TD61-7604

ApresiaLightGM200 シリーズ

Ver. 2.00

ソフトウェアマニュアル

APRESIA Systems 株式会社

制 定 ・ 改 訂 来 歴 表

No.	年　　月　　日	内　　容
-	2021 年 7 月 15 日	新規制定

目次

1 はじめに

■本書の目的
本書は、Web ブラウザーを使用して ApresiaLightGM200 シリーズを設定、管理、および監視するユーザーインターフェース(Web UI)について説明します。
それ以外の説明事項については、以下の各種ドキュメントをご参照ください。

名称	概要
ハードウェアマニュアル	ハードウェアの説明と設置から基本的なコマンド入力までの説明
CLI マニュアル	コマンドラインインターフェース(CLI)での操作方法、コマンドラインによるコマンド内容の説明
MIB 項目の実装仕様	実装している MIB 項目の説明
ログ・トラップ対応一覧	システムログ、SNMP トラップで出力するメッセージの説明

Web UI とコマンドラインインターフェース（CLI）は、どちらも装置内のスイッチングソフトウェアにアクセスして、装置の操作コマンドを実行する機能です。Web UI で変更できるすべての設定は CLI でも同様に設定を行うことができます。

■製品名の表記について
本書では、ApresiaLightGM200 シリーズ製品を「装置」「ブリッジ」または「スイッチ」と表記します。

■使用条件と免責事項
ユーザーは、本製品を使用することにより、本ハードウェア内部で動作するすべてのソフトウェア(以下、本ソフトウェアといいます）に関して、以下の諸条件に同意したものといたします。

本ソフトウェアの使用に起因する、または本ソフトウェアの使用不能によって生じたいかなる直接的、または間接的な損失・損害等（人の生命・身体に対する被害、事業の中断、事業情報の損失、またはその他の金銭的損害を含み、これに限定されない）については、その責を負わないものとします。

- 本ソフトウェアを逆コンパイル、リバースエンジニアリング、逆アセンブルすることはできません。
- 本ソフトウェアを本ハードウェアから分離すること、または本ハードウェアに組み込まれた状態以外で本ソフトウェアを使用すること、または本ハードウェアでの使用を目的とせず本ソフトウェアを移動することはできません。
- 本ソフトウェアでは、本資料に記載しているコマンドのみをサポートしています。未記載のコマンドを入力した場合の動作は保証されません。

■商標登録
APRESIA は、APRESIA Systems 株式会社の登録商標です。
AccessDefender は、APRESIA Systems 株式会社の登録商標です。
Ethernet/イーサネットは、富士フイルムビジネスイノベーション株式会社の登録商標です。
その他ブランド名は、各所有者の商標、または登録商標です。

1.1 本文中の表記について

本文中の表記について、以下に示します。

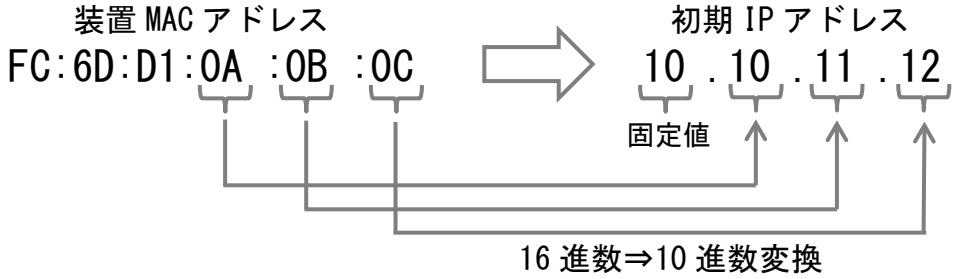
表記	説明
太字フォント	以下の UI を示します。 • 画面名 • ボタン • ツールバーアイコン • メニュー • メニュー項目 • コマンド 例）**File** メニューを開き、**Cancel** を選択します。 また、強調にも使用されます。画面に表示されるシステムメッセージやプロンプトを示す場合もあります。
斜体	フィールドを示します。また、実際の値に置き換える変数またはパラメーターを示します。 例）*filename* この場合、斜体で表示されている単語ではなく、実際のファイル名を入力します。
メニュー名 > メニューオプション	メニュー構造を示します。 例）**Device > Port > Port Properties** この場合、**Device** メニューの下にある **Port** メニューオプションの下の **Port Properties** メニューオプションを意味します。
頭文字の大文字	キーボードのキーの名前は、頭文字を大文字にしています。 例）**Enter** を押します。

この注意シンボルは、そこに記述されている事項が人身の安全と直接関係しない注意書きに関するものであることを示し、注目させる為に用います。

1.2 初期 IP アドレスの設定

本装置は、IP アドレスが初期設定で以下の設定ルールに従って自動設定されています。

■初期 IP アドレスの設定ルール
初期 IP アドレスの先頭 1 バイトは 10 の固定とし、2 バイトから 4 バイトまでは装置の MAC アドレスの下位 3 バイトを 16 進数から 10 進数に変換した値で自動的に設定されます。
装置の MAC アドレスが FC:6D:D1:0A:0B:0C の場合、初期 IP アドレスは 10.10.11.12 となります。



■サブネットマスク
サブネットマスクは、固定長 8 ビット（255.0.0.0）に設定されます。

■初期 IP アドレスの確認方法
初期 IP アドレスは、装置のトップパネルやリアパネルのラベル上に記載されています。ラベルの記載を直接確認できない場合、ユーザーインターフェースから装置の MAC アドレス表示を確認し、設定ルールに従って算出できます。

2 Web UI について

本装置は、Web ブラウザーを使用してネットワーク経由で Web UI にアクセスして、装置の運用管理を行うことができます。

Web UI の基本的な動作確認は、以下の Web ブラウザーで実施しています。

- Internet Explorer 9 以降
- Mozilla Firefox 50 以降
- Google Chrome 50 以降
- Safari 5 以降（Apple の macOS のみ）

2.1 Web UI の接続方法

装置の管理を開始するには、管理 PC にインストールされている Web ブラウザーを起動し、アドレスバーに Web UI の URL を入力して、**Enter** キーを押します。
Web UI の URL は、「http：//*装置の IP アドレス*/」です。

装置のデフォルト IP アドレスについては、「1.2 初期 IP アドレスの設定」を参照してください。

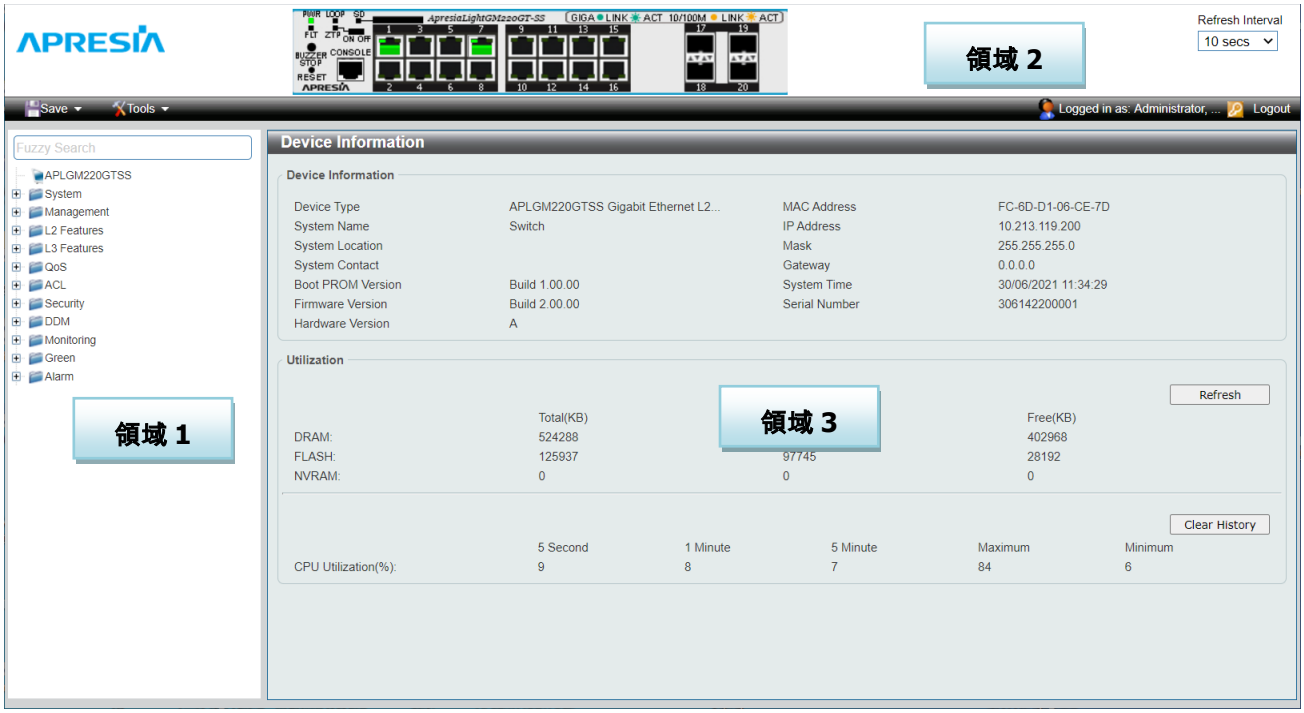
注意事項

デフォルトの User Name は adpro です。Password は設定されていません。

Web UI の URL を Web ブラウザーのアドレスバーに入力して実行すると、Web UI の認証画面が表示されます。**User Name** と **Password** を入力し、**Login** ボタンをクリックしてください。

2.2 Web UI の画面説明

Web UI の画面は、3 つの**領域**に分かれています。



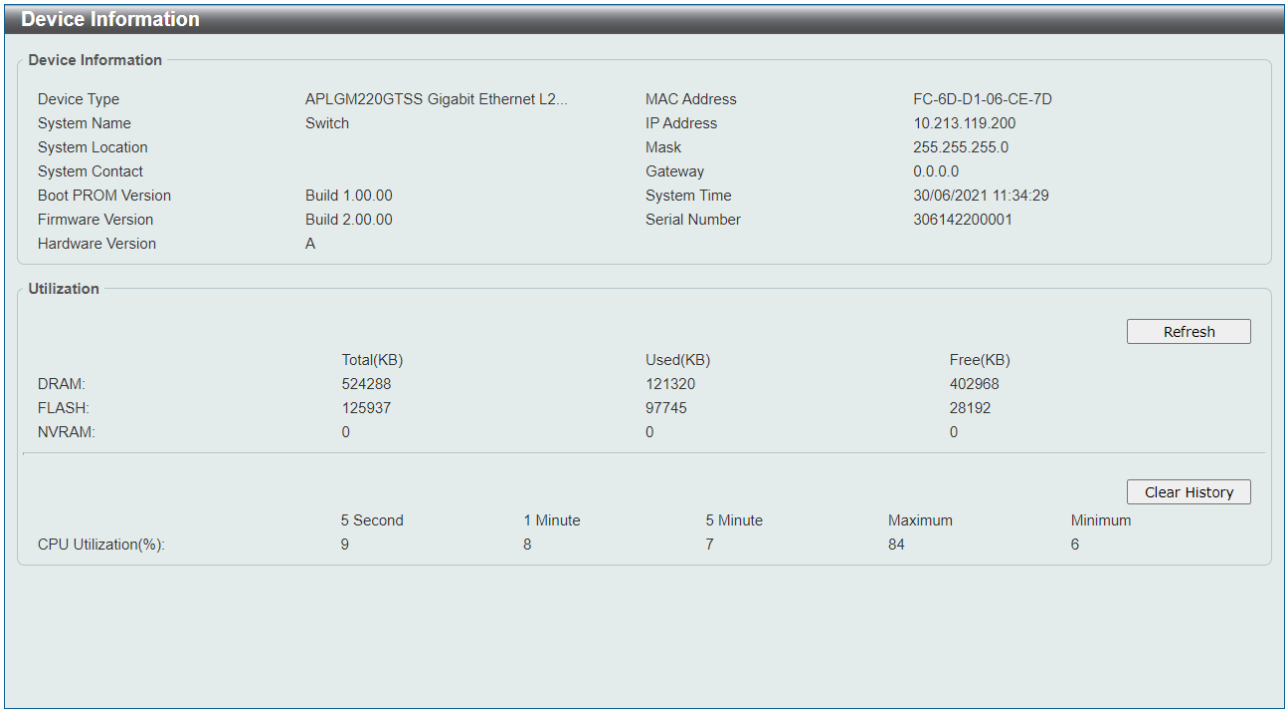
Web UI 画面の各領域の説明を、以下に示します。

領域	説明
領域 1 **(サイドメニュー)**	メニューがリスト表示されます。メニューをクリックすると、**領域 3** に設定項目や情報が表示されます。 メニューの左の+をクリックすると、サブメニューが表示されます。 サイドメニューの画面上の検索ボックスに検索語を入力すると、部分一致するメニューとサブメニューがハイライト表示されます。該当するサブメニューが折りたたみで非表示になっている場合、自動的に展開されます。
領域 2 **(フロントパネルビュー)**	**領域 2** の中央にある装置のフロントパネルのグラフィックは、スイッチのステータスやポートのリンク状態などの情報を表示します。この表示情報は、画面右側にある **Refresh Interval** の周期で更新されます。 画面左上の APRESIA のロゴをクリックすると、Apresia の Web サイトにアクセスします。 ツールバーの左側にある **Save, Tools** ボタンでは、設定の保存やイメージファイルの取得など、運用管理に関わる操作を行うことができます。詳細は **Save, Tools** の説明に記載しています。 ツールバーの右側にある **Logout** ボタンをクリックすると、Web UI からログアウトします。
領域 3 **(メイン画面)**	ログイン直後は、**Device Information** 画面が表示されます。 **領域 1** でいずれかのメニューを選択すると、選択したメニューの設定項目や情報が表示されます。

2.3 デバイス情報

Web UI にログインすると、**Device Information** 画面がメイン画面に表示されます。
この画面では、装置のハードウェア、ソフトウェアに関する情報や、システム関連の設定などを確認できます。

他の画面を表示した後でこの画面に戻るには、サイドメニューの一番上にある装置型式のリンク(前ページの例では **APLGM220GTSS**)をクリックします。



表示されている使用率情報を更新するには、**Refresh** ボタンをクリックします。
表示されている CPU 使用率情報をクリアするには、**Clear History** ボタンをクリックします。

2.4 メニューの内容

Web UI にログインすると、**Device Information** 画面がメイン画面に表示されます。
この画面では、装置のハードウェア、ソフトウェアに関する情報や、システム関連の設定などを確認できます。

サイドメニューの各メニューの概要を以下の表に示します。

章	メニュー名	概要
3	System	装置のシステム情報やハードウェアに関連する設定
4	Management	システム管理に関する設定
5	L2 Features	レイヤー2 の機能に関する設定
6	L3 Features	IP アドレス設定などレイヤー3 の機能に関する設定
7	QoS	優先制御に関する設定
8	ACL	ACL によるアクセス制御に関する設定
9	Security	ポートアクセス認証設定などセキュアネットワークに関する設定
10	DDM	SFP モジュールの状態確認
11	Monitoring	ハードウェアの利用状況の監視に関する設定
12	Green	省電力機能に関する設定
13	Alarm	ブザーや警告 LED の設定

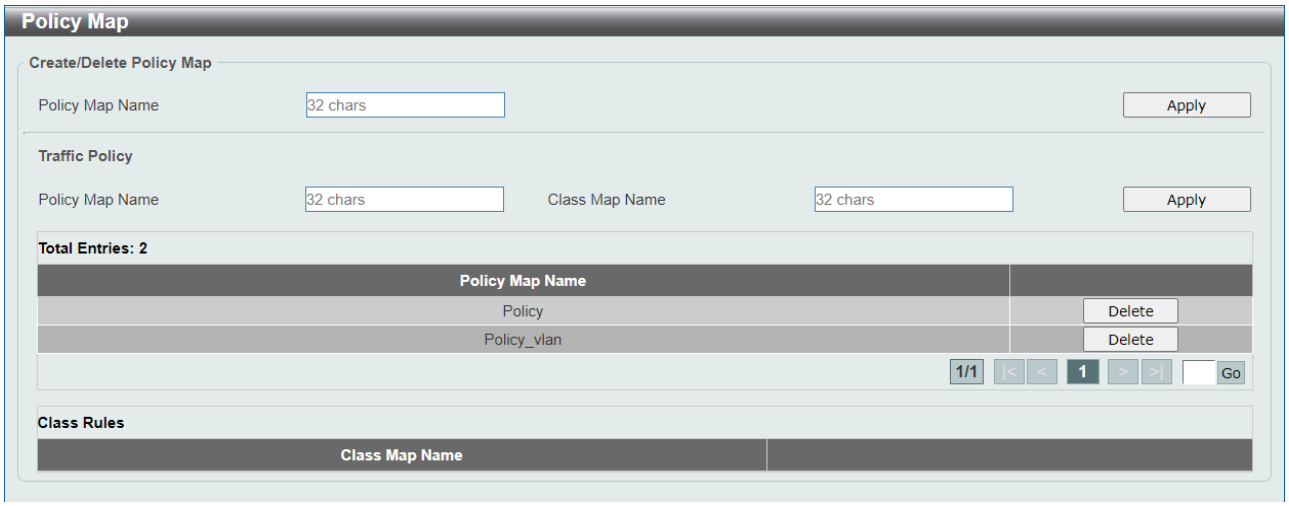
また、ツールバーには以下のメニューがあり、システムのメンテナンスに関わる操作を行うことができます。

章	メニュー名	概要
14	Save	変更した設定を起動時設定に保存
15	Tools	ファイルのバックアップ/リストアや再起動などのメンテナンス操作

2.5 本書での説明の記載内容について

本書での画面の説明は、サイドメニューのツリー構成に従って記載しています。
サイドメニューの各メニュー（System、Management、L2 Features・・・）で章が構成されており、メニューの階層に沿って各節にサブメニューの説明が記載されています。

各画面の説明では、画面に移行するためのサイドメニューのナビゲーションが冒頭に示されています。たとえば、**QoS** > **Advanced Settings** > **Policy Map** というナビゲーションの場合は、サイドメニューの **QoS** メニューを展開して表示される **Advanced Settings** サブメニューをさらに展開して、表示された **Policy Map** サブメニューをクリックすると、該当する画面に移行します。



各節では、表示された画面の各設定項目やボタンの説明が記載されています。

設定項目がいくつかのセクションで区切られている場合、設定の反映はセクション単位で行われます。上記の設定画面の例では **Apply** ボタンが 2 箇所に表示されていますが、それぞれの **Apply** ボタンが対応するセクションの設定のみ反映されます。

表示された画面には、現在の設定情報や状態を表示するテーブルが含まれる場合があります。テーブルには表示できる行数のサイズが決められており、それを超えたエントリーが存在する場合は複数のページにまたがります。この場合、テーブル右下にあるページ番号ボタンをクリックするか、またはテキストボックスにページ番号を入力して **Go** ボタンをクリックすると、指定したページに移動します。

3 System

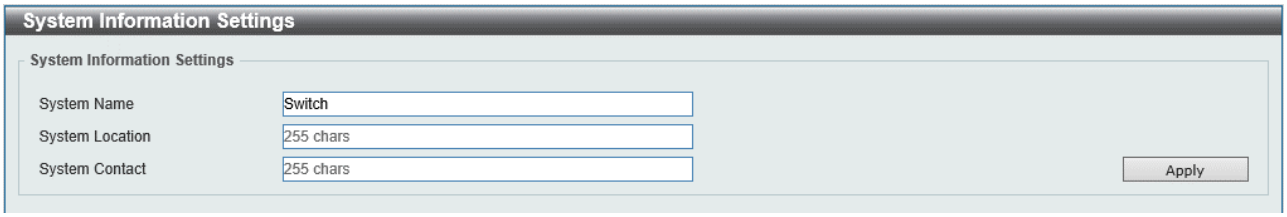
System メニューでは、システム管理に関わる情報の表示や、設定変更を行うことができます。また、物理ポートのリンク速度などの設定を行うことができます。

System の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
3.1	System Information Settings	システム情報の設定
3.2	Peripheral Settings	環境温度に関する設定
3.3	Port Configuration	物理ポートの設定
3.4	System Log	システムログの設定
3.5	Time and SNTP	時刻情報の設定

3.1 System Information Settings

System Information Settings 画面では、装置のシステム情報を設定します。
本画面を表示するには、System > System Information Settings をクリックします。



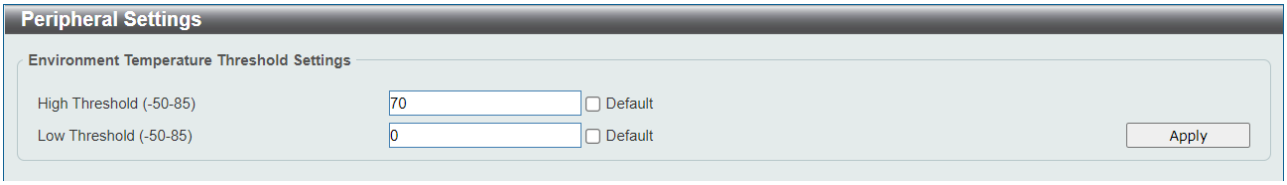
本画面の各項目の説明を以下に示します。

パラメーター	説明
System Name	装置のシステム名を入力します。
System Location	装置のシステムロケーションを入力します。
System Contact	装置の連絡先を入力します。

設定を適用するには、Apply ボタンをクリックします。

3.2 Peripheral Settings

Peripheral Settings 画面では、警告温度のしきい値の上限と下限を設定します。
本画面を表示するには、System > Peripheral Settings をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
High Threshold	警告温度設定の上限しきい値を-50～85（℃）の範囲で入力します。 デフォルト値を使用するには、Default をチェックします。
Low Threshold	警告温度設定の下限しきい値を-50～85（℃）の範囲で入力します。 デフォルト値を使用するには、Default をチェックします。

設定を適用するには、Apply ボタンをクリックします。

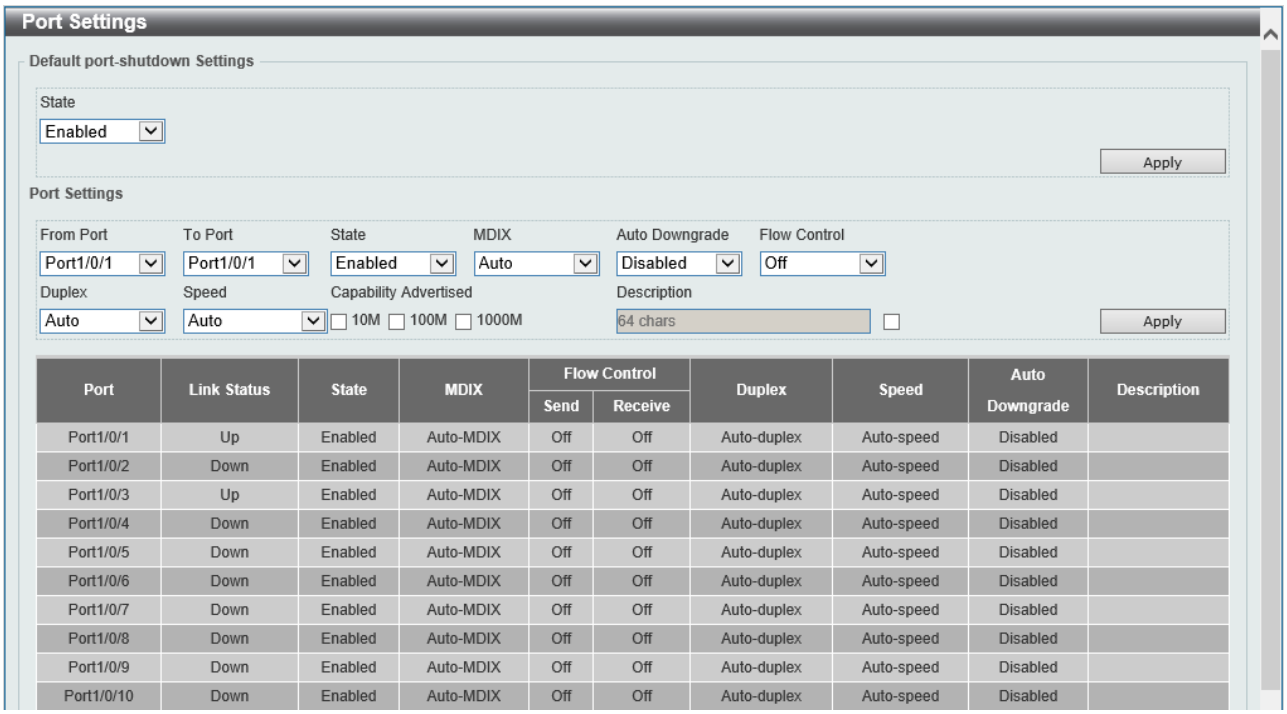
3.3 Port Configuration

Port Configuration サブメニューでは、物理ポートの設定を行うことができます。
Port Configuration の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
3.3.1	Port Settings	物理ポートの物理設定
3.3.2	Port Status	ポートの状態表示
3.3.3	Port GBIC	光ポートのデバイス情報表示
3.3.4	Port Auto Negotiation	オートネゴシエーションの情報表示
3.3.5	Error Disable Settings	ポートエラー自動復旧機能の設定
3.3.6	Jumbo Frame	ジャンボフレームの設定

3.3.1 Port Settings

Port Settings 画面では、装置の物理ポートの設定を行います。
本画面を表示するには、System > Port Configuration > Port Settings をクリックします。



Default port shutdown Settings では、設定の初期化を実施したときに全ポートを閉塞するデフォルトポート閉塞機能の設定を行います。各項目の説明を以下に示します。

パラメーター	説明
State	デフォルトポート閉塞機能の状態（Enabled / Disabled）を選択します。本機能は通常の運用では使用しません。CLI マニュアルで default port-shutdown コマンドの動作をご確認の上、ご使用ください。

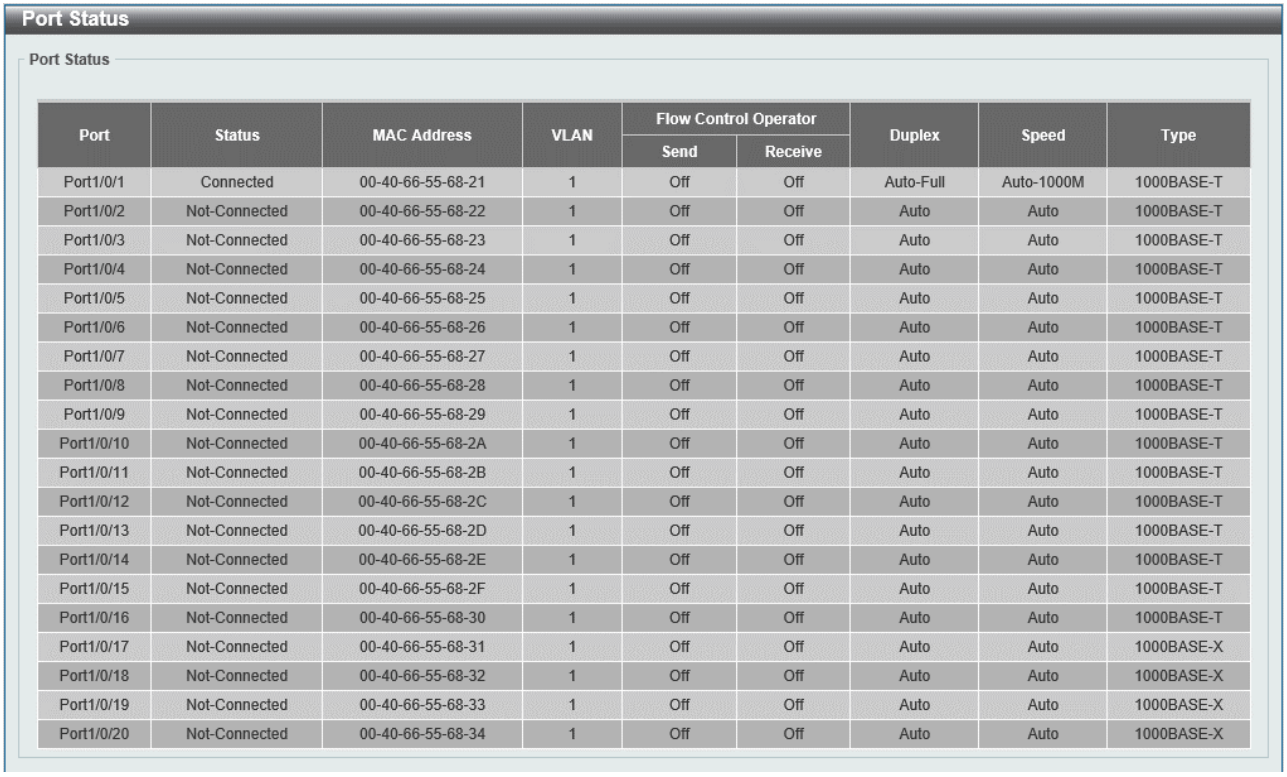
Port Settings では各ポートの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
State	物理ポートの状態（Enabled / Disabled）を選択します。
MDIX	MDI/MDIX の設定（Auto / Normal / Cross）を選択します。
Auto Downgrade	自動ダウングレード機能の状態（Enabled / Disabled）を選択します。
Flow Control	フロー制御の状態（On / Off）を選択します。
Duplex	ポートのデュプレックス（Auto / Half / Full）を選択します。
Speed	ポートの動作速度を選択します。 Auto の場合、オートネゴシエーションを使用します。 Auto を使用せずにポートの動作速度を 1000M 固定にする場合は、Master または Slave を選択する必要があります。また、対向デバイスで、もう一方のモードを指定します。
Capability Advertised	Speed が Auto に設定されている場合、オートネゴシエーションでアドバタイズするポートの動作速度をチェックします。
Description	チェックボックスをチェックし、対応するポートの説明を 64 文字以内で入力します。

設定を適用するには、Apply ボタンをクリックします。

3.3.2 Port Status

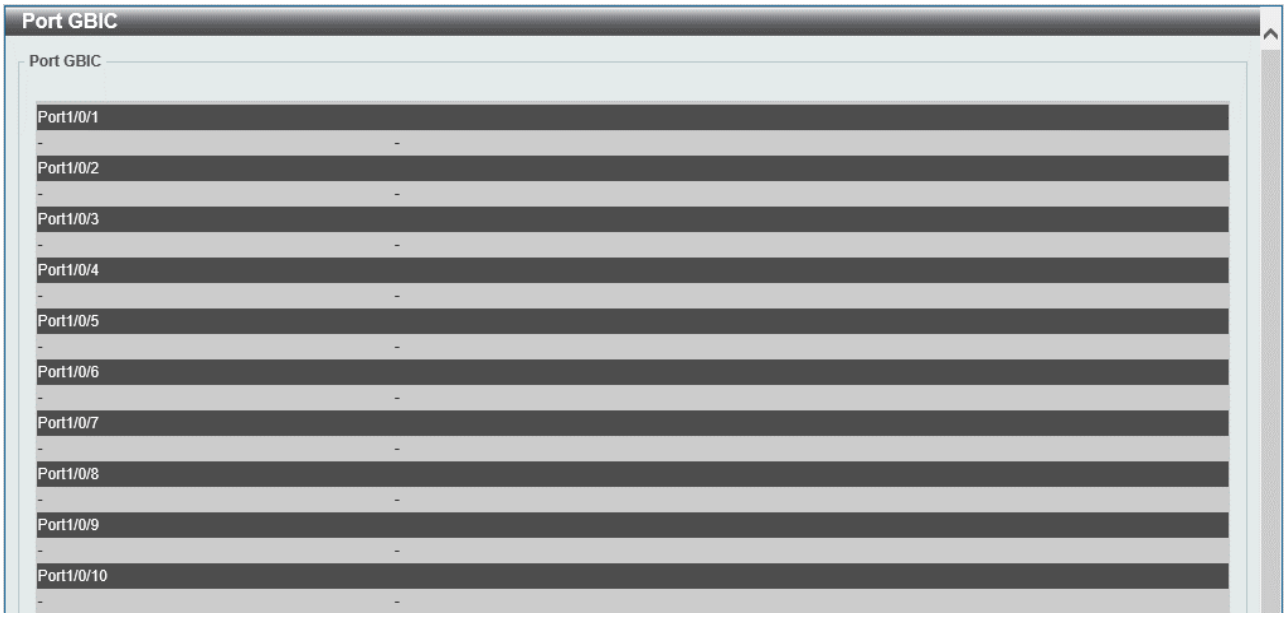
Port Status 画面では、装置の物理ポートのステータスと設定を確認できます。
本画面を表示するには、System > Port Configuration > Port Status をクリックします。



Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
Port1/0/1	Connected	00-40-66-55-68-21	1	Off	Off	Auto-Full	Auto-1000M	1000BASE-T
Port1/0/2	Not-Connected	00-40-66-55-68-22	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/3	Not-Connected	00-40-66-55-68-23	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/4	Not-Connected	00-40-66-55-68-24	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/5	Not-Connected	00-40-66-55-68-25	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/6	Not-Connected	00-40-66-55-68-26	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/7	Not-Connected	00-40-66-55-68-27	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/8	Not-Connected	00-40-66-55-68-28	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/9	Not-Connected	00-40-66-55-68-29	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/10	Not-Connected	00-40-66-55-68-2A	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/11	Not-Connected	00-40-66-55-68-2B	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/12	Not-Connected	00-40-66-55-68-2C	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/13	Not-Connected	00-40-66-55-68-2D	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/14	Not-Connected	00-40-66-55-68-2E	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/15	Not-Connected	00-40-66-55-68-2F	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/16	Not-Connected	00-40-66-55-68-30	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/17	Not-Connected	00-40-66-55-68-31	1	Off	Off	Auto	Auto	1000BASE-X
Port1/0/18	Not-Connected	00-40-66-55-68-32	1	Off	Off	Auto	Auto	1000BASE-X
Port1/0/19	Not-Connected	00-40-66-55-68-33	1	Off	Off	Auto	Auto	1000BASE-X
Port1/0/20	Not-Connected	00-40-66-55-68-34	1	Off	Off	Auto	Auto	1000BASE-X

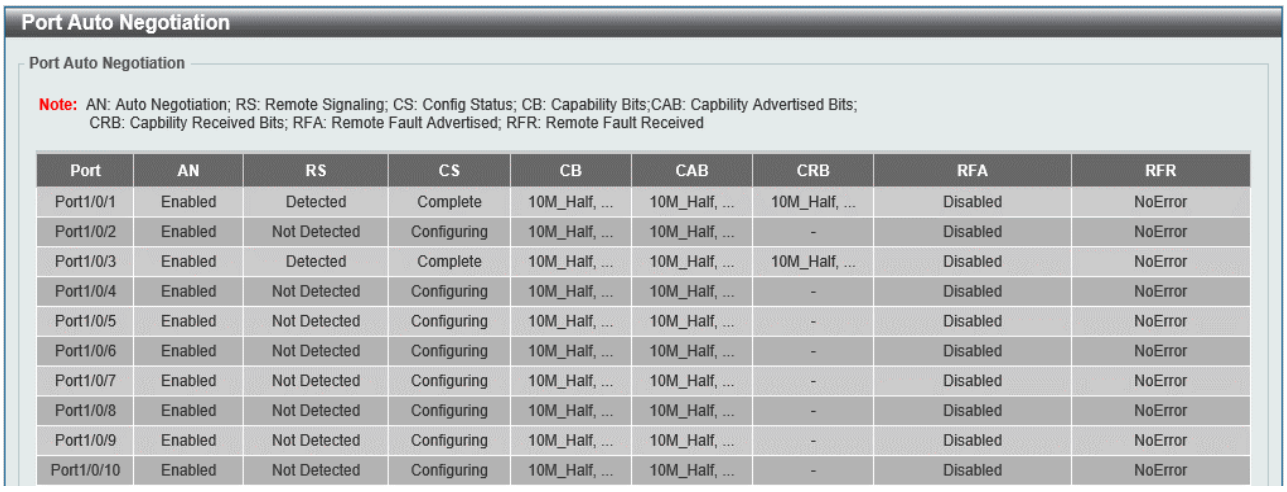
3.3.3 Port GBIC

Port GBIC 画面では、装置の各 SFP ポートで検出されたモジュールの情報を確認できます。
本画面を表示するには、System > Port Configuration > Port GBIC をクリックします。



3.3.4 Port Auto Negotiation

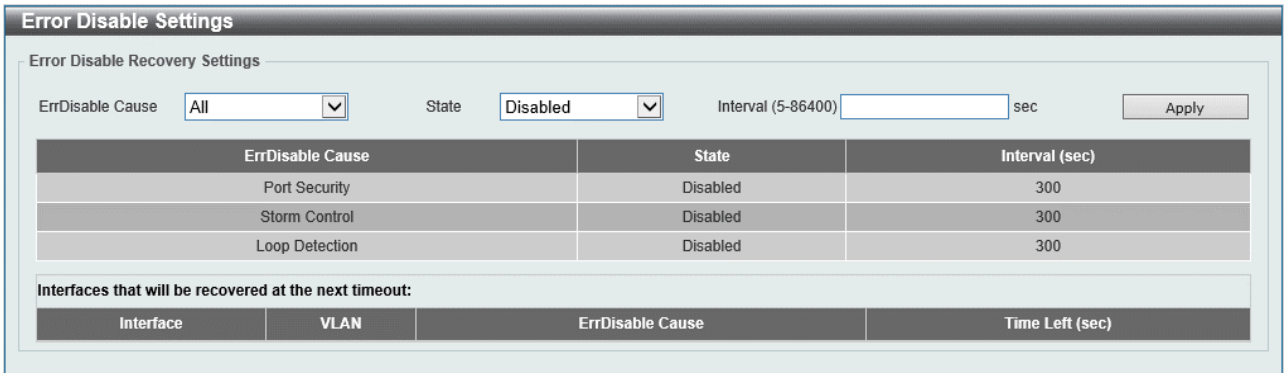
Port Auto Negotiation 画面では、オートネゴシエーション情報の詳細を確認できます。
本画面を表示するには、System > Port Configuration > Port Auto Negotiation をクリックします。



Port	AN	RS	CS	CB	CAB	CRB	RFA	RFR
Port1/0/1	Enabled	Detected	Complete	10M_Half, ...	10M_Half, ...	10M_Half, ...	Disabled	NoError
Port1/0/2	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Port1/0/3	Enabled	Detected	Complete	10M_Half, ...	10M_Half, ...	10M_Half, ...	Disabled	NoError
Port1/0/4	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Port1/0/5	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Port1/0/6	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Port1/0/7	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Port1/0/8	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Port1/0/9	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Port1/0/10	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError

3.3.5 Error Disable Settings

Error Disable Settings 画面では、装置の機能によりポートが閉塞された場合（Error Disabled 状態）の、自動復旧機能の有効／無効、およびポートが復旧するまでの時間を設定します。
本画面を表示するには、System > Port Configuration > Error Disable Settings をクリックします。



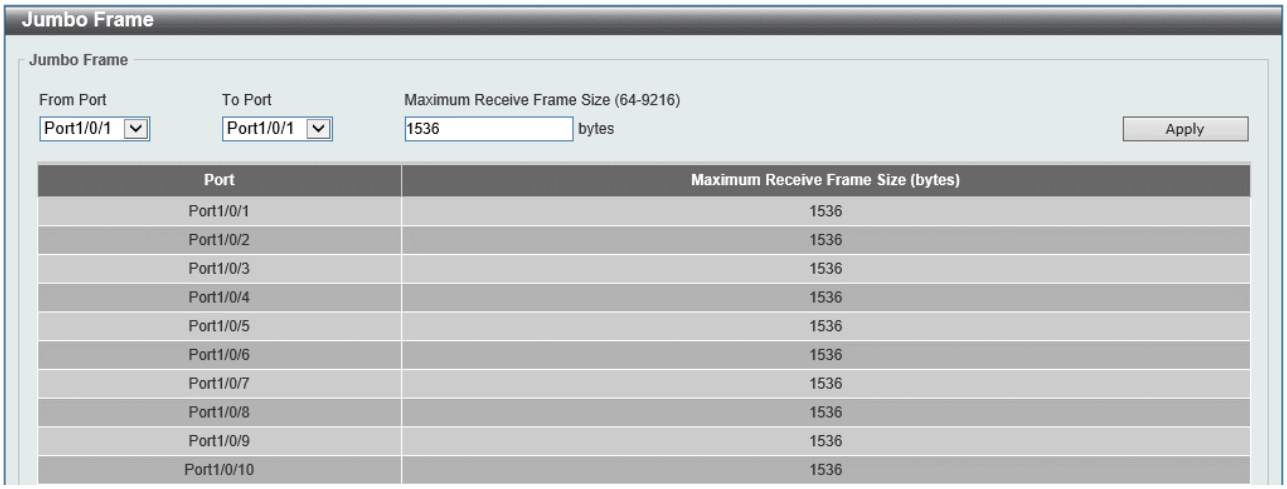
本画面の各項目の説明を以下に示します。

パラメーター	説明
ErrDisable Cause	Error Disabled の原因となった機能（All / Port Security / Storm Control / Loop Detect）を選択します。
State	自動復旧機能の状態（Enabled / Disabled）を選択します。
Interval	Error Disabled でのポート閉塞状態から自動復旧するまでの時間を 5～86400（秒）の範囲で入力します。

設定を適用するには、Apply ボタンをクリックします。

3.3.6 Jumbo Frame

Jumbo Frame 画面では、ジャンボフレームのサイズを設定します。
本画面を表示するには、System > Port Configuration > Jumbo Frame をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Maximum Receive Frame Size	最大受信フレームサイズを 64～9216（バイト）の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

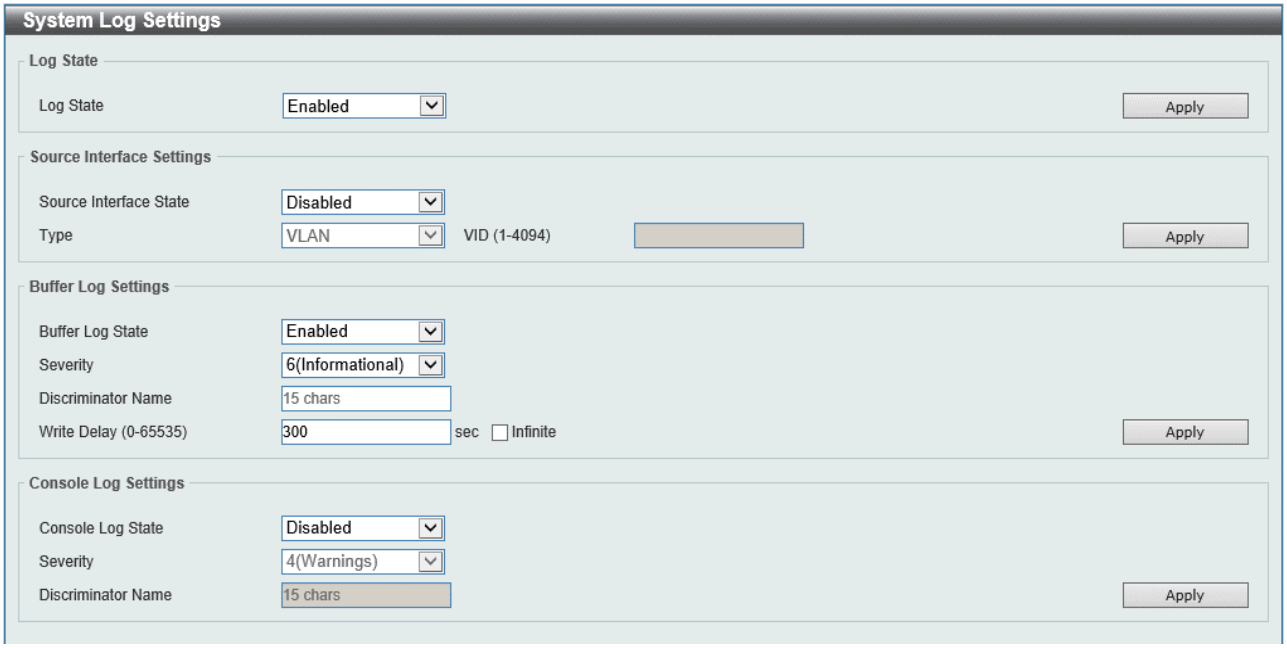
3.4 System Log

System Log サブメニューでは、物理ポートの設定を行うことができます。
System Log の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
3.4.1	System Log Settings	物理ポートの物理設定
3.4.2	System Log Discriminator Settings	ポートの状態表示
3.4.3	System Log Server Settings	光ポートのデバイス情報表示
3.4.4	System Log	オートネゴシエーションの情報表示
3.4.5	System Attack Log	ポートエラー自動復旧機能の設定

3.4.1 System Log Settings

System Log Settings 画面では、システムログの詳細を設定します。
本画面を表示するには、System > System Log > System Log Settings をクリックします。



Log State では、システムログを出力する機能の設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Log State	システムログ出力機能の状態（Enabled / Disabled）を選択します。Disabled の場合、システムログのレベルによらず、すべてのメッセージが出力されません。

設定を適用するには、Apply ボタンをクリックします。

Source Interface Settings では、システムログを Syslog でサーバーに送信する場合の送信インターフェースについて設定します。本装置では使用しません。各項目の説明を以下に示します。

パラメーター	説明
Source Interface State	インターフェースの指定の有無（**Enabled** / **Disabled**）を選択します。
Type	インターフェースのタイプを選択します。**VLAN** のみ使用可能です。
VID	VLAN ID を 1～4094 の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

Buffer Log Settings では、装置内部のログの記録（バッファーロギング）について設定します。各項目の説明を以下に示します。

パラメーター	説明
Buffer Log State	バッファーロギングの状態（**Enabled** / **Disabled** / **Default**）を選択します。**Default** を選択した場合、バッファーロギングの動作はデフォルトに戻ります。
Severity	装置内部に記録するログのレベル(Severity)を指定します。指定したレベル以上の Sevirity に該当するログが記録されます。
Discriminator Name	バッファーロギングの振り分けで使用する Discriminator を 15 文字以内で入力します。Dicsriminator は、**System > System Log > System Log Discriminator Settings** で登録したプロファイルを指定します。
Write Delay	ログ書き込み遅延値を 0～65535（秒）の範囲で入力します。 書き込み遅延機能を無効にするには、**Infinite** をチェックします。

設定を適用するには、**Apply** ボタンをクリックします。

Console Log Settings では、コンソールポートに出力するログ（コンソールログ）について設定します。各項目の説明を以下に示します。

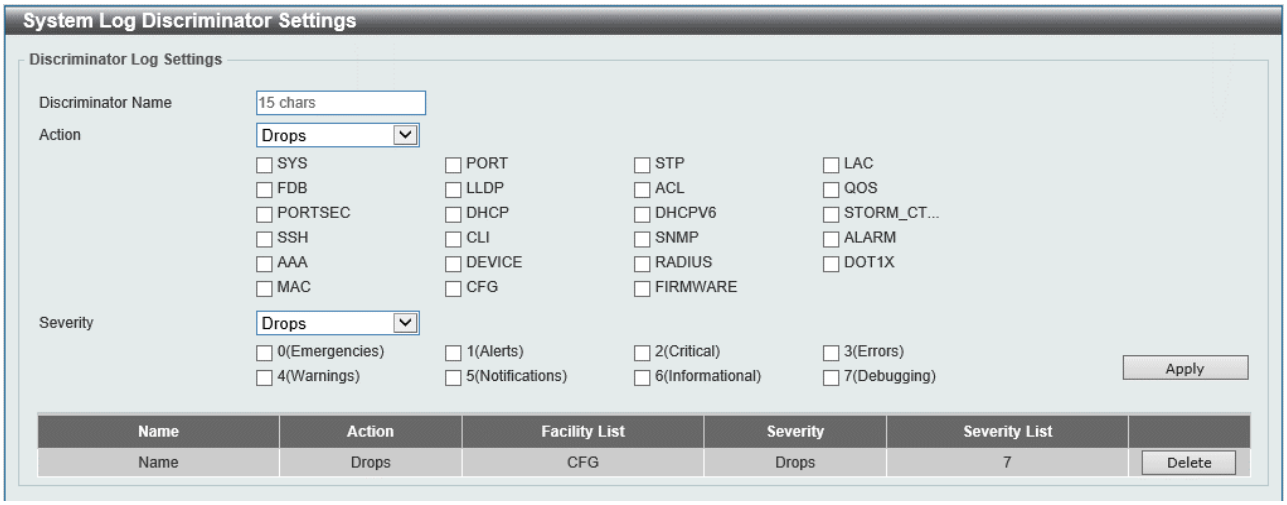
パラメーター	説明
Console Log State	コンソールログの状態（**Enabled** / **Disabled**）を選択します。
Severity	コンソールログで出力するログのレベル（Severity）を指定します。指定したレベル以上の Severity に該当するログが出力されます。
Discriminator Name	コンソールログの出力の振り分けで使用する Discriminator を 15 文字以内で入力します。Dicsriminator は、**System > System Log > System Log Discriminator Settings** で登録したプロファイルを指定します。

