェアファイルをアップロードします。

パラメータ

パラメータ	説明
firmware_toTFTP	ファームウェアを TFTP サーバにアップロードします。 <ul style="list-style-type: none"> tftp://ip-address/ - TFTP サーバの IPv4 アドレスを指定します。 filename - ファームウェアファイルのパスとファイル名を指定します。
cfg_toTFTP	コンフィグレーションファイルを TFTP サーバにアップロードします。 <ul style="list-style-type: none"> tftp://ip-address/ - TFTP サーバの IPv4 アドレスを指定します。 filename - コンフィグレーションファイルのパスとファイル名を指定します。

使用例

```
DGS-1210-24> upload cfg_toTFTP tftp://192.168.1.12/conf_file_backup.cfg
DGS-1210-24>
```


config ipif system

目的

スイッチの IP アドレスを設定します。

構文

```
config ipif system { ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp }
```

説明

スイッチの IP アドレスを設定します。

パラメータ

パラメータ	説明
ipaddress <ip-address> <subnet-mask>	IP アドレスとサブネットマスクを指定します。
gateway <gw-address>	ルータの IP アドレス、またはゲートウェイを指定します。
dhcp	IP アドレスの割り当てに DHCP プロトコルを有効にします。

使用例

```
DGS-1210-24> config ipif system ipaddress 192.168.1.10 255.255.255.0 gateway
192.168.1.1
% The IP setting mode change to static will cause CLI disconnect.
```

logout

目的

接続を終了しログアウトします。

構文

```
logout
```

説明

接続を終了しログアウトします。ログアウトの前にスイッチの設定を保存しておくことをお勧めします。

パラメータ

なし

使用例

```
DGS-1210-24> logout
```

ping

目的

ネットワークデバイス間の接続性をテストします。

構文

```
ping <ipaddr>
```

説明

Ping コマンドはリモート IP アドレスに Internet Control Message Protocol (ICMP) エコーメッセージを送信します。その後、リモート IP アドレスは、「エコー」するか、またはメッセージを返します。これは、スイッチとリモートデバイス間の接続性を確認するために使用されます。

パラメータ

パラメータ	説明
<ipaddr>	ホストの IP アドレスを指定します。

使用例

```
DGS-1210-24> ping 192.168.1.12
Reply Not Received From : 192.168.1.12, Timeout : 5 secs
Reply Not Received From : 192.168.1.12, Timeout : 5 secs
Reply Not Received From : 192.168.1.12, Timeout : 5 secs
Reply Not Received From : 192.168.1.12, Timeout : 5 secs
Reply Not Received From : 192.168.1.12, Timeout : 5 secs

--- 192.168.1.12 Ping Statistics ---
5 Packets Transmitted, 0 Packets Received, 100% Packets Loss
```

reboot

目的

スイッチを再起動します。

構文

reboot

説明

スイッチを再起動します。全てのネットワーク接続は切断されます。

使用例

```
DGS-1210-24> reboot
% Device will reboot, please wait a few minutes to re-login.
```

reset

目的

スイッチを工場出荷時設定に戻します。

構文

reset config

説明

スイッチの設定を工場で割り当てられた初期設定に戻します。

パラメータ

パラメータ	説明
config	IPアドレス、ユーザアカウントなどのパラメータが工場出荷時設定にリストアされます。スイッチは保存または再起動しません。

使用例

```
DGS-1210-24> reset config
% Device will reboot after reset configuration successfully.
DGS-1210-24>
```

show ipif

目的

スイッチの現在の IP アドレスを表示します。

構文

show ipif

説明

スイッチの現在の IP モード /IP アドレス /サブネットマスク /ゲートウェイを表示します。

使用例

IP アドレスを表示します。

```
DGS-1210-24> show ipif
IP Setting Mode           : Static
IP Address                : 192.168.1.10
Subnet Mask               : 255.255.255.0
Default Gateway          : 192.168.1.1

DGS-1210-24>
```