設定を適用するには、**Apply** ボタンをクリックします。

3.4.2 System Log Discriminator Settings

System Log Discriminator Settings 画面では、装置内部のバッファーに記録するログやコンソールログ、Syslog サーバーに出力するログを振り分けるフィルタリングプロファイル（Discriminator）を設定します。Discriminator を適用することで、出力するログを Severity ベースよりも細かく指定することができます。

本画面を表示するには、**System > System Log > System Log Discriminator Settings** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Discriminator Name	Discriminator 名を 15 文字以内で入力します。
Action	チェックボックスで機能を選択し、指定した機能に対する動作オプション（Drops / Includes）を選択します。
Severity	チェックボックスでログの Sevirity を選択し、指定した Sevirity に対する動作オプション（Drops / Includes）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。
登録した Discriminator を削除するには、**Delete** ボタンをクリックします。

3.4.3 System Log Server Settings

System Log Server Settings 画面では、システムログを送信する Syslog サーバーを登録します。
本画面を表示するには、**System > System Log > System Log Server Settings** をクリックします。

本画面の各項目の説明を以下に示します。

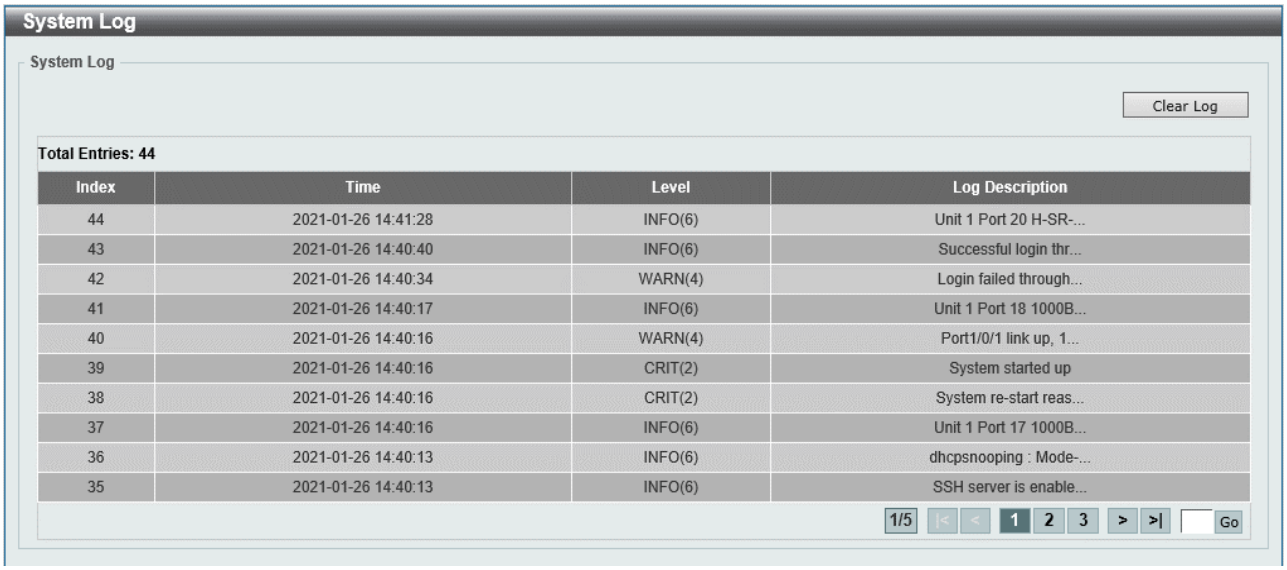
<table>
<tr><th>パラメーター</th><th>説明</th></tr>
<tr><td>Host IPv4 Address</td><td>Syslog サーバーの IPv4 アドレスを入力します。</td></tr>
<tr><td>Host IPv6 Address</td><td>Syslog サーバーの IPv6 アドレスを入力します。</td></tr>
<tr><td>UDP Port</td><td>Syslog サーバーの UDP ポート番号を、514 または 1024～65535 の範囲で入力します。</td></tr>
<tr><td>Severity</td><td>Syslog サーバーに出力するログのレベル（Sevirity）を指定します。指定したレベル以上の Severity に該当するログが出力されます。</td></tr>
<tr><td>Facility</td><td>Syslog サーバーに出力するファシリティーの番号（0～23）を選択します。
各ファシリティーの番号は、特定のファシリティーに関連付けられています。以下の表を参照してください。
<table>
<tr><th>番号</th><th>Name</th></tr>
<tr><td>1</td><td>user</td></tr>
<tr><td>2</td><td>mail</td></tr>
<tr><td>3</td><td>daemon</td></tr>
<tr><td>4</td><td>auth1</td></tr>
<tr><td>5</td><td>Syslog</td></tr>
<tr><td>6</td><td>lpr</td></tr>
<tr><td>7</td><td>news</td></tr>
<tr><td>8</td><td>uucp</td></tr>
</table>
<table>
<tr><th>番号</th><th>Name</th></tr>
<tr><td>9</td><td>clock1</td></tr>
<tr><td>10</td><td>auth2</td></tr>
<tr><td>11</td><td>ftp</td></tr>
<tr><td>12</td><td>ntp</td></tr>
<tr><td>13</td><td>logaudit</td></tr>
<tr><td>14</td><td>logalert</td></tr>
<tr><td>15</td><td>clock2</td></tr>
<tr><td>16</td><td>local0</td></tr>
</table>
<table>
<tr><th>番号</th><th>Name</th></tr>
<tr><td>17</td><td>local1</td></tr>
<tr><td>18</td><td>local2</td></tr>
<tr><td>19</td><td>local3</td></tr>
<tr><td>20</td><td>local4</td></tr>
<tr><td>21</td><td>local5</td></tr>
<tr><td>22</td><td>local6</td></tr>
<tr><td>23</td><td>local7</td></tr>
</table>
</td></tr>
<tr><td>Discriminator Name</td><td>Syslog サーバーへの出力の振り分けで使用する Discriminator を 15 文字以内で入力します。Dicsriminator は、System > System Log > System Log Discriminator Settings で登録されたフィルタリングプロファイルです。</td></tr>
</table>

設定を適用するには、**Apply** ボタンをクリックします。

登録した Syslog サーバーを削除するには、**Delete** ボタンをクリックします。

3.4.4 System Log

System Log 画面では、システムログを確認およびクリアします。
本画面を表示するには、System > System Log > System Log をクリックします。



表示されているシステムログをクリアする場合は、Clear Log ボタンをクリックします。

3.4.5 System Attack Log

System Attack Log 画面では、アタックログを確認およびクリアします。
本画面を表示するには、System > System Log > System Attack Log をクリックします。

表示されているアタックログをクリアするには、Clear Attack Log ボタンをクリックします。

3.5 Time and SNTP

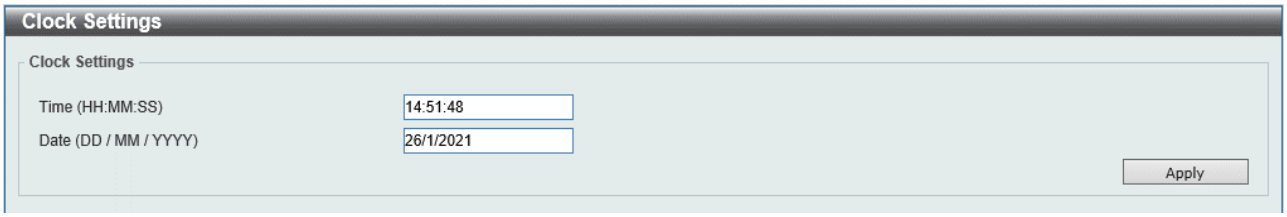
Time and SNTP サブメニューでは、装置のシステム時間に関する設定を行うことができます。システム時間は、現在の時刻を手動で設定する他に、指定した SNTP サーバーから SNTP クライアント機能を使用して時刻情報を取得することもできます。

Time and SNTP の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
3.5.1	Clock Settings	システム時間の手動設定
3.5.2	Time Zone Settings	タイムゾーンとサマータイムの設定
3.5.3	SNTP Settings	SNTP サーバーの設定

3.5.1 Clock Settings

Clock Settings 画面では、装置の時間情報を手動で設定します。
本画面を表示するには、System > Time and SNTP > Clock Settings をクリックします。



本画面の各項目の説明を以下に示します。

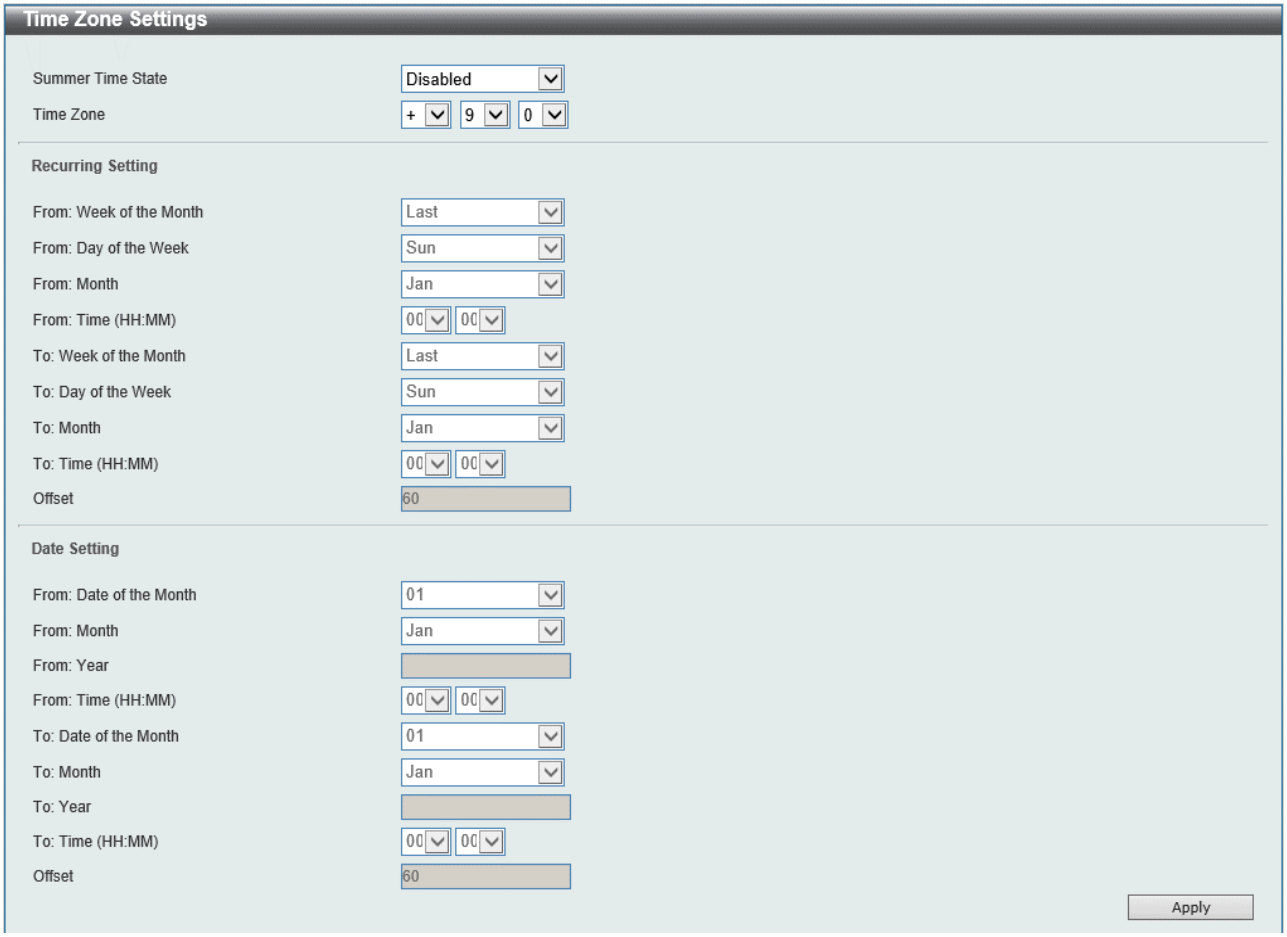
パラメーター	説明
Time	現在の時刻を時間（HH）、分（MM）、秒（SS）で入力します。 例：18:30:30
Date	現在の年月日を日（DD）、月（MM）、年（YYYY）で入力します。 例：31/12/2021

設定を適用するには、Apply ボタンをクリックします。

3.5.2 Time Zone Settings

Time Zone Settings 画面ではタイムゾーンとサマータイムを設定します。
タイムゾーンは、デフォルトで+9:00（日本標準時）が指定されています。
サマータイムの指定は、特定月の指定週の曜日で指定する Recurring モードと、特定月の指定の日付で指定する Date モードの 2 種類から選択できます。
通常、日本国内で使用する場合は、タイムゾーンとサマータイムの設定を変更する必要はありません。

本画面を表示するには、**System > Time and SNTP > Time Zone Settings** をクリックします。



画面最上部でタイムゾーンとサマータイムの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Summer Time State	サマータイムの設定を（Disabled / Recurring Setting / Date Setting）で指定します。
Time Zone	協定世界時（UTC）との時差を設定します。

サマータイムで **Recurring Setting** を選択した場合の、各設定項目の説明を以下に示します。一部の設定項目は **Date Setting** を選択した場合と共通です。

パラメーター	説明
From: Week of the Month	サマータイムを開始する月の週を選択します。
From: Day of the Week	サマータイムを開始する曜日を選択します。
From: Month	サマータイムを開始する月を選択します。
From: Time	サマータイムを開始する時刻を選択します。
To: Week of the Month	サマータイムを終了する月の週を選択します。
To: Day of the Week	サマータイムを終了する曜日を選択します。
To: Month	サマータイムを終了する月を選択します。
To: Time	サマータイムを終了する時刻を選択します。
Offset	オフセットの分数を（30 / 60 / 90 / 120）から選択します。

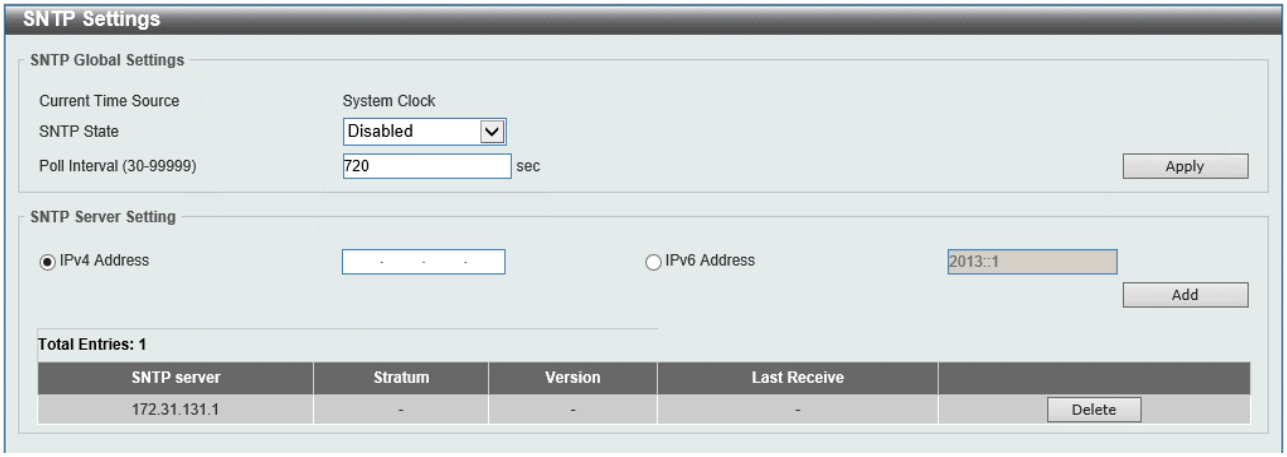
サマータイムで **Date Setting** を選択した場合の、各設定項目の説明を以下に示します。ここでは、**Recurring Setting** と共通の設定項目は省きます。

パラメーター	説明
From: Date of the Month	サマータイムを開始する月の日付を選択します。
From: Year	サマータイムを開始する年を入力します。
To: Date of the Month	サマータイムを終了する月の日付を選択します。
To: Year	サマータイムを終了する年を入力します。

設定を適用するには、**Apply** ボタンをクリックします。

3.5.3 SNTP Settings

SNTP Settings 画面では、SNTP クライアント機能の設定を行い、SNTP サーバーを登録します。装置のシステム時間を、手動ではなく SNTP サーバーとの時刻同期で設定する場合に使用します。
本画面を表示するには、**System > Time and SNTP > SNTP Settings** をクリックします。



SNTP Global Settings では SNTP クライアント機能の設定を行います。各項目の説明を以下に示します。

パラメーター	説明
SNTP State	SNTP クライアント機能の状態（**Enabled** / **Disabled**）を選択します。
Poll Interval	SNTP サーバーとの同期間隔を 30～99999（秒）の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

SNTP Server Settings では SNTP サーバーの登録を行います。各項目の説明を以下に示します。

パラメーター	説明
IPv4 Address	SNTP サーバーの IPv4 アドレスを入力します。
IPv6 Address	SNTP サーバーの IPv6 アドレスを入力します。

SNTP サーバーを追加するには、**Add** ボタンをクリックします。
SNTP サーバーを削除するには、**Delete** ボタンをクリックします。

4 Management

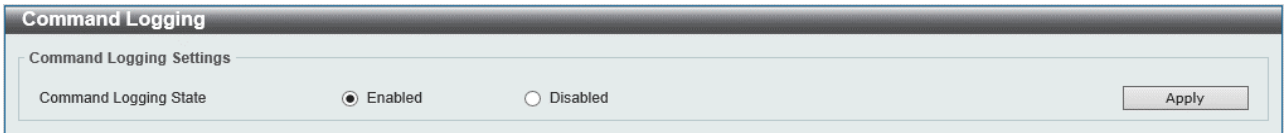
Management メニューでは、運用管理に関わる情報の表示や、設定変更を行うことができます。
Management の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
4.1	Command Logging	コマンドロギング機能の設定
4.2	User Accounts Settings	ユーザーアカウントの設定
4.3	User Accounts Encryption	ユーザーアカウントの暗号化の設定
4.4	Login Method	CLI のログイン方法の設定
4.5	SNMP	SNMP の設定
4.6	RMON	RMON の設定
4.7	Telnet/Web	Telnet 接続および WEB UI の設定
4.8	Session Timeout	各 CLI および WEB UI セッション時間の設定
4.9	CPU Protection	CPU 保護機能の設定
4.10	IP Source Interface	FTP/TFTP の送信インターフェースの設定
4.11	File System	装置のファイル操作

4.1 Command Logging

Command Logging 画面では、コマンドロギング機能を設定します。
コマンドロギングは、コマンドラインインターフェースで実行されたすべてのコマンドをログに記録する機能です。記録されたログは、コマンドを入力したユーザーに関する情報とともに、システムログに保存されます。

本画面を表示するには、Management > Command Logging をクリックします。



本画面の各項目の説明を以下に示します。

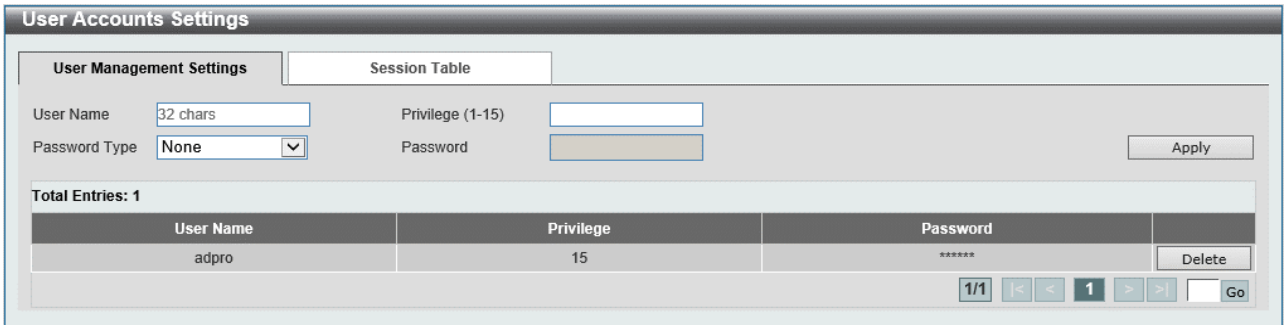
パラメーター	説明
Command Logging State	コマンドロギング機能の状態（Enabled / Disabled）を選択します。

設定を適用するには、Apply ボタンをクリックします。

4.2 User Accounts Settings

User Accounts Settings 画面では、ユーザーアカウントを作成／更新します。また、アクティブなユーザーアカウントのセッションの情報を表示して、Web UI のアクセスユーザーの権限レベルを一時的に変更することもできます。権限レベルを上げるためには、事前に Management > Login Method の画面から、移行する権限レベルに対する移行パスワードが設定されている必要があります。

本画面を表示するには、Management > User Accounts Settings をクリックします。



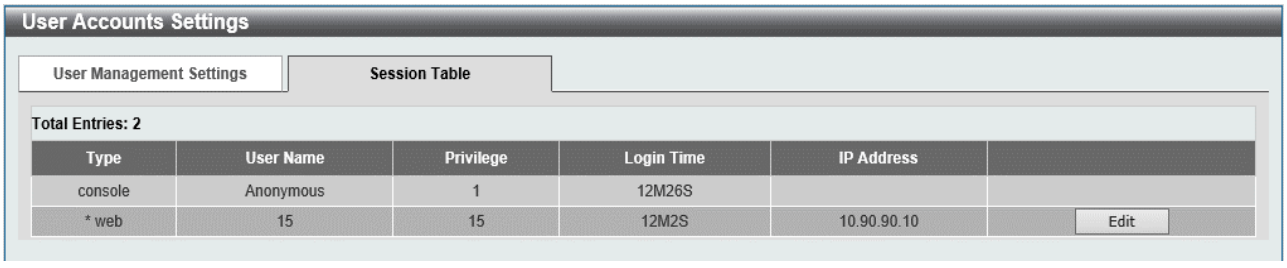
本画面には、User Management Settings タブと Session Table タブがあります。

User Management Settings タブでは、ユーザーアカウントの登録/確認/削除などの操作ができます。各項目の説明を以下に示します。

パラメーター	説明
User Name	ユーザーアカウント名を 32 文字以内で入力します。
Privilege	ユーザーアカウントの特権レベルを 1～15 の範囲で入力します。
Password Type	パスワードのタイプ（None / Plain Text / Encrypted）を選択します。
Password	Password Type で Plain Text または Encrypted を選択した場合、ユーザーアカウントのパスワードを入力します。

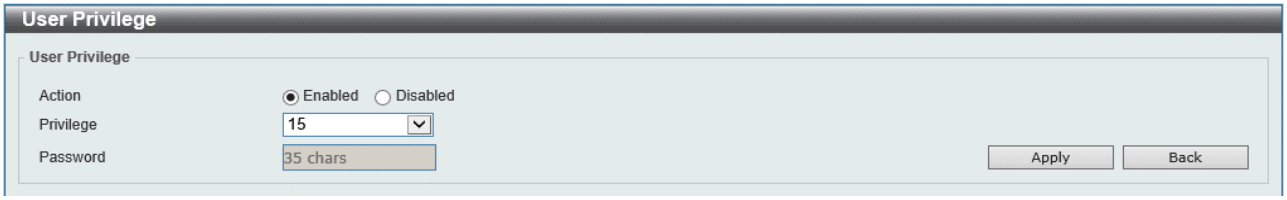
設定を適用するには、Apply ボタンをクリックします。
ユーザーアカウントを削除するには、Delete ボタンをクリックします。

Session Table タブでは、アクティブなユーザーアカウントのセッションが一覧で表示されます。



Web UI にアクセスしているユーザーには、Edit ボタンが表示されます。Edit ボタンをクリックすると、アカウントの User Privilege 画面が表示されます。

User Privilege の画面では、現在のユーザーの権限レベルを変更できます。



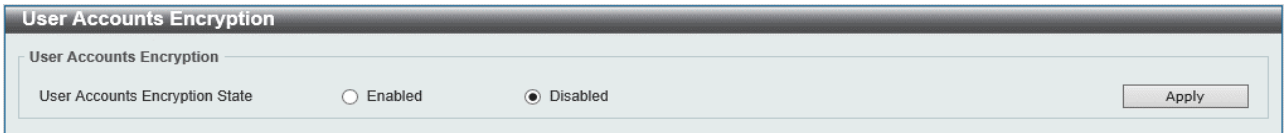
User Privilege の各項目の説明を以下に示します。

パラメーター	説明
Action	権限レベルを上げる場合は Enabled を選択します。権限レベルを下げる場合は Disabled を選択します。
Privilege	移行する特権レベル（1～15）を選択します。Action が Disabled の場合、現在の特権レベルよりも上のレベルを指定する必要があります。
Password	権限レベルに設定されたパスワードを 35 文字以内で入力します。特権レベルを下げる場合は入力する必要はありません。

設定を適用するには、Apply ボタンをクリックします。
前の画面に戻るには、Back ボタンをクリックします。

4.3 User Accounts Encryption

User Accounts Encryption 画面では、ユーザーアカウントの暗号化を設定します。設定情報でユーザーアカウントのパスワードを暗号化するかどうかを決定します。
本画面を表示するには、Management > User Accounts Encryption をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
User Accounts Encryption State	ユーザーアカウントの暗号化の状態（Enabled / Disabled）を選択します。

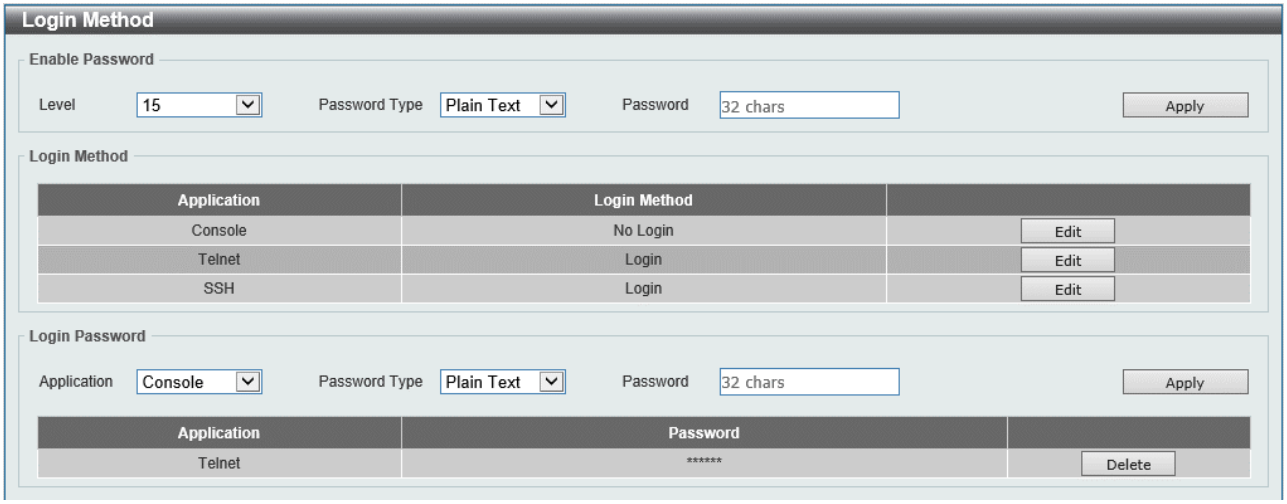
設定を適用するには、Apply ボタンをクリックします。

4.4 Login Method

Login Method 画面では、AAA モジュールを使用しない場合の CLI のログイン方法や、ログインおよび権限レベル変更で使用するパスワードを設定します。

装置のデフォルト設定では、CLI へのアクセスはコンソールポートのみログイン方式が Login Local に設定されており、初期ユーザーアカウント「adpro」を使用してログインできます。
Telnet と SSH のアクセスは、ログイン方式が Login に設定されており、ログイン時にログインパスワードが必要になります。また、ログイン時点での権限レベルが 1 であり、各種設定を行うには権限レベルを上げる必要がありますが、権限レベルの移行には移行パスワードが必要になります。
Telnet または SSH で設定操作をするためには、それぞれのログイン方式自体を Login Local に変更する（または AAA モジュールを有効にする）か、ログインパスワードと権限レベル 12 以上の移行パスワードを設定する必要があります。SSH の場合は、さらに SSH サーバー機能に関する設定も必要です。

本画面を表示するには、**Management** > **Login Method** をクリックします。



Enable Password では、指定した権限レベルへの移行パスワードを設定します。各項目の説明を以下に示します。

パラメーター	説明
Level	指定する特権レベル（1～15）を選択します。
Password Type	指定した特権レベルに移行する場合のパスワードの入力タイプを、以下のどちらかから選択します。 • **Plain Text**：平文パスワードを入力する場合に選択します。 • **Encrypted**：暗号化パスワードを暗号化する場合に選択します。
Password	特権レベル移行のパスワードを入力します。 **Password Type** が **Plain Text** の場合は、32 文字以内でパスワードを入力します。大文字と小文字は区別され、スペースを含めることができます。**Password Type** が **Encrypted** の場合は、35 バイト長でパスワードを入力します。大文字と小文字は区別されます。

設定を適用するには、**Apply** ボタンをクリックします。

Login Method では、各ライン種別のログイン方法を指定します。この画面は、AAA モジュールが無効の場合のみ表示されます。各項目の説明を以下に示します。

パラメーター	説明
Login Method	指定したライン種別でのログイン方法を、以下のいずれかから選択します。 • No Login：ログイン認証を実行しない場合に選択します。 • Login：パスワードで認証を行う場合に選択します。 • Login Local：ローカルに設定されたユーザー名とパスワードを入力させる場合に選択します。

各ライン種別のログイン方法を設定するには、Edit ボタンをクリックします。
設定を適用するには、Apply ボタンをクリックします。

Login Password では、ログイン方法（Login Method）が Login のライン種別に対するログインパスワードを登録します。各項目の説明を以下に示します。

パラメーター	説明
Application	設定するライン種別（Console / Telnet / SSH）を選択します。
Password Type	設定するパスワードの入力タイプ（Plain Text / Encrypted）を指定します。
Password	ログイン時のパスワードを入力します。 Password Type が Plain Text の場合は、32 文字以内でパスワードを入力します。大文字と小文字は区別され、スペースを含めることができます。Password Type が Encrypted の場合は、35 バイト長でパスワードを入力します。大文字と小文字は区別されます。

設定を適用するには、Apply ボタンをクリックします。
登録したパスワードを削除するには、Delete ボタンをクリックします。

4.5 SNMP

SNMP サブメニューでは、SNMP エージェント機能の設定を行います。SNMP マネージャーからの操作を実行する機能と、イベント発生時に外部ホストに SNMP トラップで通知する機能があります。

SNMP マネージャーの操作は、装置の管理情報である MIB オブジェクトに対して行われます。MIB オブジェクトは、整数をピリオドで区切ったオブジェクト識別子（OID）で指定されます。MIB オブジェクトはツリー型の階層構造を持ち、OID は階層構造における位置を表現することもできます。

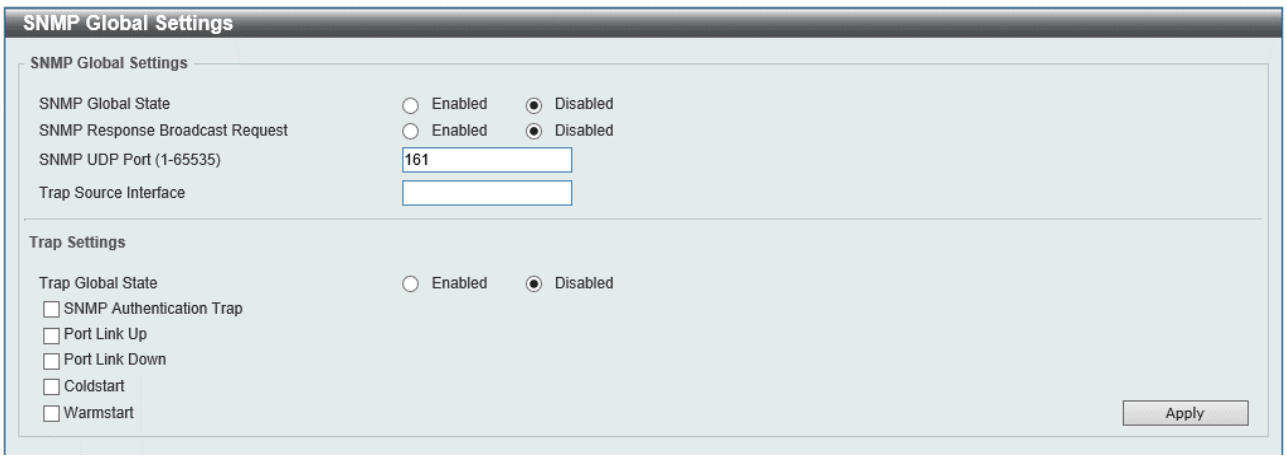
SNMP マネージャーからアクセスが行われると、SNMP ユーザー名や SNMP コミュニティー名によりユーザーが識別されます。装置では、ユーザーが所属する SNMP グループの各操作に対して SNMP ビューを割り当てることで、アクセス可能な MIB オブジェクトの範囲を定めることができます。

SNMP の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
4.5.1	SNMP Global Settings	SNMP のグローバル設定
4.5.2	SNMP Linkchange Trap Settings	SNMP トラップの物理ポートでの設定
4.5.3	SNMP View Table Settings	SNMP ビューの設定
4.5.4	SNMP Community Table Settings	SNMP コミュニティーの設定
4.5.5	SNMP Group Table Settings	SNMP グループの設定
4.5.6	SNMP Engine ID Local Settings	SNMP エンジン ID の設定
4.5.7	SNMP User Table Settings	SNMP ユーザーの設定
4.5.8	SNMP Host Table Settings	SNMP トラップの通知ホストの設定

4.5.1 SNMP Global Settings

SNMP Global Settings 画面では、SNMP のグローバル設定や SNMP トラップの設定を行います。
本画面を表示するには、**Management** > **SNMP** > **SNMP Global Settings** をクリックします。



SNMP Global Settings では、SNMP のグローバル設定を行います。各項目の説明を以下に示します。

パラメーター	説明
SNMP Global State	SNMP 機能の状態（Enabled / Disabled）を選択します。
SNMP Response Broadcast Request	ブロードキャスト SNMP GetRequest パケットに応答するサーバーの状態（Enabled / Disabled）を選択します。
SNMP UDP Port	SNMP の UDP ポート番号を 1～65535 の範囲で入力します。
Trap Source Interface	SNMP トラップパケットを送信するための送信元アドレスとして、IP アドレスが使用されるインターフェースを入力します。

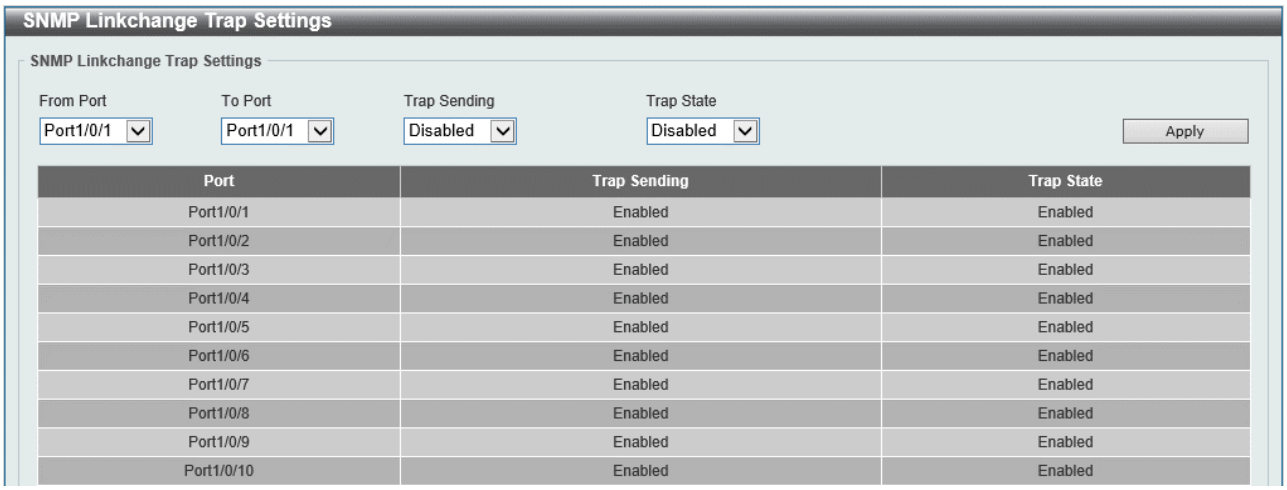
Trap Settings では、SNMP トラップの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Trap Global State	トラップ通知のグローバル設定（Enabled / Disabled）を選択します。
SNMP Authentication Trap	装置に対する SNMP アクセスで認証に失敗した際のトラップ通知を行う場合にチェックします。
Port Link Up	リンクアップ時のトラップを送信する場合にチェックします。
Port Link Down	リンクダウン時のトラップを送信する場合にチェックします。
Coldstart	コールドスタートのトラップを送信する場合にチェックします。
Warmstart	ウォームスタートのトラップを送信する場合にチェックします。

設定を適用するには、Apply ボタンをクリックします。

4.5.2 SNMP Linkchange Trap Settings

SNMP Linkchange Trap Settings 画面では、ポート単位での SNMP トラップ通知設定を行います。
本画面を表示するには、Management > SNMP > SNMP Linkchange Trap Settings をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Trap Sending	対象ポートからトラップを送信しない場合は Disabled を指定します。送信する場合は Enabled を指定します。
Trap State	対象ポートのリンク状態変更時に SNMP トラップを送信する場合は Enabled を指定します。送信しない場合は Disabled を指定します。

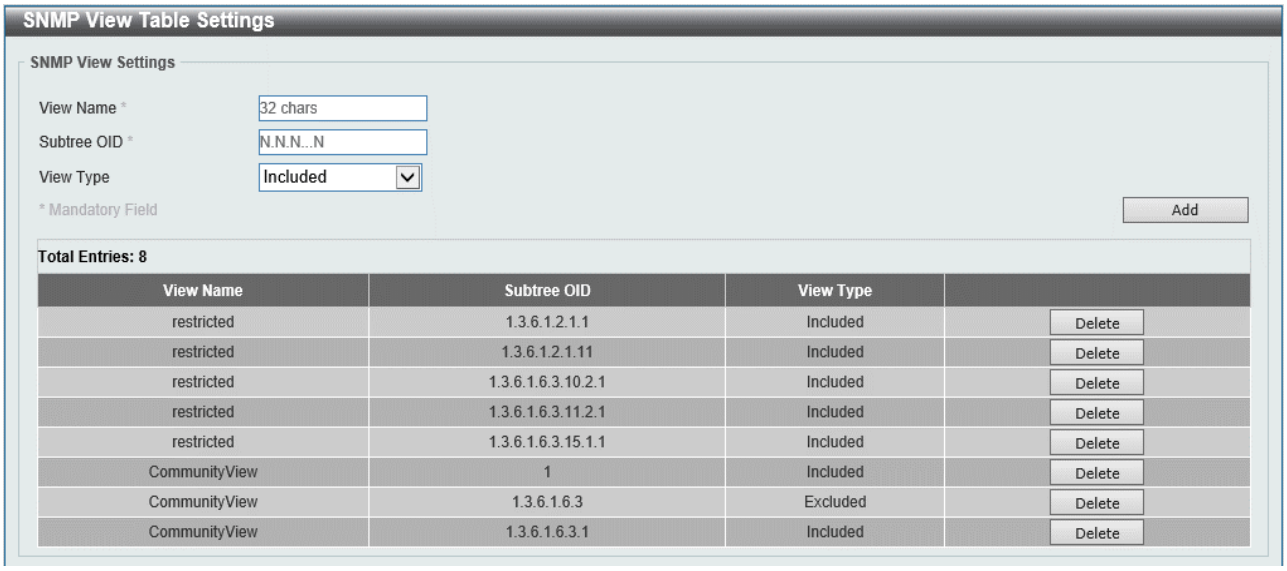
設定を適用するには、Apply ボタンをクリックします。

4.5.3 SNMP View Table Settings

SNMP View Table Settings 画面では、SNMP マネージャーの操作に対するアクセス範囲を定める SNMP ビューを作成します。

SNMP ビューは複数の OID エントリーで構成されます。OID エントリーでは、OID をキーとしてその OID の下位階層（サブツリー）に含まれる MIB オブジェクトに対するアクセス権限を、Included（操作の許可）と Excluded（操作の禁止）で指定します。MIB オブジェクトが複数の OID エントリーに該当する場合は、キーとなる OID（Subtree OID）が最も長いエントリーのアクセス権限が適用されます。

本画面を表示するには、Management > SNMP > SNMP View Table Settings をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
View Name	SNMP ビュー名を 32 文字以内で入力します。
Subtree OID	OID エントリーのキーとなる Subtree OID を指定します。
View Type	対象の MIB オブジェクトの操作に対するアクセス権限を以下のどちらかで指定します。 • Included：SNMP マネージャーからの操作を許可 • Excluded：SNMP マネージャーからの操作を禁止

SNMP ビューまたは OID エントリーを追加するには、Add ボタンをクリックします。
SNMP ビューまたは OID エントリーを削除するには、Delete ボタンをクリックします。

4.5.4 SNMP Community Table Settings

SNMP Community Table Settings 画面では、SNMPv1/v2c でユーザーの識別に使用される SNMP コミュニティーの設定を行います。

SNMP コミュニティーの設定では、ユーザーが行う操作とその対象となる MIB オブジェクトの範囲を定めるためにアクセス権限と SNMP ビューを指定します。アクセス権限が Read Only の場合、読み込み操作のみを許可します。アクセス権限が Read Write の場合、読み込みと書き込みを許可します。SNMP ビューは、アクセス権限の設定で許可した操作に対して適用されます。

注意事項

本装置ではデフォルトで「public」と「private」という 2 種類の SNMP コミュニティーが登録されています。SNMP を有効にする場合は、デフォルトエントリーを削除することを推奨します。

本画面を表示するには、Management > SNMP > SNMP Community Table Settings をクリックします。

本画面の各項目の説明を以下に示します。

パラメーター	説明
Key Type	SNMP コミュニティーのキータイプ（Plain Text / Encrypted）を選択します。
Community Name	SNMP コミュニティー名を指定します。Key Type で指定した方式(平文、暗号化形式)に合わせて入力してください。
View Name	SNMP ビュー名を 32 文字以内で入力します。 ビュー名は、SNMP ビューテーブルに存在する必要があります。
Access Right	以下のどちらかのアクセス権限を選択します。 • Read Only：読み込み操作のみを許可します。 • Read Write：読み込み、書き込みの両方の操作を許可します。
IP Access-List Name	ACL を使用して SNMP でアクセスできるユーザーを制限します。

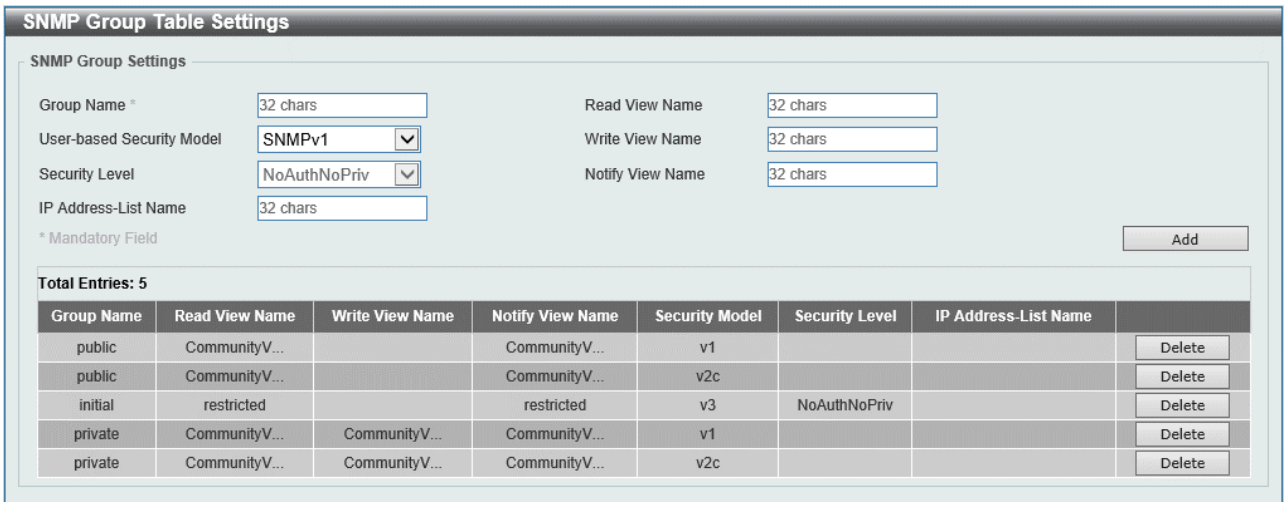
SNMP コミュニティーを追加するには、Add ボタンをクリックします。
SNMP コミュニティーを削除するには、Delete ボタンをクリックします。

4.5.5 SNMP Group Table Settings

SNMP Group Table Settings 画面では、SNMP グループを作成します。SNMP グループは、登録した SNMP ユーザーをグループ化して、アクセス権限を一括で指定します。

MIB オブジェクトのアクセス範囲を示す SNMP ビューは、SNMP グループに対して操作種別（読み込み、書き込み、通知）ごとに適用します。SNMP ユーザーはいずれかの SNMP グループに分類され、SNMP グループに割り当てた SNMP ビューに応じたアクセス権限を持ちます。
SNMP コミュニティーを登録した場合、対応する SNMP グループが自動的に作成されます。

本画面を表示するには、Management > SNMP > SNMP Group Table Settings をクリックします。



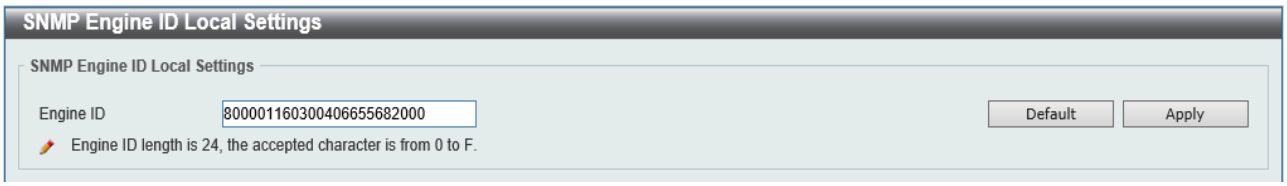
本画面の各項目の説明を以下に示します。

パラメーター	説明
Group Name	SNMP グループ名を 32 文字以内で入力します。
Read View Name	読み取り操作の SNMP ビュー名を 32 文字以内で入力します。
User-based Security Model	対応する SNMP バージョンを指定します。新規に SNMP グループを登録する場合は **SNMPv3** を指定します。
Write View Name	書き込み操作の SNMP ビュー名を 32 文字以内で入力します。
Security Level	以下のいずれかの SNMPv3 セキュリティーレベルを選択します。 • **NoAuthNoPriv**：認証と暗号化を行いません。 • **AuthNoPriv**：認証を行いますが、暗号化を行いません。 • **AuthPriv**：認証と暗号化を行います。
Notify View Name	トラップ通知の SNMP ビュー名を 32 文字以内で入力します。
IP Access-List Name	ACL を使用して SNMP でアクセスできるユーザーを制限します。

入力した情報で SNMP グループを追加するには、**Add** ボタンをクリックします。
SNMP グループを削除するには、**Delete** ボタンをクリックします。

4.5.6 SNMP Engine ID Local Settings

SNMP Engine ID Local Settings 画面では、SNMP エンジン ID を設定します。エンジン ID は、SNMPv3 で使用される一意の識別子です。
本画面を表示するには、**Management** > **SNMP** > **SNMP Engine ID Local Settings** をクリックします。