show switch

目的

スイッチの現在の状態を表示します。

構文

```
show switch
```

説明

スイッチの現在の状態を表示します。

使用例

スイッチの状態を表示します。

```
DGS-1210-24> show switch
System name           :
System Contact        :
System Location       :
System up time        : 0 days, 0 hrs, 1 min, 16 secs
System Time           : 01/01/2009 01:09:25
System hardware version : A1
System firmware version : 1.00.015
System boot version    : 1.00.003
System Protocol version : 2.001.004
System serial number   : QB2F1A2000004
MAC Address           : 00-26-5A-F0-2D-87

DGS-1210-24>
```

config account admin password

目的

管理者パスワードを設定します。

構文

```
config account admin password <passwd>
```

説明

スイッチの管理者パスワードを設定します。

パラメータ

パラメータ	説明
<passwd>	新しい管理者パスワードを指定します。

使用例

```
DGS-1210-24> config account admin password dlink
DGS-1210-24>
```

save

目的

設定内容の変更を保存します。

構文

```
save
```

説明

設定内容の変更を保存します。

使用例

IP アドレスを表示します。

```
DGS-1210-24> save
Building configuration ...
[OK]
DGS-1210-24>
```

第7章 スwitchのメンテナンス

工場出荷時設定に戻す

リセットボタンを押下することで本製品の設定を工場出荷状態に戻します。

1. 必要に応じて設定ファイルのバックアップを行い、本製品からログアウトします。
2. 前面のリセットボタンを5秒間押下します。
この間の前面パネルのLEDステータスは以下の通りです。

LED	状態
PWR	点灯
Link/Act (リンクしている場合)	点灯

3. リセットボタンを放すと本製品は再起動します。
4. 初期化が完了すると前面パネルのLED表示は以下の通りになります。

LED	状態
PWR	点灯
Link/Act (リンクしている場合)	消灯後に点灯

注意

リセットボタンを押下する前に必ずご使用の製品の設定を保存してください。リセットボタンを押下すると、すべての設定が消去されます。

付録 A ケーブルとコネクタ

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、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。

以下の図と表は標準の RJ-45 プラグ/コネクタとピンアサインです。

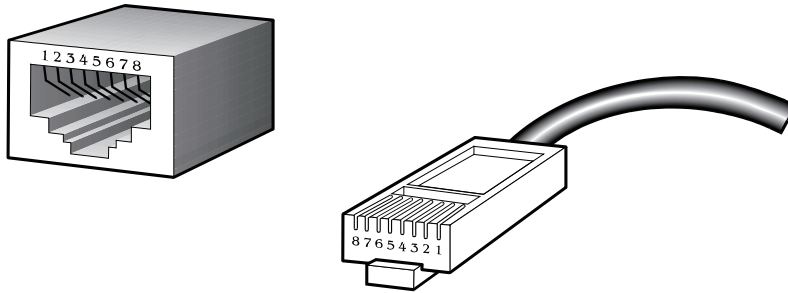


図 A-1 標準的な RJ-45 プラグとコネクタ

表 A-1 標準的な RJ-45 ピンアサイン

RJ-45 ピンアサイン		
コンタクト (ピン番号)	MDI-X 信号	MDI-II 信号
1	RD+ (受信)	TD+ (送信)
2	RD- (受信)	TD- (送信)
3	TD+ (送信)	RD+ (受信)
4	未使用	未使用
5	未使用	未使用
6	TD- (送信)	RD- (受信)
7	未使用	未使用
8	未使用	未使用

付録 B ケーブル長

以下の表は各規格に対応するケーブル長 (最大) です。

表 B-1 ケーブル長

規格	メディアタイプ	最大伝送距離
SFP	1000BASE-LX、シングルモードファイバモジュール	10km
	1000BASE-SX、マルチモードファイバモジュール	550m
	1000BASE-LH、シングルモードファイバモジュール	40km
	1000BASE-ZX、シングルモードファイバモジュール	80km
1000BASE-T	エンハンスドカテゴリ 5 UTP ケーブル カテゴリ 5 UTP ケーブル (1000Mbps)	100m
100BASE-TX	カテゴリ 5 UTP ケーブル (100Mbps)	100m
10BASE-T	カテゴリ 3 UTP ケーブル (10Mbps)	100m