本画面の各項目の説明を以下に示します。

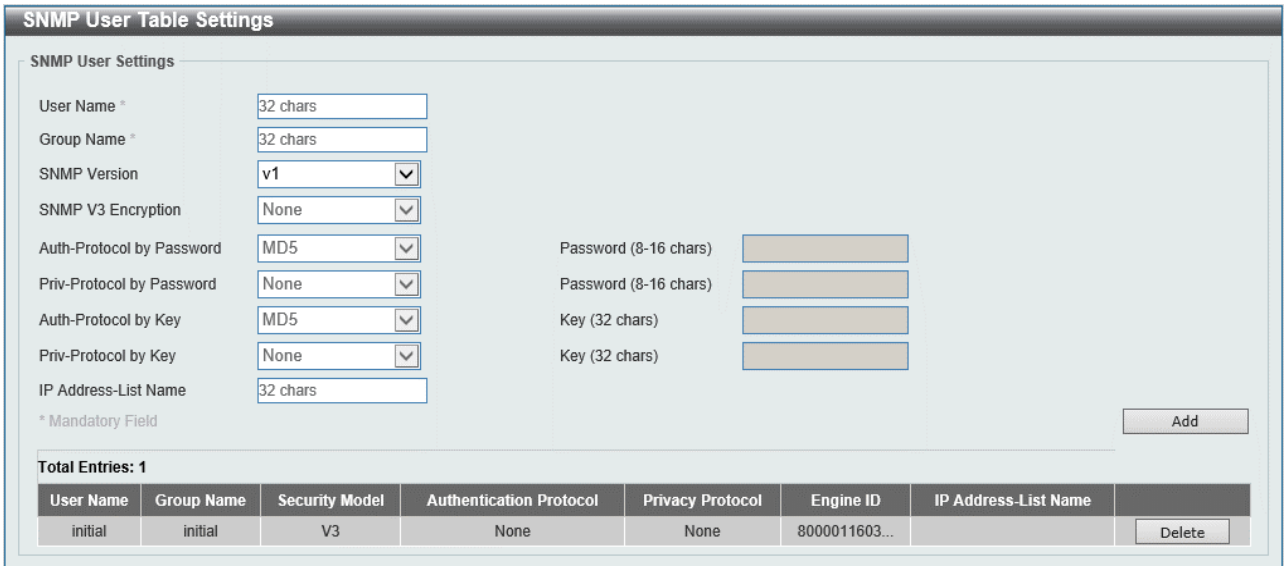
パラメーター	説明
Engine ID	SNMP エンジン ID 文字列を 24 文字以内で入力します。

エンジン ID をデフォルトに戻すには、**Default** ボタンをクリックします。
設定を適用するには、**Apply** ボタンをクリックします。

4.5.7 SNMP User Table Settings

SNMP User Table Settings 画面では、SNMPv3 で使用する SNMP ユーザーを登録します。SNMPv3 では SNMP ユーザーにより識別を行います。
登録する SNMP ユーザーには、SNMP グループを紐付けます。該当する SNMP グループのアクセス権限（各操作に対して指定された SNMP ビュー）に応じて、SNMP で許可される操作が決定されます。

本画面を表示するには、**Management** > **SNMP** > **SNMP User Table Settings** をクリックします。



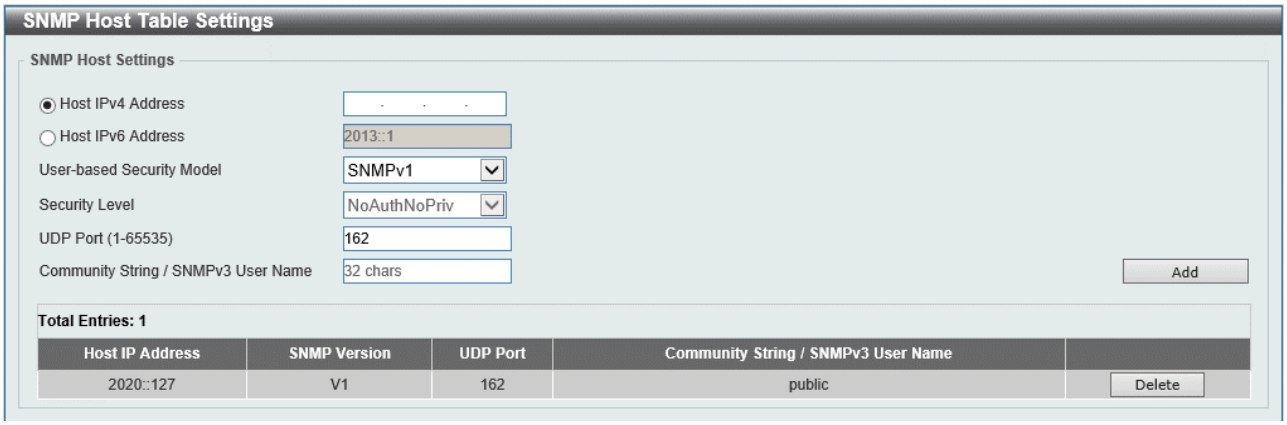
本画面の各項目の説明を以下に示します。

パラメーター	説明
User Name	SNMP ユーザー名を 32 文字以内で入力します。
Group Name	SNMP グループ名を 32 文字以内で入力します。
SNMP Version	SNMP バージョンを指定します。**v3** を選択してください。
SNMPv3 Encryption	SNMPv3 暗号化タイプ（**None** / **Password** / **Key**）を選択します。
Auth-Protocol by Password	**SNMPv3 Encryption** で **Password** を選択した場合に、以下のどちらかの認証プロトコルを選択し、テキストボックスにパスワードを指定します。 • **MD5**：HMAC-MD5-96 認証プロトコルを使用する場合に選択します。 • **SHA**：HMAC-SHA 認証プロトコルを使用する場合に指定します。
Priv-Protocol by Password	**SNMPv3 Encryption** で **Password** を選択した場合に、暗号化について以下のどちらかを選択します。 • **None**：暗号化を使用しません。 • **DES56**： DES56 ビット暗号化を使用する場合に選択します。テキストボックスにパスワードを入力します。
Auth-Protocol by Key	**SNMPv3 Encryption** で **Key** を選択した場合に、以下のどちらかの認証プロトコルを選択し、テキストボックスにキーを指定します。 • **MD5**：HMAC-MD5-96 認証プロトコルを使用する場合に選択します。 • **SHA**：HMAC-SHA 認証プロトコルを使用する場合に選択します。
Priv-Protocol by Key	**SNMPv3 Encryption** で **Key** を選択した場合に、暗号化について以下のどちらかを選択します。 • **None**：認証プロトコルを使用しない場合に選択します。 • **DES56**：DES56 ビット暗号化を使用する場合に選択します。テキストボックスには、キーを入力します。
IP Access-List Name	ユーザーに関連付ける標準 IP ACL の名称を 32 文字以内で入力します。

入力した情報で SNMP ユーザーを追加するには、**Add** ボタンをクリックします。
SNMP ユーザーを削除するには、**Delete** ボタンをクリックします。

4.5.8 SNMP Host Table Settings

SNMP Host Table Settings 画面では、SNMP トラップの通知ホストを設定します。所定のイベントが発生すると、装置は登録したホスト宛に SNMP トラップを送信します。
本画面を表示するには、**Management** > **SNMP** > **SNMP Host Table Settings** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Host IPv4 Address	SNMP トラップの通知ホストの IPv4 アドレスを入力します。
Host IPv6 Address	SNMP トラップの通知ホストの IPv6 アドレスを入力します。
User-based Security Model	以下のいずれかのセキュリティーモデルを選択します。 • **SNMPv1**：SNMPv1 を使用します。 • **SNMPv2c**：SNMPv2c を使用します。 • **SNMPv3**： SNMPv3 を使用します。このセキュリティーモデルの場合、**Security Level** で SNMPv3 セキュリティーレベルを指定する必要があります。
Security Level	**User-based Security Model** で **SNMPv3** を選択した場合、以下のいずれかのセキュリティーレベルを選択します。 • **NoAuthNoPriv**：認証と暗号化を行いません。 • **AuthNoPriv**：認証を行いますが、暗号化を行いません。 • **AuthPriv**：認証と暗号化を行います。
UDP Port	UDP ポート番号を 1～65535 の範囲で入力します。
Community String / SNMPv3 User Name	SNMP トラップを送信する際に使用する SNMP コミュニティー名、または SNMPv3 ユーザー名を 32 文字以内で入力します。

入力した情報で SNMP ホストを追加するには、**Add** ボタンをクリックします。
SNMP ホストを削除するには、**Delete** ボタンをクリックします。

4.6 RMON

RMON サブメニューでは、RMON に関する設定を行います。RMON は、RMON-MIB の MIB オブジェクトをモニタリングし、所定のイベント発生時に SNMP トラップなどにより通知することで、ネットワークの監視を行います。

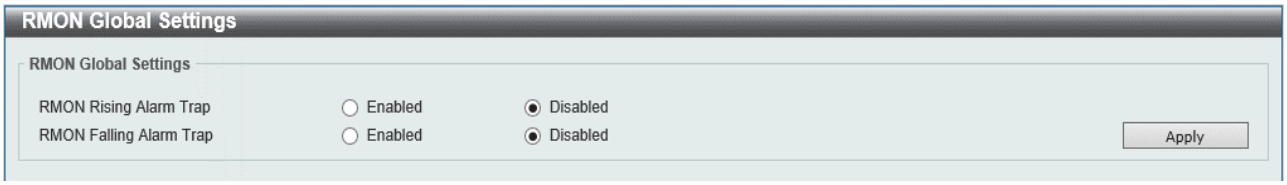
RMON の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
4.6.1	RMON Global Settings	RMON の SNMP トラップ送信のグローバル設定
4.6.2	RMON Statistics Settings	RMON 統計情報の設定
4.6.3	RMON History Settings	RMON 履歴情報の設定
4.6.4	RMON Alarm Settings	RMON アラームの設定
4.6.5	RMON Event Settings	RMON アラームのイベントの設定

4.6.1 RMON Global Settings

RMON Global Settings 画面では、RMON 上昇／下降アラームトラップ機能の有効／無効を設定します。RMON では、モニタリングする MIB 情報が所定のしきい値を超過した場合に、登録したイベントに沿って SNMP トラップ（risingAlarm: 1.3.6.1.2.1.16.0.1、fallingAlarm: 1.3.6.1.2.1.16.0.2）を送信できます。ここでは、SNMP トラップを送信する機能のグローバル設定を行います。SNMP トラップを送信する条件（モニタリングする MIB オブジェクト、しきい値など）は RMON アラーム設定（**Management > RMON > RMON Alarm Settings**）で設定します。

本画面を表示するには、**Management > RMON > RMON Global Settings** をクリックします。



本画面の各項目の説明を以下に示します。

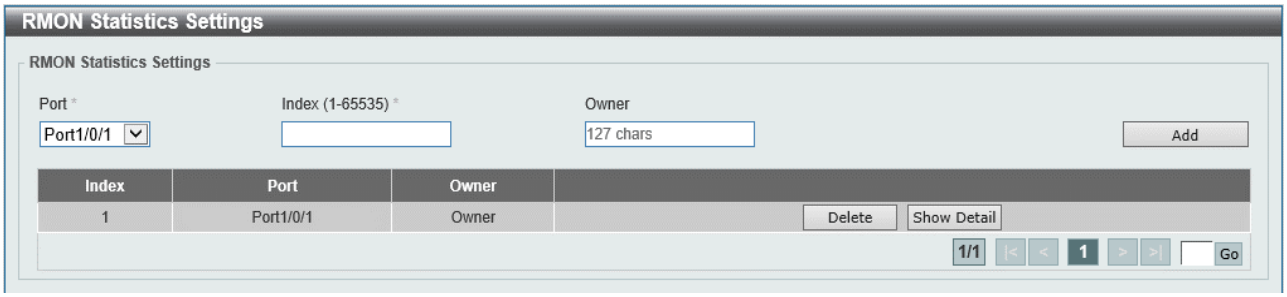
パラメーター	説明
RMON Rising Alarm Trap	上昇アラーム（risingAlarm）トラップを送信する場合は **Enabled** を選択します。送信しない場合は **Disabled** を選択します。
RMON Falling Alarm Trap	下降アラーム（fallingAlarm）トラップを送信する場合は **Enabled** を選択します。送信しない場合は **Disabled** を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

4.6.2 RMON Statistics Settings

RMON Statistics Settings 画面では、RMON 統計情報を収集するポートの設定や、取得した統計情報の確認を行うことができます。RMON 統計情報は、RMON-MIB の statistics グループで規定されている、パケット数やエラー数などの統計情報です。

本画面を表示するには、Management > RMON > RMON Statistics Settings をクリックします。

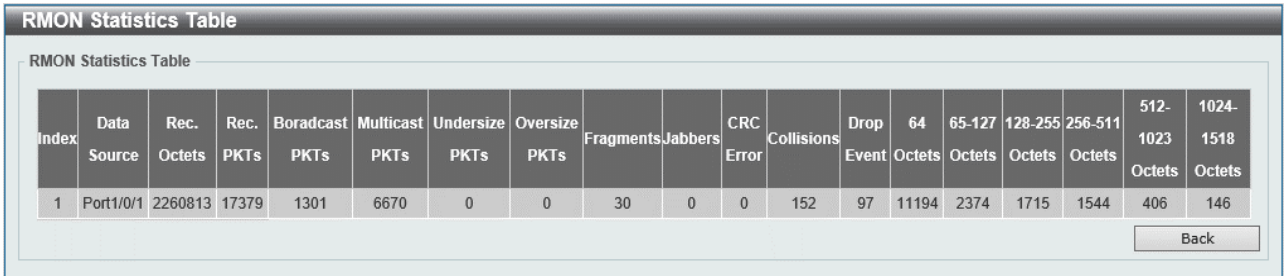


本画面の各項目の説明を以下に示します。

パラメーター	説明
Port	ポートを選択します。
Index	インデックスを 1～65535 の範囲で入力します。
Owner	オーナー情報を 127 文字以内で入力します。

入力した情報で RMON 統計を収集するポートを追加するには、Add ボタンをクリックします。
ポートを削除するには、Delete ボタンをクリックします。
特定のポートの詳細情報を表示するには、Show Detail ボタンをクリックします。

Show Detail ボタンをクリックすると、RMON Statistics Table 画面が表示されます。

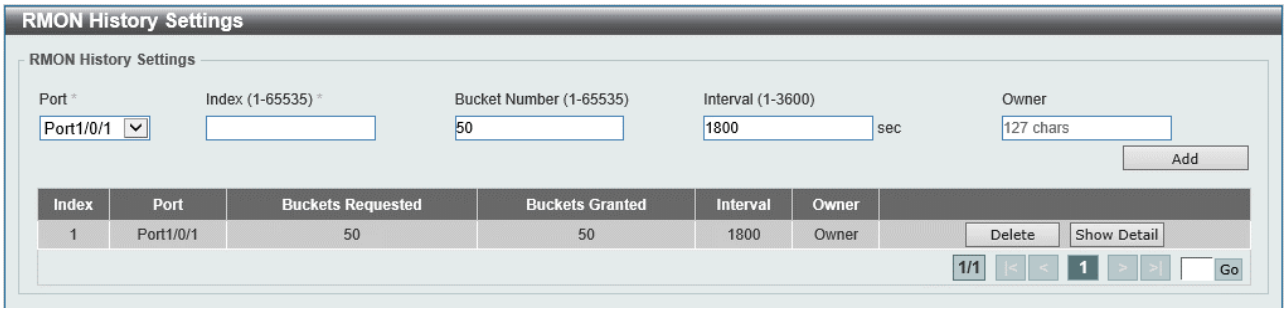


前の画面に戻るには、Back ボタンをクリックします。

4.6.3 RMON History Settings

RMON History Settings 画面では、RMON 履歴情報を取得するポートや取得条件の設定や、取得した履歴情報の確認を行うことができます。RMON 履歴情報は、RMON-MIB の history グループで規定されている、パケット数やエラー数などのスナップショット情報です。

本画面を表示するには、**Management** > **RMON** > **RMON History Settings** をクリックします。

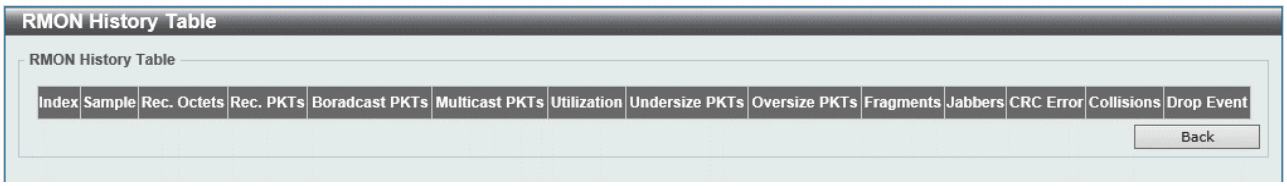


本画面の各項目の説明を以下に示します。

パラメーター	説明
Port	ポートを選択します。
Index	インデックスを 1～65535 の範囲で入力します。
Bucket Number	履歴情報のスナップショットを保存するバケットの数を 1～65535 の範囲で入力します。
Interval	スナップショットの取得間隔を 1～3600（秒）の範囲で入力します。
Owner	オーナー情報を 127 文字以内で入力します。

入力した情報で RMON MIB 履歴統計を収集するポートを追加するには、**Add** ボタンをクリックします。
ポートを削除するには、**Delete** ボタンをクリックします。
ポートの詳細情報を表示するには、**Show Detail** ボタンをクリックします。

Show Detail ボタンをクリックすると、**RMON History Table** 画面が表示されます。

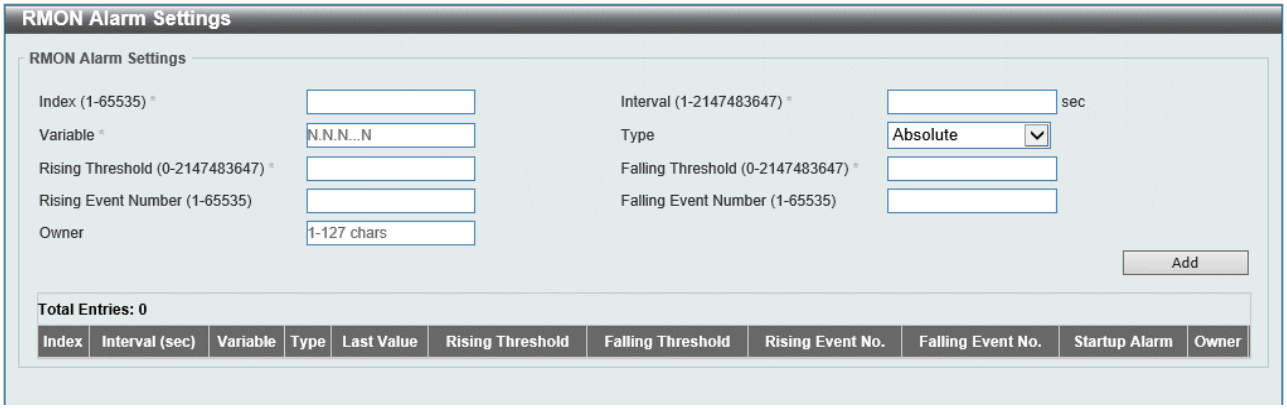


前の画面に戻るには、**Back** ボタンをクリックします。

4.6.4 RMON Alarm Settings

RMON Alarm Settings 画面では、RMON アラーム設定を行います。RMON アラームは、特定の MIB 値をモニタリングして、指定したしきい値を超過した場合に RMON イベント（上昇イベント、下降イベント）を発行します。イベント発行時のアクションには、SNMP トラップでの通知やログの出力などがあり、**Management** > **RMON** > **RMON Event Settings** で登録したアクションから指定します。

本画面を表示するには、**Management** > **RMON** > **RMON Alarm Settings** をクリックします。



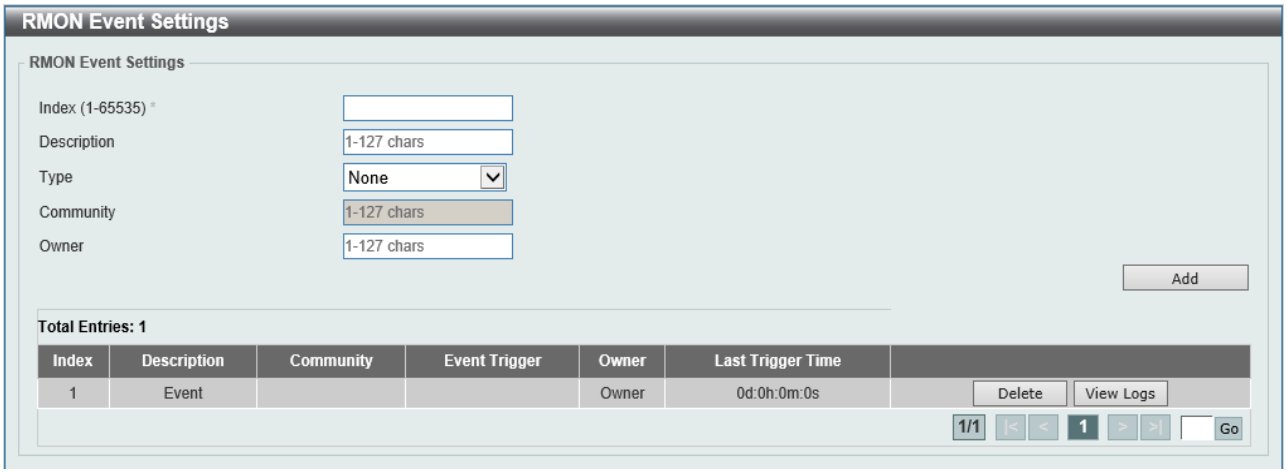
本画面の各項目の説明を以下に示します。

パラメーター	説明
Index	インデックスを 1～65535 の範囲で入力します。
Interval	サンプリングとしきい値のチェックの間隔を 1～2147483647（秒）の範囲で入力します。
Variable	サンプリングする MIB オブジェクトの OID を入力します。
Type	監視タイプ（**Absolute** / **Delta**）を選択します。
Rising Threshold	上昇しきい値を 0～2147483647 の範囲で入力します。
Falling Threshold	下降しきい値を 0～2147483647 の範囲で入力します。
Rising Event Number	上昇イベント発行時のアクションのイベントインデックスを 1～65535 の範囲で入力します。 指定しない場合、上限値を超えてもアクションは実行されません。
Falling Event Number	下降イベント発行時のアクションのイベントインデックスを 1～65535 の範囲で入力します。 指定しない場合、下限値を超えてもアクションは実行されません。
Owner	オーナー情報を 127 文字以内で入力します。

入力した情報でアラームエントリーを追加するには、**Add** ボタンをクリックします。
アラームエントリーを削除するには、**Delete** ボタンをクリックします。

4.6.5 RMON Event Settings

RMON Event Settings 画面では、RMON アラームのイベントのアクションエントリーを設定します。
本画面を表示するには、Management > RMON > RMON Event Settings をクリックします。

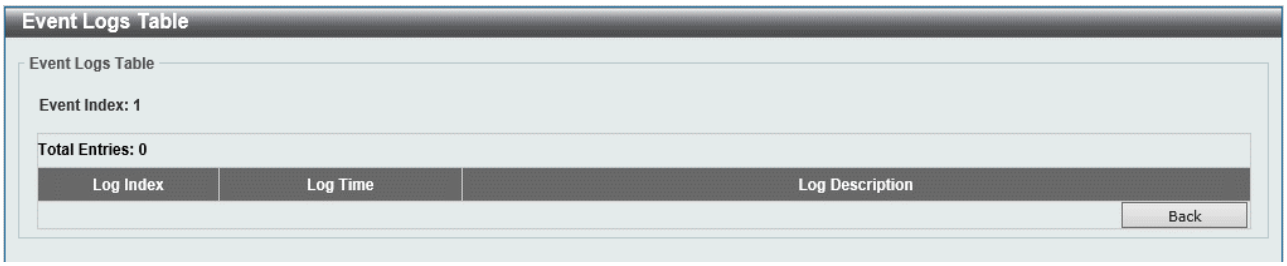


本画面の各項目の説明を以下に示します。

パラメーター	説明
Index	インデックス値を 1～65535 の範囲で入力します。
Description	RMON イベントエントリーの説明を 127 文字以内で入力します。
Type	RMON イベントのアクションの種類（None / Log / Trap / Log and Trap）を選択します。Log はイベントログを出力し、Trap は SNMP トラップを送信します。Log and Trap の場合には両方を実行します。
Community	Type で Trap または Log and Trap を選択した場合に、SNMP コミュニティーを 127 文字以内で入力します。
Owner	オーナー情報を 127 文字以内で入力します。

入力した情報でイベントエントリーを追加するには、Add ボタンをクリックします。
イベントエントリーを削除するには、Delete ボタンをクリックします。
イベントログを表示するには、View Logs ボタンをクリックします。

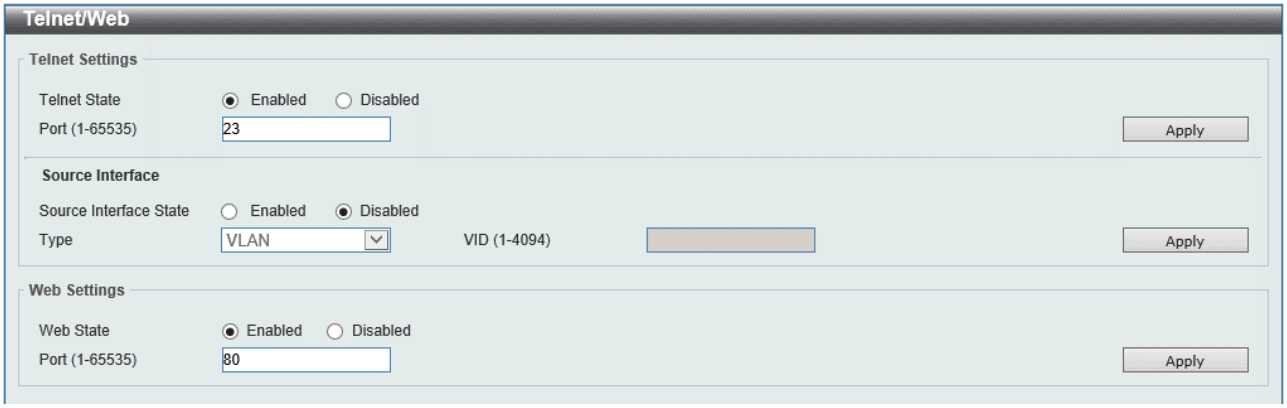
View Logs ボタンをクリックすると、Event Logs Table 画面が表示されます。



前の画面に戻るには、Back ボタンをクリックします。

4.7 Telnet/Web

Telnet/Web 画面では、CLI の Telnet サーバー機能、および Web UI の Web サーバー機能のグローバル設定を行います。
本画面を表示するには、**Management** > **Telnet/Web** をクリックします。



Telnet Settings では、Telnet サーバー機能の設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Telnet State	Telnet サーバー機能の状態（**Enabled** / **Disabled**）を選択します。
Port	Telnet 接続の TCP ポート番号を 1～65535 の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

Source Interface では、Telnet サーバーの送信インターフェースの設定を行います。本装置では使用しません。

パラメーター	説明
Source Interface State	インターフェースの指定の有無（**Enabled** / **Disabled**）を選択します。
Type	インターフェースのタイプを選択します。**VLAN** のみ使用可能です。
VID	VLAN ID を 1～4094 の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

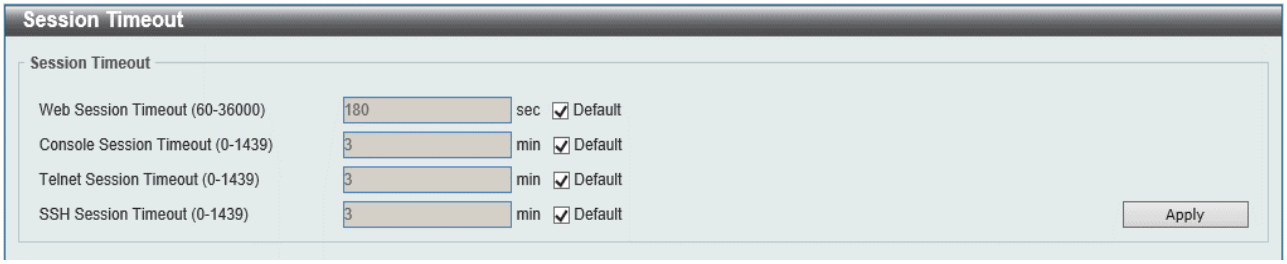
Web Settings では、Web サーバー機能の設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Web State	Web サーバー機能の状態（**Enabled** / **Disabled**）を選択します。
Port	HTTP 接続の TCP ポート番号を 1～65535 の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

4.8 Session Timeout

Session Timeout 画面では、CLI および Web UI のセッションタイムアウトを設定します。CLI のセッションタイムアウトは、コンソール接続、Telnet 接続、SSH 接続でそれぞれ個別に指定できます。
本画面を表示するには、**Management** > **Session Timeout** をクリックします。



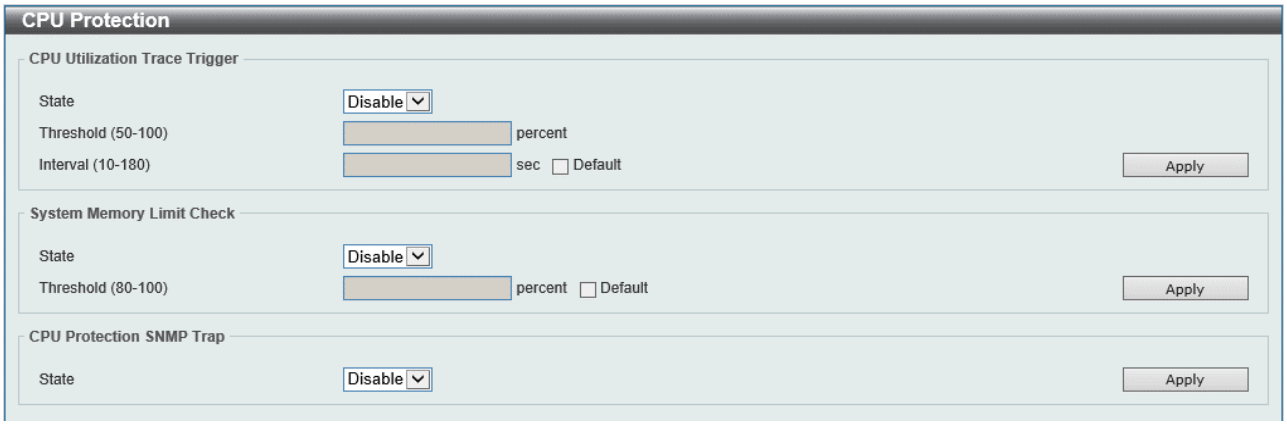
本画面の各項目の説明を以下に示します。

パラメーター	説明
Web Session Timeout	Web UI のセッションタイムアウト値を 60～36000（秒）の範囲で入力します。**Default** をチェックするとデフォルト値（180 秒）に戻ります。
Console Session Timeout	CLI のコンソール接続でのセッションタイムアウト値を 0～1439（分）の範囲で入力します。タイムアウトを無効にするには 0 を入力します。 **Default** をチェックするとデフォルト値（3 分）に戻ります。
Telnet Session Timeout	CLI の Telnet 接続でのセッションタイムアウト値を 0～1439（分）の範囲で入力します。タイムアウトを無効にするには 0 を入力します。 **Default** をチェックするとデフォルト値（3 分）に戻ります。
SSH Session Timeout	CLI の SSH 接続でのセッションタイムアウト値を 0～1439（分）の範囲で入力します。タイムアウトを無効にするには 0 を入力します。 **Default** をチェックするとデフォルト値（3 分）に戻ります。

設定を適用するには、**Apply** ボタンをクリックします。

4.9 CPU Protection

CPU Protection 画面では、CPU 保護機能を設定します。CPU 保護機能には、CPU 使用率チェック機能と、システムメモリー使用率チェック機能があります。
本画面を表示するには、Management > CPU Protection をクリックします。



CPU Utilization Trace Trigger では、CPU 使用率チェック機能について設定します。各項目の説明を以下に示します。

パラメーター	説明
State	CPU 使用率チェック機能の状態（Enabled / Disabled）を選択します。
Threshold	しきい値を 50～100（%）の範囲で入力します。
Interval	監視間隔を 10～180（秒）の範囲で入力します（デフォルト：10 秒）。 デフォルト値を使用するには、Default をチェックします。

設定を適用するには、Apply ボタンをクリックします。

System Memory Limit Check では、システムメモリー使用率チェック機能について設定します。各項目の説明を以下に示します。

パラメーター	説明
State	システムメモリー使用率チェック機能の状態（Enabled / Disabled）を選択します。
Threshold	しきい値を 80～100（%）の範囲で入力します（デフォルト：90 %）。 デフォルト値を使用するには、Default をチェックします。

設定を適用するには、Apply ボタンをクリックします。

CPU Protection SNMP Trap では、CPU 使用率チェック機能の SNMP トラップ通知の設定を行います。各項目の説明を以下に示します。

パラメーター	説明
State	CPU 使用率チェックの SNMP トラップ通知を行う場合は Enabled を選択します。通知しない場合は Disabled を選択します。

設定を適用するには、Apply ボタンをクリックします。

4.10 IP Source Interface

IP Source Interface 画面では、装置が TFTP と FTP で使用する送信元 IP インターフェースを設定します。本装置では使用しません。
本画面を表示するには、Management > IP Source Interface をクリックします。

IP TFTP Source Interface の各項目の説明を以下に示します。

パラメーター	説明
Source Interface State	TFTP での送信元 IP インターフェースの状態（Enabled / Disabled）を選択します。
Interface Type	インターフェースタイプを選択します。VLAN のみ使用できます。
VID	VLAN ID を 1～4094 の範囲で入力します。

設定を適用するには、Apply ボタンをクリックします。

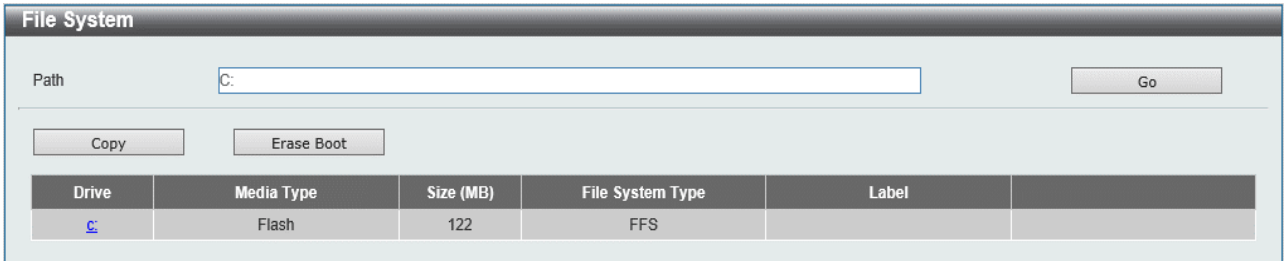
IP FTP Source Interface の各項目の説明を以下に示します。

パラメーター	説明
Source Interface State	FTP での送信元インターフェースの状態（Enabled / Disabled）を選択します。
Interface Type	インターフェースタイプを選択します。VLAN のみ使用できます。
VID	VLAN ID を 1～4094 の範囲で入力します。

設定を適用するには、Apply ボタンをクリックします。

4.11 File System

File System 画面では、装置のファイルシステムを表示、管理、および設定します。
本画面を表示するには、Management > File System をクリックします。

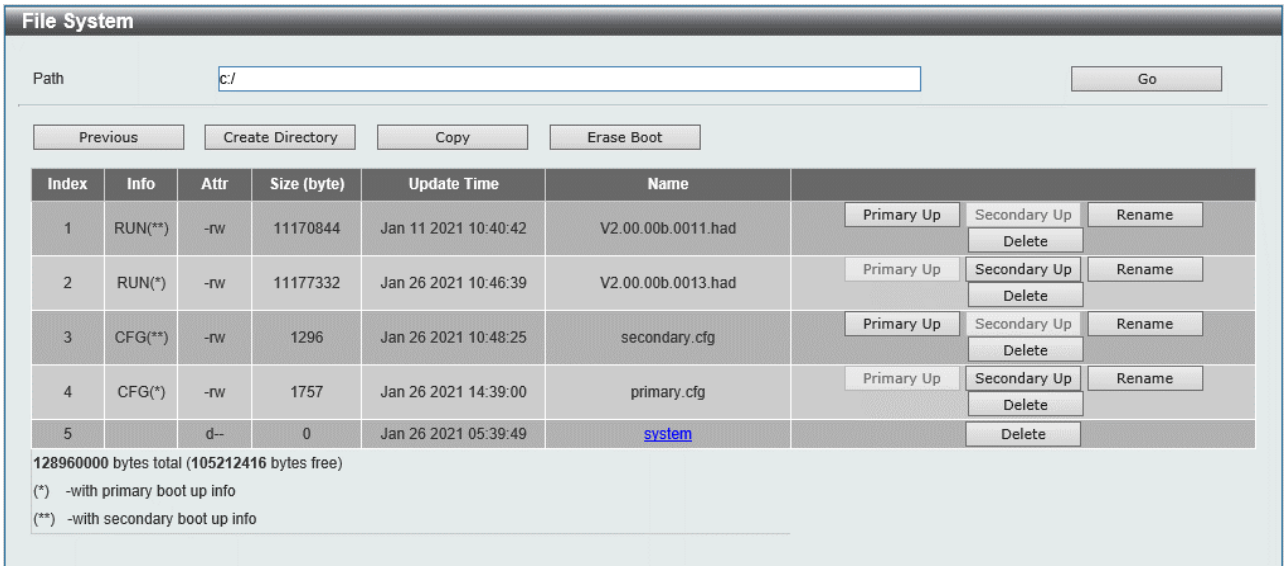


本画面の各項目の説明を以下に示します。

パラメーター	説明
Path	パスを入力します。

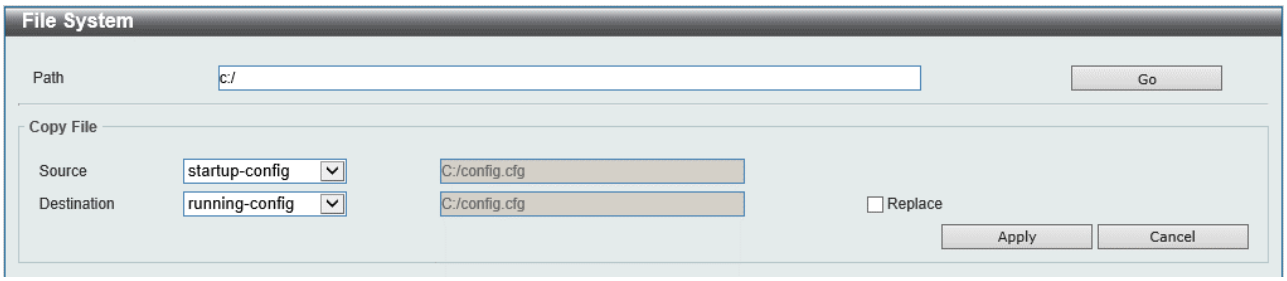
入力したパスに移動するには、Go ボタンをクリックします。
特定のファイルを装置にコピーするには、Copy ボタンをクリックします。
ブートファイルを消去するには、Erase Boot ボタンをクリックします。
装置のファイルシステムのルートディレクトリーに移動するには、Drive に表示されている「c:」のハイパーリンクをクリックします。

「c:」のハイパーリンクをクリックすると、以下に示す画面が表示されます。



入力したパスに移動するには、Go ボタンをクリックします。
前の画面に戻るには、Previous ボタンをクリックします。
装置のファイルシステム内に新しいディレクトリを作成するには、Create Directory をクリックします。
ファイルを装置にコピーするには、Copy ボタンをクリックします。
ブートファイルを消去するには、Erase Boot ボタンをクリックします。

Copy ボタンをクリックすると、以下に示す画面が表示されます。



Copy File の各項目の説明を以下に示します。

パラメーター	説明
Source	コピー元のファイルを以下から選択します。 • startup-config：起動時設定ファイルをコピー元とします。 • Source File：コピー元をファイル名とパスで指定します。 • http-certificate： HTTPS 証明書ファイルをコピー元とします。 • https-private-key：HTTPS 秘密鍵ファイルをコピー元とします。 • aaa-local-db：ローカル AAA データベースのファイルをコピー元とします。 • primary-config：プライマリー設定ファイルをコピー元とします。
Destination	コピー先を以下のいずれかから選択します。 • running-config：装置の現在の設定に反映します。 • startup-config：起動時設定ファイルに反映します。 • Destination File：コピー先をファイル名とパスで指定します。 • http-certificate： HTTPS 証明書ファイルをコピー先とします。SSL または Web 認証が有効になっている場合、このファイルは更新できません。 • https-private-key：HTTPS 秘密鍵ファイルをコピー先とします。SSL または Web 認証が有効になっている場合、このファイルは更新できません。 • secondary-config：セカンダリー設定ファイルをコピー先とします。 現在のコピー先ファイルをコピー元ファイルに置き換えるには、Replace をチェックします。

コピーを開始するには、Apply ボタンをクリックします。
プロセスを破棄するには、Cancel ボタンをクリックします。

各ファイルの操作について

ファイルをプライマリーブートイメージ、またはプライマリー設定ファイルに指定するには、Primary Up ボタンをクリックします。
ファイルをセカンダリーブートイメージ、またはセカンダリー設定ファイルに指定するには、Secondary Up ボタンをクリックします。
ファイル名を変更するには、Rename ボタンをクリックします。
ファイルを削除するには、Delete ボタンをクリックします。

注意事項

起動時設定ファイルが破損している場合、装置は自動的にデフォルト構成に戻ります。

ブートイメージファイルが破損している場合、装置は次回の起動時にバックアップイメージファイルを自動的に使用します。

5 L2 Features

L2 Features メニューでは、イーサネットスイッチの基本的な機能であるレイヤー2 関連機能の設定を行います。ネットワークトポロジーに関するすべての設定は、このメニューで管理できます。
L2 Features の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
5.1	FDB	MAC アドレステーブルの状態やスタティック設定
5.2	VLAN	VLAN の設定
5.3	VLAN Tunnel	VLAN トンネル機能の設定
5.4	STP	スパニングツリープロトコルの設定
5.5	Loop Detection	ループ検知機能の設定
5.6	Link Aggregation	リンクアグリゲーションの設定
5.7	L2 Multicast Control	マルチキャスト通信制御の設定
5.8	LLDP	LLDP の設定

5.1 FDB

FDB サブメニューでは、装置の MAC アドレステーブルに関する設定や、情報取得を行います。
FDB の下にあるサブメニューの一覧を以下の表に示します。

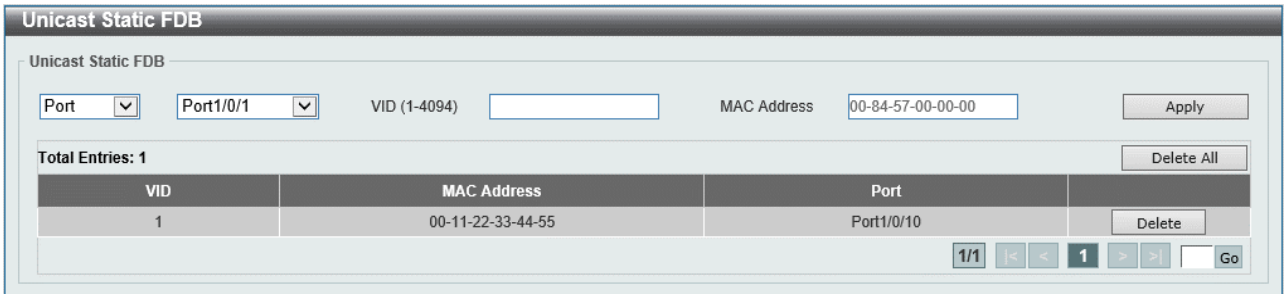
項番	メニュー名	概要
5.1.1	Static FDB	スタティックエントリーの登録
5.1.2	MAC Address Table Settings	MAC アドレステーブルのエージング設定
5.1.3	MAC Address Table	MAC アドレステーブルの情報を表示

5.1.1 Static FDB

Static FDB サブメニューでは、MAC アドレステーブルに登録するスタティックエントリーを作成します。ユニキャストアドレスとマルチキャストアドレスでエントリーの設定画面が異なります。

Unicast Static FDB

Unicast Static FDB 画面では、MAC アドレステーブル登録するユニキャスト MAC アドレスのスタティックエントリーを設定します。
本画面を表示するには、L2 Features > FDB > Static FDB > Unicast Static FDB をクリックします。



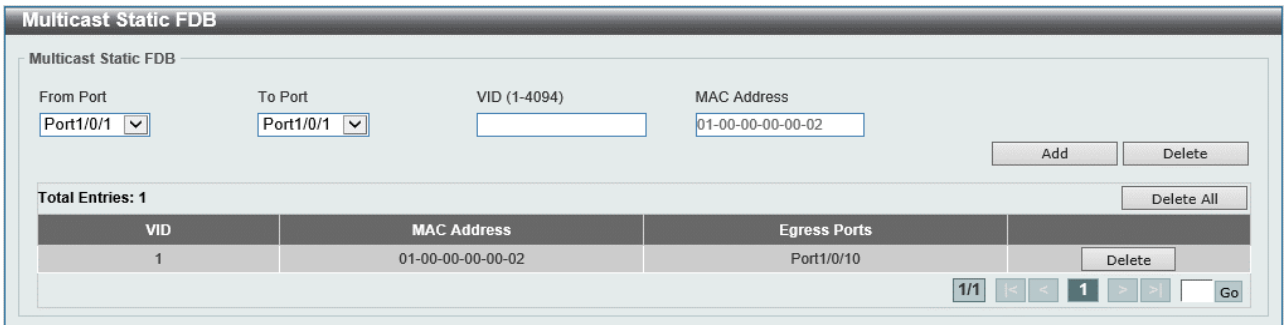
本画面の各項目の説明を以下に示します。

パラメーター	説明
Port/Drop	特定のポートのスタティックエントリーを作成する場合、Port を選択し、右にあるドロップダウンからポート番号を指定します。Drop を選択すると、送信元または宛先が特定の MAC アドレスを持つフレームを破棄するエントリーを作成します。
Port Number	登録するエントリーのポート番号を選択します。
VID	登録するエントリーの VLAN ID を 1～4094 の範囲で入力します。
MAC Address	登録するユニキャスト MAC アドレスを入力します。

設定を適用するには、Apply ボタンをクリックします。
すべてのエントリーを削除するには、Delete All ボタンをクリックします。
エントリーを削除するには、Delete ボタンをクリックします。

Multicast Static FDB

Multicast Static FDB 画面では、マルチキャスト MAC アドレステーブル登録するスタティックエントリーを設定します。
本画面を表示するには、Static FDB > Multicast Static FDB をクリックします。



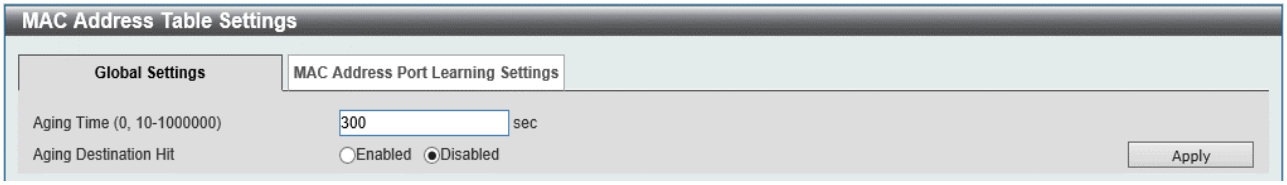
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	登録するエントリーのポートの範囲を選択します。
VID	登録するエントリーの VLAN ID を 1～4094 の範囲で入力します。
MAC Address	登録するマルチキャスト MAC アドレスを入力します。

設定を適用するには、Apply ボタンをクリックします。
すべてのエントリーを削除するには、Delete All ボタンをクリックします。
エントリーを削除するには、Delete ボタンをクリックします。

5.1.2 MAC Address Table Settings

MAC Address Table Settings 画面では、MAC アドレステーブルのアドレス学習に関する詳細設定を行います。
本画面を表示するには、L2 Features > FDB > MAC Address Table Settings をクリックします。