付録 C 用語解説

用語	説明
1000BASE-LX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。長い光波長で長距離伝送用に使用されます。伝送距離 (最大) はシングルモード光ファイバを使用した場合で 10km。
1000BASE-SX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。短い光波長でマルチモード光ファイバを使用した場合伝送距離 (最大) は 550km。
100BASE-FX	光ファイバを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
100BASE-TX	カテゴリ 5 以上の UTP ケーブルを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
10BASE-T	IEEE 802.3 準拠でカテゴリ 3 以上の UTP ケーブルを使用する最大伝送速度 10Mbps の Ethernet の規格のひとつ。
エージング	タイムアウトし、無効のスイッチのダイナミックデータベースを自動的に消去します。
ATM	非同期転送モード。セルと呼ばれる固定長のセル (パケット) ベースで転送するプロトコル。ATM は音声、データおよびビデオ信号を含むユーザトラフィックの完全な列を転送するために開発されたものです。
オートネゴシエーション	スピード、デュプレックスおよびフローコントロールを自動的に認識する機能。オートネゴシエーションをサポートする端末と接続すると、リンクは自動的に最適なリンク条件に設定されます。
バックボーンポート	デバイスのアドレスを学習せず不明なアドレスを持つすべてのフレームを受信するポート。バックボーンポートは通常で使用するネットワークのバックボーンにスイッチを接続するために使用されるポートです。バックボーンポートは以前はダウンリンクポートとして知られていました。
バックボーン帯域	ネットワークセグメント間でトラフィックが転送される場合に優先パスとして使用されるネットワークの一部。1 秒あたりのビット数で計算される 1 チャンネルが転送できる情報量。イーサネットの帯域は 10Mbps、ファーストイーサネットは 100Mbps。
ボーレート	ラインのスイッチングスピード。ネットワークセグメント間のラインスピードとして知られています。
BOOTP	BOOTP プロトコルはデバイスが起動するたびに IP アドレスを MAC アドレスに自動マッピングします。さらにデバイスにサブネットマスク、デフォルトゲートウェイを割り当てます。
ブリッジ	たとえ高いレベルのプロトコルが関連してもローカルまたはリモートネットワークを相互接続するデバイス。ブリッジはネットワーク管理を中央に集めて 1 個の論理ネットワークを形成します。
ブロードキャスト	ネットワーク上のすべての終点デバイスに送信されるメッセージ。
ブロードキャストストーム	が主として可能なネットワーク帯域を奪い、ネットワークエラーを引き起こす Multiple simultaneous ブロードキャストストーム。
コンソールポート	端末またはモデムコネクタと接続可能なスイッチ上のポート。コンピュータ内でパラレル配列のデータをデータ転送リンクで使用されるシリアル形式に変換します。このポートはほとんどの場合ローカル管理のために使用されます。
CSMA/CD	イーサネットと IEEE 802.3 標準によって使用されるチャンネルアクセス方法で検索したデータチャンネルが一定期間後クリアされた後にだけデバイスに転送します。2 つのデバイスが同時に転送する場合、コリジョンが発生し、コリジョンが発生したデバイスは任意の時間再転送を遅らせます。
データセンタースイッチング	スイッチがサーバファームへの高パフォーマンスアクセス、高速バックボーン接続、およびネットワーク管理とセキュリティのためのコントロールポイントを提供するコアポートネットワーク内のアグリゲーションポイント
イーサネット	Xerox、Intel および DEC が共同で開発した LAN 仕様。イーサネットネットワークは CSMA/CD を使用して 10Mbps で処理を行います。
ファーストイーサネット	Ethernet/CD ネットワークアクセス方法をベースにした 100Mbps 技術。
フローコントロール	(IEEE 802.3z) 端末に接続した転送ポートへのパケットを抑制します。受信バッファがあふれそうになった場合にパケットロスを防ぎます。
フォーワーディング	中間のネットワークデバイスによりパケットを到達点に向けて送信するプロセス。
フルデュプレックス	同時にパケットの送受信を可能とし、スループットを 2 倍にするシステム。
ハーフデュプレックス	パケットの送受信を行うが、同時には行えないシステム。
IP アドレス	Internet Protocol アドレス。TCP/IP を使用するネットワークに付属するデバイスの固有な識別子。IPv4 アドレスは 8 ビットずつピリオドで区切られ、ネットワークセクション、サブネットセクション、ホストセクションで構成されます。
IPX (Internetwork Packet Exchange)	ネットワーク通信で使用するプロトコル。
LAN - ローカルエリアネットワーク	通常フロアもしくはビルのような規模の小さいエリアで PC、プリンタ、サーバのようなコンピュータリソースを接続するネットワーク。高速で低エラー率が特長です。
レイテンシ	デバイスがパケットを受信する時間とパケットが到達点ポートに転送される時間の遅延。
ラインスピード	ボーレートを参照。
メインポート	通常の場合でデータトラフィックを送信する Resilient リンク内のポート。
MDI (Medium Dependent Interface)	1 つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。
MDI-X (Medium Dependent Interface Cross-over)	接続送受信のラインが交差しているイーサネットポート接続。
MIB (Management Information Base)	デバイスの管理特性とパラメータを保持します。MIB は SNMP で使用され、管理システムの属性を持っています。スイッチは自身の内部 MIB を持っています。
マルチキャスト	シングルパケットはネットワークアドレスの特定のサブセットにコピーします。これらのアドレスはパケットの到達点アドレス内に記述されます。
プロトコル	ネットワーク上のデバイス間通信のルール。ルールは形式、タイミング、配列およびエラー制御を定義しています。
Resilient link	他のポートがエラーになった場合に一方のポートがデータ転送を引き継ぐように設定された 1 対のポート。
RJ-45	10BASE-T や 100BASE-TX などを使用する標準 8 線コネクタ
RMON	リモート監視。SNMP MIB II のサブセットはアドレッシングによって異なる最大 10 個のグループまでのモニタリングや管理を可能にします。