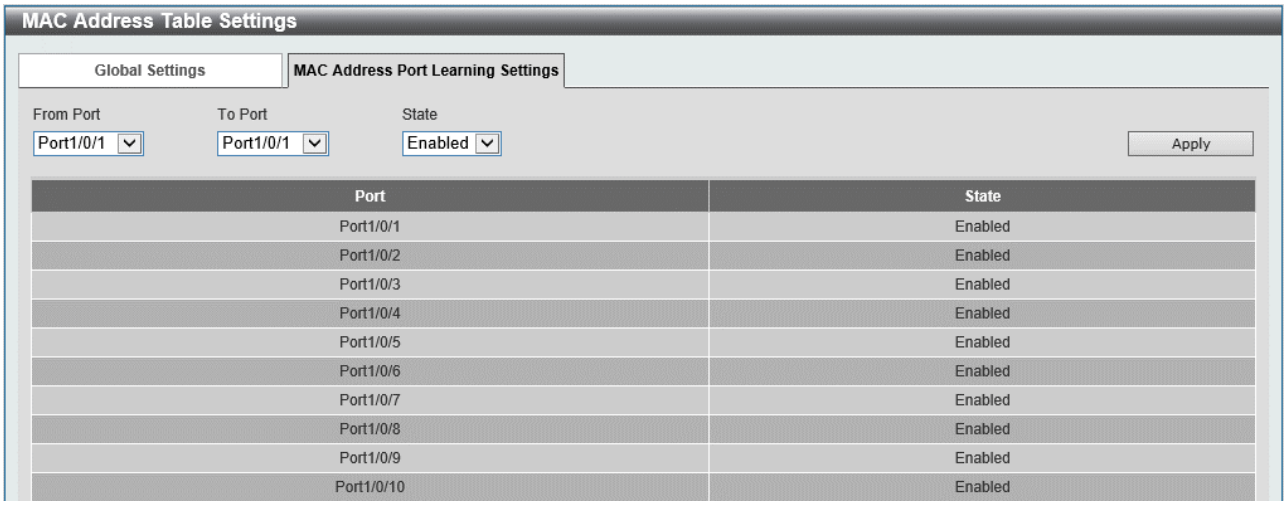
本画面には、Global Settings タブと MAC Address Port Learning Settings タブがあります。

Global Settings タブでは、MAC アドレステーブルのエージングに関する設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Aging Time	MAC アドレステーブルのエージングタイムを 0 または 10～1000000（秒）の範囲で入力します。0 の場合、エージング処理がされません。
Aging Destination Hit	受信したフレームでの送信元 MAC アドレスや VLAN 情報が学習済みのダイナミックエントリーと同じだった場合に、エントリーの有効期間を更新する機能の状態（Enabled / Disabled）を選択します。

設定を適用するには、Apply ボタンをクリックします。

MAC Address Port Learning Settings タブでは、MAC アドレス学習の有効/無効を設定します。



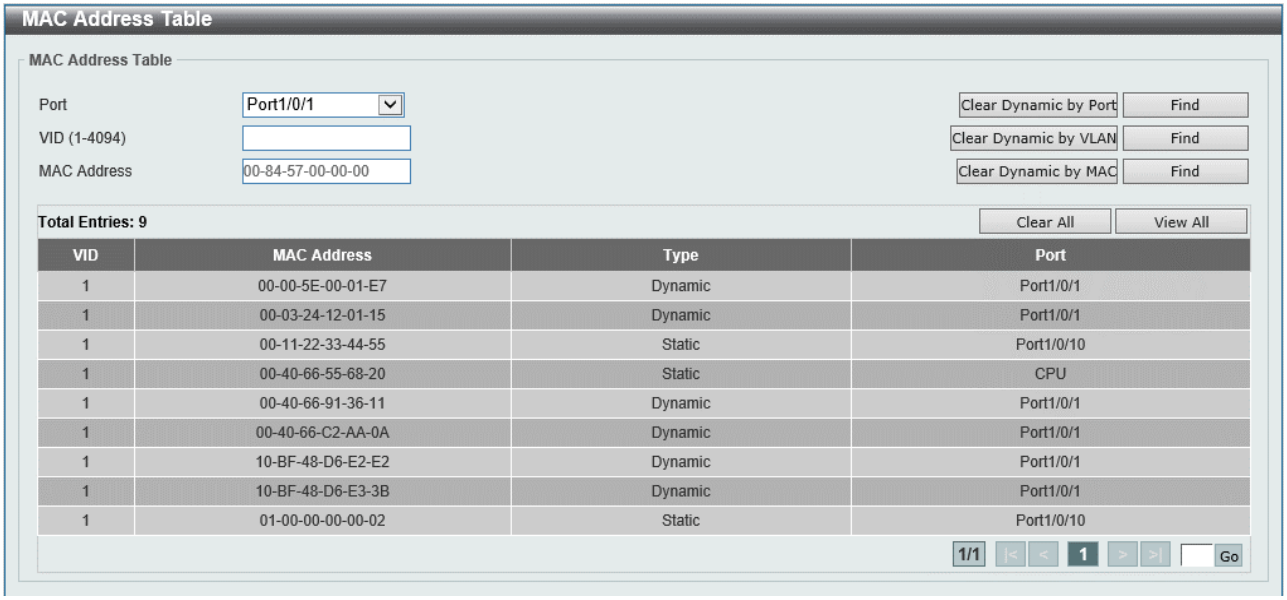
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートの範囲を選択します。
Status	選択したポートでの MAC アドレス学習の状態（Enabled / Disabled）を選択します。

設定を適用するには、Apply ボタンをクリックします。

5.1.3 MAC Address Table

MAC Address Table 画面では、MAC アドレステーブルのエントリーを表示します。
本画面を表示するには、L2 Features > FDB > MAC Address Table をクリックします。



MAC アドレステーブルの情報を絞り込む場合には、以下の項目を使用できます。

パラメーター	説明
Port	ポート番号を選択して絞り込みます。
VID	VLAN ID を 1～4094 の範囲で入力して絞り込みます。
MAC Address	MAC アドレスを入力して絞り込みます。

選択したポートにエントリーされているダイナミック MAC アドレスをクリアするには、Clear Dynamic by Port ボタンをクリックします。
選択した VLAN ID にエントリーされているダイナミック MAC アドレスをクリアするには、Clear Dynamic by VLAN ボタンをクリックします。
入力したダイナミック MAC アドレスをクリアするには、Clear Dynamic by MAC ボタンをクリックします。
入力した情報でエントリーを検索するには、Find ボタンをクリックします。
すべてのダイナミック MAC アドレスをクリアするには、Clear All ボタンをクリックします。
MAC アドレステーブルにエントリーされているすべての MAC アドレスを表示するには、View All ボタンをクリックします。

5.2 VLAN

VLAN サブメニューでは、VLAN の登録やポートへの割り当てなどの設定を行います。
VLAN の下にあるサブメニューの一覧を以下の表に示します。

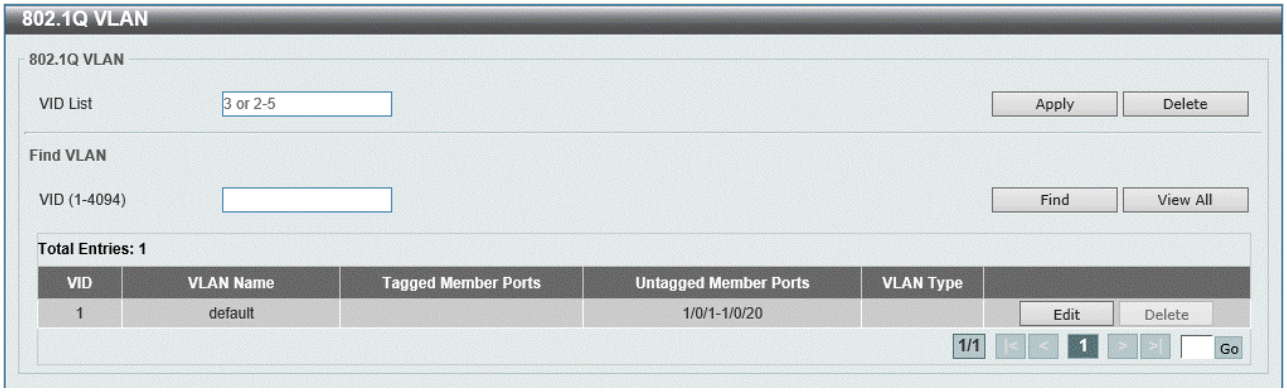
項番	メニュー名	概要
5.2.1	802.1Q VLAN	VLAN の作成
5.2.2	802.1v Protocol VLAN	プロトコル VLAN の設定
5.2.3	VLAN Interface	VLAN の割り当て
5.2.4	L2VLAN Interface Description	L2VLAN インターフェースの説明の設定

5.2.1 802.1Q VLAN

802.1Q VLAN 画面では、VLAN を設定します。
本画面で VLAN を作成すると、指定した VLAN ID の VLAN が登録されます。VLAN 名は自動的に VLANXXXX（XXXX は VLAN ID の 4 桁表示）と設定されます。VLAN 名は、表示されている VLAN 情報テーブルから編集できます。

デフォルトでは、VLAN 名が default である VLAN ID が 1 の VLAN が登録されています。このエントリーは削除できません。

本画面を表示するには、**L2 Features > VLAN > 802.1Q VLAN** をクリックします。



802.1Q VLAN の各項目の説明を以下に示します。

パラメーター	説明
VID List	作成または削除する VLAN ID のリストを入力します。

802.1Q VLAN を作成するには、**Apply** ボタンをクリックします。
802.1Q VLAN を削除するには、**Delete** ボタンをクリックします。

Find VLAN の各項目の説明を以下に示します。

パラメーター	説明
VID	検索する VLAN ID を 1～4094 の範囲で入力します。
VLAN Name	Edit ボタンをクリックした後、VLAN の名称を入力します。

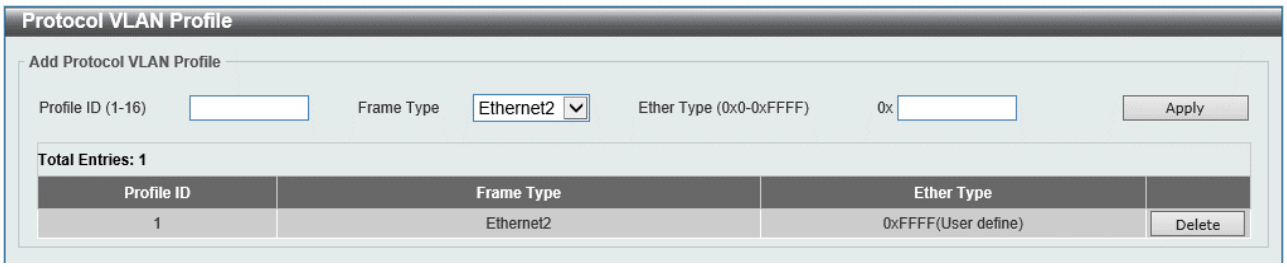
入力した情報で VLAN を検索するには、Find ボタンをクリックします。
すべての VLAN を表示するには、View All ボタンをクリックします。
VLAN を再設定するには、Edit ボタンをクリックします。
VLAN を削除するには、Delete ボタンをクリックします。

5.2.2 802.1v Protocol VLAN

802.1v Protocol VLAN サブメニューでは、プロトコル VLAN の設定を行います。
プロトコル VLAN は、Ethernet ヘッダーなどのデータリンク層のフレーム情報から上位層のプロトコル（たとえば IP や IPv6、ARP など）を識別し、所定の VLAN にマッピングする機能です。

Protocol VLAN Profile

Protocol VLAN Profile 画面では、プロトコル VLAN のプロファイルを設定します。
本画面を表示するには、L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile をクリックします。



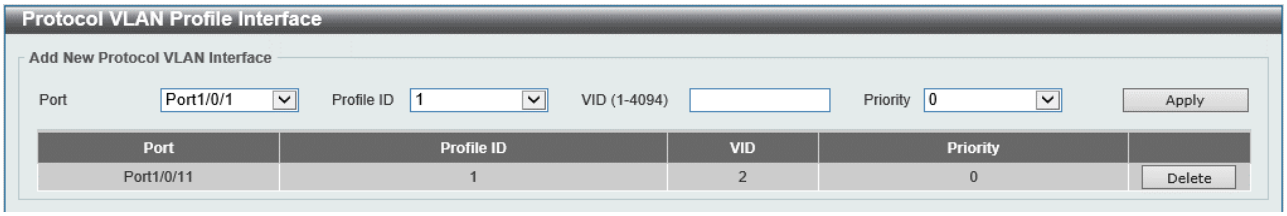
本画面の各項目の説明を以下に示します。

パラメーター	説明
Profile ID	プロファイル ID を 1～16 の範囲で入力します。
Frame Type	フレームタイプ（Ethernet2 / SNAP / LLC）を選択します。
Ether Type	イーサネットタイプ値を 0x0～0xFFFF の範囲で入力します。 フレームタイプに応じて、オクテット文字列は以下のいずれかの値になります。 • Ethernet2：EtherType の 2 オクテット情報。 • SNAP：Protocol ID の 2 オクテット情報 • LLC：LSAP ペア（DSAP、SSAP）の 2 オクテット情報。

設定を適用するには、Apply ボタンをクリックします。
802.1v プロトコル VLAN プロファイルを削除するには、Delete ボタンをクリックします。

Protocol VLAN Profile Interface

Protocol VLAN Profile Interface 画面では、ポートにプロトコル VLAN プロファイルを割り当てます。
本画面を表示するには、**802.1v Protocol VLAN > Protocol VLAN Profile Interface** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Port	構成する装置のポート番号を選択します。
Profile ID	802.1v プロトコル VLAN プロファイル ID を選択します。
VID	使用する VLAN ID を 1～4094 の範囲で入力します。
Priority	優先度の値として 0～7 のいずれかを選択します。

設定を適用するには、**Apply** ボタンをクリックします。
プロトコル VLAN プロファイルの割り当てを削除するには、**Delete** ボタンをクリックします。

5.2.3 VLAN Interface

VLAN Interface 画面では、VLAN をポートに割り当てます。
各物理ポートには 1 個以上の VLAN が割り当てられます。VLAN の割り当てには、VLAN タグ付きでフレームを処理するタグ VLAN と、VLAN タグなしで処理するタグなし VLAN があり、割り当てる VLAN の種類は各ポートに設定する VLAN モードによって異なります。VLAN モードには、以下の 4 種類があります。

- アクセスモード：1 個のタグなし VLAN のみが割り当てられます。
- トランクモード：複数のタグ VLAN と、1 個までのタグなし VLAN を割り当てられます。
- ハイブリッドモード：複数のタグ VLAN と複数のタグなし VLAN を割り当てられます。
- トンネルモード：VLAN トンネル機能のトンネルポートで使用されるモードです。

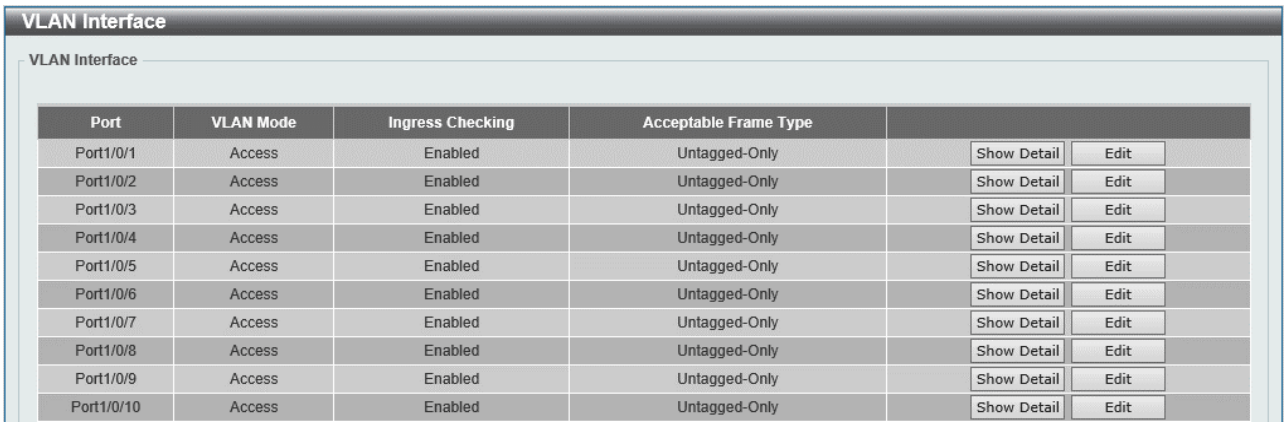
アクセスモードは、ポートに 1 個のタグなし VLAN のみを割り当てるモードで、ポートベース VLAN とも呼ばれます。対象ポートでは、原則として（ダイナミック VLAN などの機能が適用されない限り）割り当てた VLAN に対するタグなしフレームの送受信処理を行います。
本装置は、デフォルトですべてのポートがアクセスモードで、VLAN ID:1 のタグなし VLAN が割り当てられています。

トランクモードは、1 つのポートに複数のタグ VLAN を割り当てることができます。タグ VLAN に割り当てた VLAN でのフレーム転送処理が発生する場合、対象ポートからタグ付きフレームで送信します。トランクモードでは、ネイティブ VLAN と呼ばれる 1 個のタグなし VLAN を割り当てることができます。ネイティブ VLAN でのフレーム転送処理が発生する場合、対象ポートからタグなしフレームで転送します。また、対象ポートで受信したタグなしフレームは、ネイティブ VLAN での入力として処理されます。

ハイブリッドモードでは、トランクモードでのタグ VLAN とネイティブ VLAN の割り当てに加えて、複数のタグなし VLAN を割り当てることができます。タグ VLAN に割り当てた VLAN でのフレーム転送の処理はトランクモードと同じです。タグなし VLAN に割り当てた VLAN での転送処理が発生した場合は、対象ポートからタグなしフレームで転送します。対象ポートで受信したタグなしフレームは、プロトコル VLAN などの機能が適用されない限り、ネイティブ VLAN での入力として処理されます。ハイブリッドモードでのネイティブ VLAN の VLAN ID は PVID とも呼ばれます。

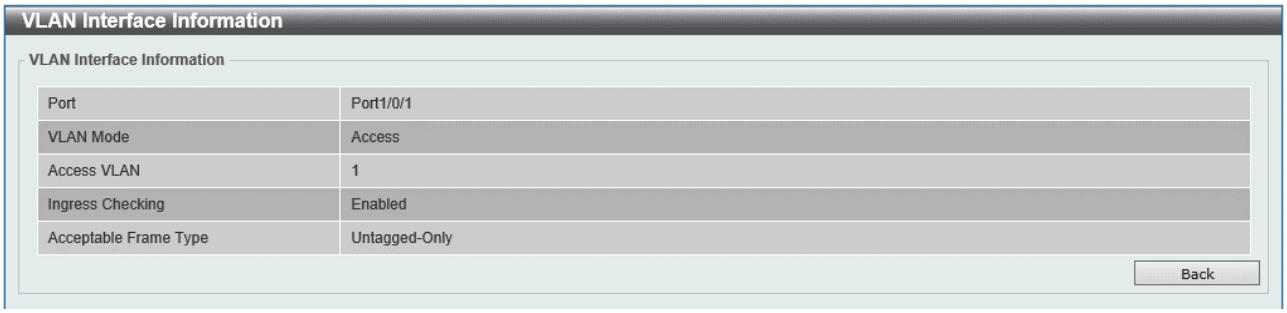
トンネルモードは、VLAN トンネル機能でのトンネルポートで適用するモードです。VLAN トンネル機能の詳細は「5.3 VLAN Tunnel」を参照ください。

本画面を表示するには、**L2 Features > VLAN > VLAN Interface** をクリックします。



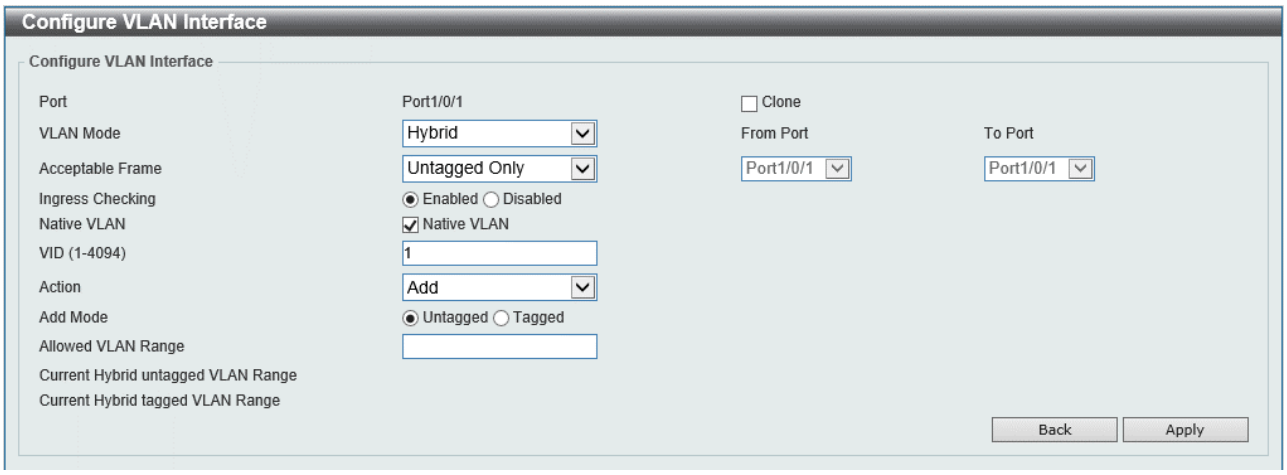
インターフェース上の VLAN の詳細情報を表示するには、**Show Detail** ボタンをクリックします。
VLAN インターフェースを再設定するには、**Edit** ボタンをクリックします。

Show Detail ボタンをクリックすると、以下に示す画面が表示されます。



インターフェース上の VLAN の詳細情報が表示されます。
前の画面に戻るには、**Back** ボタンをクリックします。

Edit ボタンをクリックすると、以下に示す画面が表示されます。以下の画面は、選択している VLAN モードによって表示内容（設定項目）が異なります。



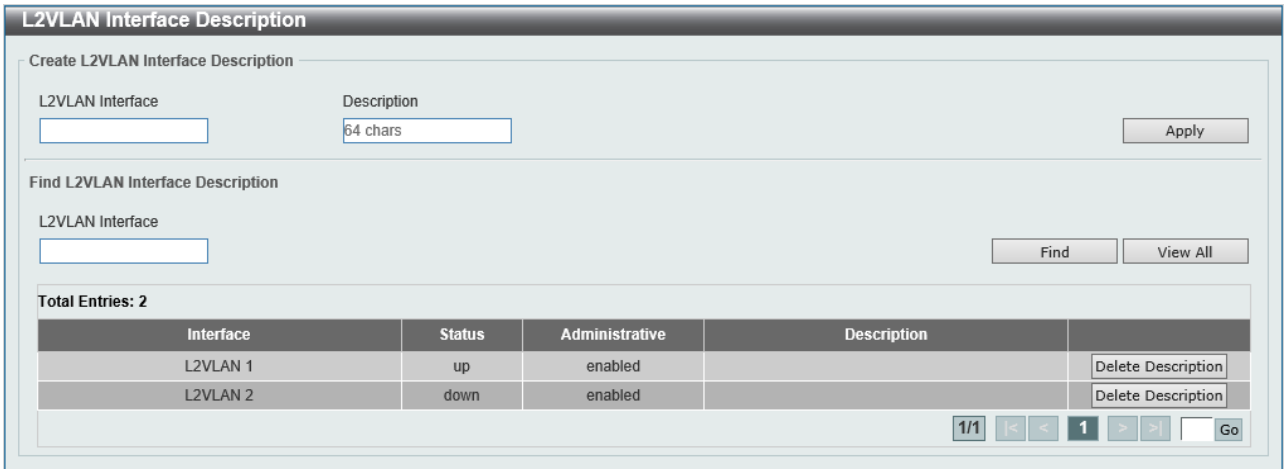
Configure VLAN Interface の各項目の説明を以下に示します。

パラメーター	説明
VLAN Mode	VLAN モード（Access / Hybrid / Trunk / Dot1q Tunnel）を選択します。
Acceptable Frame	受信許可するフレームの種別（Tagged Only / Untagged Only / Admit All）を選択します。
Ingress Checking	イングレスチェック機能の状態（Enabled / Disabled）を選択します。
Native VLAN	ネイティブ VLAN 機能を指定する場合にチェックします。 VLAN Mode が Hybrid または Trunk の場合に表示されます。
VID	VLAN ID を 1～4094 の範囲で入力します。
Action	VLAN Mode で Hybrid、Trunk、または Dot1q Tunnel を選択した後、実行するアクション（None / All / Add / Remove / Tagged / Untagged / Except / Replace）を選択します。 Add の場合は VLAN の追加を行います。Remove では、VLAN の割り当てを削除します。 Tagged と Untagged は VLAN Mode が Hybrid の場合に選択可能で、VLAN 割り当ての設定の上書きを行います。 None、All、Except、Replace は VLAN Mode が Trunk の場合に選択可能です。None は、VLAN の割り当てを変更しません。All は、すべての VLAN をメンバーに含めます。Except は、指定した VLAN をメンバーから削除します。Replace は、上書きで VLAN 割り当てを変更します。
Add Mode	VLAN Mode で Hybrid または Dot1q Tunnel を選択し、Action で Add を選択した場合に、Untagged または Tagged を選択します。
Allowed VLAN Range	VLAN Mode で Hybrid、Trunk、または Dot1q Tunnel を選択した後、アクションを行う VLAN の範囲を入力します。
Clone	同じ設定を他のポートにも反映する場合にチェックします。
From Port / To Port	Clone をチェックしている場合に、反映するポートの範囲を選択します。

設定を適用するには、Apply ボタンをクリックします。
前の画面に戻るには、Back ボタンをクリックします。

5.2.4 L2VLAN Interface Description

L2VLAN Interface Description 画面では、レイヤー2VLAN インターフェースの説明を設定します。
本画面を表示するには、L2 Features > VLAN > L2VLAN Interface Description をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
L2VLAN Interface	レイヤー2VLAN インターフェース ID を入力します。
Description	レイヤー2VLAN インターフェースの説明を 64 文字以内で入力します。

設定を適用するには、Apply ボタンをクリックします。
入力した情報でレイヤー2VLAN インターフェースを検索するには、Find ボタンをクリックします。
すべてのレイヤー2VLAN を表示するには、View All ボタンをクリックします。
レイヤー2VLAN から説明を削除するには、Delete Description ボタンをクリックします。

5.3 VLAN Tunnel

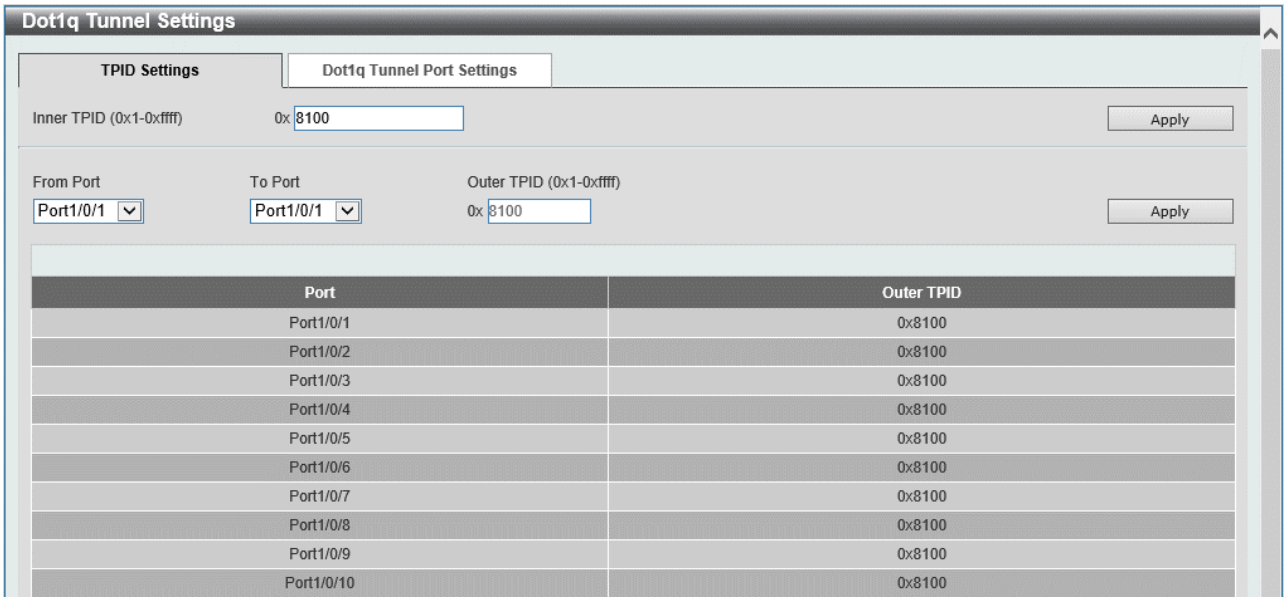
VLAN Tunnel サブメニューでは、VLAN トンネル機能の設定を行います。
VLAN トンネルは、QinQ というフレームのカプセリングにより、サービスプロバイダーネットワークを経由する拠点間のネットワーク通信で、VLAN 情報の保持を実現する機能です。本機能は、サービスプロバイダーネットワークとカスタマーネットワークの境界にある装置で使用されます。カスタマーネットワークでのトラフィックはカプセリングされ、プロバイダーネットワーク用の VLAN タグ（S-tag）情報を付与してプロバイダーネットワークに転送されます。プロバイダーネットワークから受信したフレームは、カプセリングされたフレーム情報からカスタマーネットワーク用の VLAN タグ（C-tag）情報をチェックし、カプセリングを解除してカスタマーネットワークに転送されます。

VLAN Tunnel の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
5.3.1	Dot1q Tunnel Settings	VLAN トンネルの基本設定
5.3.2	VLAN Mapping Settings	VLAN トンネルの VLAN 変換マップの設定

5.3.1 Dot1q Tunnel Settings

Dot1q Tunnel Settings 画面では、802.1Q VLAN トンネルを設定します。
本画面を表示するには、**L2 Features > VLAN Tunnel > Dot1q Tunnel Settings** をクリックします。



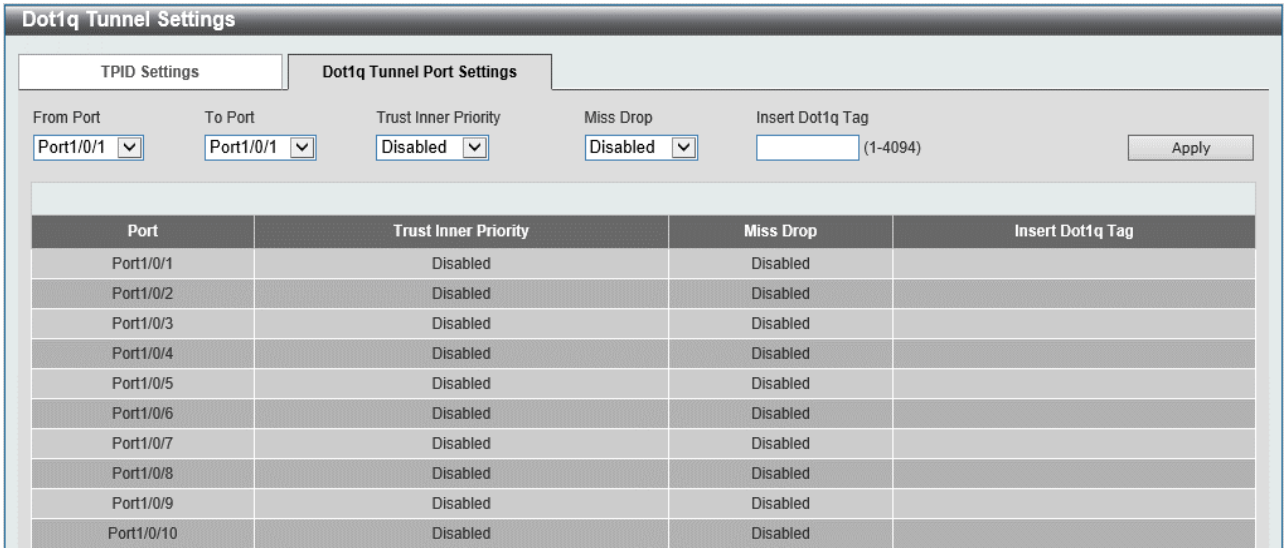
本画面には、**TPID Settings** タブと **Dot1q Tunnel Port Settings** タブがあります。

TPID Settings タブでは、VLAN タグの識別に使用する TPID を設定します。各項目の説明を以下に示します。

パラメーター	説明
Inner TPID	内部 TPID 値を 0x1～0xFFFF の範囲で入力します。 内部 TPID 値は 16 進形式です。カスタマーVLAN タグの TPID は、受信パケットに C-tag が付けられているかどうかを判断するために使用されます。内部 TPID は、システムごとに設定できます。
From Port / To Port	使用するポート範囲を選択します。
Outer TPID	外部 TPID 値を 0x1～0xFFFF の範囲で入力します（デフォルト：0x8100）。

設定を適用するには、**Apply** ボタンをクリックします。

Dot1q Tunnel Port Settings タブでは、トンネルポートでの動作の設定を行います。



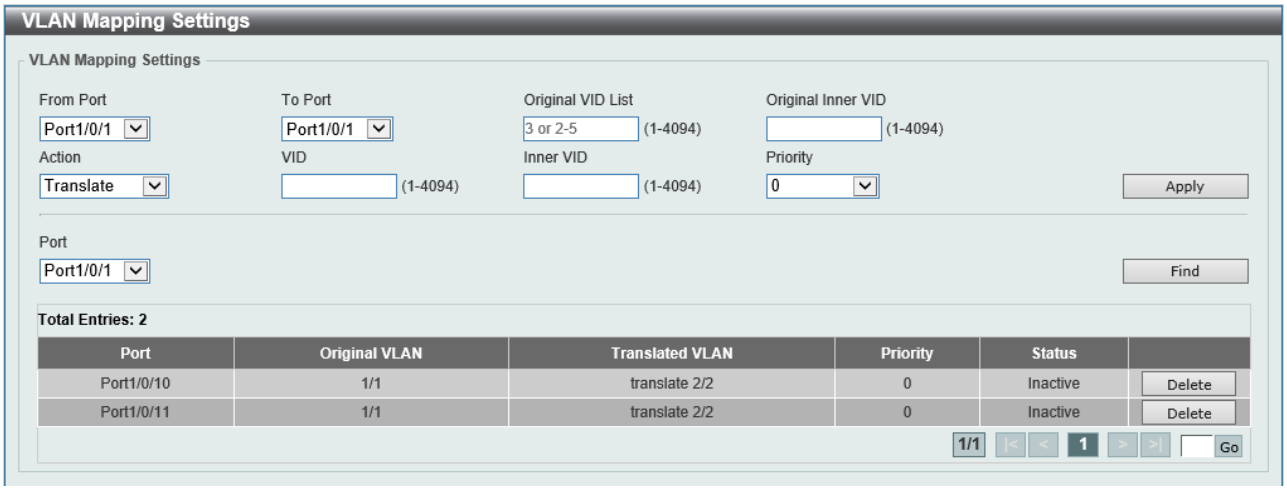
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	使用するポート範囲を選択します。
Trust Inner Priority	この設定が **Enabled** の場合、受信したタグ付きフレームの VLAN タグの優先度情報がサービス VLAN タグに反映されます。
Miss Drop	この設定が **Enabled** の場合、受信したタグ付きフレームの VLAN 情報が VLAN マッピングエントリーまたはルールと一致しない場合、受信フレームは破棄されます。
Insert Dot1q Tag	トンネルポートで受信したタグなしフレームに挿入する 802.1Q VLAN ID を 1～4094 の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

5.3.2 VLAN Mapping Settings

VLAN Mapping Settings 画面では、VLAN マッピングを設定します。
本画面を表示するには、L2 Features > VLAN Tunnel > VLAN Mapping Settings をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	使用するポート範囲を選択します。
Original VID List	VLAN ID リストを 1～4094 の範囲で入力します。
Original Inner VID	カスタマーVLAN ID を 1～4094 の範囲で入力します。Action が Dot1q-tunnel の場合は使用しません。
Action	以下のどちらかのアクションを選択します。 • Translate：トランクポートで VLAN 変換を実行する場合に選択します。受信フレームの VLAN 情報が Original VLAN に一致すると、指定した VLAN によって置き換えられます。 • Dot1q-tunnel：トンネルポートで受信したフレームの VLAN 情報が指定された Original VLAN と一致すると、VID で指定された S-VLAN タグが追加されます。
VID	VLAN ID を 1～4094 の範囲で入力します。
Inner VID	変換するカスタマーVLAN ID を 1～4094 の範囲で入力します。Action が Dot1q-tunnel の場合は使用しません。
Priority	802.1p 優先度の値として 0～7 のいずれかを選択します。
Port	検索に使用するポートを選択します。

設定を適用するには、Apply ボタンをクリックします。
入力した情報で VLAN マッピングを検索するには、Find ボタンをクリックします。
VLAN マッピングを削除するには、Delete ボタンをクリックします。

5.4 STP

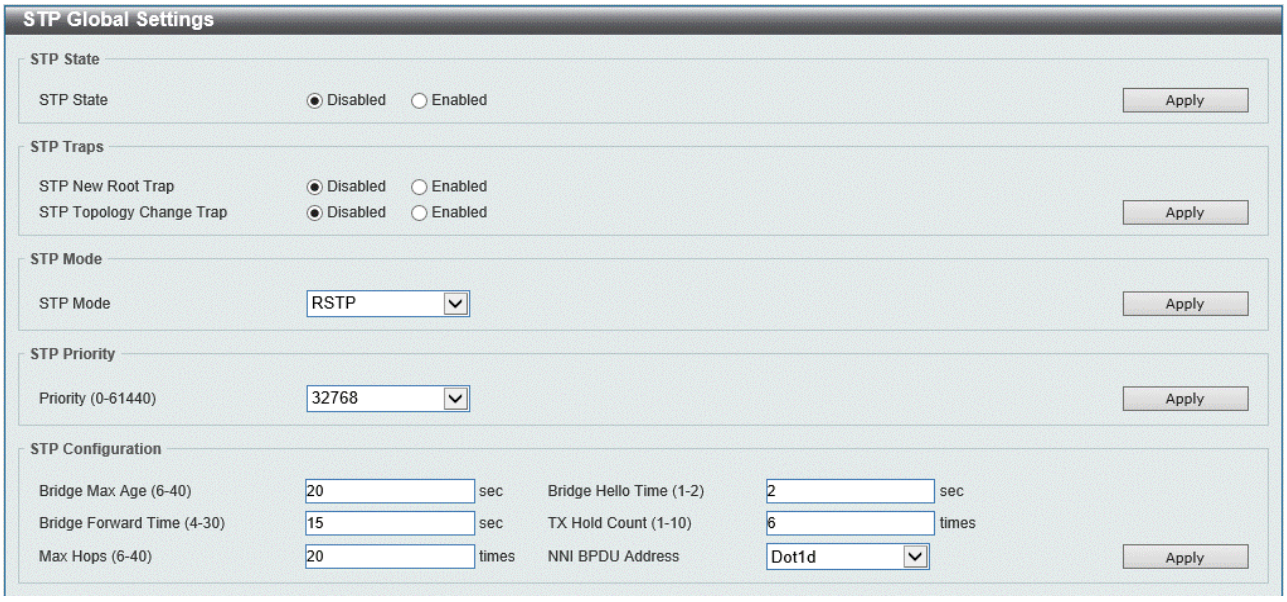
STP サブメニューでは、スパニングツリープロトコルに関連する設定を行います。本装置では、STP、RSTP、および MSTP の 3 種類のバージョンに対応します。

STP の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
5.4.1	STP Global Settings	STP のグローバル設定
5.4.2	STP Port Settings	STP のポート設定
5.4.3	MST Configuration Identification	MSTP の設定
5.4.4	STP Instance	MSTP のインスタンスの優先度設定
5.4.5	MSTP Port Information	MSTP のポート設定

5.4.1 STP Global Settings

STP Global Settings 画面では、STP のグローバル設定を行います。
本画面を表示するには、L2 Features > STP > STP Global Settings をクリックします。



STP State では、STP 機能のグローバル設定を行います。各項目の説明を以下に示します。

パラメーター	説明
STP State	STP 機能の状態（Enabled / Disabled）を選択します。

設定を適用するには、Apply ボタンをクリックします。

STP Traps では、STP の SNMP トラップ通知の設定を行います。各項目の説明を以下に示します。

パラメーター	説明
STP New Root Trap	新ルートブリッジ選出時に SNMP トラップを送信する場合は **Enabled** を選択します。
STP Topology Change Trap	トポロジー変更時に SNMP トラップを送信する場合は **Enabled** を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

STP Mode では、STP の動作モードを設定します。各項目の説明を以下に示します。

パラメーター	説明
STP Mode	使用する STP モード（**MSTP / RSTP / STP**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

STP Priority では STP のブリッジ優先度を設定します。各項目の説明を以下に示します。

パラメーター	説明
Priority	ブリッジ優先度の値を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

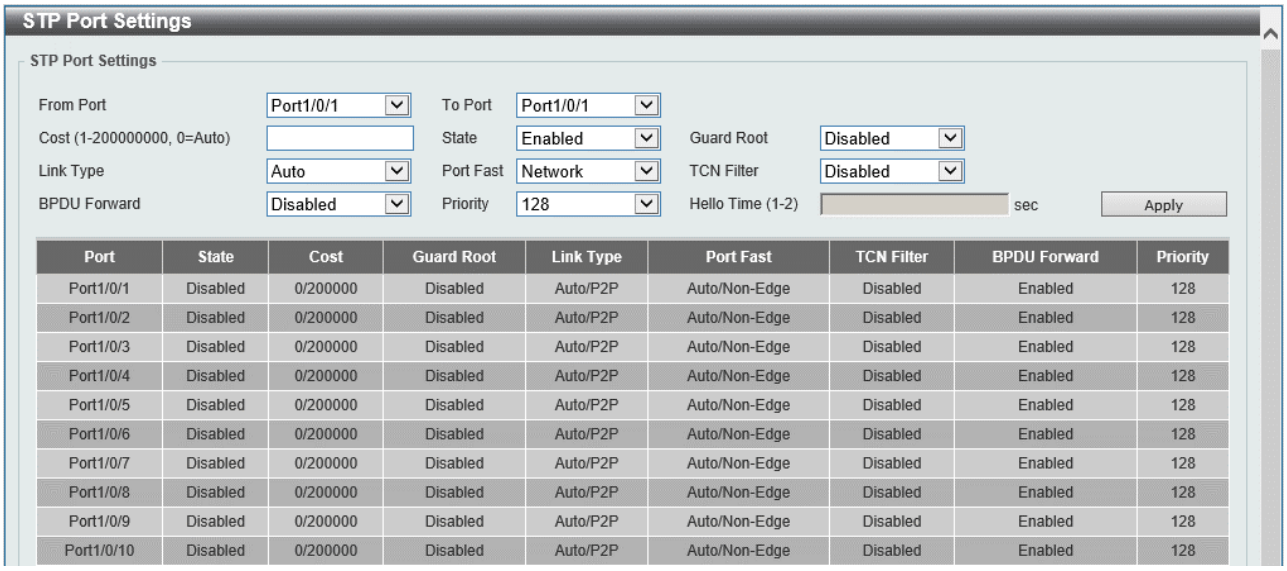
STP Configuration では、STP の各種パラメーターを設定します。各項目の説明を以下に示します。

パラメーター	説明
Bridge Max Age	ブリッジのエージング時間を 6～40（秒）の範囲で入力します。この値は、STP でルートブリッジから定期的に送信される BPDU の待ち時間を示します。
Bridge Hello Time	**STP Mode** で **RSTP** または **STP** を選択した場合に、ブリッジのハロータイム値を 1～2（秒）の範囲で入力します。この値は、BPDU の送信間隔を示します。
Bridge Forward Time	ブリッジの状態遷移の保留時間を 4～30（秒）の範囲で入力します。この値は、STP で状態がフォワーディングになるまでの各状態遷移の保留時間を示します。
TX Hold Count	送信保留カウント値を 1～10（回）の範囲で入力します。連続してトポロジー変更が発生した場合の処理負荷を抑制できるように、1 秒間に送信する BPDU の最大数を規定します。
Max Hops	最大ホップ数を 6～40（ホップ）の範囲で入力します。
NNI BPDU Address	BPDU の宛先アドレスを指定します。 **Dot1d** を選択すると、01-80-C2-00-00-00 が使用されます。これは、通常のローカルネットワークで使用される BPDU 宛先アドレスです。 **Dot1ad** を選択すると、01-80-C2-00-00-08 が使用されます。これは、サービスプロバイダーサイトで使用される BPDU 宛先アドレスです。

設定を適用するには、**Apply** ボタンをクリックします。

5.4.2 STP Port Settings

STP Port Settings 画面では、STP ポートを設定します。
本画面を表示するには、L2 Features > STP > STP Port Settings をクリックします。



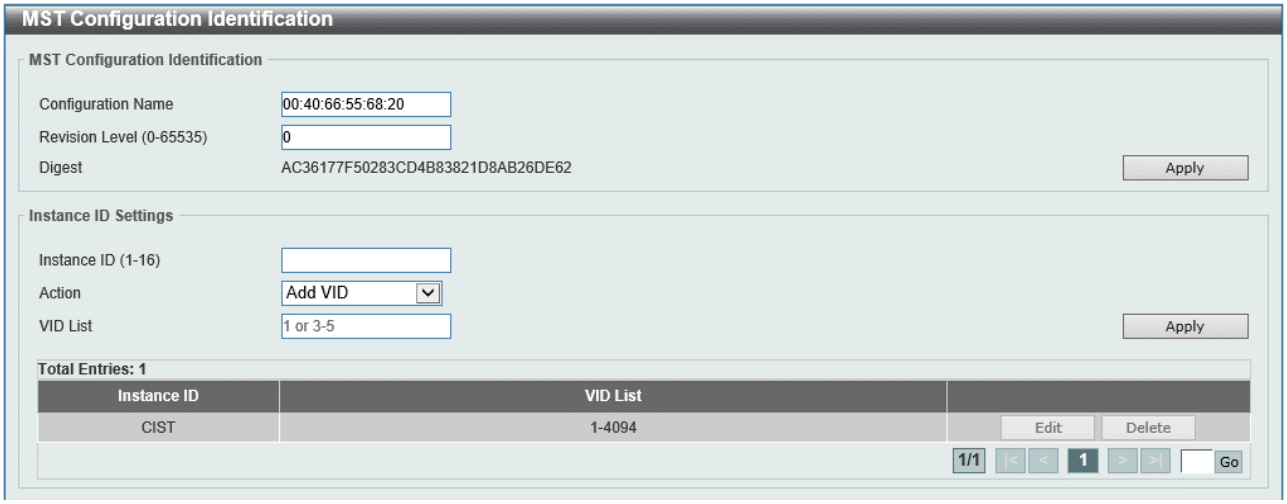
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートの範囲を選択します。
Cost	コスト値を 0～200000000 の範囲で入力します。0 の場合、コストはリンク速度に応じた値が自動で使用されます。
State	ポートの STP 機能の状態（Enabled / Disabled）を選択します。
Guard Root	ガードルート機能の状態（Enabled / Disabled）を選択します。
Link Type	リンクタイプ（Auto / P2P / Shared）を選択します。Shared の場合、RSTP の高速遷移は行えません。Auto は、リンクタイプを自動で切り替えます。P2P は、全二重ポートに対してのみ適用されます。
Port Fast	Port Fast のモード（Network / Disabled / Edge）を選択します。 • Network：Port Fast の状態を自動で切り替えます。3 秒間 BPDU を受信しない場合、ポートは port-fast 状態に遷移します。その後 BPDU を受信すると、Non-port-fast 状態に戻ります。 • Disabled：ポートは常に Non-port-fast 状態になります。 • Edge：エッジポートとみなして port-fast 状態になります。BPDU を受信すると、動作状態は Non-port-fast 状態に変更されます。
TCN Filter	TCN フィルターの状態（Enabled / Disabled）を選択します。Enabled の場合、受信した TCN の情報は他のポートに配信しません。
BPDU Forward	BPDU 転送の状態（Enabled / Disabled）を選択します。Enabled の場合、受信した BPDU はすべての VLAN メンバーポートにタグなしフレームで転送されます。
Priority	ポート優先度の値を選択します。
Hello Time	MSTP のハロータイムの値を 1～2（秒）の範囲で入力します。