用語	説明
RPS (リダンダント電源システム)	スイッチに接続されて、バックアップ電源を供給するデバイス。
サーバファーム	大量のユーザにサービスを提供する中央に位置するサーバグループ。
SLIP (Serial Line Internet Protocol)	IP がシリアルライン接続を経由して動作することが可能なプロトコル。
SNMP (Simple Network Management Protocol)	当初は TCP/IP インターネットを管理するために開発されたプロトコル。SNMP は現在広範囲のコンピュータとネットワークの装置で実行され、多くのネットワークおよび端末操作の状況を管理するために使用されます。
スパニングツリープロトコル (STP)	ネットワーク上のフォールトトレランスを提供するブリッジベースのシステム。STP はネットワークトラフィックに対してパラレルパスを実行し、メインのパスにエラーが発生してもメインのパスが操作できる場合はリダンダントパスを無効にすることを保証します。
スタック	1 個の論理的なデバイスの形をとするために統合されたネットワークデバイスのグループ。
スタンバイポート	リンクしているメインポートにエラーが発生すると、Resilient リンク内のスタンバイポートはデータ転送を受け継ぎます。
スイッチ	パケットの終点アドレスを元にパケットのフィルタ、フォワードするデバイス。スイッチは各スイッチポートで関連するアドレスを学習し、この情報を元に表を作成してスイッチの決定に使用します。
TCP/IP	Telnet 端末エミュレーション、FTP ファイル転送などコンピュータ装置の広い範囲で通信サービスを提供する通信プロトコルです。
telnet	仮想端末サービスを提供する TCP/IP アプリケーションプロトコルで、ユーザが別のコンピュータシステムにログインし、ユーザが直接ホストに接続しているようにホストにアクセスすることができます。
TFTP (Trivial File Transfer Protocol)	スイッチのローカルの管理能力を使用してリモートデバイスからファイルを転送する (ソフトウェアアップグレードなど) ことができます。
UDP (User Datagram Protocol)	インターネットの標準プロトコルで、あるデバイスのアプリケーションプログラムがデータを別のデバイス上のアプリケーションプログラムに送信することができます。
VLAN (Virtual LAN)	物理的に接続した LAN のように通信する位置やトポロジが独立しているデバイスのグループ。
VLT (Virtual LAN Trunk)	各スイッチ上のすべての VLAN トラフィックを転送するスイッチ間のリンク。
VT100	ASCII コードを使用するターミナルタイプ。VT100 画面はテキストベースの表示をします。