設定を適用するには、Apply ボタンをクリックします。

5.4.3 MST Configuration Identification

MST Configuration Identification 画面では、MST の構成を設定します。
本画面を表示するには、L2 Features > STP > MST Configuration Identification をクリックします。



MST Configuration Identification では、MST リージョンの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Configuration Name	MST のリージョン名を入力します。デフォルトでは、MSTP を実行しているスイッチの MAC アドレスが使用されます。
Revision Level	リビジョンレベルの値を 0～65535 の範囲で入力します。 リビジョンレベルの値は、Configuration Name とともに、装置に設定されている MSTP リージョンを識別します。

設定を適用するには、Apply ボタンをクリックします。

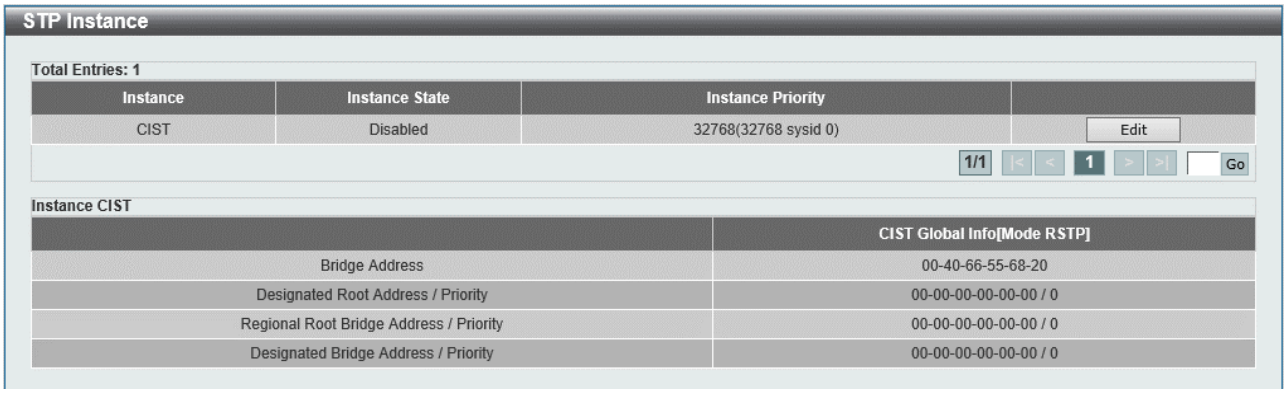
Instance ID Settings では、インスタンスの登録を行います。各項目の説明を以下に示します。

パラメーター	説明
Instance ID	インスタンス ID を 1～16 の範囲で入力します。
Action	実行するアクション（Add VID / Remove VID）を選択します。
VID List	VID リストの値を入力します。

設定を適用するには、Apply ボタンをクリックします。
インスタンス ID を再設定するには、Edit ボタンをクリックします。
インスタンス ID を削除するには、Delete ボタンをクリックします。

5.4.4 STP Instance

STP Instance 画面では、STP インスタンスを設定します。
本画面を表示するには、L2 Features > STP > STP Instance をクリックします。



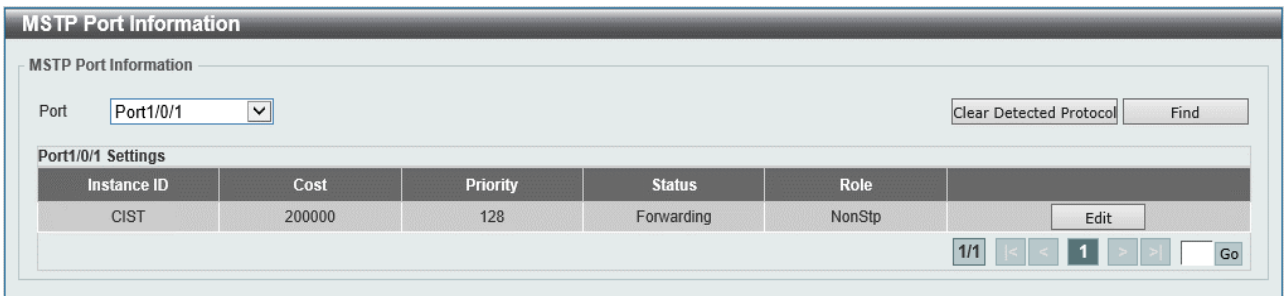
本画面の各項目の説明を以下に示します。

パラメーター	説明
Instance Priority	Edit ボタンをクリックした後、インスタンスのブリッジ優先度の値を 0～61440 の範囲で入力します。

STP インスタンスを再設定するには、Edit ボタンをクリックします。
設定を適用するには、Apply ボタンをクリックします。

5.4.5 MSTP Port Information

MSTP Port Information 画面では、MSTP ポート情報を設定します。
本画面を表示するには、L2 Features > STP > MSTP Port Information をクリックします。



本画面の各項目の説明を以下に示します。

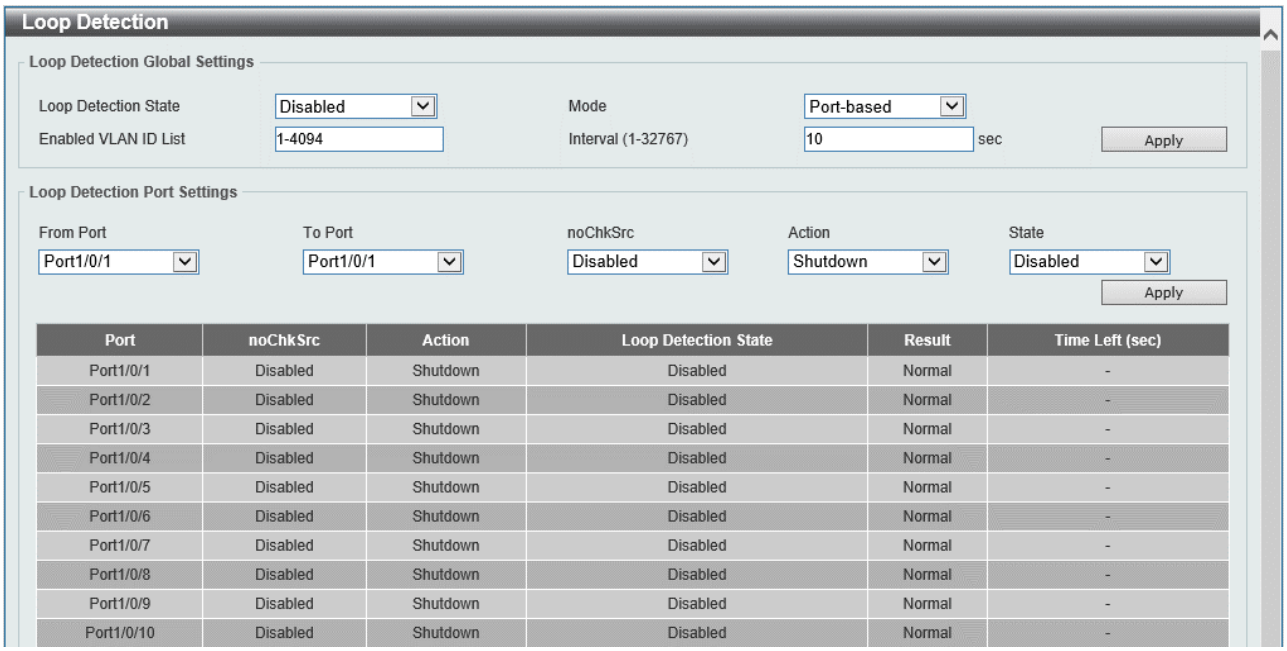
パラメーター	説明
Port	クリアするポート番号を選択します。
Cost	Edit ボタンをクリックした後、コスト値を 1～200000000 の範囲で入力します。
Priority	Edit ボタンをクリックした後、優先度の値として 0～240 のいずれかを選択します（デフォルト：128）。 値が小さいほど優先度が高くなります。

選択したポートで検出されたプロトコル設定をクリアするには、Clear Detected Protocol ボタンをクリックします。
入力した情報で MSTP ポート情報を検索するには、Find ボタンをクリックします。
MSTP ポート情報を再設定するには、Edit ボタンをクリックします。

5.5 Loop Detection

Loop Detection 画面では、ループ検知機能を設定します。
ループ検知機能では、Configuration Testing Protocol（以後、CTP）フレームを送信し、送信したフレームを自身が受信した場合にループ発生と判定し、ポートを一時的に閉塞します。ループ検知の自動復旧時間を経過すると、ポートが復旧して通常の状態に戻ります。

本画面を表示するには、L2 Features > Loop Detection をクリックします。



Loop Detection Global Settings では、ループ検知機能のグローバル設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Loop Detection State	ループ検知機能の状態（Enabled / Disabled）を選択します。
Mode	ループ検知の動作モード（Port-based / VLAN-based）を選択します。
Enabled VLAN ID List	ループ検知を有効にする VLAN の VLAN ID を 1～4094 の範囲で入力します。本設定は Mode で VLAN-based を選択した場合にのみ適用されます。
Interval	CTP フレームの送信間隔を 1～32767（秒）の範囲で入力します。

設定を適用するには、Apply ボタンをクリックします。

Loop Detection Port Settings では、ポート単位でのループ検知の動作を指定します。各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
noChkSrc	本オプションを有効（**Enabled**）にすると、他の装置から送信された CTP フレームを受信した際にループ検知と同様の処理を行います。本設定はイーサネットスイッチ間のループ構成を伴わない誤接続の検知に効果がありますが、ループの誤検知が発生する恐れがあります。
Action	以下のどちらかのアクションモードを選択します。 • **Shutdown**：ループを検知した場合に、**Port-based** モードでは該当する物理ポートを Error Disabled 状態に変更して閉塞します。**VLAN-based** モードの場合は、該当する VLAN のトラフィックをブロックします。SNMP トラップやシステムログの通知も行います。 • **Notify Only**：ループを検知した場合に、SNMP トラップやシステムログでの通知のみを行います。物理ポートの閉塞やトラフィックのブロックを行いません。
State	物理ポートでのループ検知機能の状態（**Enabled** / **Disabled**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

5.6 Link Aggregation

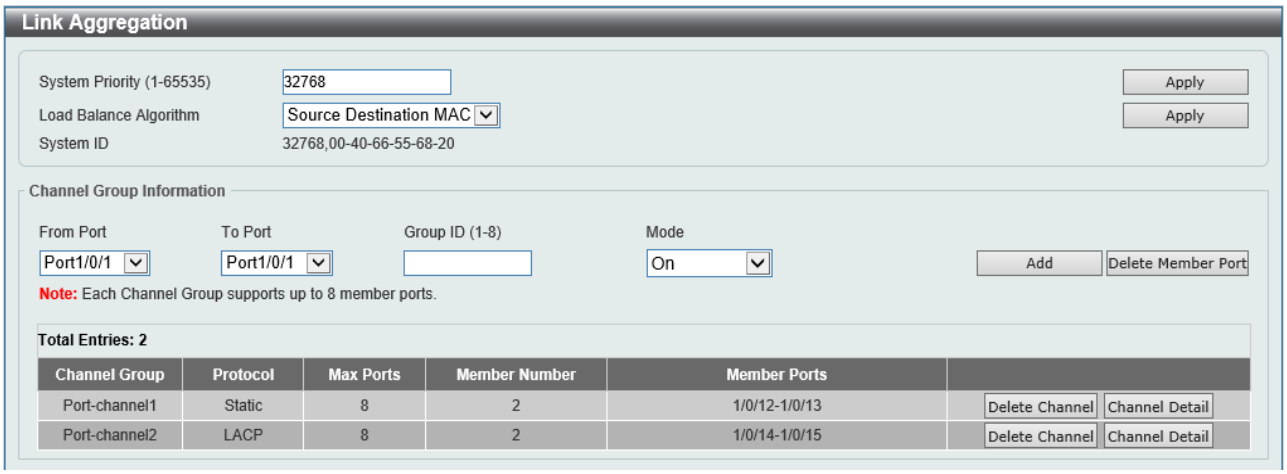
Link Aggregation 画面では、リンクアグリゲーションを設定します。リンクアグリゲーションでは、ポートチャネルと呼ばれる複数のポートを束ねた結合リンクを設定します。

ポートチャネルは、LACP フレームを送受信してネゴシエーションを行う LACP モードと、固定で登録するスタティックモードがあります。LACP モードでは、ポートがリンクアップ状態になると直ちに LACP フレームの送信を開始する Active と、LACP フレームを受信するまで LACP フレームの送信を保留する Passive があります。接続する双方のポートチャネル間の動作モードは整合している必要があり、たとえばポートチャネル間の動作モードが両方 Passive の場合や、LACP とスタティックの組み合わせの場合、ポートチャネルがアップ状態になりません。Passive は、たとえばエッジスイッチ同士の誤接続による悪影響を防ぐ目的で、エッジスイッチのアップリンクに適用する場合などに使用されます。

ポートチャネルの登録では、グループ番号とメンバーポートを登録します。ポートチャネルは単一の論理リンクとして動作し、グループ番号に対応した ID で識別されます。各グループのメンバーポートは最大 8 ポートです。

LACP のネゴシエーションでは、最初に優先デバイスの選出を行います。優先デバイスは、システム優先度がより小さいデバイスが選出されます。システム優先度値が等しい場合は、システム ID（MAC アドレス）の比較で選出されます。

本画面を表示するには、**L2 Features > Link Aggregation** をクリックします。



最初の部分では、リンクアグリゲーションの共通設定を行います。各項目の説明を以下に示します。

パラメーター	説明
System Priority	システム優先度の値を 1～65535 の範囲で入力します。
Load Balance Algorithm	使用する負荷分散アルゴリズム（Source MAC / Destination MAC / Source Destination MAC / Source IP / Destination IP / Source Destination IP）を選択します。

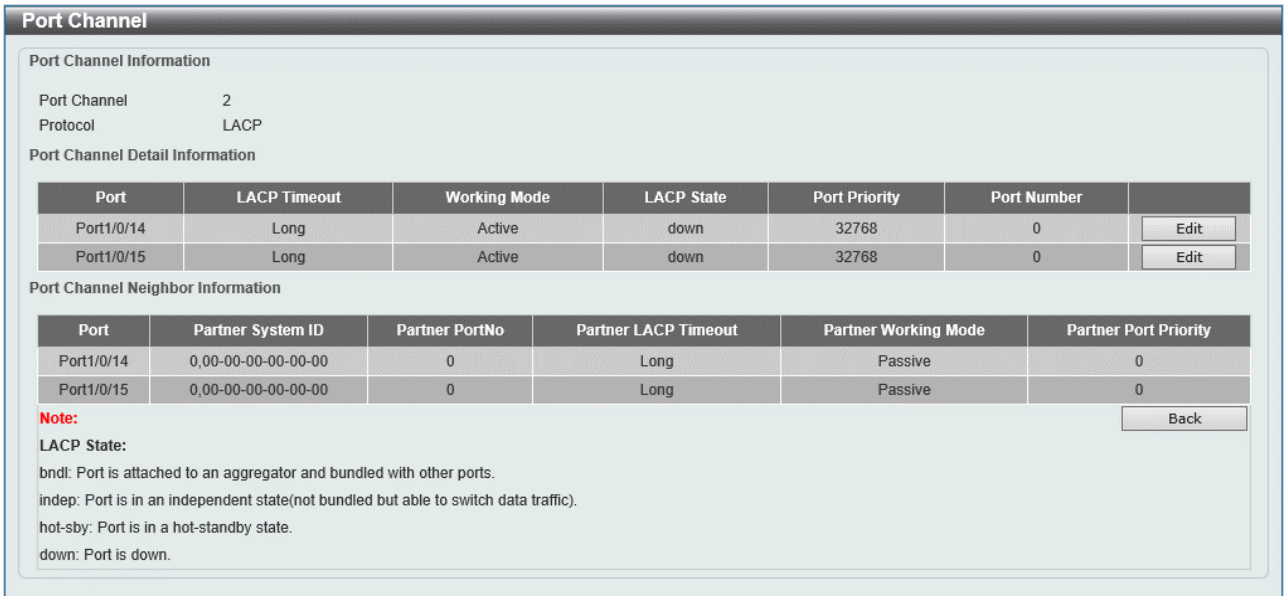
設定を適用するには、**Apply** ボタンをクリックします。

Channel Group Information では、ポートチャネルを登録します。各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	メンバーポートのリストを選択します。
Group ID	ポートチャネルのグループ番号を 1～8 の範囲で入力します。
Mode	ポートチャネルの動作モード（On / Active / Passive）を選択します。モードが On の場合、動作モードはスタティックです。

チャネルグループを追加するには、Add ボタンをクリックします。
グループからメンバーポートを削除するには、Delete Member Port ボタンをクリックします。
チャネルグループを削除するには、Delete Channel ボタンをクリックします。
チャネルの詳細情報を表示するには、Channel Detail ボタンをクリックします。

Channel Detail ボタンをクリックすると、以下に示す画面が表示されます。



ポートチャネルを再設定するには、Edit ボタンをクリックします。
設定を適用するには、Apply ボタンをクリックします。
前の画面に戻るには、Back ボタンをクリックします。

Edit ボタンをクリックした後の各項目の説明を以下に示します。

パラメーター	説明
LACP Timeout	LACP タイムアウトのモード（Short / Long）を選択します。Short の場合は 3 秒間に LACP フレームを受信しないときにダウンとみなします。Long の場合は 90 秒間に LACP フレームを受信しないときにダウンとみなします。 このパラメーターを LACP フレームで通知することで、Short の場合は 1 秒間隔、Long の場合は 30 秒間隔で、対向デバイスが LACP フレームを送信します。
Working Mode	LACP の動作モード（Active / Passive）を選択します。
Port Priority	ポート優先度の値を入力します。

設定を適用するには、Apply ボタンをクリックします。

5.7 L2 Multicast Control

L2 Multicast Control サブメニューでは、マルチキャストトラフィック制御に関する設定を行います。マルチキャストトラフィック制御を行わないスイッチでは、マルチキャストフレームは VLAN の設定に基づき、対象ポートすべてに転送されます。これにより、利用帯域の増加やマルチキャストフレームの処理に伴う各デバイスの負荷増大など、ネットワーク全体に悪影響を及ぼすことがあります。
マルチキャストトラフィック制御を行うと、スイッチはマルチキャスト通信のメンバーを学習し、メンバーが存在するポートを対象にしたマルチキャストトラフィックの転送を行うことができます。

L2 Multicast Control の下にあるサブメニューの一覧を以下の表に示します。

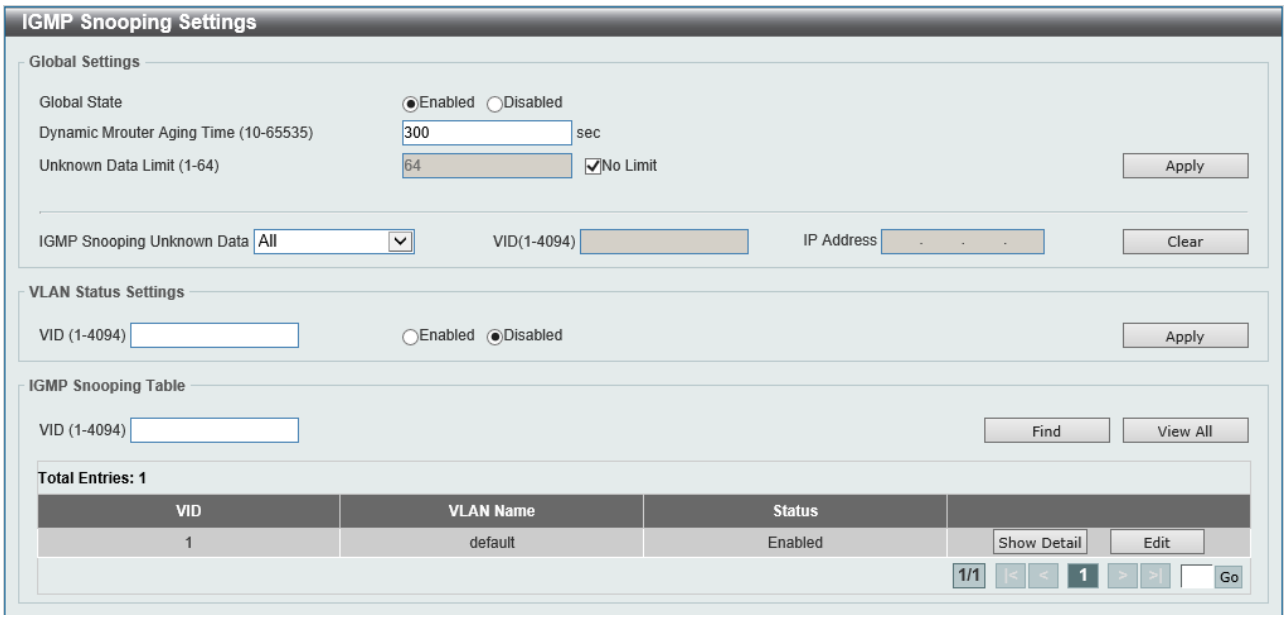
項番	メニュー名	概要
5.7.1	IGMP Snooping	IGMP スヌーピングの設定
5.7.2	MLD Snooping	MLD スヌーピングの設定
5.7.3	Multicast Filtering	マルチキャストフィルタリングの設定

5.7.1 IGMP Snooping

IGMP Snooping サブメニューでは、IGMP スヌーピング機能の設定を行います。
IGMP スヌーピングは、マルチキャストホストやマルチキャストルーターが送信する IGMP メッセージをチェックし、各ポートでのマルチキャストメンバーの存在を自動学習する機能です。各ポートのメンバーの登録は状態で管理され、受信した IGMP メッセージの内容により更新されます。

IGMP Snooping Settings

IGMP Snooping Settings 画面では、IGMP スヌーピングのグローバル設定を行います。
本画面を表示するには L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings をクリックします。



Global Settings では、IGMP スヌーピングのグローバル設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Global State	IGMP スヌーピングの状態（**Enabled** / **Disabled**）を選択します。
Dynamic Mrouter Aging Time	IGMP スヌーピングで学習したグループ情報のエージングタイムを 10～65535（秒）の範囲で入力します。
Unknown Data Limit	メンバー情報がないマルチキャストフレームを受信した場合の、メンバー不在のエントリーの最大登録数を設定します。**Default** がチェックされている場合、デフォルトの 64 を使用します。変更する場合は **Default** のチェックを外し、エントリーの上限値を 1～64 の範囲で入力します。
IGMP Snooping Unknown Data	メンバー情報がないダイナミックエントリーをクリアする場合に指定します。クリアする対象を以下のいずれかから選択します。 • **All**：すべてのエントリーをクリアします。 • **VLAN**：指定した VLAN のエントリーをクリアします。 　○ **VID**：VLAN ID を 1～4094 の範囲で入力します。 • **Group**：指定したグループのエントリーをクリアします。 　○ **IP Address**：グループアドレスを入力します。

設定を適用するには、**Apply** ボタンをクリックします。
メンバー情報がないエントリーをクリアするには、**Clear** ボタンをクリックします。

VLAN Status Settings では、IGMP スヌーピングを使用する VLAN を登録します。各項目の説明を以下に示します。

パラメーター	説明
VID	VLAN ID を 1～4094 の範囲で入力します。 また、指定した VLAN での IGMP スヌーピングの状態（**Enabled** / **Disabled**）を選択します。

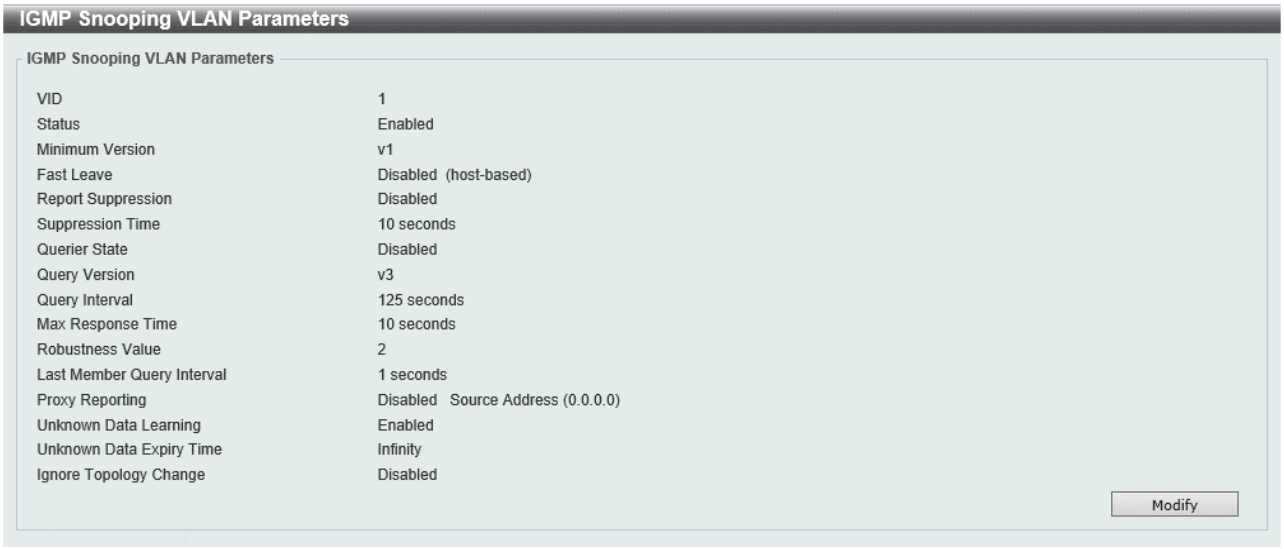
設定を適用するには、**Apply** ボタンをクリックします。

IGMP Snooping Table では、IGMP スヌーピングの VLAN 設定を確認します。各項目の説明を以下に示します。

パラメーター	説明
VID	VLAN ID を 1～4094 の範囲で入力します。

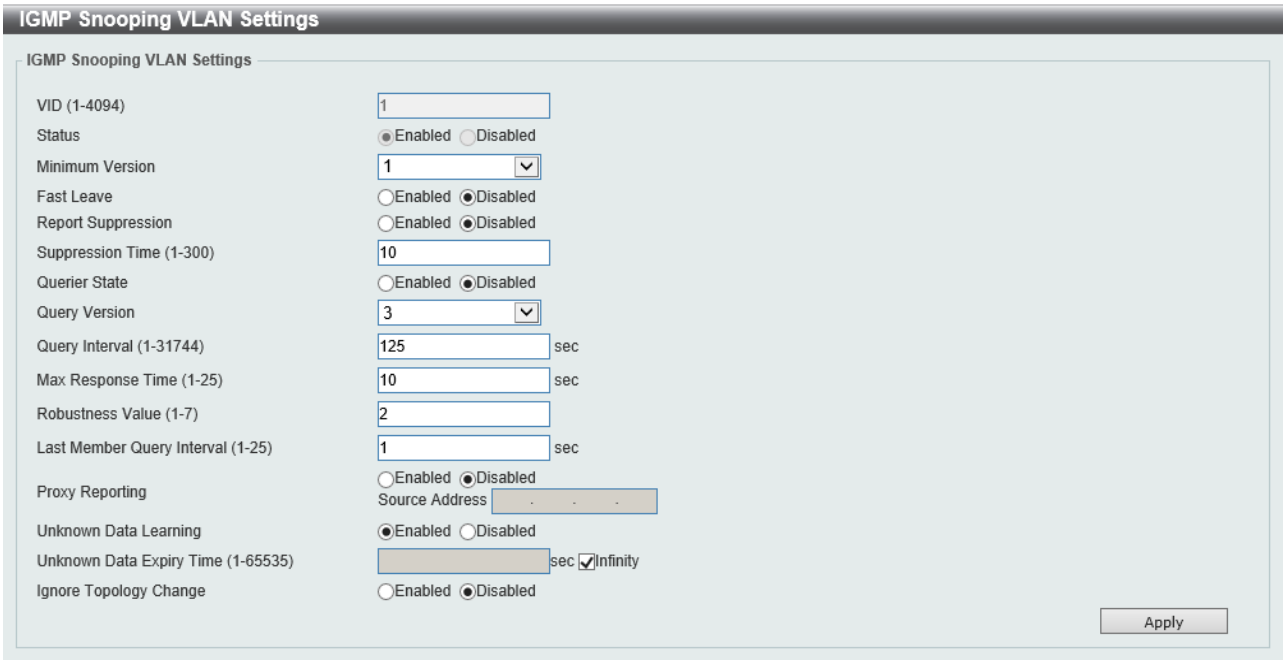
入力した情報で IGMP スヌーピングを検索するには、**Find** ボタンをクリックします。
すべての IGMP スヌーピングを表示するには、**View All** ボタンをクリックします。
VLAN の詳細情報を表示するには、**Show Detail** ボタンをクリックします。
IGMP スヌーピングの詳細設定を行うには、**Edit** ボタンをクリックします。

Show Detail ボタンをクリックすると、以下に示す画面が表示されます。



IGMP Snooping VLAN Parameters 画面には、IGMP スヌーピングの詳細情報が表示されます。
情報を編集するには、**Modify** ボタンをクリックします。

IGMP Snooping Table で **Edit** ボタンをクリックするか、または **IGMP Snooping VLAN Parameters** 画面で **Modify** ボタンをクリックすると、以下に示す画面が表示されます。



IGMP Snooping VLAN Settings では、IGMP スヌーピングの詳細設定を行います。各項目の説明を以下に示します。

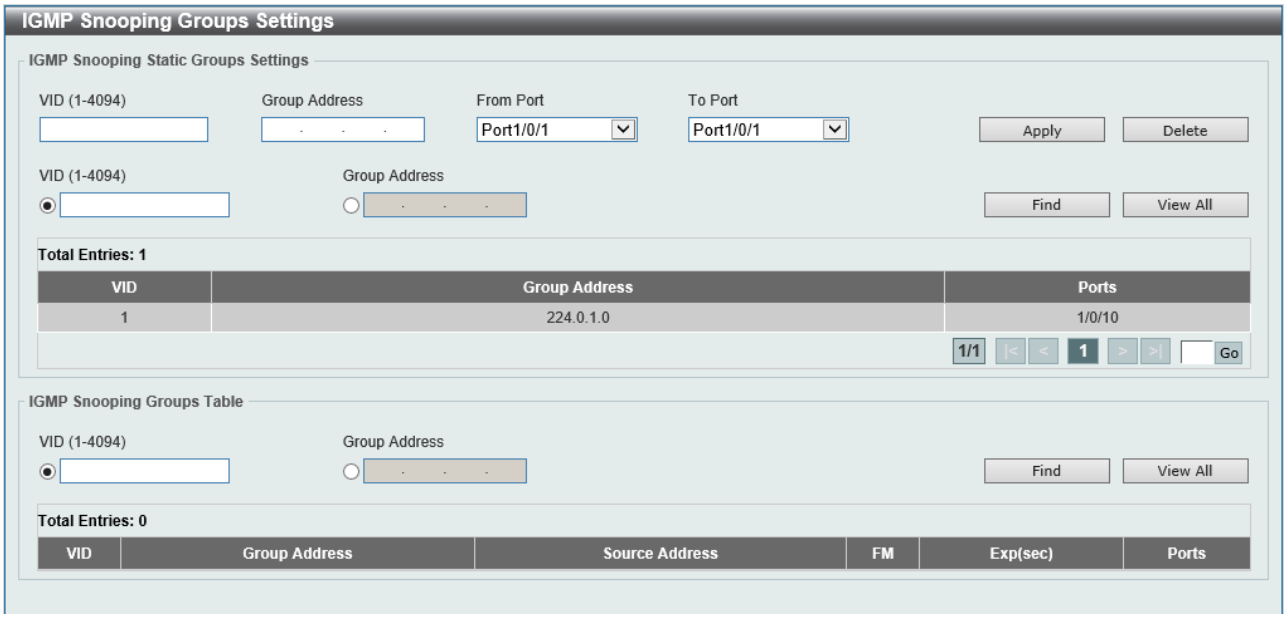
パラメーター	説明
Minimum Version	IGMP バージョン（**1** / **2** / **3**）を選択します。
Fast Leave	IGMP スヌーピング即時離脱機能の状態（**Enabled** / **Disabled**）を選択します。**Enabled** の場合、メンバーから IGMP グループ離脱メッセージを受信すると、メンバーを即座に削除します。
Report Suppression	レポート抑制の状態（**Enabled** / **Disabled**）を選択します。 レポート抑制機能は、IGMPv1 および IGMPv2 メッセージに対してのみ動作します。 レポート抑制が無効の場合、装置はマルチキャストノードからの IGMP メッセージをすべてマルチキャストルーターに転送します。レポート抑制が有効の場合、**Suppression Time** で指定した期間内にマルチキャストノードからの同じタイプ(メンバーシップレポート/グループ離脱)のメッセージを複数受信すると、1 個のメッセージに集約してマルチキャストルーターに転送します。
Suppression Time	レポート抑制機能の抑制時間(秒)を 1～300 の範囲で入力します（デフォルト：10 秒）。
Querier State	クエリア機能の状態（**Enabled** / **Disabled**）を選択します。クエリア機能は、通常はマルチキャストルーターが送信する IGMP クエリーを代行して送信する機能です。マルチキャストルーターが存在しない環境で、マルチキャストノードの情報を適切に更新するために必要になります。
Query Version	クエリアが送信するジェネラルクエリーのバージョン（**1** / **2** / **3**）を選択します。
Query Interval	クエリアが送信するジェネラルクエリーの送信間隔を 1～31744（秒）の範囲で入力します。
Max Response Time	ジェネラルクエリーの応答待ち時間を 1～25（秒）の範囲で入力します。
Robustness Value	ロバストネス変数を 1～7 の範囲で入力します（デフォルト：2）。
Last Member Query Interval	クエリアがメンバー離脱時のグループスペシフィッククエリーを送信する間隔を 1～25（秒）の範囲で入力します。
Proxy Reporting	プロキシレポート機能の状態（**Enabled** / **Disabled**）を指定します。 • **Source Address**：プロキシレポートの送信元アドレスを入力します。
Unknown Data Learning	マルチキャストトラフィックを受信した際に、メンバー不在のエントリーを作成する場合は **Enabled** を選択します。 • **Unknown Data Expiry Time**：メンバー不在のエントリーの有効期限を 1～65535（秒）の範囲で入力します。
Ignore Topology Change	トポロジー変更の無視機能の状態（**Enabled** / **Disabled**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

IGMP Snooping Groups Settings

IGMP Snooping Groups Settings 画面では、IGMP スヌーピングのエントリーを確認します。また、IGMP スヌーピングのスタティックエントリーを登録することもできます。

本画面を表示するには、**IGMP Snooping > IGMP Snooping Groups Settings** をクリックします。



IGMP Snooping Static Groups Settings では、スタティックエントリーの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
VID	マルチキャストグループの VLAN ID を 1～4094 の範囲で入力します。
Group Address	IP マルチキャストグループアドレスを入力します。
From Port / To Port	ポートまたはポートの範囲を選択します。
VID	ラジオボタンをクリックし、マルチキャストグループの VLAN ID を 1～4094 の範囲で入力します。
Group Address	ラジオボタンをクリックし、マルチキャストグループアドレスを入力します。

設定を適用するには、**Apply** ボタンをクリックします。

IGMP スヌーピングスタティックグループを削除するには、**Delete** ボタンをクリックします。

入力した情報から IGMP スヌーピングスタティックグループを検索するには、**Find** ボタンをクリックします。

すべての IGMP スヌーピングスタティックグループを表示するには、**View All** ボタンをクリックします。

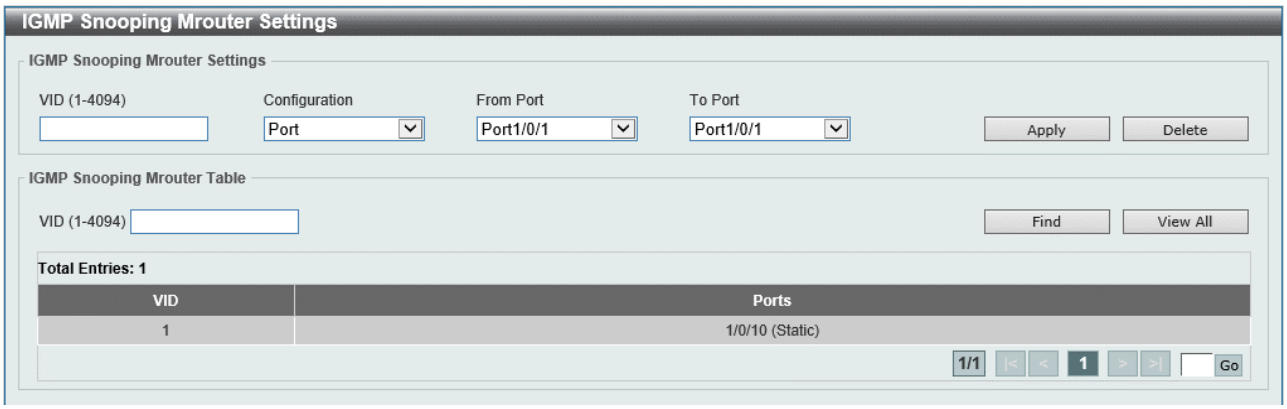
IGMP Snooping Groups Table では、IGMP スヌーピングのエントリーが表示されます。各項目の説明を以下に示します。

パラメーター	説明
VID	ラジオボタンをクリックし、マルチキャストグループの VLAN ID を 1～4094 の範囲で入力します。
Group Address	ラジオボタンをクリックし、グループアドレスを入力します。

入力した情報で IGMP スヌーピンググループを検索するには、**Find** ボタンをクリックします。
すべての IGMP スヌーピンググループを表示するには、**View All** ボタンをクリックします。

IGMP Snooping Mrouter Settings

IGMP Snooping Mrouter Settings 画面では、IGMP スヌーピングのルーターポートを設定します。
本画面を表示するには、**IGMP Snooping > IGMP Snooping Mrouter Settings** をクリックします。



IGMP Snooping Mrouter Settings では、ルーターポートを登録します。各項目の説明を以下に示します。

パラメーター	説明
VID	使用する VLAN ID を 1～4094 の範囲で入力します。
Configuration	以下のどちらかのポート構成を選択します。 • **Port**：対象ポートをスタティックのルーターポートにします。 • **Forbidden Port**：対象ポートを非ルーターポートに指定します。
From Port / To Port	ポートの範囲を選択します。

設定を適用するには、**Apply** ボタンをクリックします。
登録したルーターポートを削除するには、**Delete** ボタンをクリックします。

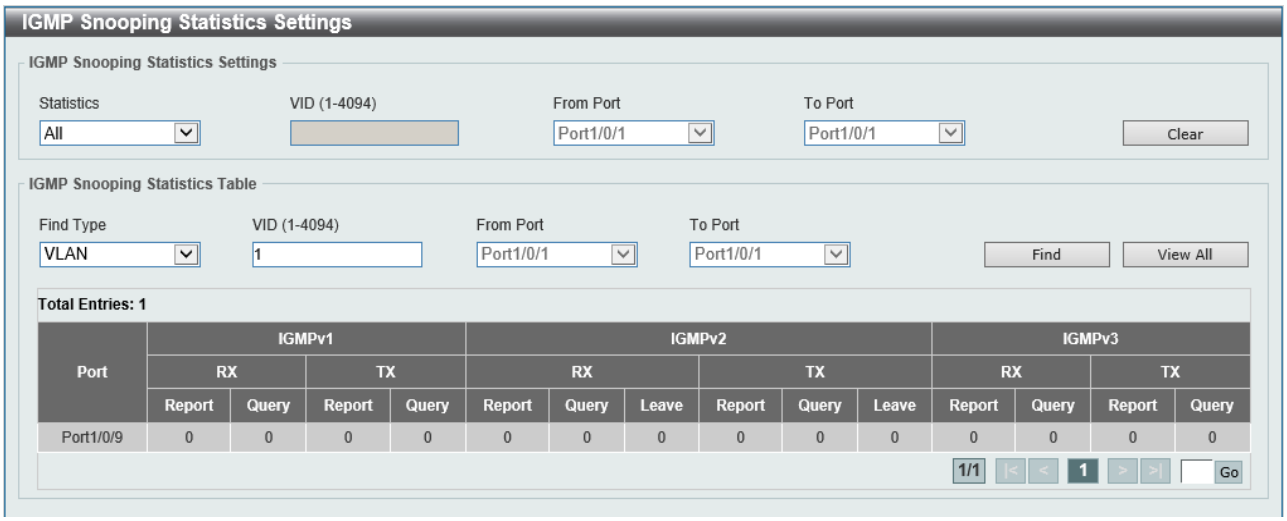
IGMP Snooping Mrouter Table では、ルーターポートを表示します。各項目の説明を以下に示します。

パラメーター	説明
VID	使用する VLAN ID を 1～4094 の範囲で入力します。

入力した情報でルーターポートを検索するには、**Find** ボタンをクリックします。
すべてのルーターポートを表示するには、**View All** ボタンをクリックします。

IGMP Snooping Statistics Settings

IGMP Snooping Statistics Settings 画面では、IGMP スヌーピング統計情報を表示します。
本画面を表示するには、**IGMP Snooping > IGMP Snooping Statistics Settings** をクリックします。



IGMP Snooping Statistics Settings では、IGMP スヌーピング統計情報をクリアできます。各項目の説明を以下に示します。

パラメーター	説明
Statistics	クリアする IGMP スヌーピング統計情報の対象を、以下のいずれかから選択します。 • **All**：すべての IGMP スヌーピング統計情報をクリアします。 • **VLAN**：対象 VLAN の IGMP スヌーピング統計情報をクリアします。 　○ **VID**：VLAN ID を 1～4094 の範囲で入力します。 • **Port**：対象ポートの IGMP スヌーピング統計情報をクリアします。 　○ **From Port / To Port**：ポートの範囲を選択します。

IGMP スヌーピング統計情報をクリアするには、**Clear** ボタンをクリックします。

IGMP Snooping Statistics Table では、IGMP スヌーピング統計情報が表示されます。各項目の説明を以下に示します。

パラメーター	説明
Find Type	IGMP スヌーピング統計テーブルの表示対象を、以下のいずれかから選択します。 • **VLAN**：対象 VLAN の IGMP スヌーピング統計情報を表示します。 　○ **VID**：VLAN ID を 1～4094 の範囲で入力します。 • **Port**：対象ポートの IGMP スヌーピング統計情報を表示します。 　○ **From Port / To Port**：ポートまたはポートの範囲を選択します。

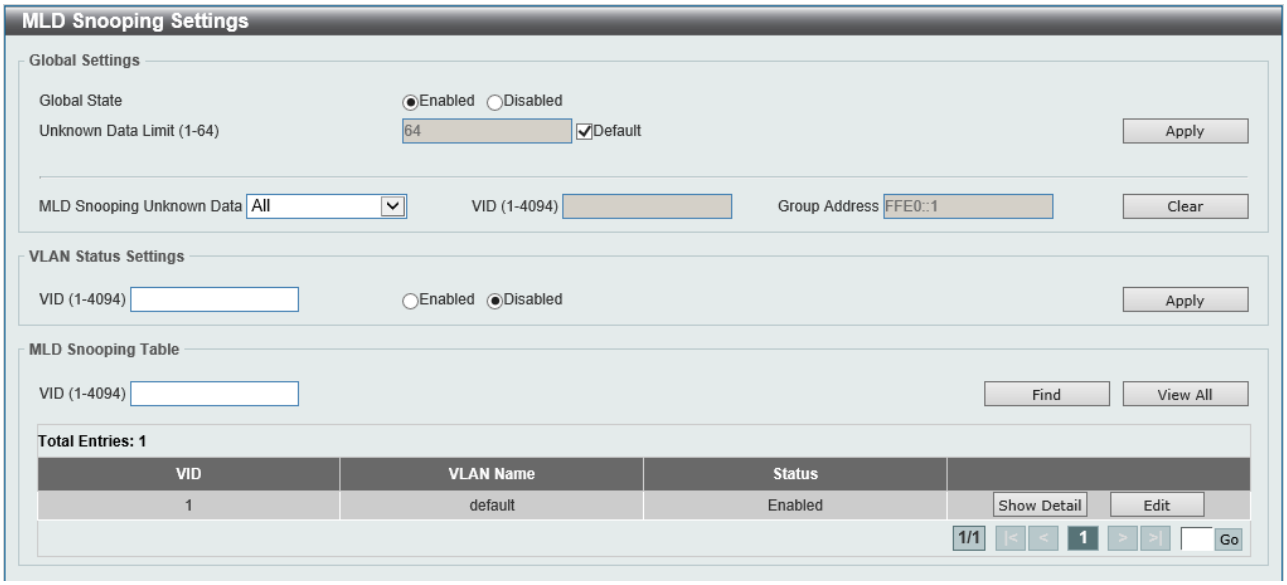
入力した情報で IGMP スヌーピング統計情報を検索するには、**Find** ボタンをクリックします。
すべての IGMP スヌーピング統計情報を表示するには、**View All** ボタンをクリックします。

5.7.2 MLD Snooping

MLD Snooping サブメニューでは、MLD スヌーピング機能の設定を行います。
MLD スヌーピングは、IPv6 マルチキャストホストやマルチキャストルーターが送信する MLD メッセージをチェックする機能で、IPv4 での IGMP スヌーピング機能に相当します。

MLD Snooping Settings

MLD Snooping Settings 画面では、MLD スヌーピングのグローバル設定を行います。
本画面を表示するには **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings** をクリックします。



Global Settings では、MLD スヌーピングのグローバル設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Global State	MLD スヌーピング機能の状態（**Enabled** / **Disabled**）を選択します。
Unknown Data Limit	メンバー情報がないマルチキャストフレームを受信した場合の、メンバー不在のエントリーの作成数を設定します。**Default** がチェックされている場合、デフォルトの 64 を使用します。変更する場合は **Default** のチェックを外して、エントリーの上限値を 1～64 の範囲で入力します。
MLD Snooping Unknown Data	メンバー情報がないダイナミックエントリーをクリアする場合に指定します。クリアする対象を、以下のいずれかから選択します。 • **All**：すべてのエントリーをクリアします。 • **VLAN**：指定した VLAN のエントリーをクリアします。 　○ **VID**：VLAN ID を 1～4094 の範囲で入力します。 • **Group**：指定したグループのエントリーをクリアします。 　○ **Group Address**： グループアドレスを入力します。

設定を適用するには、**Apply** ボタンをクリックします。
メンバー情報がないエントリーをクリアするには、**Clear** ボタンをクリックします。

VLAN Status Settings では、MLD スヌーピングを使用する VLAN を登録します。各項目の説明を以下に示します。

パラメーター	説明
VID	VLAN ID を 1～4094 の範囲で入力します。 また、指定した VLAN での MLD スヌーピングの状態（**Enabled** / **Disabled**）を選択します。

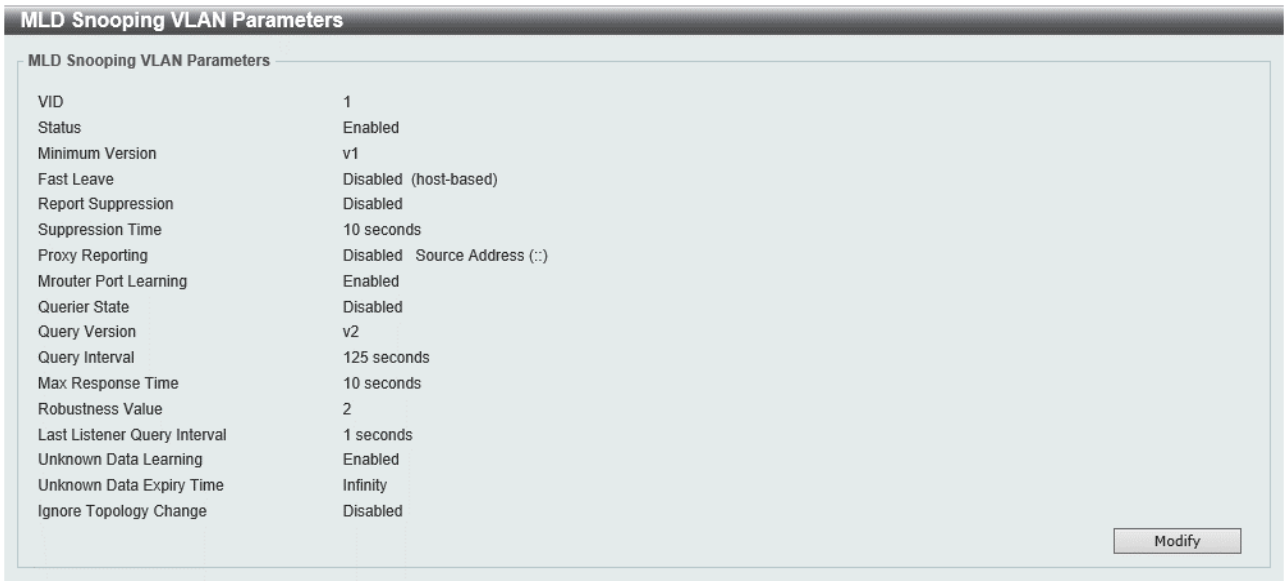
設定を適用するには、**Apply** ボタンをクリックします。

MLD Snooping Table では、MLD スヌーピングの VLAN 設定を確認します。各項目の説明を以下に示します。

パラメーター	説明
VID	VLAN ID を 1～4094 の範囲で入力します。

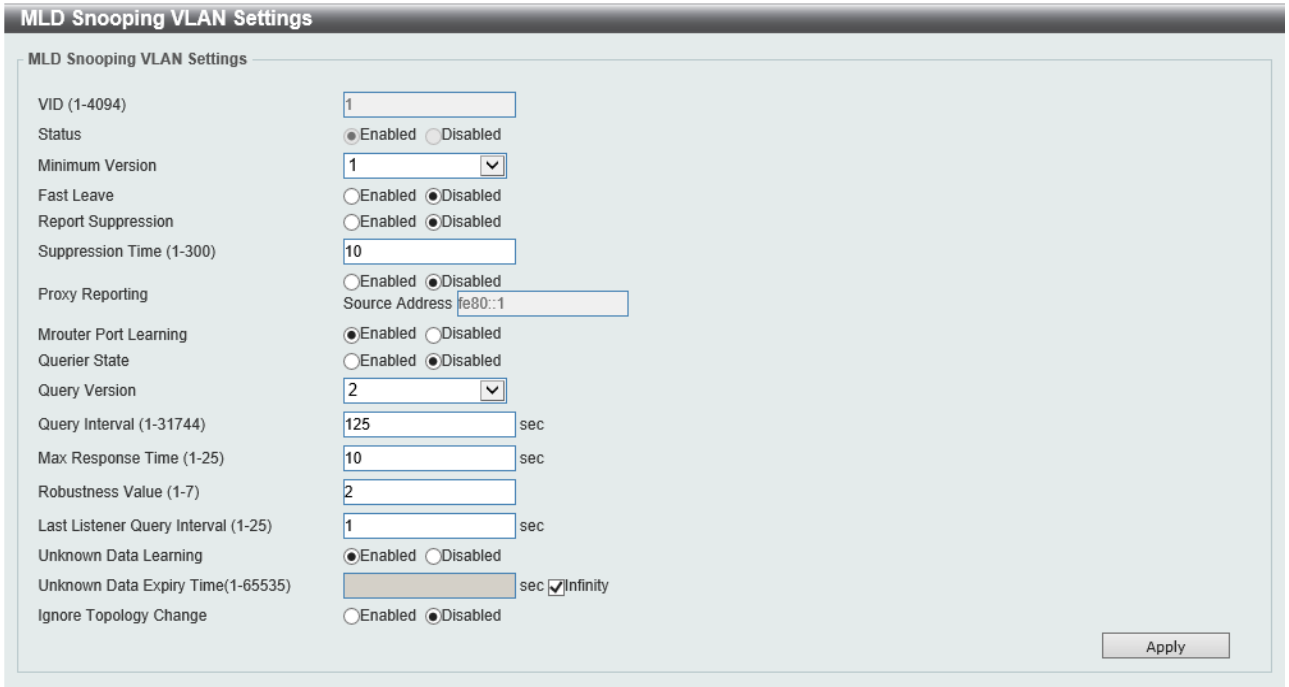
入力した情報で MLD スヌーピングを検索するには、**Find** ボタンをクリックします。
すべての MLD スヌーピングを表示するには、**View All** ボタンをクリックします。
VLAN の詳細情報を表示するには、**Show Detail** ボタンをクリックします。
MLD スヌーピングを再設定するには、**Edit** ボタンをクリックします。

Show Detail ボタンをクリックすると、以下に示す画面が表示されます。



MLD Snooping VLAN Parameters 画面には、MLD スヌーピングの詳細情報が表示されます。
情報を編集するには、**Modify** ボタンをクリックします。

MLD Snooping Table で **Edit** ボタンをクリックするか、または **MLD Snooping VLAN Parameters** 画面で **Modify** ボタンをクリックすると、以下に示す画面が表示されます。



MLD Snooping VLAN Settings では、MLD スヌーピングの詳細設定を行います。各項目の説明を以下に示します。

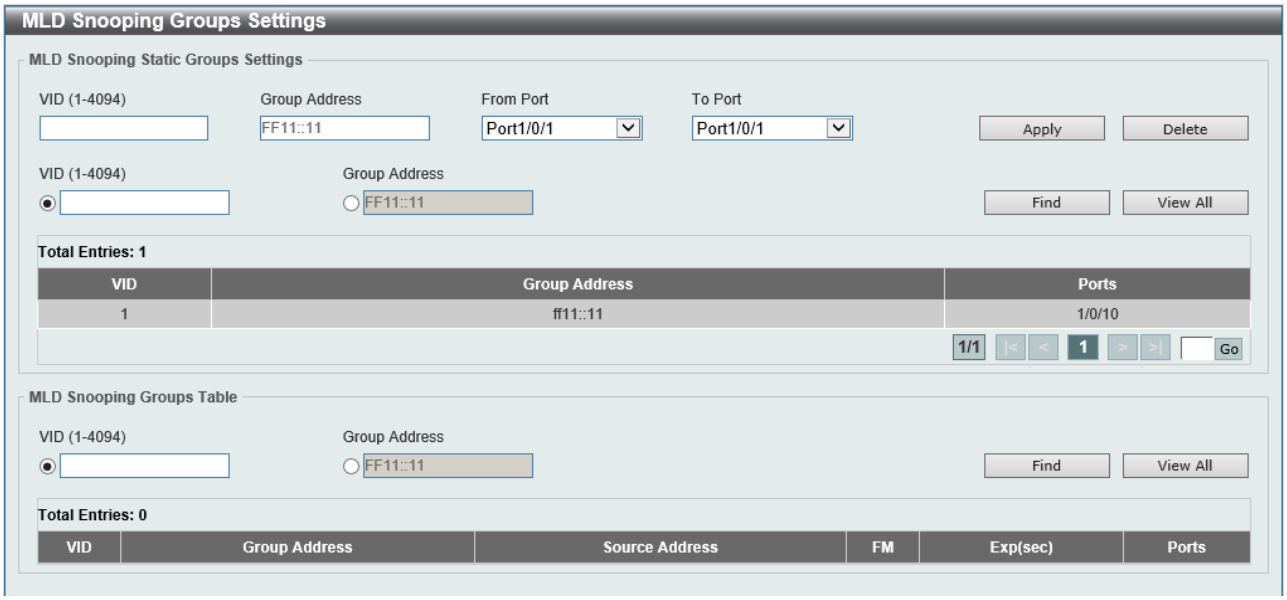
パラメーター	説明
Minimum Version	MLD バージョン（**1** / **2**）を選択します。
Fast Leave	MLD スヌーピング即時離脱機能の状態（**Enabled** / **Disabled**）を選択します。**Enabled** の場合、メンバーから離脱メッセージを受信すると、メンバーを即座に削除されます。
Report Suppression	レポート抑制の状態（**Enabled** / **Disabled**）を選択します。
Suppression Time	重複する MLD レポートまたは離脱を抑制する間隔を 1～300 の範囲で入力します（デフォルト：10）。
Proxy Reporting	プロキシレポート機能の状態（**Enabled** / **Disabled**）を選択します。 • **Source Address**：プロキシレポートの送信元アドレスを入力します。
Mrouter Port Learning	ルーターポート学習機能の状態（**Enabled** / **Disabled**）を選択します。
Querier State	クエリア機能の状態（**Enabled** / **Disabled**）を選択します。
Query Version	クエリアが送信するジェネラルクエリーのバージョン（**1** / **2**）を選択します。
Query Interval	クエリアが送信するジェネラルクエリーの送信間隔を 1～31744（秒）の範囲で入力します。
Max Response Time	ジェネラルクエリーの応答待ち時間を 1～25（秒）の範囲で入力します。
Robustness Value	ロバストネス変数を 1～7 の範囲で入力します（デフォルト：2）。
Last Listener Query Interval	クエリアがメンバー離脱時のグループスペシフィッククエリーを送信する間隔を 1～25（秒）の範囲で入力します。
Unknown Data Learning	マルチキャストトラフィックを受信した際に、メンバー不在のエントリーを作成する場合は **Enabled** を選択します。 • **Unknown Data Expiry Time**：メンバー不在のエントリーの有効期限を 1～65535（秒）の範囲で入力します。
Ignore Topology Change	トポロジー変更の無視機能の状態（**Enabled** / **Disabled**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

MLD Snooping Groups Settings

MLD Snooping Groups Settings 画面では、MLD スヌーピングのエントリーを確認します。また、MLLD スヌーピングのスタティックエントリーを登録することもできます。

本画面を表示するには、**MLD Snooping > MLD Snooping Groups Settings** をクリックします。



MLD Snooping Static Groups Settings では、スタティックエントリーの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
VID	マルチキャストグループの VLAN ID を 1～4094 の範囲で入力します。
Group Address	IPv6 マルチキャストグループアドレスを入力します。
From Port / To Port	ポートまたはポートの範囲を選択します。
VID	ラジオボタンをクリックし、マルチキャストグループの VLAN ID を 1～4094 の範囲で入力します。
Group Address	ラジオボタンをクリックし、IPv6 マルチキャストグループアドレスを入力します。

設定を適用するには、**Apply** ボタンをクリックします。

MLD スヌーピングスタティックグループを削除するには、**Delete** ボタンをクリックします。

入力した情報で MLD スヌーピングスタティックグループを検索するには、**Find** ボタンをクリックします。

すべての MLD スヌーピングスタティックグループを表示するには、**View All** ボタンをクリックします。

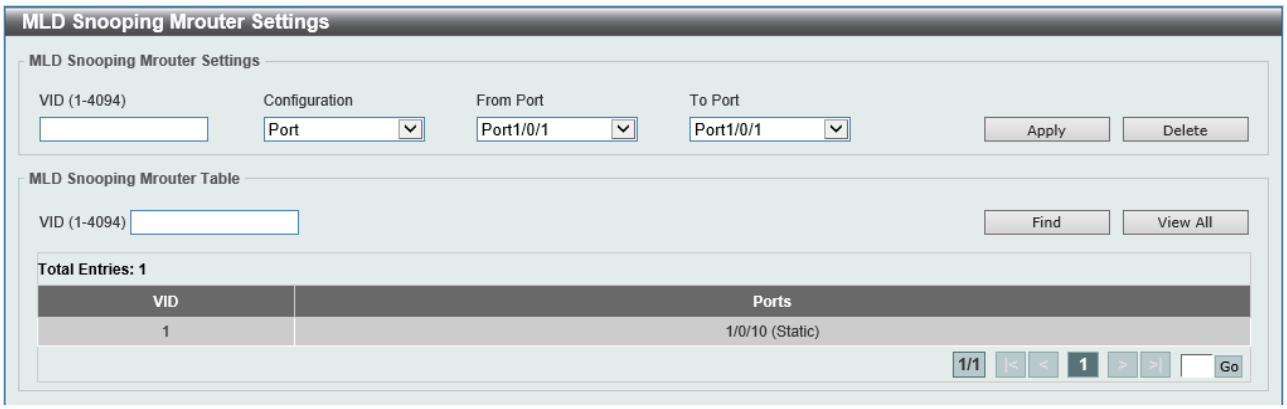
MLD Snooping Groups Table では、MLD スヌーピングのエントリーが表示されます。各項目の説明を以下に示します。

パラメーター	説明
VID	ラジオボタンをクリックし、マルチキャストグループの VLAN ID を 1～4094 の範囲で入力します。
Group Address	ラジオボタンをクリックし、グループアドレスを入力します。

入力した情報で MLD スヌーピンググループを検索するには、**Find** ボタンをクリックします。
すべての MLD スヌーピンググループを表示するには、**View All** ボタンをクリックします。

MLD Snooping Mrouter Settings

MLD Snooping Mrouter Settings 画面では、MLD スヌーピングのルーターポートを設定します。
本画面を表示するには、**MLD Snooping > MLD Snooping Mrouter Settings** をクリックします。



MLD Snooping Mrouter Settings では、ルーターポートを登録します。各項目の説明を以下に示します。

パラメーター	説明
VID	VLAN ID を 1～4094 の範囲で入力します。
Configuration	ポート構成を以下のいずれかから選択します。 • **Port**：対象ポートをスタティックのルーターポートにします。 • **Forbidden Port**：対象ポートを非ルーターポートにします。 • **Learn PIMv6**：対象ポートで IPv6 PIM でのルーターポートの学習を行います。
From Port / To Port	ポートまたはポートの範囲を選択します。

設定を適用するには、**Apply** ボタンをクリックします。
登録したルーターポートを削除するには、**Delete** ボタンをクリックします。

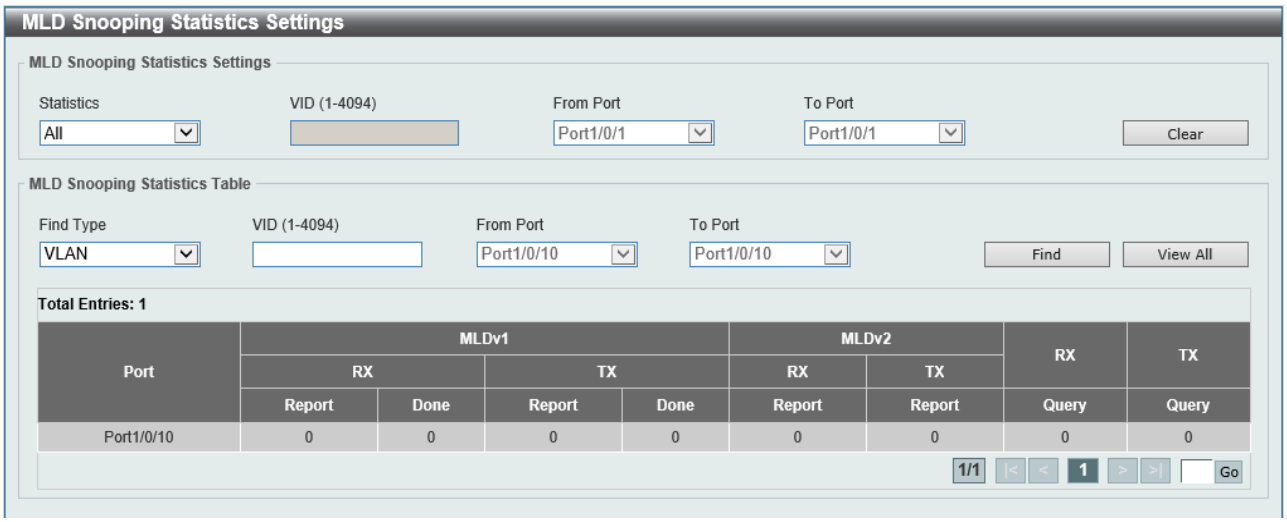
MLD Snooping Mrouter Table では、ルーターポートを表示します。各項目の説明を以下に示します。

パラメーター	説明
VID	VLAN ID を 1～4094 の範囲で入力します。

入力した情報でルーターポートを検索するには、**Find** ボタンをクリックします。
すべてのルーターポートを表示するには、**View All** ボタンをクリックします。

MLD Snooping Statistics Settings

MLD Snooping Statistics Settings 画面では、MLD スヌーピング統計情報を表示します。
本画面を表示するには、**MLD Snooping > MLD Snooping Statistics Settings** をクリックします。



MLD Snooping Statistics Settings では、MLD スヌーピング統計情報をクリアできます。各項目の説明を以下に示します。

パラメーター	説明
Statistics	クリアする MLD スヌーピング統計情報の対象を、以下のいずれかから選択します。 • **All**：すべての MLD スヌーピング統計情報をクリアします。 • **VLAN**：対象 VLAN の MLD スヌーピング統計情報をクリアします。 　○ **VID**：VLAN ID を 1～4094 の範囲で入力します。 • **Port**：対象ポートの MLD スヌーピング統計情報をクリアします。 　○ **From Port / To Port**：ポートの範囲を選択します。

MLD スヌーピング統計情報をクリアするには、**Clear** ボタンをクリックします。

MLD Snooping Statistics Table では、MLD スヌーピング統計情報が表示されます。各項目の説明を以下に示します。

パラメーター	説明
Find Type	MLD スヌーピング統計テーブルの表示対象を、以下のいずれかから選択します。 • **VLAN**：対象 VLAN の MLD スヌーピング統計情報を表示します。 　○ **VID**：VLAN ID を 1～4094 の範囲で入力します。 • **Port**：対象ポートの MLD スヌーピング統計情報を表示します。 　○ **From Port / To Port**：ポートの範囲を選択します。

入力した情報で MLD スヌーピング統計情報を検索するには、**Find** ボタンをクリックします。
すべての MLD スヌーピング統計情報を表示するには、**View All** ボタンをクリックします。

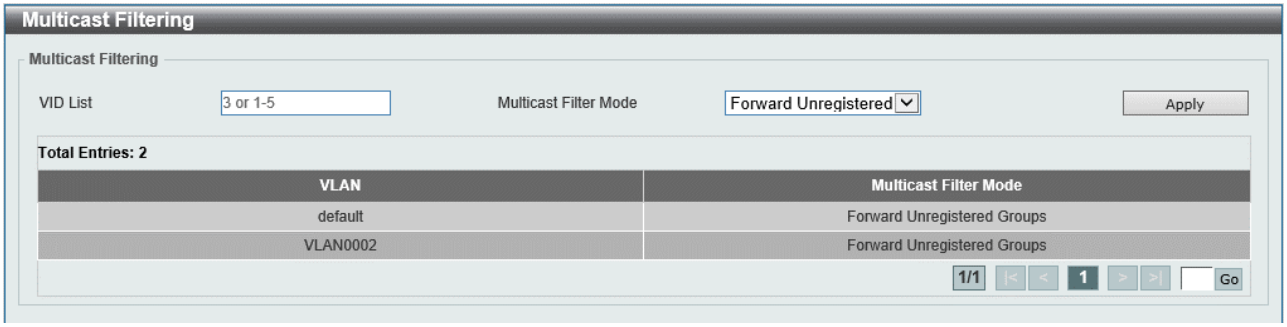
5.7.3 Multicast Filtering

Multicast Filtering 画面では、マルチキャストフィルタリングの設定を行います。

マルチキャストフィルタリングは、マルチキャストフレームを受信した場合の転送処理のモードを指定します。デフォルトの **Forward All** の場合、IGMP スヌーピングなどによりマルチキャストメンバーを学習していたとしても、VLAN の設定に基づく対象ポートすべてに転送します。それ以外のモード（**Forward Unregistered** および **Filter Unregistered**）では、マルチキャストメンバーが登録されている場合はメンバーが存在するポートに対して転送処理を行います。

Forward Unregistered モードと **Filter Unregistered** モードの違いは、未登録のマルチキャストトラフィックに対する処理です。**Forward Unregistered** の場合、未登録のマルチキャストトラフィックはフラッディングされます。**Filter Unregistered** の場合は、転送されません。

本画面を表示するには、**L2 Features > L2 Multicast Control > Multicast Filtering** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
VID List	VLAN ID リストを入力します。
Multicast Filtering Mode	マルチキャストフィルタリングモードを以下のいずれかから選択します。 • **Forward Unregistered**：登録済みのマルチキャストパケットは転送テーブルに基づいて転送され、未登録のマルチキャストパケットは VLAN ドメインに基づいてフラッディングされます。 • **Forward All**：すべてのマルチキャストパケットは、VLAN ドメインに基づいてフラッディングされます。 • **Filter Unregistered**：登録済みのパケットは転送テーブルに基づいて転送され、すべての未登録のマルチキャストパケットはフィルタリングされます。

設定を適用するには、**Apply** ボタンをクリックします。

5.8 LLDP

LLDP サブメニューでは、LLDP に関連する設定を行います。
LLDP を使用すると、隣接する機器（ネイバー）と相互に LLDP 情報を交換し、ネイバー情報を収集できます。これらの情報は、調査目的でスイッチが接続しているデバイスを確認する場合や、ネットワーク管理ツールなどによって構成管理を行う際に有用となります。

LLDP で使用されるフレームは、原則として受信したデバイスで終端され、他のポートには転送されません。ただし、LLDP を使用しないデバイスで、LLDP 透過機能をサポートしている場合、LLDP フレームを転送することがあります。この場合、LLDP 対応機器同士を LLDP 透過機能をサポートしている機器で中継して接続しても LLDP での情報交換を行うことはできますが、中継するデバイスがその他の LLDP 対応機器を収容している場合、LLDP のネイバー情報が不定になり、構成管理が困難になる恐れがあります。

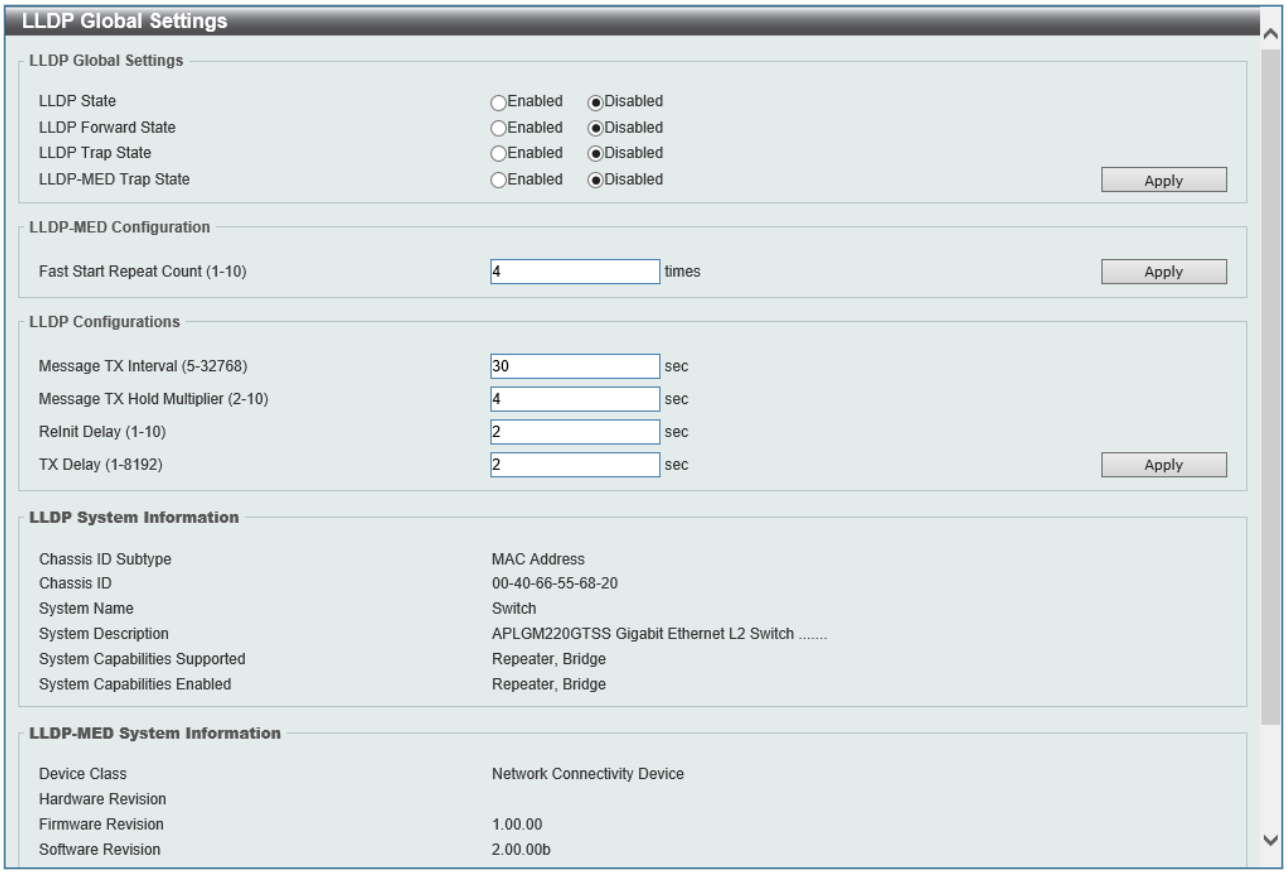
LLDP の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
5.8.1	LLDP Global Settings	LLDP のグローバル設定
5.8.2	LLDP Port Settings	LLDP のポート設定
5.8.3	LLDP Management Address List	LLDP で通知する管理アドレスの表示
5.8.4	LLDP Basic TLVs Settings	基本管理 TLV の設定
5.8.5	LLDP Dot1 TLVs Settings	IEEE802.1 TLV の設定
5.8.6	LLDP Dot3 TLVs Settings	IEEE802.3 TLV の設定
5.8.7	LLDP-MED Port Settings	LLDP-MED TLV の設定
5.8.8	LLDP Statistics Information	LLDP の統計情報の表示
5.8.9	LLDP Local Port Information	LLDP で通知する情報の表示
5.8.10	LLDP Neighbor Port Information	ネイバー情報の表示

LLDP フレームでは、フレームのデータに装置自身の属性情報を含めます。この属性情報は、TLV という形式で指定されます。LLDP フレームに含まれる属性情報は、その属性情報の TLV 形式を定めた規格によって大別されます。本装置では、ポート ID や LLDP 情報の有効期限などの LLDP で必須となる情報や、システム名などのオプション情報を含む基本管理 TLV の他に、VLAN などの情報を含む IEEE802.1 TLV や、物理層に関する情報を含む IEEE802.3 TLV、エンドポイントデバイス向けの情報を含む LLDP-MED TLV の属性情報に対応します。

5.8.1 LLDP Global Settings

LLDP Global Settings 画面では、LLDP のグローバル設定を行います。
本画面を表示するには、L2 Features > LLDP > LLDP Global Settings をクリックします。



LLDP Global Settings では、LLDP のグローバル設定を行います。各項目の説明を以下に示します。

パラメーター	説明
LLDP State	LLDP 機能の状態（Enabled / Disabled）を選択します。
LLDP Forward State	LLDP 透過機能の状態（Enabled / Disabled）を選択します。 LLDP State が Enabled で、LLDP Forward State が Disabled の場合は、受信した LLDP フレームが転送されます。
LLDP Trap State	LLDP 関連の SNMP トラップを送信する場合は Enabled を選択します。送信しない場合は Disabled を選択します。
LLDP-MED Trap State	LLDP-MED 関連の SNMP トラップを送信する場合は Enabled を選択します。送信しない場合は Disabled を選択します。

設定を適用するには、Apply ボタンをクリックします。

LLDP-MED Configuration では、LLDP-MED 関連のパラメーターを設定します。各項目の説明を以下に示します。

パラメーター	説明
Fast Start Repeat Count	LLDP-MED ファストスタート処理のフレーム送信回数を 1～10（回）の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

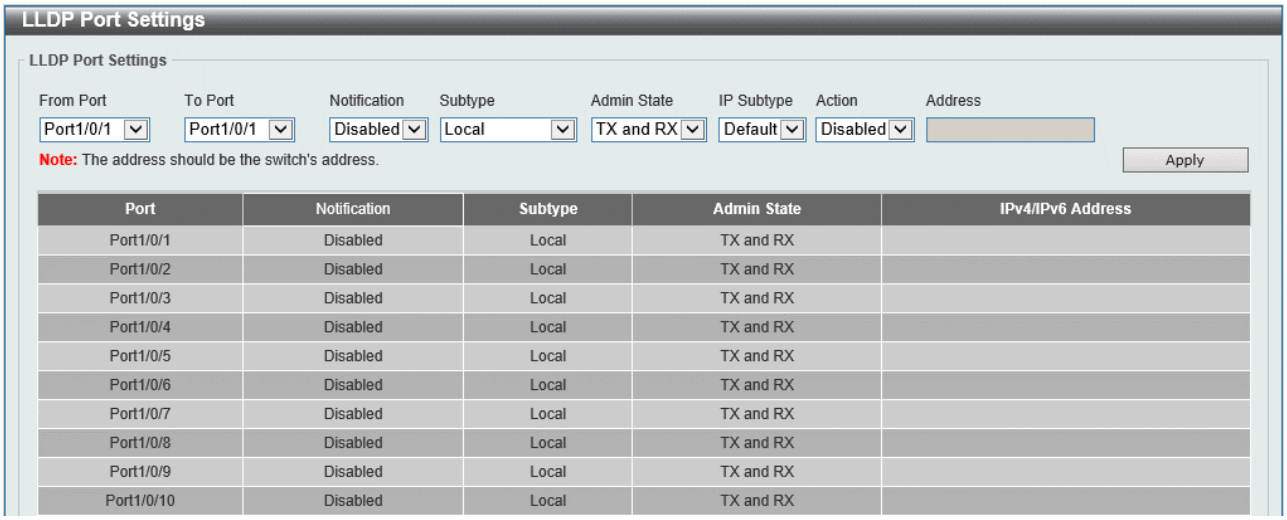
LLDP Configurations では、LLDP 関連のパラメーターを設定します。各項目の説明を以下に示します。

パラメーター	説明
Message TX Interval	LLDP フレームの送信間隔を 5～32768（秒）の範囲で入力します。
Message TX Hold Multiplier	LLDP のホールド乗数を 2～10 の範囲で入力します。この値は、LLDP フレームの TTL 値（存続時間）の計算に使用されます。
ReInit Delay	LLDP 再初期化の実行保留時間を 1～10（秒）の範囲で入力します。
TX Delay	LLDP フレームの連続送信時の最小送信間隔（保留時間）を 1～8192（秒）の範囲で入力します。**Message TX Interval** の 1/4 以下の値を設定してください。

設定を適用するには、**Apply** ボタンをクリックします。

5.8.2 LLDP Port Settings

LLDP Port Settings 画面では、LLDP のポート設定を行います。
本画面を表示するには、**L2 Features > LLDP > LLDP Port Settings** をクリックします。



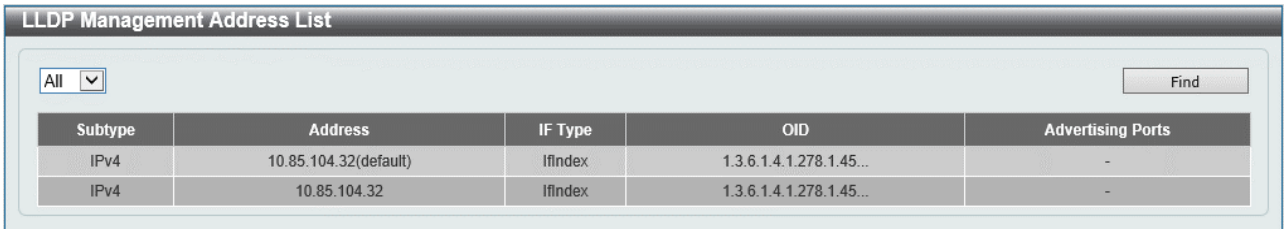
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Notification	LLDP 関連の SNMP トラップを送信するかどうかをポート単位で設定します。SNMP トラップを送信する場合は Enabled を選択します。送信しない場合は Disabled を選択します。
Subtype	通知するポート ID サブタイプ（MAC Address / Local）を選択します。
Admin State	LLDP フレーム送受信の設定を、以下のいずれかから選択します。 • TX：LLDP フレームの送信のみ実行します。 • RX：LLDP フレームの受信のみ実行します。 • TX and RX：LLDP フレームの送信と受信を実行します。 • Disabled：LLDP フレームの送信と受信を実行しません。
IP Subtype	通知する管理アドレスの種類（Default / IPv4 / IPv6）を選択します。Default では自動的にアドレスが選択されます。
Action	管理アドレス情報を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。
Address	通知する管理アドレスを入力します。

設定を適用するには、Apply ボタンをクリックします。

5.8.3 LLDP Management Address List

LLDP Management Address List 画面では、LLDP 管理アドレスリストを表示します。
本画面を表示するには、L2 Features > LLDP > LLDP Management Address List をクリックします。



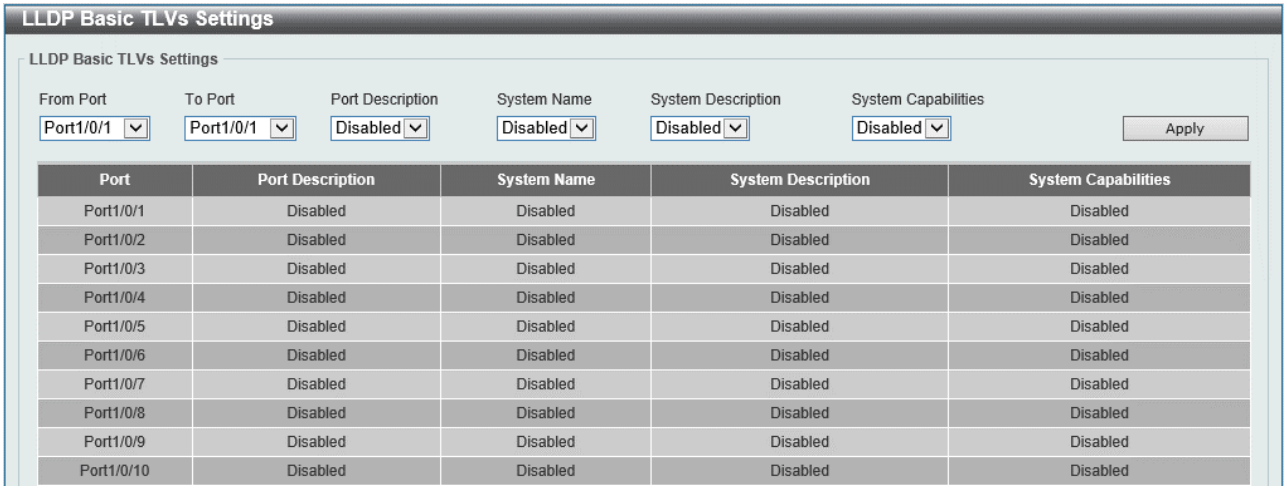
本画面の各項目の説明を以下に示します。

パラメーター	説明
Subtype	以下のいずれかのサブタイプを選択します。 • All：すべてのエントリーを表示する場合に選択します。 • IPv4：IPv4 アドレスで検索します。IPv4 を選択すると表示される右側のボックスに、検索する IPv4 アドレスを入力します。 • IPv6：IPv6 アドレスで検索します。IPv6 を選択すると表示される右側のボックスに、検索する IPv6 アドレスを入力します。

指定した内容で LLDP 管理アドレスを検索するには、Find ボタンをクリックします。

5.8.4 LLDP Basic TLVs Settings

LLDP Basic TLVs Settings 画面では、基本管理 TLV の設定を行います。
本画面を表示するには、L2 Features > LLDP > LLDP Basic TLVs Settings をクリックします。



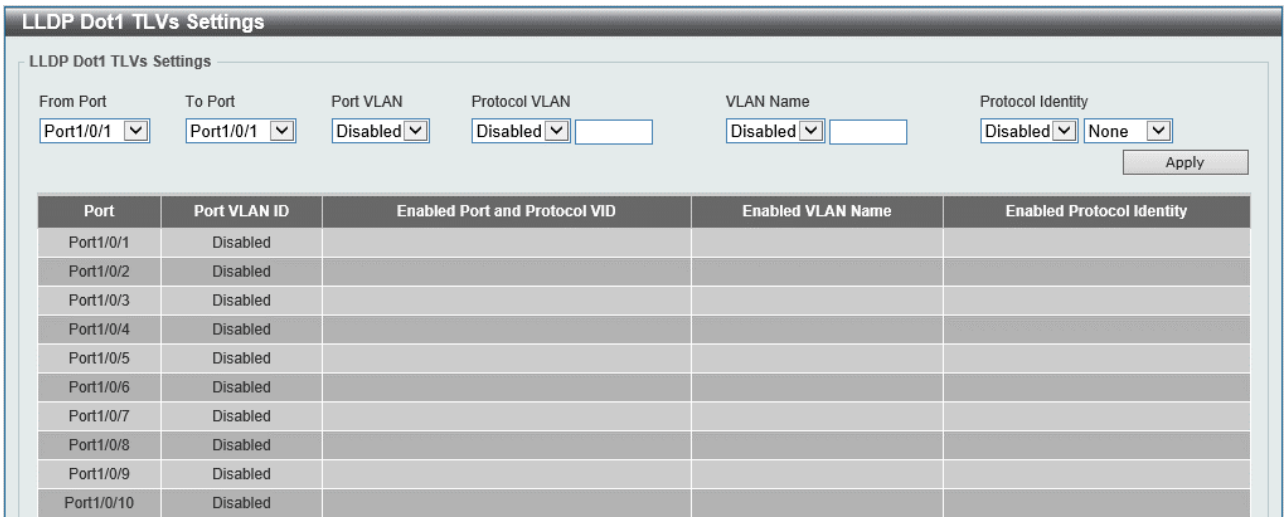
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Port Description	ポートの説明を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。
System Name	システム名を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。
System Description	システムの説明を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。
System Capabilities	システムの機能を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。

設定を適用するには、Apply ボタンをクリックします。

5.8.5 LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs Settings 画面では、IEEE 802.1 TLV の設定を行います。
本画面を表示するには、L2 Features > LLDP > LLDP Dot1 TLVs Settings をクリックします。



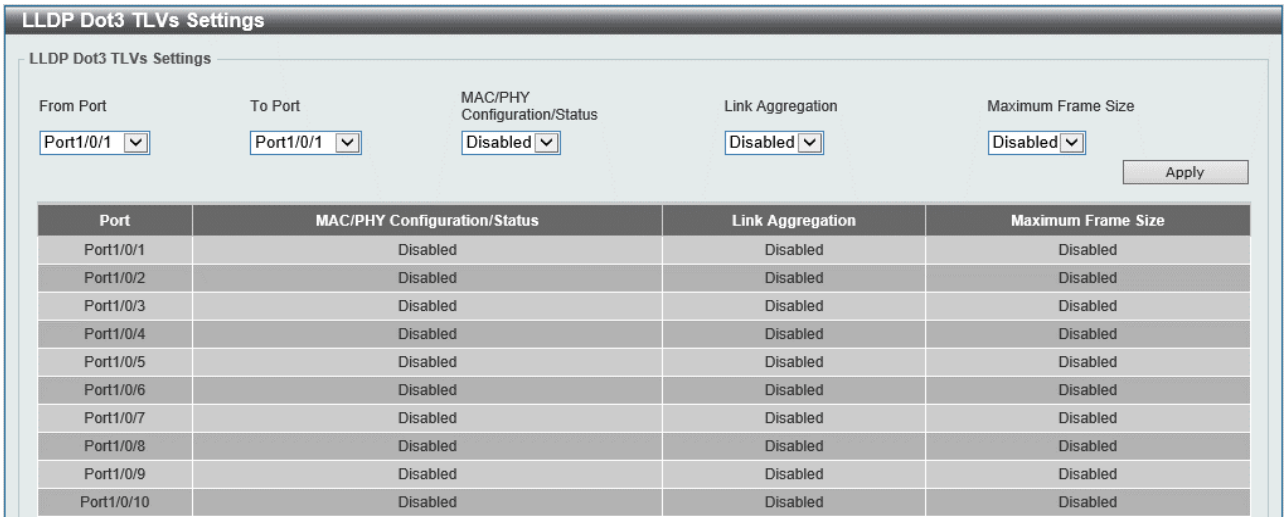
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Port VLAN	ポート VLAN ID を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。
Protocol VLAN	PPVID を通知する場合は Enabled を選択し、テキストボックスに通知する VLAN の VLAN ID を入力します。通知しない場合は Disabled を選択します。
VLAN Name	VLAN 名を通知する場合は Enabled を選択し、テキストボックスに通知する VLAN の VLAN ID を入力します。通知しない場合は Disabled を選択します。
Protocol Identity	サポートするプロトコルの情報を通知する場合は Enabled を選択し、ドロップダウンリストでプロトコル（None / EAPOL / LACP / STP / All）を選択します。通知しない場合は Disabled を選択します。

設定を適用するには、Apply ボタンをクリックします。

5.8.6 LLDP Dot3 TLVs Settings

LLDP Dot3 TLVs Settings 画面では、IEEE 802.3 TLV を設定します。
本画面を表示するには、L2 Features > LLDP > LLDP Dot3 TLVs Settings をクリックします。



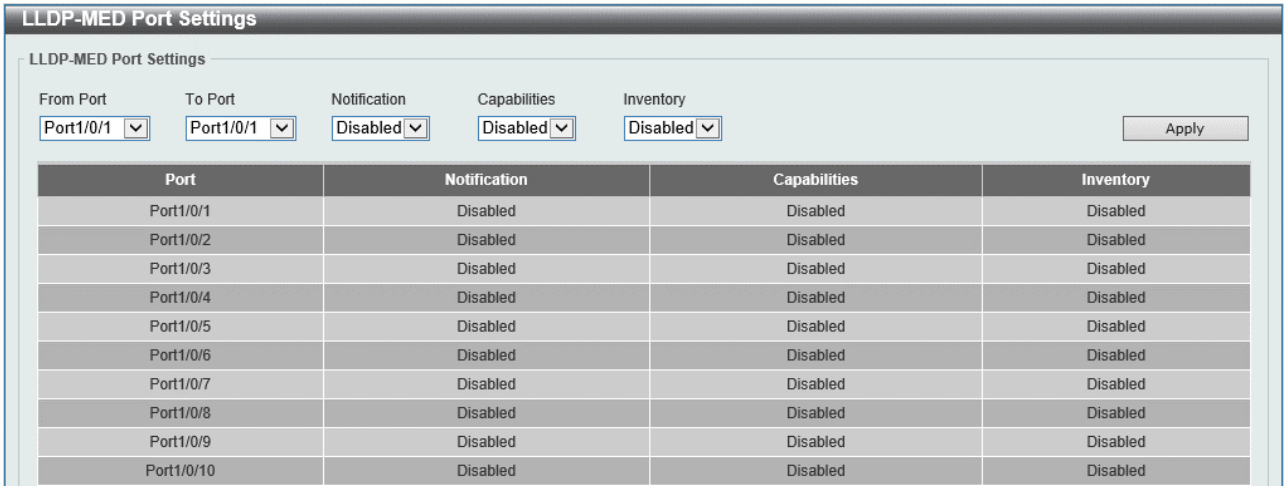
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
MAC/PHY Configuration/Status	MAC/PHY 設定状態の情報を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。
Link Aggregation	リンクアグリゲーションの情報を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。
Maximum Frame Size	最大フレームサイズの情報を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。

設定を適用するには、Apply ボタンをクリックします。

5.8.7 LLDP-MED Port Settings

LLDP-MED Port Settings 画面では、LLDP-MED TLV の設定を行います。
本画面を表示するには、L2 Features > LLDP > LLDP-MED Port Settings をクリックします。



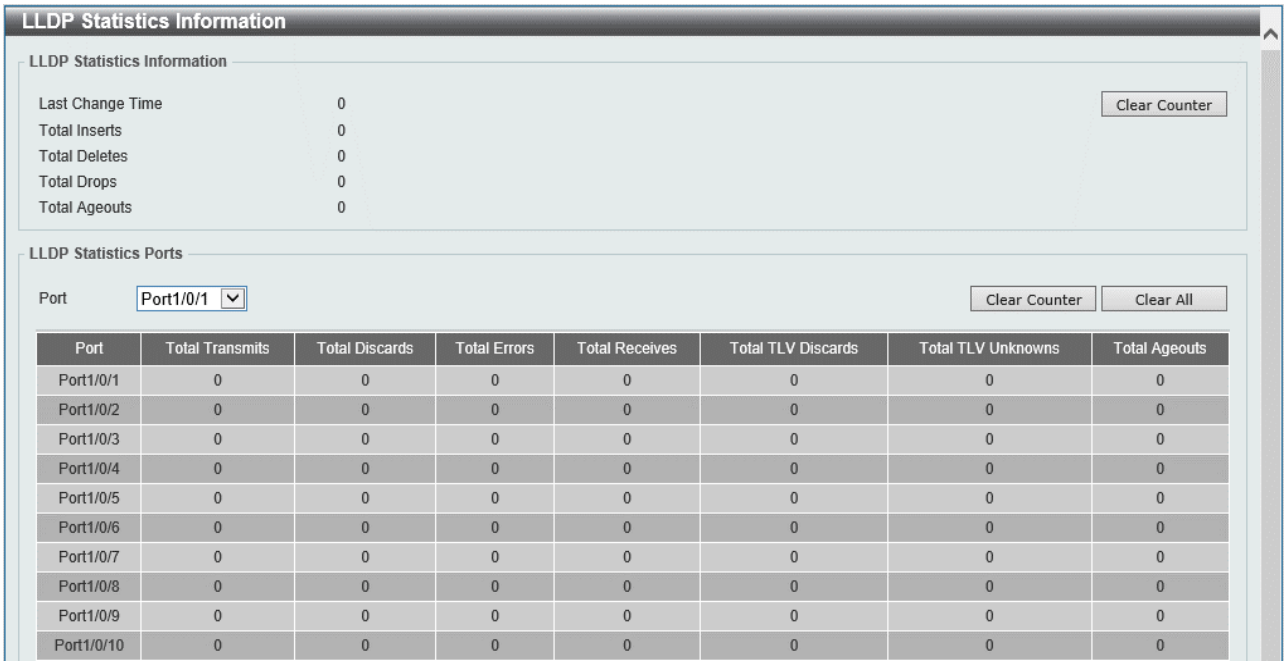
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Notification	LLDP-MED 関連の SNMP トラップを送信するかどうかをポート単位で設定します。SNMP トラップを送信する場合は Enabled を選択します。送信しない場合は Disabled を選択します。
Capabilities	LLDP-MED の機能情報を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。
Inventory	LLDP-MED の資産管理情報を通知する場合は Enabled を選択します。通知しない場合は Disabled を選択します。

設定を適用するには、Apply ボタンをクリックします。

5.8.8 LLDP Statistics Information

LLDP Statistics Information 画面では、LLDP 統計情報を表示します。
本画面を表示するには、L2 Features > LLDP > LLDP Statistics Information をクリックします。



LLDP Statistics Information では、LLDP 統計のグローバル情報が表示されます。
表示されているカウンター情報をクリアするには、Clear Counter ボタンをクリックします。

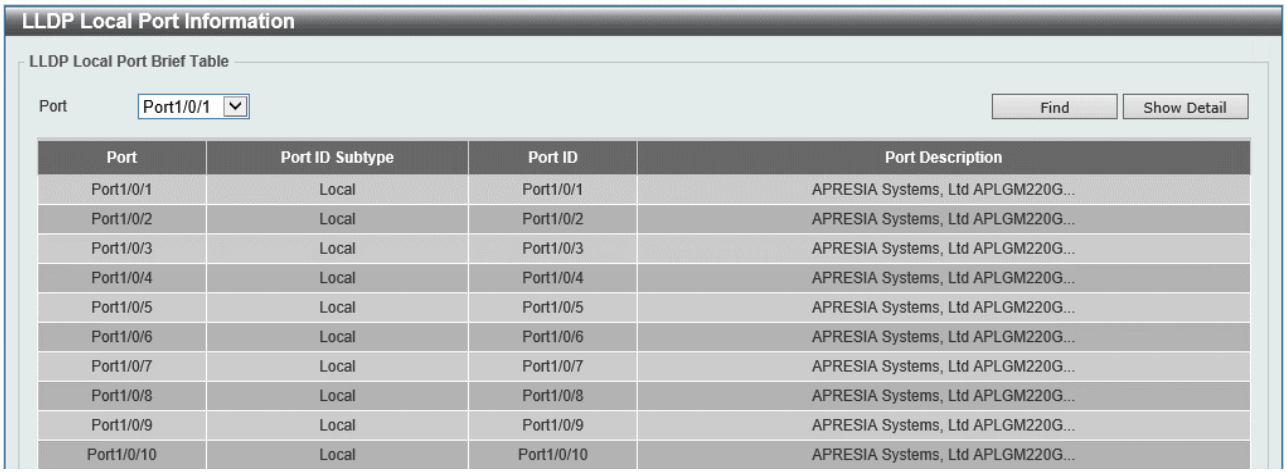
LLDP Statistics Ports では、ポート単位での LLDP 統計情報が表示されます。各項目の説明を以下に示します。

パラメーター	説明
Port	ポート番号を選択して絞り込みを行います。

表示されている LLDP 統計情報のカウンター情報をクリアするには、Clear Counter ボタンをクリックします。
すべての LLDP 統計情報のカウンター情報をクリアするには、Clear All ボタンをクリックします。

5.8.9 LLDP Local Port Information

LLDP Local Port Information 画面では、隣接するデバイスに通知する LLDP 情報を表示します。
本画面を表示するには、L2 Features > LLDP > LLDP Local Port Information をクリックします。

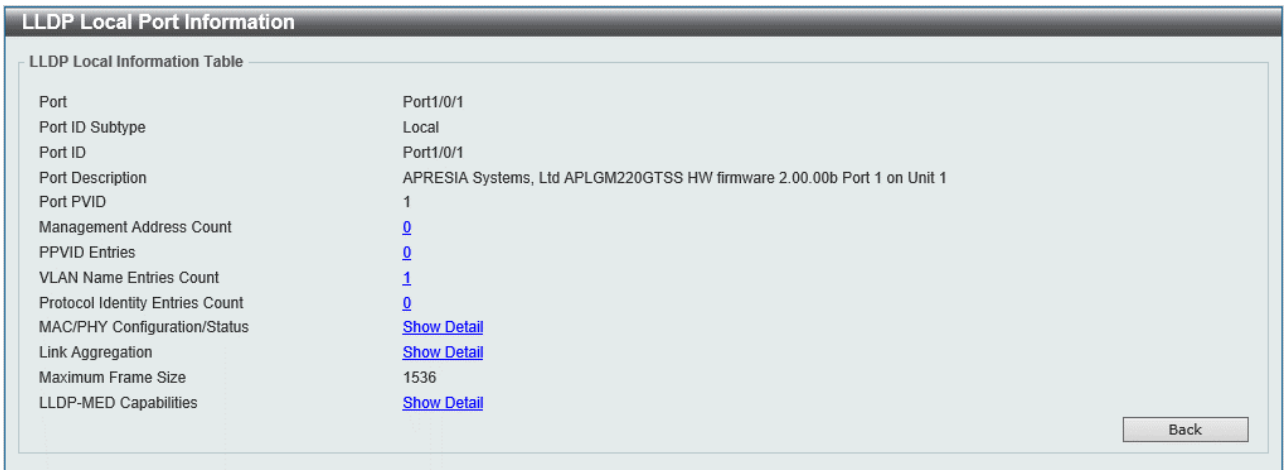


本画面の各項目の説明を以下に示します。

パラメーター	説明
Port	情報を表示するポート番号を選択します。

入力した情報で LLDP ローカルポート情報を検索するには、Find ボタンをクリックします。
LLDP ローカルポート情報の詳細を表示するには、Show Detail ボタンをクリックします。

Show Detail ボタンをクリックすると、以下に示す画面が表示されます。



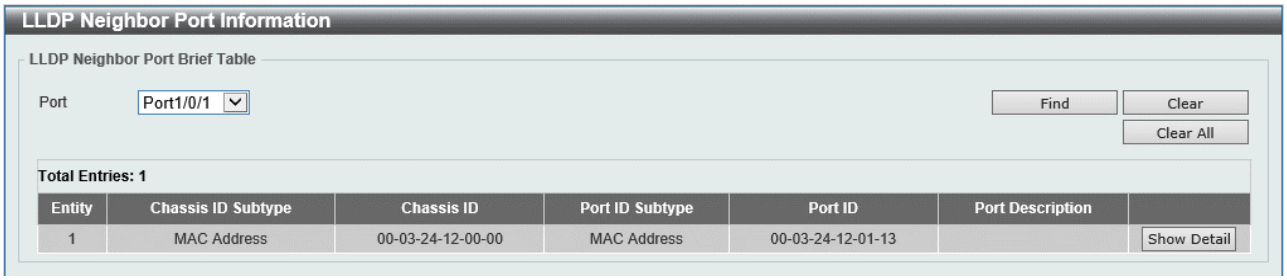
表示結果のハイパーリンクをクリックすると、その項目に対する詳細情報が表示されます。
前の画面に戻るには、Back ボタンをクリックします。

以下の画面は、**MAC/PHY Configuration/Status** の Show Detail をクリックした例です。

前の画面に戻るには、**Back** ボタンをクリックします。

5.8.10 LLDP Neighbor Port Information

LLDP Neighbor Port Information 画面では、隣接デバイスから通知された LLDP 情報を表示します。
本画面を表示するには、**L2 Features > LLDP > LLDP Neighbor Port Information** をクリックします。

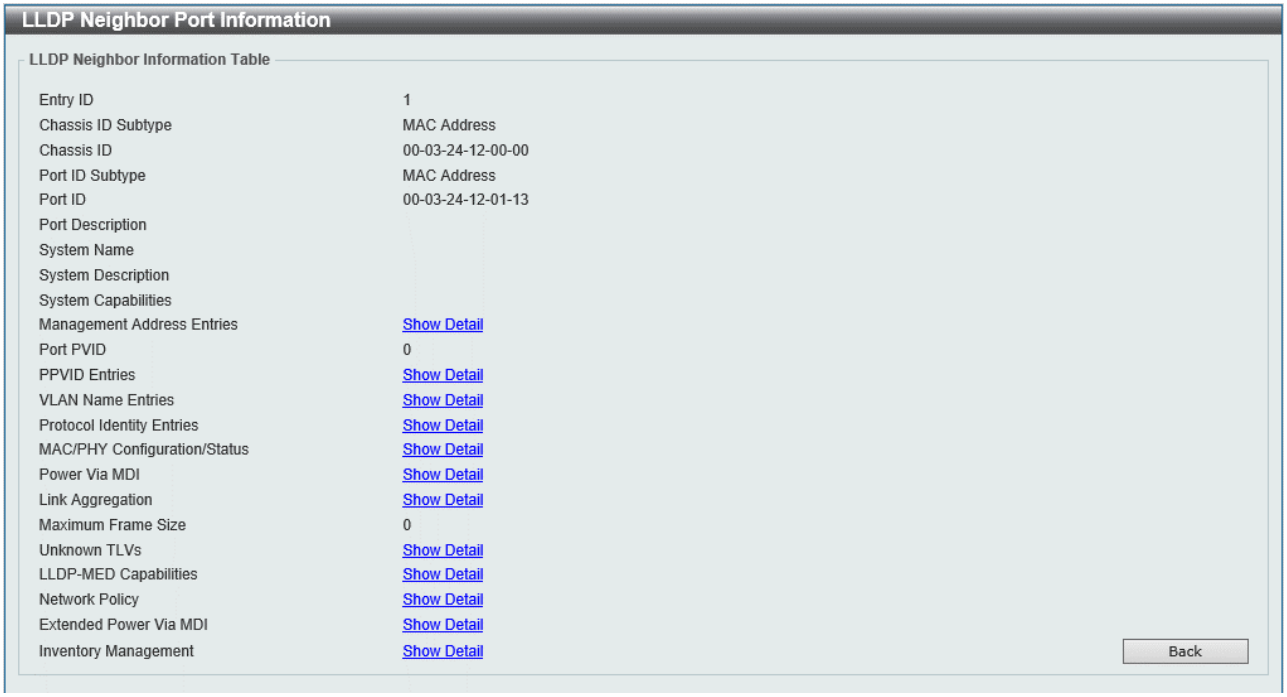


本画面の各項目の説明を以下に示します。

パラメーター	説明
Port	情報を表示するポート番号を選択します。

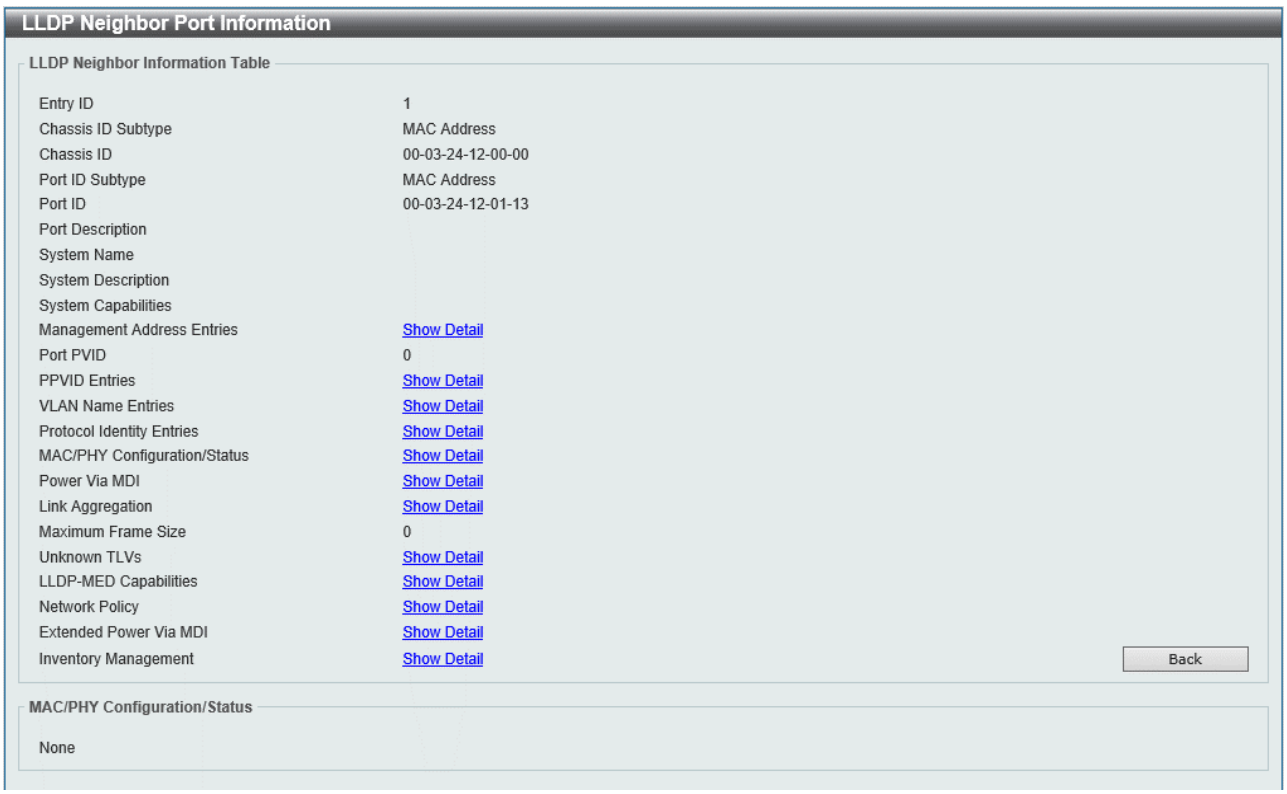
ポートの LLDP 情報を検索するには、**Find** ボタンをクリックします。
ポートの LLDP 情報をクリアするには、**Clear** ボタンをクリックします。
表示されているすべての LLDP 情報をクリアするには、**Clear All** ボタンをクリックします。
LLDP 情報の詳細を表示するには、**Show Detail** ボタンをクリックします。

Show Detail ボタンをクリックすると、以下に示す画面が表示されます。



表示結果のハイパーリンクをクリックすると、その項目に対する詳細情報が表示されます。
前の画面に戻るには、**Back** ボタンをクリックします。

以下の画面は、**MAC/PHY Configuration/Status** の Show Detail をクリックした例です。



前の画面に戻るには、**Back** ボタンをクリックします。

6 L3 Features

L3 Features メニューでは、IP アドレス設定などのレイヤー3 関連の設定を行うことができます。
L3 Features の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
6.1	ARP	ARP の設定や ARP テーブルの表示
6.2	IPv6 Neighbor	IPv6 ネイバーの設定やネイバーテーブルの表示
6.3	Interface	IPv4 アドレス／IPv6 アドレスの設定
6.4	IPv4 Default Route	IPv4 デフォルトルートの設定
6.5	IPv4 Route Table	IPv4 ルートテーブルの表示
6.6	IPv6 Default Route	IPv6 デフォルトルートの設定
6.7	IPv6 Route Table	IPv6 ルートテーブルの表示

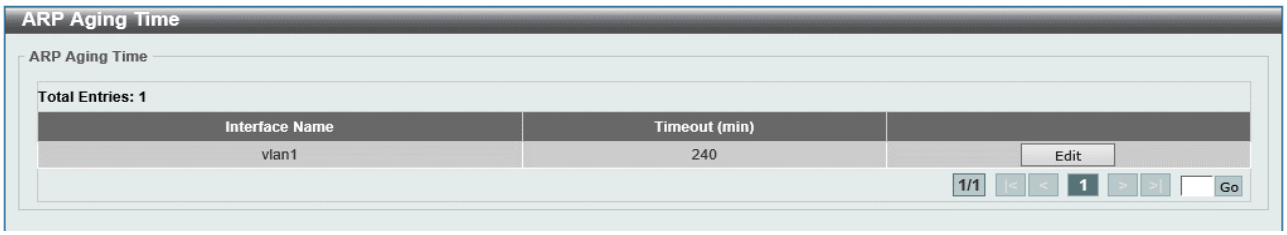
6.1 ARP

ARP サブメニューでは、ARP 登録に関する設定を行います。
ARP の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
6.1.1	ARP Aging Time	ARP テーブルのエージング時間の設定
6.1.2	Static ARP	スタティック ARP エントリーの登録
6.1.3	ARP Table	ARP テーブルの情報表示

6.1.1 ARP Aging Time

ARP Aging Time 画面では、ARP エージングタイムを設定します。
本画面を表示するには、**L3 Features > ARP > ARP Aging Time** をクリックします。



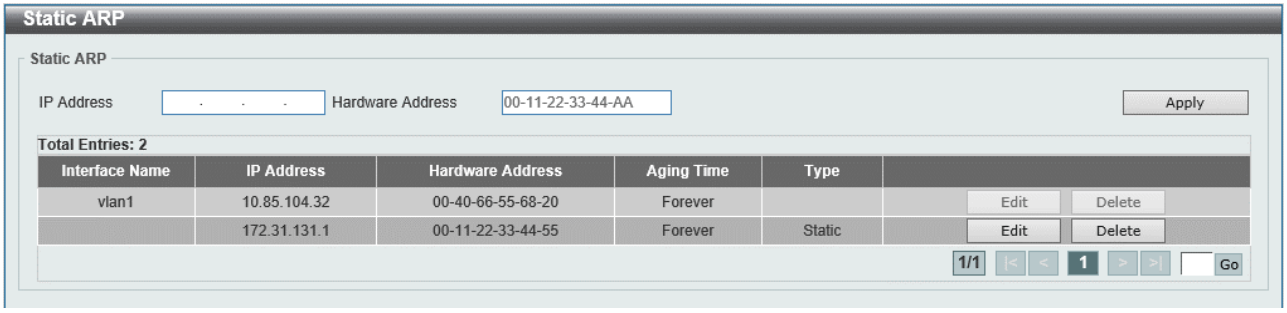
本画面の各項目の説明を以下に示します。

パラメーター	説明
Timeout	**Edit** ボタンをクリックした後、ARP エージングタイムアウト値を入力します。

ARP エージングタイムアウト値を設定するには、**Edit** ボタンをクリックします。
設定を適用するには、**Apply** ボタンをクリックします。

6.1.2 Static ARP

Static ARP 画面では、スタティック ARP を設定します。
本画面を表示するには、L3 Features > ARP > Static ARP をクリックします。



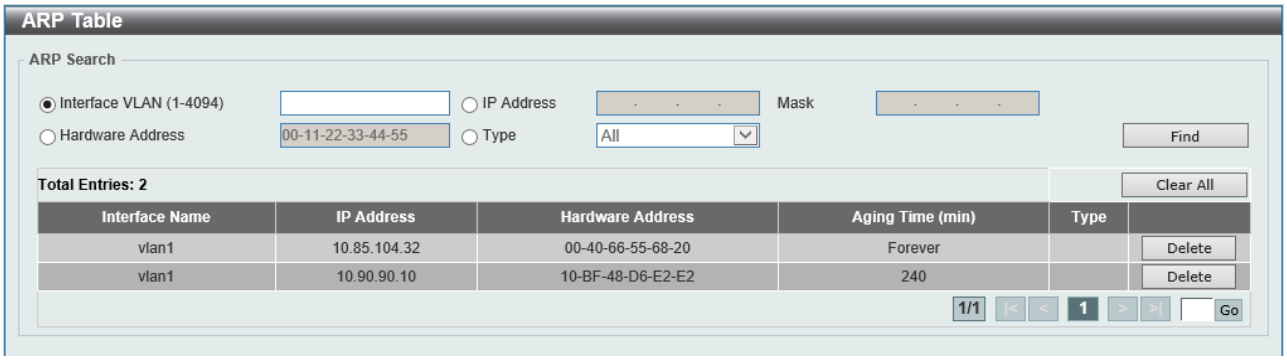
本画面の各項目の説明を以下に示します。

パラメーター	説明
IP Address	登録する IP アドレスを入力します。
Hardware Address	IP アドレスに関連付ける MAC アドレスを入力します。

設定を適用するには、Apply ボタンをクリックします。
スタティック ARP を再設定するには、Edit ボタンをクリックします。
スタティック ARP を削除するには、Delete ボタンをクリックします。

6.1.3 ARP Table

ARP Table 画面では、ARP テーブルのエントリーを表示します。
本画面を表示するには、L3 Features > ARP > ARP Table をクリックします。



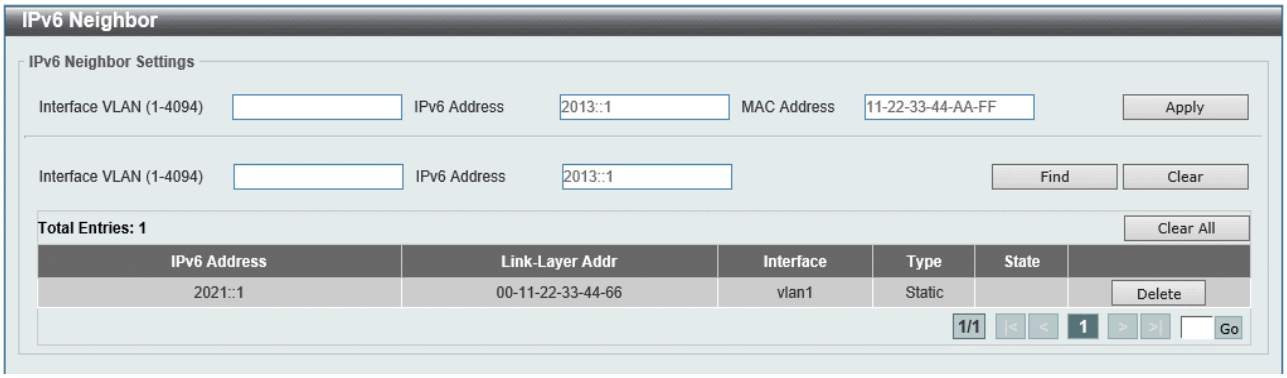
本画面の各項目の説明を以下に示します。

パラメーター	説明
Interface VLAN	VLAN ID で検索する場合にラジオボタンをクリックし、検索する VLAN ID を 1～4094 の範囲で入力します。
IP Address	IP アドレスで検索する場合にラジオボタンをクリックし、検索する IP アドレスを入力します。 • Mask：IP アドレスのサブネットマスクを入力します。
Hardware Address	MAC アドレスで検索する場合にラジオボタンをクリックし、検索する MAC アドレスを入力します。
Type	タイプで検索する場合にラジオボタンをクリックし、検索するタイプ（All / Dynamic）を選択します。

入力した情報でエントリーを検索するには、Find ボタンをクリックします。
すべてのダイナミック ARP キャッシュをクリアするには、Clear All ボタンをクリックします。
エントリーに関連付けられているダイナミック ARP キャッシュをクリアするには、Delete ボタンをクリックします。

6.2 IPv6 Neighbor

IPv6 Neighbor 画面では、IPv6 ネイバーを設定します。
本画面を表示するには、**L3 Features > IPv6 Neighbor** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Interface VLAN	VLAN インターフェースの VLAN ID を 1～4094 の範囲で入力します。
IPv6 Address	IPv6 アドレスを入力します。
MAC Address	MAC アドレスを入力します。

設定を適用するには、**Apply** ボタンをクリックします。
入力した情報で IPv6 ネイバーを検索するには、**Find** ボタンをクリックします。
インターフェースのすべてのダイナミック IPv6 ネイバー情報をクリアするには、**Clear** ボタンをクリックします。
すべてのダイナミック IPv6 ネイバー情報をクリアするには、**Clear All** ボタンをクリックします。
IPv6 ネイバーを削除するには、**Delete** ボタンをクリックします。

6.3 Interface

Interface サブメニューでは、VLAN インターフェースで IP アドレスの設定を行います。
VLAN インターフェースは、レイヤー2 の VLAN とその上位レイヤーを接続するための論理インターフェースです。本装置では、1 個の VLAN インターフェースを設定できます。登録した VLAN インターフェースには、IP アドレスなどの上位レイヤーの設定を登録します。

Interface の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
6.3.1	IPv4 Interface	IPv4 アドレスの設定
6.3.2	IPv6 Interface	IPv6 アドレスの設定

6.3.1 IPv4 Interface

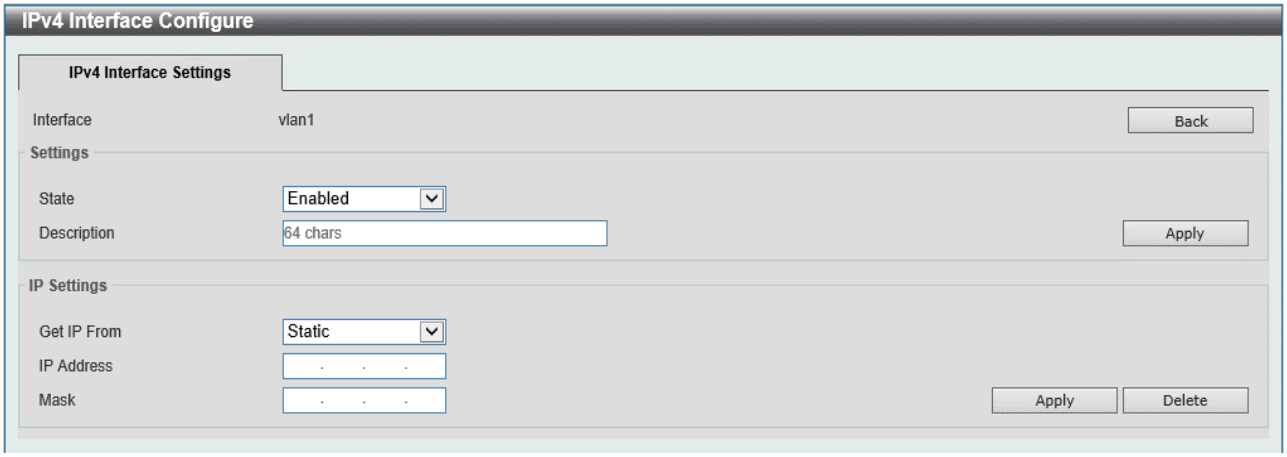
IPv4 Interface 画面では、VLAN インターフェースの IPv4 アドレス設定を行います。
本画面を表示するには、**L3 Features > Interface > IPv4 Interface** をクリックします。

本画面の各項目の説明を以下に示します。

パラメーター	説明
Interface VLAN	VLAN インターフェースの VLAN ID を 1～4094 の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。
入力した情報で IPv4 インターフェースを検索するには、**Find** ボタンをクリックします。
IPv4 インターフェースを再設定するには、**Edit** ボタンをクリックします。
IPv4 インターフェースを削除するには、**Delete** ボタンをクリックします。

Edit ボタンをクリックすると、以下に示す画面が表示されます。



Settings では、VLAN インターフェース全般の設定を行います。各項目の説明を以下に示します。

パラメーター	説明
State	VLAN インターフェースの状態（Enabled / Disabled）を選択します。Disabled を選択すると、VLAN インターフェースが shutdown 状態になります。
Description	VLAN インターフェースの説明を 64 文字以内で入力します。

前の画面に戻るには、Back ボタンをクリックします。
設定を適用するには、Apply ボタンをクリックします。

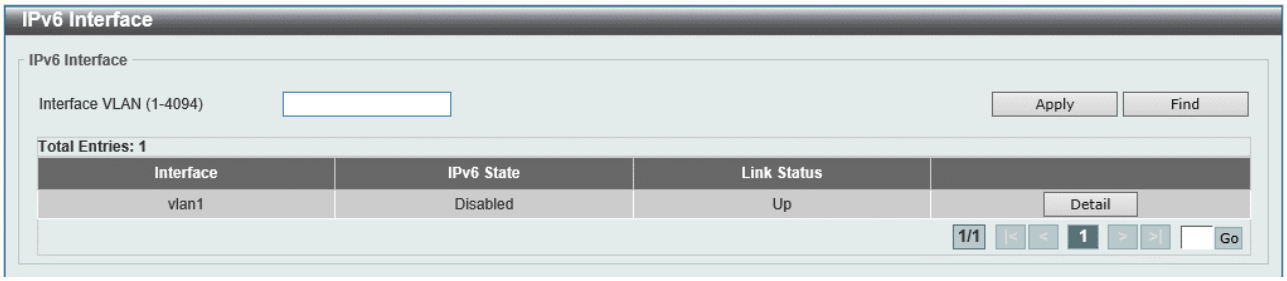
IP Settings では、IP アドレスの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Get IP From	IP アドレスの設定方法を以下のどちらかから選択します。 • Static：IPv4 アドレスを手動で入力します。 • DHCP：DHCP サーバーから IPv4 アドレスを自動取得します。
IP Address	装置の IPv4 アドレスを入力します。
Mask	装置の IPv4 アドレスのサブネットマスクを入力します。

設定を適用するには、Apply ボタンをクリックします。
設定を削除するには、Delete ボタンをクリックします。

6.3.2 IPv6 Interface

IPv6 Interface 画面では、VLAN インターフェースで IPv6 アドレスを設定します。
本画面を表示するには、**L3 Features > Interface > IPv6 Interface** をクリックします。

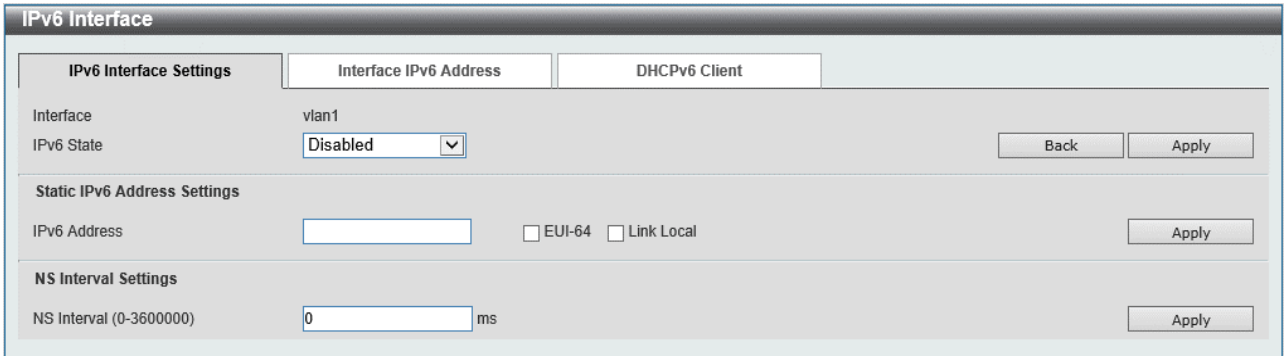


本画面の各項目の説明を以下に示します。

パラメーター	説明
Interface VLAN	VLAN インターフェースの VLAN ID を 1～4094 の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。
入力した情報で IPv6 インターフェースを検索するには、**Find** ボタンをクリックします。
IPv6 インターフェースの詳細を表示および設定するには、**Detail** ボタンをクリックします。

Detail ボタンをクリックすると、以下に示す画面が表示されます。



IPv6 Interface Settings タブの最初の部分では、VLAN インターフェースの IPv6 の設定を行います。
各項目の説明を以下に示します。

パラメーター	説明
IPv6 State	VLAN インターフェースの IPv6 の状態（**Enabled** / **Disabled**）を選択します。**Disabled** の場合、IPv6 を使用しません。

設定を適用するには、**Apply** ボタンをクリックします。
前の画面に戻るには、**Back** ボタンをクリックします。

Static IPv6 Address Settings の部分では、IPv6 アドレスの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
IPv6 Address	IPv6 インターフェースの IPv6 アドレスを入力します。
EUI-64	EUI-64 形式のインターフェース ID を使用して IPv6 アドレスを設定する場合にチェックします。
Link-Local	リンクローカルアドレスを設定する場合にチェックします。

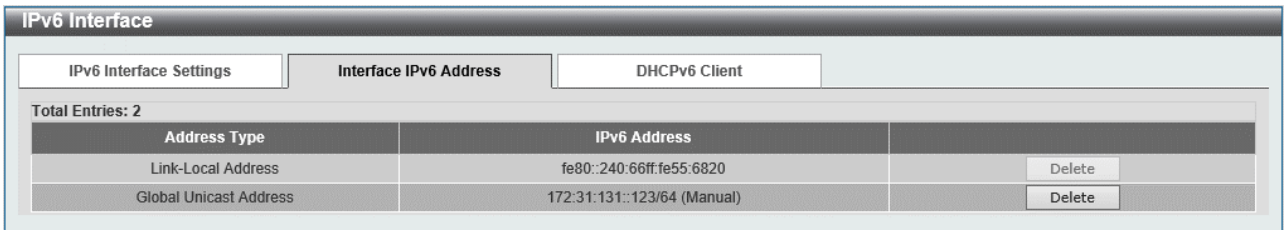
設定を適用するには、**Apply** ボタンをクリックします。

NS Interval Settings では、近隣要請メッセージの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
NS Interval	近隣要請（以後、NS）メッセージの再送信間隔の値を 0～3600000（ミリ秒）の範囲で入力します（デフォルト：0 ミリ秒）。 0 を入力した場合、装置は 1 秒を使用します。

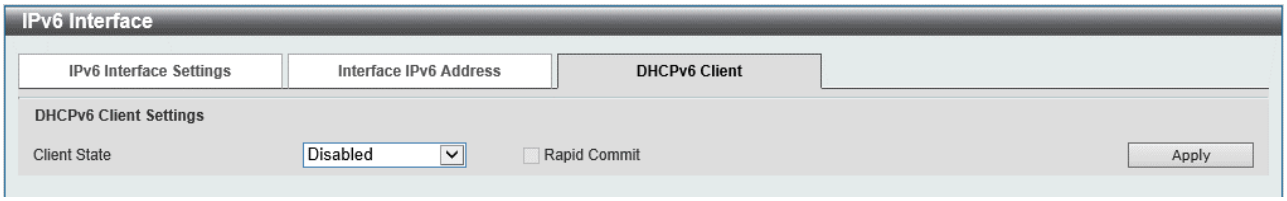
設定を適用するには、**Apply** ボタンをクリックします。

Interface IPv6 Address タブでは IPv6 アドレスを表示します。以下に示す画面が表示されます。



エントリーを削除するには、**Delete** ボタンをクリックします。

DHCPv6 Client タブでは、DHCPv6 クライアント機能の設定を行います。以下に示す画面が表示されます。



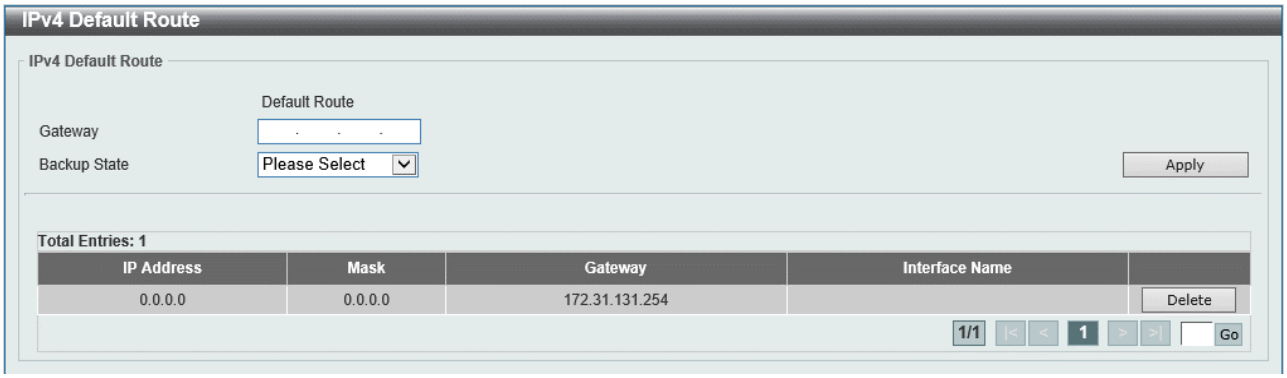
DHCPv6 Client Settings の各項目の説明を以下に示します。

パラメーター	説明
Client State	DHCPv6 クライアント機能の状態（**Enabled** / **Disabled**）を選択します。 **Rapid Commit** をチェックすると、DHCPv6 の高速コミットの要求を行います。

設定を適用するには、**Apply** ボタンをクリックします。

6.4 IPv4 Default Route

IPv4 Default Route 画面では、IPv4 デフォルトルートを設定します。
本画面を表示するには、**L3 Features > IPv4 Default Route** をクリックします。



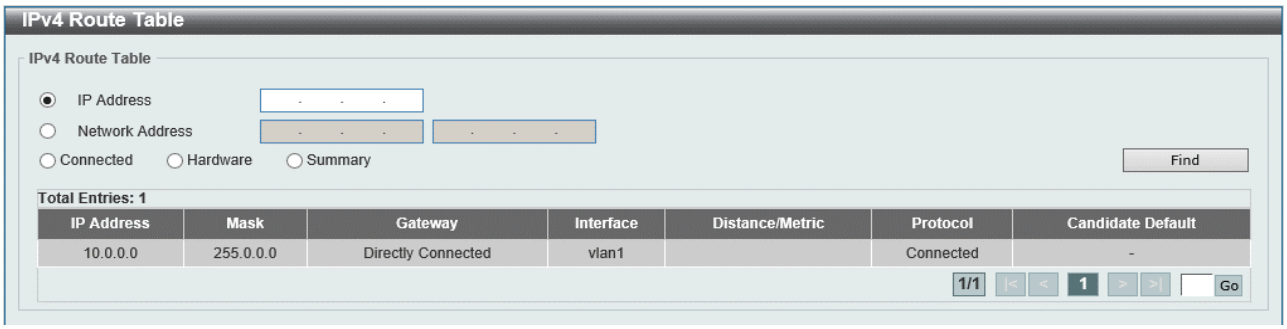
本画面の各項目の説明を以下に示します。

パラメーター	説明
Gateway	ルートのゲートウェイの IPv4 アドレスを入力します。
Backup State	以下のどちらかのバックアップ状態を選択します。 • **Primary**：プライマリールートを登録します。 • **Backup**：バックアップルートを登録します。

設定を適用するには、**Apply** ボタンをクリックします。
IPv4 デフォルトルートを削除するには、**Delete** ボタンをクリックします。

6.5 IPv4 Route Table

IPv4 Route Table 画面では、IPv4 ルートテーブルのエントリーを表示します。
本画面を表示するには、**L3 Features > IPv4 Route Table** をクリックします。



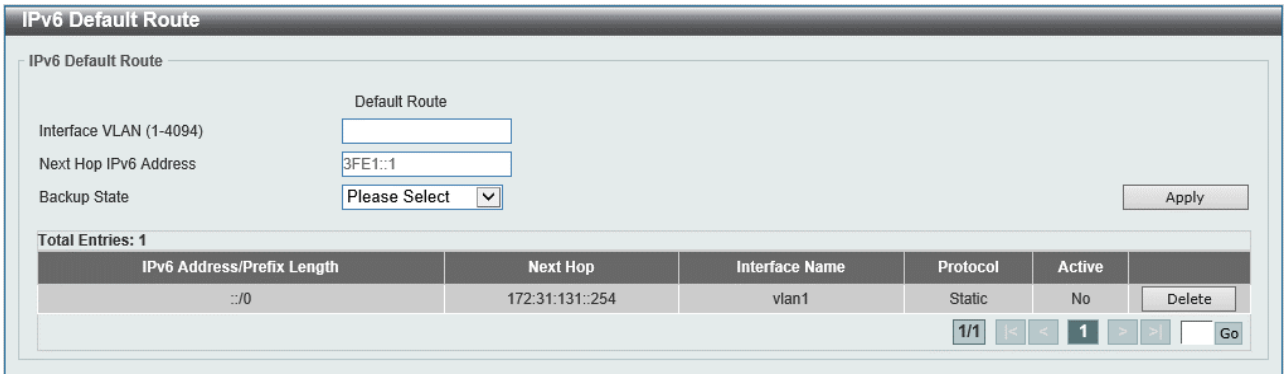
本画面の各項目の説明を以下に示します。

パラメーター	説明
IP Address	検索するルート情報を IPv4 アドレスで指定する場合にラジオボタンをクリックし、IPv4 アドレスを入力します。
Network Address	検索するルート情報を IPv4 ネットワークアドレスで指定する場合にラジオボタンをクリックし、IPv4 ネットワークアドレスを入力します。左のボックスにネットワークプレフィックスを入力し、右のボックスにネットワークマスクを入力します。
Connected	コネクテッドルートのみを表示する場合にラジオボタンをクリックします。
Hardware	ハードウェアルートのみを表示する場合にラジオボタンをクリックします。ハードウェアルートは、スイッチ LSI に登録されているルート情報です。
Summary	装置のルート情報の概要を表示する場合にラジオボタンをクリックします。

入力した情報で IPv4 ルートテーブルを検索するには、**Find** ボタンをクリックします。

6.6 IPv6 Default Route

IPv6 Default Route 画面では、IPv6 デフォルトルートを設定します。
本画面を表示するには、**L3 Features > IPv6 Default Route** をクリックします。



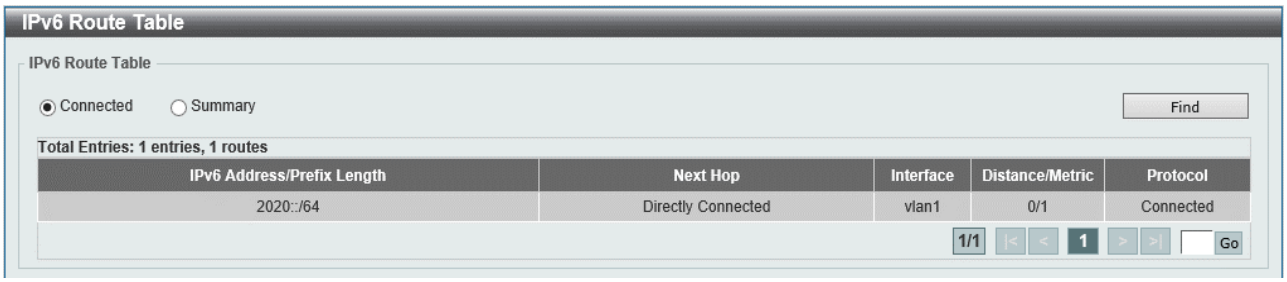
本画面の各項目の説明を以下に示します。

パラメーター	説明
Interface VLAN	VLAN インターフェースの VLAN ID を 1～4094 の範囲で入力します。
Next Hop IPv6 Address	ルートのネクストホップの IPv6 アドレスを入力します。
Backup State	以下のどちらかのバックアップ状態を選択します。 • **Primary**：ルートを、宛先へのプライマリールートとして指定する場合に選択します。 • **Backup**：ルートを、宛先へのバックアップルートとして指定する場合に選択します。

設定を適用するには、**Apply** ボタンをクリックします。
IPv6 デフォルトルートを削除するには、**Delete** ボタンをクリックします。

6.7 IPv6 Route Table

IPv6 Route Table 画面では、IPv6 ルートテーブルのエントリーを表示します。
本画面を表示するには、**L3 Features > IPv6 Route Table** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Connected	コネクテッドルートのみを表示する場合にラジオボタンをクリックします。
Summary	装置の IPv6 ルート情報の概要を表示する場合にラジオボタンをクリックします。

入力した情報で IPv6 ルートテーブルを検索するには、**Find** ボタンをクリックします。

7 QoS

QoS メニューでは、優先制御に関する設定を行うことができます。
イーサネットスイッチでは、入力したフレームの情報や受信ポートから各フレームに対して CoS による優先順位を定め、転送処理の順番を調整できます。優先制御が有効になると、各入力フレームは分類されて所定の CoS の割り当てが行われます（クラシフィケーション）。その後、CoS をベースにして 8 個のハードウェアキューのいずれかに振り分けられます（キューイング）。キューへの振り分けの前に、トラフィック経路上の他の通信機器でも QoS 処理を行えるように、CoS 値または DSCP 値の情報を付与することもあります（マーキング）。各キューに蓄積されたフレームは、所定のスケジューリング方法に沿って処理順番を決定し（スケジューリング）、順番に沿って転送されます。

QoS の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
7.1	Basic Settings	基本的な QoS 機能の設定
7.2	Advanced Settings	高度な QoS 機能の設定

基本的な QoS 機能の設定では、QoS を意識しないアプリケーションにも適用可能な、QoS の基本的な設定を行います。タグなしフレームに対するクラシフィケーションの設定、キューイング、およびスケジューリングに関する設定があります。また、ポートやハードウェアキュー単位での帯域制限の設定も含まれます。

高度な QoS 機能の設定では、QoS を意識するアプリケーション（音声や映像トラフィックなど）が混在するトラフィックを対象とした QoS の設定を行います。IP ヘッダーに含まれる DSCP 値を指標としたクラシフィケーションや、DSCP 値のリマーキングに関する設定があります。また、トラフィック分類によるポリシングの機能の設定も含まれます。

7.1 Basic Settings

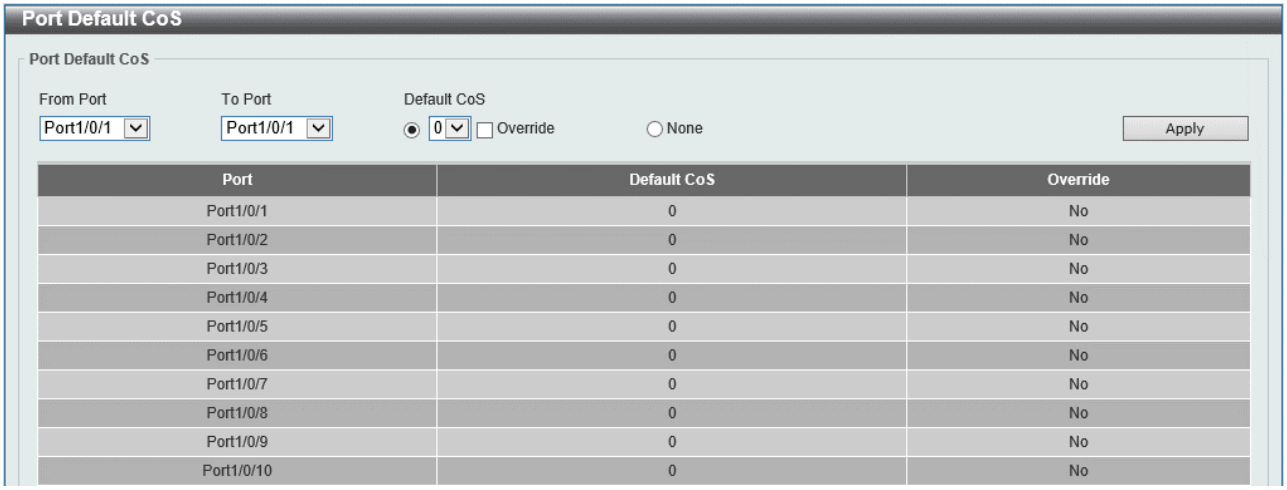
Basic Settings サブメニューでは、基本的な QoS 機能の設定を行います。ここでは、受信したタグなしフレームへの CoS の指定や、CoS とハードウェアキューとの紐付け、スケジューリング方式など、QoS の基本的な設定を行います。

Basic Settings の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
7.1.1	Port Default CoS	タグなしフレームの CoS の割り当ての設定
7.1.2	Port Scheduler Method	スケジューリング方式の設定
7.1.3	Queue Settings	各キューの重み付けの設定
7.1.4	CoS to Queue Mapping	CoS とハードウェアキューのマッピング設定
7.1.5	Port Rate Limiting	物理ポートでの帯域制限の設定
7.1.6	Queue Rate Limiting	ハードウェアキューでの帯域制限の設定

7.1.1 Port Default CoS

Port Default CoS 画面では、受信したタグなしフレームに割り当てる CoS 値を設定します。
本画面を表示するには、QoS > Basic Settings > Port Default CoS をクリックします。



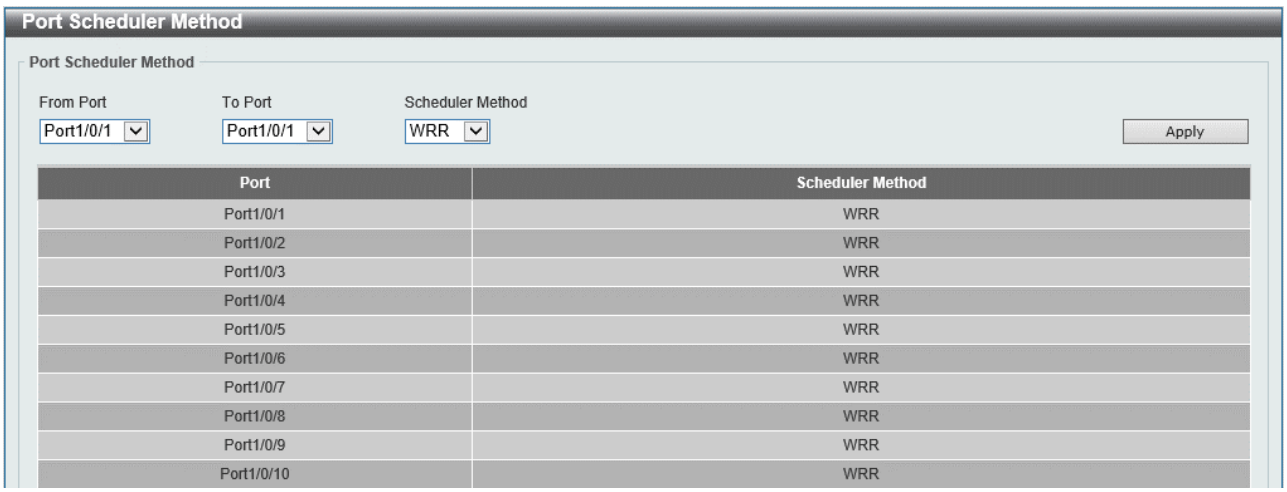
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	設定するポートの範囲を選択します。
Default CoS	ポートでの CoS の指標が CoS 値だった場合の、受信したタグなしフレームの CoS を 0～7 から選択します。 Override をチェックすると、すべてのフレームに対してポートに指定した CoS を優先します。CoS の指標が DSCP 値の場合でも同様です。

設定を適用するには、Apply ボタンをクリックします。

7.1.2 Port Scheduler Method

Port Scheduler Method 画面では、ポートの QoS スケジューリング方法を設定します。
本画面を表示するには、QoS > Basic Settings > Port Scheduler Method をクリックします。



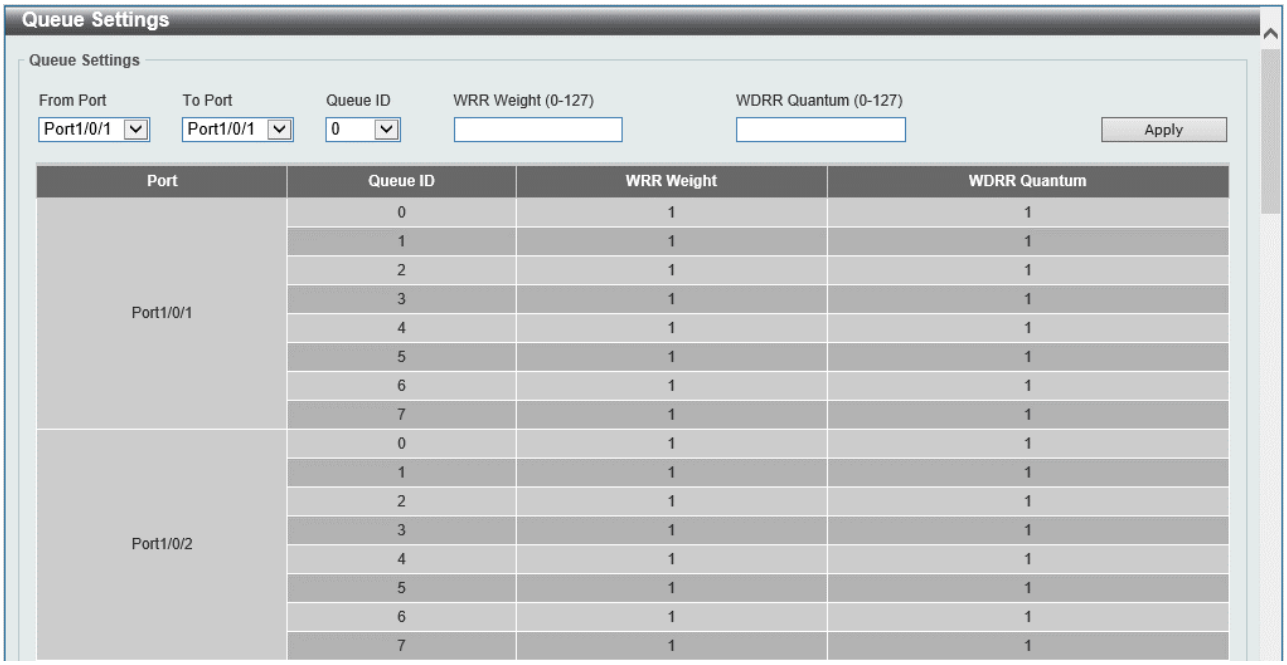
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	スケジューリング方法を設定するポートの範囲を選択します。
Scheduler Method	スケジューリング方法を、以下のいずれかから選択します。 • SP（Strict Priority）：すべてのキューで完全優先制御方式を使用します。優先度が高いキューが空になるまで低いキューでの転送処理は行われません。 • RR（Round-Robin）：すべてのキューでラウンドロビン方式を使用します。キュー同士での優先的な処理は行わず、各キューで 1 つのパケットを順番に処理します。 • WRR（Weighted Round-Robin）：加重ラウンドロビン方式を使用します。各キューに設定した重みの値と、処理したパケット数に対応したカウンターで、パケットの処理順番を決定します。単位時間に処理できる各キューでのパケット数は、設定した重みに比例します。 • WDRR（Weighted Deficit Round-Robin）：加重不足ラウンドロビン方式を使用します。この方式は、各キューに設定したクォンタム値と、処理したパケットのサイズに対応したカウンターで、パケットの処理順番を決定します。 デフォルトでは、WRR が使用されます。

設定を適用するには、Apply ボタンをクリックします。

7.1.3 Queue Settings

Queue Settings 画面では、各キューの WRR の重みと WDRR のクォンタム値を設定します。
本画面を表示するには、QoS > Basic Settings > Queue Settings をクリックします。



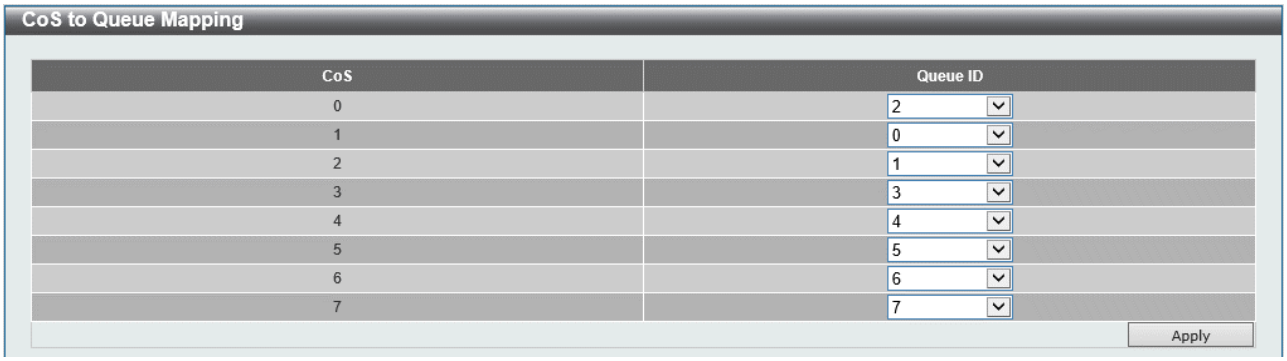
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	キューを設定するポートの範囲を選択します。
Queue ID	キューIDの値として0～7のいずれかを選択します。
WRR Weight	WRRの重み値を0～127の範囲で入力します。重み値が0に設定されたキューは、SPモードで動作します。
WDRR Quantum	WDRRクォンタム値を0～127の範囲で入力します。クォンタム値が0に設定されたキューは、SPモードで動作します。

設定を適用するには、Applyボタンをクリックします。

7.1.4 CoS to Queue Mapping

CoS to Queue Mapping画面では、CoSからハードウェアキューへのマッピングを設定します。QoS機能では、設定したマッピングルールに従ってキューイングが行われます。
本画面を表示するには、QoS > Basic Settings > CoS to Queue Mappingをクリックします。



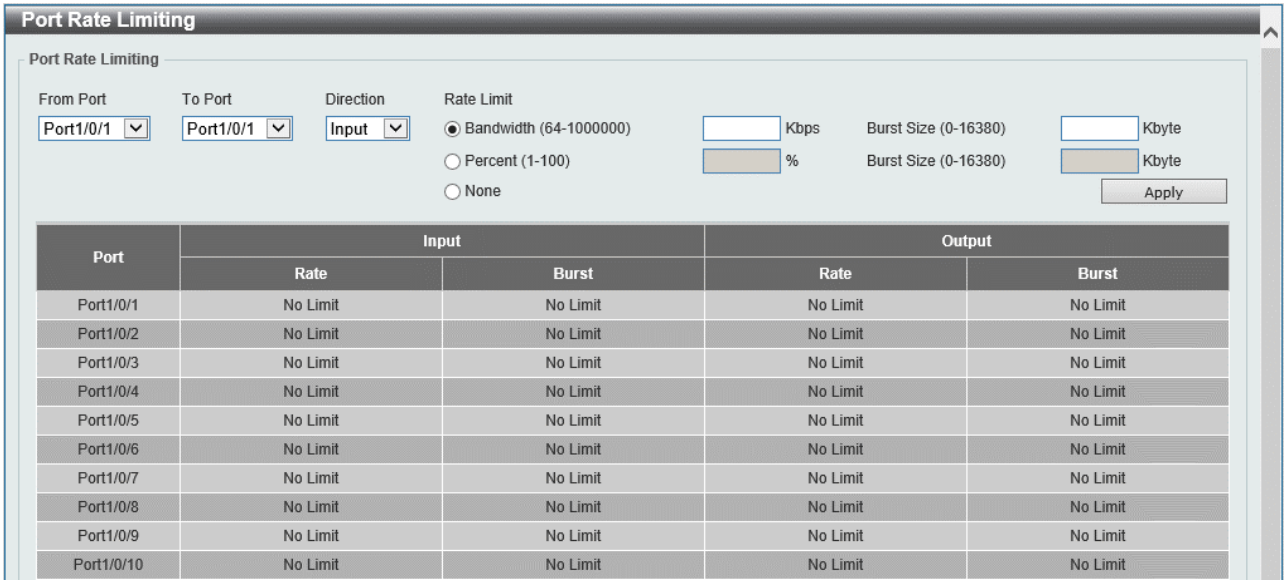
本画面の各項目の説明を以下に示します。

パラメーター	説明
Queue ID	CoSにマップされるキューのIDを0～7から選択します。

設定を適用するには、Applyボタンをクリックします。

7.1.5 Port Rate Limiting

Port Rate Limiting 画面では、ポートでの帯域制限値を設定します。
本画面を表示するには、QoS > Basic Settings > Port Rate Limiting をクリックします。



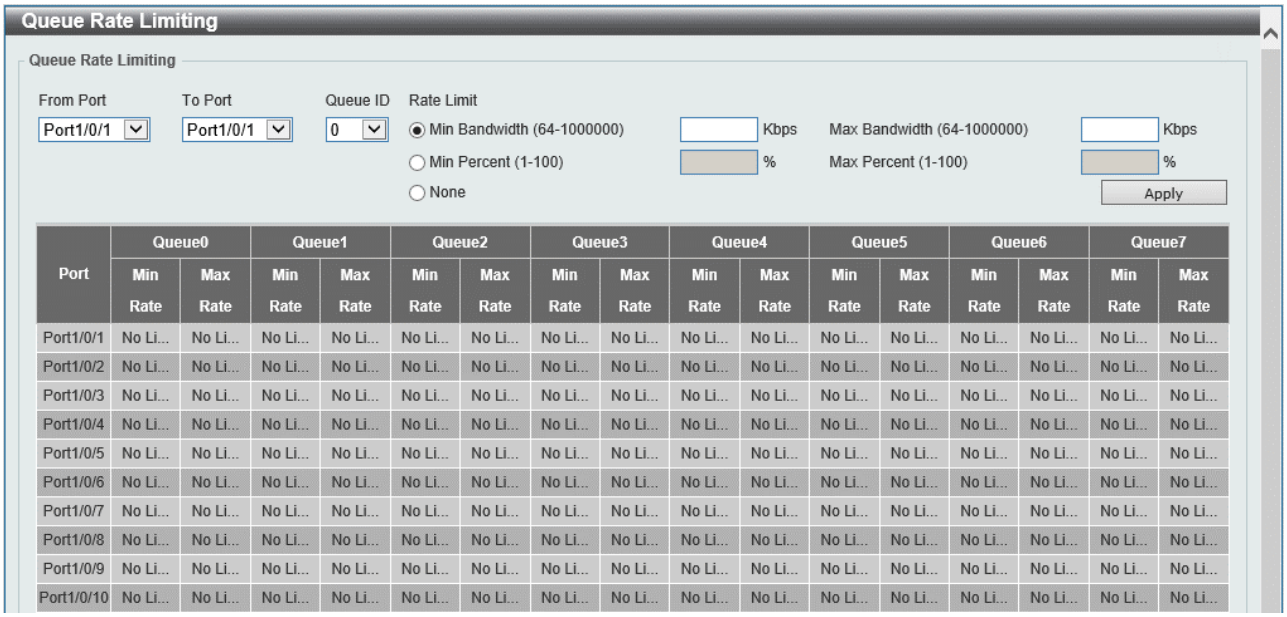
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	帯域制限を設定するポートの範囲を選択します。
Direction	データトラフィックの方向として、以下のどちらかを選択します。 • Input：入力トラフィックに帯域制限を適用します。 • Output：出力トラフィックに帯域制限を適用します。
Rate Limit	レート制限値を以下のいずれかから選択します。 選択したインターフェースの最大速度を超える制限は指定できません。 受信側帯域の制限の場合、受信したトラフィックが制限を超えると、ポーズフレームまたはフロー制御フレームが送信されます。 • Bandwidth：物理ポートの制限帯域幅を 64～1000000（Kbps）の範囲で指定します。 　○ Burst Size：バーストサイズを 0～16380（キロバイト）の範囲で入力します。 • Percent：物理ポートの制限帯域幅を百分率で入力します。入力範囲は 1～100（%）です。 　○ Burst Size：バーストサイズを 0～16380（キロバイト）の範囲で入力します。 • None：選択したポートのレート制限を解除する場合に選択します。デフォルトでは、すべてのポートの入力と出力でこの設定が選択されています。

設定を適用するには、Apply ボタンをクリックします。

7.1.6 Queue Rate Limiting

Queue Rate Limiting 画面では、ハードウェアキュー単位の帯域制限を設定します。
本画面を表示するには、QoS > Basic Settings > Queue Rate Limiting をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	キューの帯域制限を設定するポートの範囲を選択します。
Queue ID	キューID の値として 0～7 のいずれかを選択します。
Rate Limit	キューの帯域制限を以下のいずれかから選択します。 • Min Bandwidth：キューの保証帯域を 64～1000000（Kbps）の範囲で指定します。 　○ Max Bandwidth：キューの制限帯域を 64～1000000（Kbps）の範囲で指定します。 • Min Percent：キューの保証帯域をポートの帯域に対する百分率で指定します。入力範囲は 1～100（%）です。 　○ Max Percent：キューの制限帯域をポートの帯域に対する百分率で指定します。入力範囲は 1～100（%）です。 • None：選択したポートのキューの帯域制限を解除する場合に選択します。デフォルトでは、すべてのポートのすべてのキューでこの設定が選択されています。

設定を適用するには、Apply ボタンをクリックします。

7.2 Advanced Settings

Advanced Settings サブメニューでは、QoS の高度な設定を行います。
QoS の高度な設定は、大別すると DSCP 値をベースにしたトラフィックの分類に関する設定と、ポリシングによる帯域制限に関する設定の 2 種類があります。

Advanced Settings の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
7.2.1	DSCP Mutation Map	DSCP 変換マップの作成
7.2.2	Port Trust State and Mutation Binding	CoS の指標の設定
7.2.3	DSCP CoS Mapping	DSCP 値と CoS のマッピングの設定
7.2.4	CoS Color Mapping	CoS 値ベースのトラフィック初期カラーの設定
7.2.5	DSCP Color Mapping	DSCP 値ベースのトラフィック初期カラーの設定
7.2.6	Class Map	クラスマップの作成
7.2.7	Aggregate Policer	集約ポリサーの設定
7.2.8	Policy Map	ポリシーマップの作成
7.2.9	Policy Binding	ポリシーマップの割り当て

■DSCP 値によるクラシフィケーション
入出力するフレームに含まれる優先制御の情報には、DSCP 値と CoS 値があります。DSCP 値は IP ヘッダー内に含まれる優先制御の情報で、CoS 値は VLAN タグで付与されます。CoS 値は、VLAN タグを使用しないタグなしポートやルーターを経由した場合は情報が消失するため、原則として装置内部またはローカルネットワークの範囲での優先制御の指標とされます。DSCP 値は、通信の途中経路で IP ヘッダーの書き換えが行われない限り、通信全体で一貫性があるため、アプリケーション自体の優先制御の指標とされます。

本装置では、ポート単位で VLAN 情報（CoS 値）と DSCP 値のどちらを CoS の指標としてクラシフィケーションを実施するかを定めることができます。

■ポリシングの基本動作
本装置のポリシングでは、所定のトラフィックの帯域をモニタリングし、帯域の利用状況に応じて指定したアクション実行します。アクションには、フレームの破棄、透過、および優先制御値の書き換えがあります。
観測されたトラフィックは、帯域の利用状況に応じて 3 段階に分類されます。ポリシングの方式によって分類方法は異なりますが、基本的には以下のトラフィックカラーに分類されます。

- グリーントラフィック：利用帯域が制限帯域を下回っている段階
- イエロートラフィック：利用帯域が制限帯域を超過しているが最大利用帯域を超えない段階
- レッドトラフィック：利用帯域が最大利用帯域を超過した段階

トラフィックカラーの分類方法には、1 レート方式と 2 レート方式の 2 種類があります。
1 レート方式では、平均レートを超過したトラフィックをイエローまたはレッドに分類します。イエローとレッドの違いは、許容する最大バーストサイズを超過するかどうかで決定されます。
2 レート方式では、保証帯域(CIR)を下回るトラフィックをグリーンに、CIR を超過して最大帯域(PIR)を超えないトラフィックをイエローに、PIR を超過したトラフィックをレッドに分類します。

また、デフォルトのカラーをカラーモードで指定できます。帯域の利用状況によらず、デフォルトのカラーよりも良いトラフィックカラーに分類されることはありません。カラーアウェアモードでは、トラフィック初期カラーの設定に基づいてデフォルトのカラーを決定します。カラーブラインドモードでは、デフォルトのカラーはグリーンです。

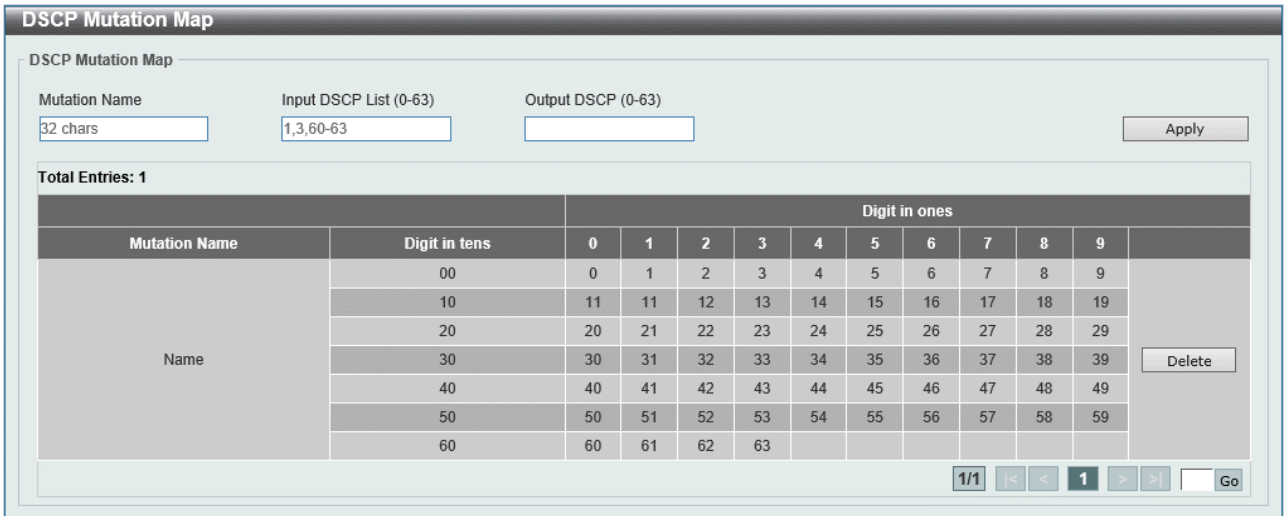
■ポリシングの設定
ポリシングの設定では、最初にクラスマップというフレーム条件を定めたプロファイルを作成します。これは、帯域制限を行うトラフィックの種類を規定します。

次に、ポリシーマップというプロファイルを作成します。これは、クラスマップに合致するフレームのトラフィックをグリーン／イエロー／レッドに分類するための帯域やバーストサイズなどのパラメーターと、各トラフィックカラーでのアクションを規定します。ポリシーマップで定義する内容は、集約ポリサーという共通プロファイルを使用して定義することもできます。

最後に、作成したポリシーマップを物理ポートに割り当てます。本装置では、ポリシングは入力側に対してのみ行われます。

7.2.1 DSCP Mutation Map

DSCP Mutation Map 画面では、DSCP の変換マップを設定します。これは、CoS の指標が DSCP 値の場合に、DSCP 値のリマーキングを行う際に使用するプロファイルです。
本画面を表示するには、**QoS > Advanced Settings > DSCP Mutation Map** をクリックします。



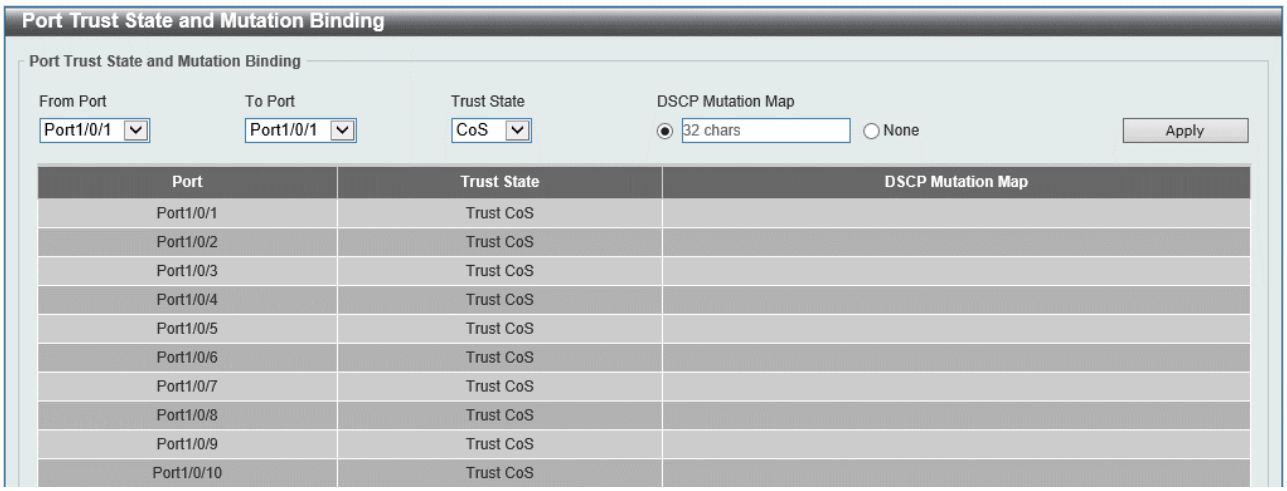
本画面の各項目の説明を以下に示します。

パラメーター	説明
Mutation Name	DSCP 変換マップ名を 32 文字以内で入力します。
Input DSCP List	入力 DSCP 値を 0～63 の範囲で入力します。
Output DSCP	出力 DSCP 値を 0～63 の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。
DSCP 変換マップを削除するには、**Delete** ボタンをクリックします。

7.2.2 Port Trust State and Mutation Binding

Port Trust State and Mutation Binding 画面では、クラシフィケーションに使用する CoS の指標（CoS 値または DSCP 値）をポート単位で指定します。また、使用する DSCP 変換マップを登録します。
本画面を表示するには、**QoS > Advanced Settings > Port Trust State and Mutation Binding** をクリックします。



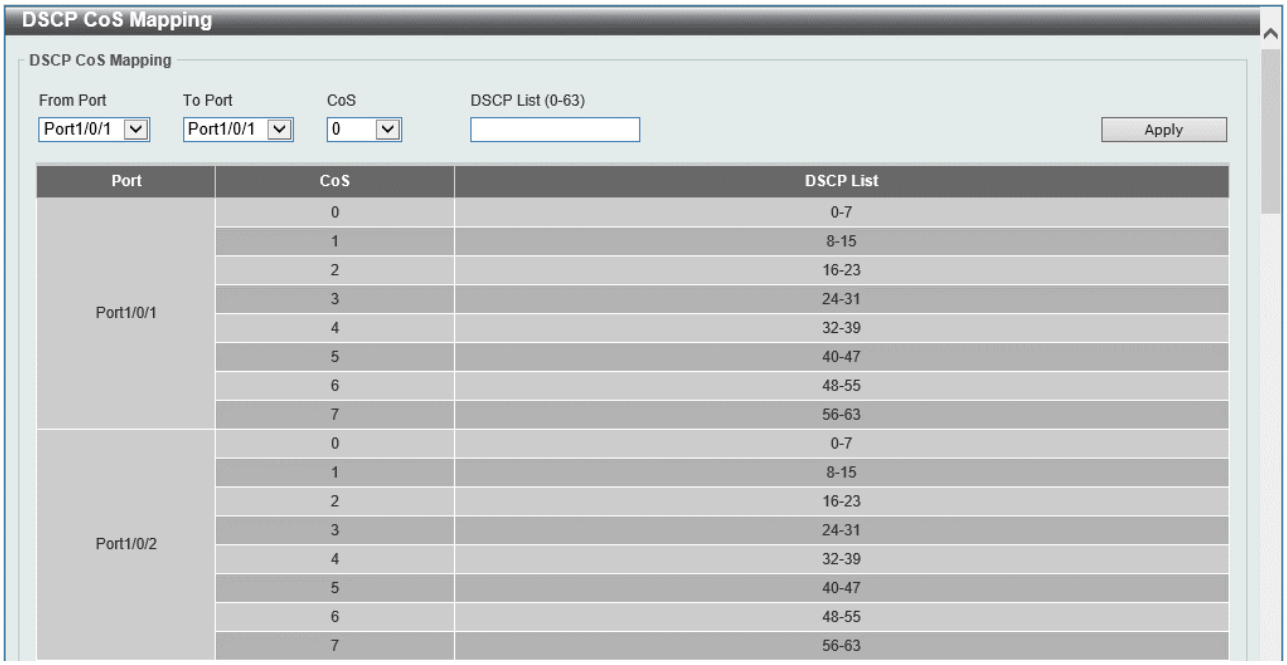
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	設定するポートの範囲を選択します。
Trust State	ポートで使用する CoS の指標（**CoS** / **DSCP**）を選択します。 **CoS** を選択した場合、VLAN タグの CoS 値を参照します。タグなしフレームでは、ポートの CoS の設定を参照します。**DSCP** の場合は DSCP 値を参照し、DSCP 値と CoS のマッピングに従って CoS を決定します。IP ヘッダーが含まれない場合、ポートの CoS の設定を参照します。
DSCP Mutation Map	DSCP 変換マップをポートに設定する場合にラジオボタンをクリックし、DSCP 変換マップ名を 32 文字以内で入力します。DSCP 変換マップに基づく DSCP 値の変換は、CoS の決定後に行われます。 DSCP 変換マップをポートに割り当てない場合は、**None** を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

7.2.3 DSCP CoS Mapping

DSCP CoS Mapping 画面では、DSCP 値と CoS のマッピングを設定します。これは、CoS の指標を DSCP 値にした場合に適用されるクラシフィケーションのルールです。
本画面を表示するには、**QoS > Advanced Settings > DSCP CoS Mapping** をクリックします。



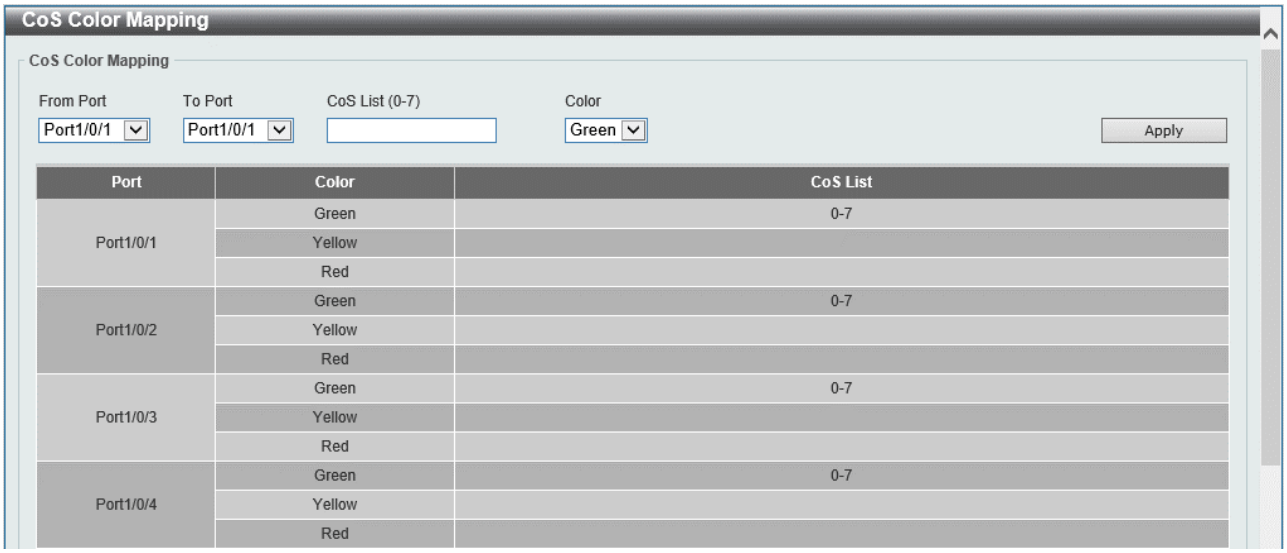
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	設定するポートの範囲を選択します。
CoS	DSCP 値のリストにマッピングする CoS を 0～7 から選択します。
DSCP List	CoS にマップする DSCP 値のリストを 0～63 の範囲で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

7.2.4 CoS Color Mapping

CoS Color Mapping 画面では、CoS カラーマップを設定します。CoS カラーマップは、CoS の指標が CoS 値の場合に、カラーアウェアモードのポリシングで適用されるトラフィック初期カラーを定めるプロファイルです。
本画面を表示するには、**QoS** > **Advanced Settings** > **CoS Color Mapping** をクリックします。



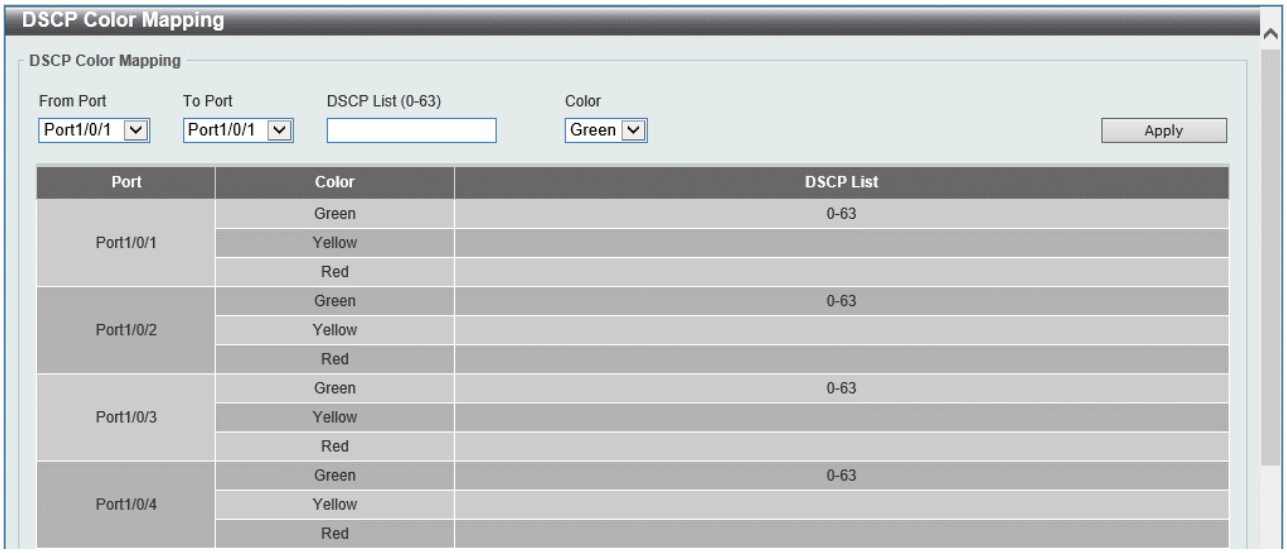
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	設定するポートの範囲を選択します。
CoS List	設定する CoS 値を 0～7 の範囲で入力します。
Color	CoS 値にマッピングされるトラフィック初期カラー（Green / Yellow / Red）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

7.2.5 DSCP Color Mapping

DSCP Color Mapping 画面では、DSCP カラーマップを設定します。DSCP カラーマップは、CoS の指標が DSCP 値の場合に、カラーモードアウェアのポリシングで適用されるトラフィック初期カラーを定めるプロファイルです。
本画面を表示するには、**QoS > Advanced Settings > DSCP Color Mapping** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	設定するポートの範囲を選択します。
DSCP List	設定する DSCP 値のリストを 0～63 の範囲で入力します。
Color	DSCP 値にマッピングされるトラフィック初期カラー（Green / Yellow / Red）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

7.2.6 Class Map

Class Map 画面では、クラスマップを設定します。クラスマップは、ポリシングで帯域制御を行うトラフィックを識別するプロファイルです。クラスマップは、該当するフレームの条件を示す複数のルールと、ルールに対する照合基準で構成されます。

ルールの照合基準は Match Any または Match All で指定します。Match All の場合、登録したすべてのルールに合致するフレームをポリシングの対象として識別します。Match Any の場合、登録したいずれかのルールに合致するフレームをポリシングの対象として識別します。

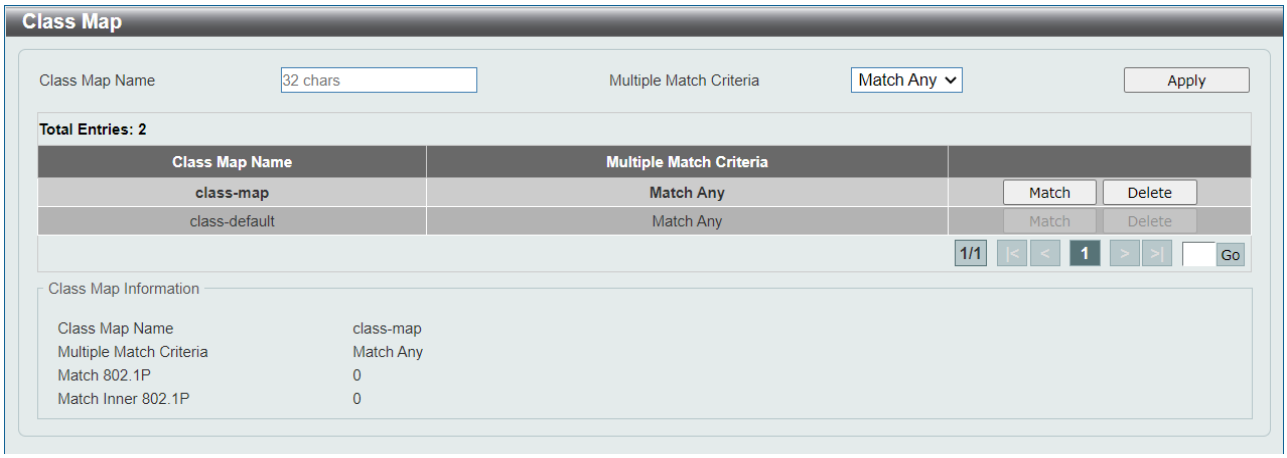
本画面を表示するには、QoS > Advanced Settings > Class Map をクリックします。

本画面の各項目の説明を以下に示します。

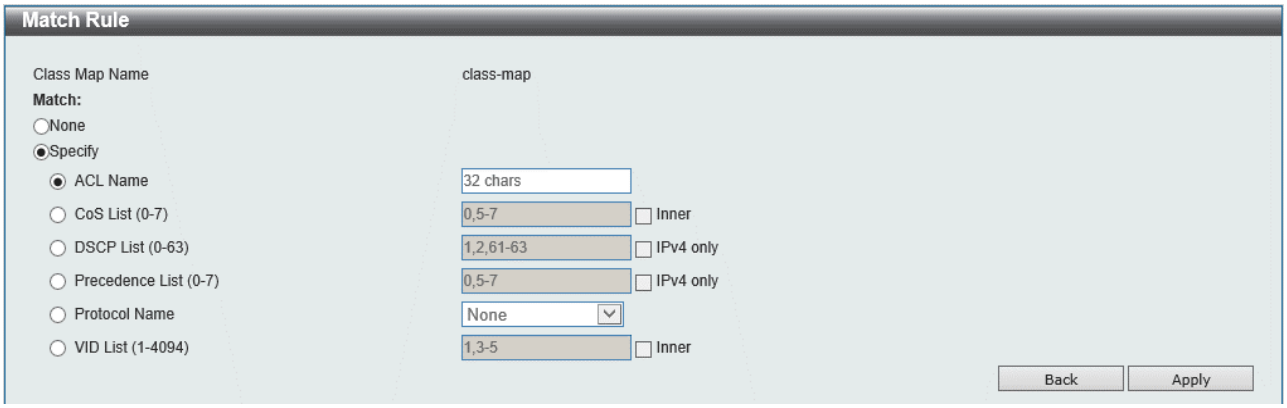
パラメーター	説明
Class Map Name	クラスマップ名を 32 文字以内で入力します。
Multiple Match Criteria	ルールの照合基準（Match All / Match Any）を選択します。

クラスマップを登録するには、Apply ボタンをクリックします。
クラスマップにルールを追加・削除するには、Match ボタンをクリックします。
クラスマップ自体を削除するには、Delete ボタンをクリックします。

クラスマップのテーブル上でいずれかのクラスマップの列をクリックすると、クラスマップ上で登録したすべてのルールが表示されます。



Match ボタンをクリックすると、以下に示すルールの追加・削除画面が表示されます。



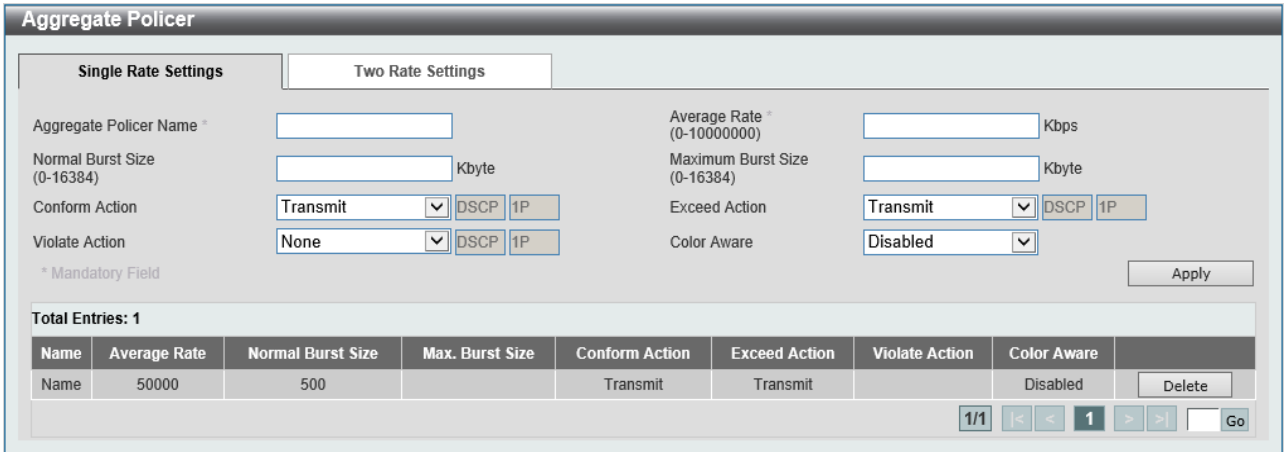
Match Rule 画面の各項目の説明を以下に示します。

パラメーター	説明
None	指定したルールを削除する場合に選択します。
Specify	指定したルールを登録する場合に選択します。
ACL Name	フレームを ACL で照合する場合にラジオボタンをクリックし、照合する ACL を 32 文字以内で入力します。
CoS List	フレームを CoS 値で照合する場合にラジオボタンをクリックし、CoS 値のリストを 0～7 の範囲で入力します。Match All の場合は、1 個の CoS 値のみ指定します。 QinQ パケットの C-tag 上の CoS 値を照合する場合、Inner をチェックします。
DSCP List	フレームを DSCP 値で照合する場合にラジオボタンをクリックし、DSCP 値のリストを 0～63 の範囲で入力します。Match All の場合は、1 個の DSCP 値のみ指定します。 IPv4 パケットのみを照合する場合、IPv4 only をチェックします。
Precedence List	フレームを IP ヘッダーの ToS 値と照合する場合にラジオボタンをクリックし、ToS 値のリストを 0～7 の範囲で入力します。Match All の場合は、1 個の DSCP 値のみ指定します。 IPv4 パケットのみと照合するには、IPv4 only をチェックします。
Protocol Name	フレームをプロトコルで照合する場合にラジオボタンをクリックし、プロトコル（ARP / BGP / DHCP / DNS / EGP / FTP / IPv4 / IPv6 / NetBIOS / NFS / NTP / OSPF / PPPOE / RIP / RTSP / SSH / Telnet / TFTP）を選択します。
VID List	フレームを VLAN で照合する場合にラジオボタンをクリックし、VLAN ID のリストを 1～4094 の範囲で入力します。 QinQ パケットの C-tag 上の CoS 値と照合する場合は、Inner をチェックします。

設定を適用するには、Apply ボタンをクリックします。
前の画面に戻るには、Back ボタンをクリックします。

7.2.7 Aggregate Policer

Aggregate Policer 画面では、集約ポリサーを設定します。集約ポリサーは、ポリシーマップに割り当てる共通プロファイルです。
本画面を表示するには、QoS > Advanced Settings > Aggregate Policer をクリックします。

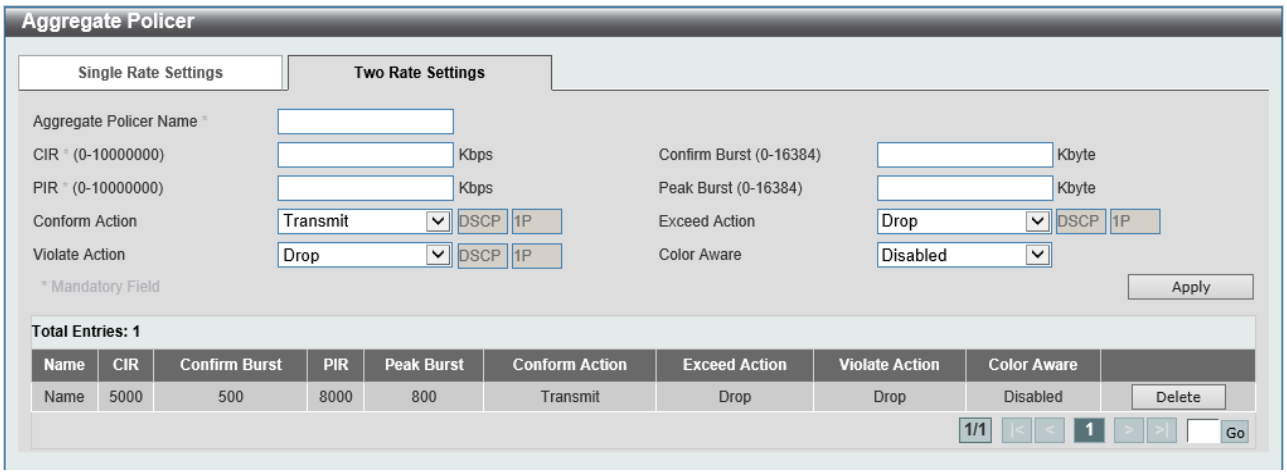


Single Rate Settings タブでは 1 レート集約ポリサーを設定します。各項目の説明を以下に示します。

パラメーター	説明
Aggregate Policer Name	1 レート集約ポリサー名を入力します。
Average Rate	平均レートを 0～10000000（Kbps）の範囲で入力します。
Normal Burst Size	通常バーストサイズを 0～16384（キロバイト）の範囲で入力します。
Maximum Burst Size	最大バーストサイズを 0～16384（キロバイト）の範囲で入力します。
Conform Action	グリーントラフィックのフレームで実行するアクションを指定します。 • Drop：フレームを破棄します。 • Set-DSCP-Transmit：指定した DSCP 値に書き換えます。 • Set-1P-Transmit：指定した CoS 値に書き換えます。 • Transmit：フレームをそのまま処理します。 • Set-DSCP-1P： 指定した DSCP 値と CoS 値に書き換えます。
Exceed Action	イエロートラフィックのフレームで実行するアクションを指定します。 指定可能なアクションは Conform Action と同じです。
Violate Action	レッドトラフィックのフレームで実行するアクションを指定します。 None 以外の指定可能なアクションは Conform Action と同じです。 • None：このアクションを指定した場合、レッドトラフィックとして分類されることはなく、イエロートラフィックとして処理します。
Color Aware	カラーモードを以下のどちらかから選択します。 • Enabled：カラーアウェアモードに指定します。 • Disabled：カラーブラインドモードに指定します。

設定を適用するには、Apply ボタンをクリックします。
集約ポリサーを削除するには、Delete ボタンをクリックします。

Two Rate Settings タブをクリックすると、以下に示す画面が表示されます。



Two Rate Settings タブの各項目の説明を以下に示します。

パラメーター	説明
Aggregate Policer Name	集約ポリサー名を入力します。
CIR	CIR の値を 0～10000000（Kbps）の範囲で入力します。
Confirm Burst	標準バーストサイズを 0～16384（キロバイト）の範囲で入力します。
PIR	PIR の値を 0～10000000（Kbps）の範囲で入力します。
Peak Burst	最大バーストサイズを 0～16384（キロバイト）の範囲で入力します。
Conform Action	グリーントラフィックのフレームで実行するアクションを指定します。 • Drop：フレームを破棄します。 • Set-DSCP-Transmit：指定した DSCP 値に書き換えます。 • Set-1P-Transmit：指定した CoS 値に書き換えます。 • Transmit：フレームをそのまま処理します。 • Set-DSCP-1P： 指定した DSCP 値および CoS 値に書き換えます。
Exceed Action	イエロートラフィックのフレームで実行するアクションを指定します。 指定可能なアクションは Conform Action と同じです。
Violate Action	レッドトラフィックのフレームで実行するアクションを指定します。 None 以外の指定可能なアクションは Conform Action と同じです。 • None：このアクションを指定した場合、レッドトラフィックとして分類されることはなく、イエロートラフィックとして処理します。
Color Aware	カラーモードを以下のどちらかから選択します。 • Enabled：カラーアウェアモードに指定します。 • Disabled：カラーブラインドモードに指定します。

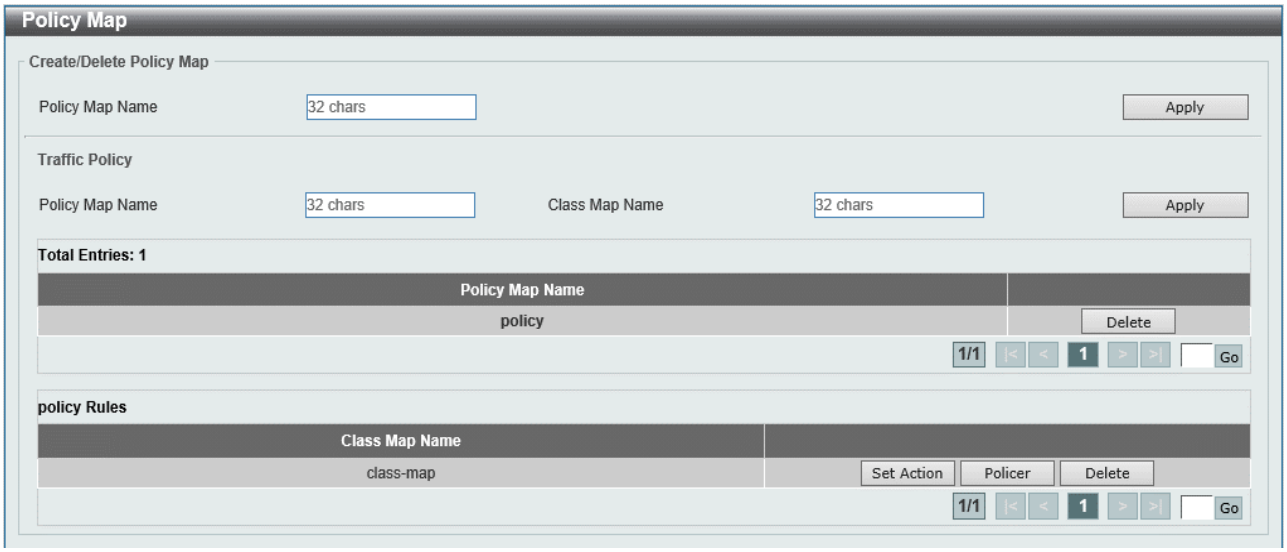
設定を適用するには、Apply ボタンをクリックします。
集約ポリサーを削除するには、Delete ボタンをクリックします。

7.2.8 Policy Map

Policy Map 画面では、ポリシーマップを設定します。ポリシーマップは、ポリシングで特定のトラフィックに対するトラフィックカラーの分類方法やアクションを指定するプロファイルです。

ポリシーマップでは、トラフィックの識別に使用するクラスマップを 1 個以上登録します。各クラスマップにマッチするトラフィックに対して、対応するアクションをそれぞれ指定できます。
ポリシーマップで適用するアクションには、トラフィックカラーによって決定するポリシングアクションの他に、CoS 値や DSCP 値などの書き換えといったマーキングに関するアクションや、CoS によらず直接ハードウェアキューを指定するキューイングに関するアクションを指定できます。

本画面を表示するには、QoS > Advanced Settings > Policy Map をクリックします。



Create/Delete Policy Map の各項目の説明を以下に示します。

パラメーター	説明
Policy Map Name	作成または削除するポリシーマップ名を 32 文字以内で入力します。

設定を適用するには、Apply ボタンをクリックします。

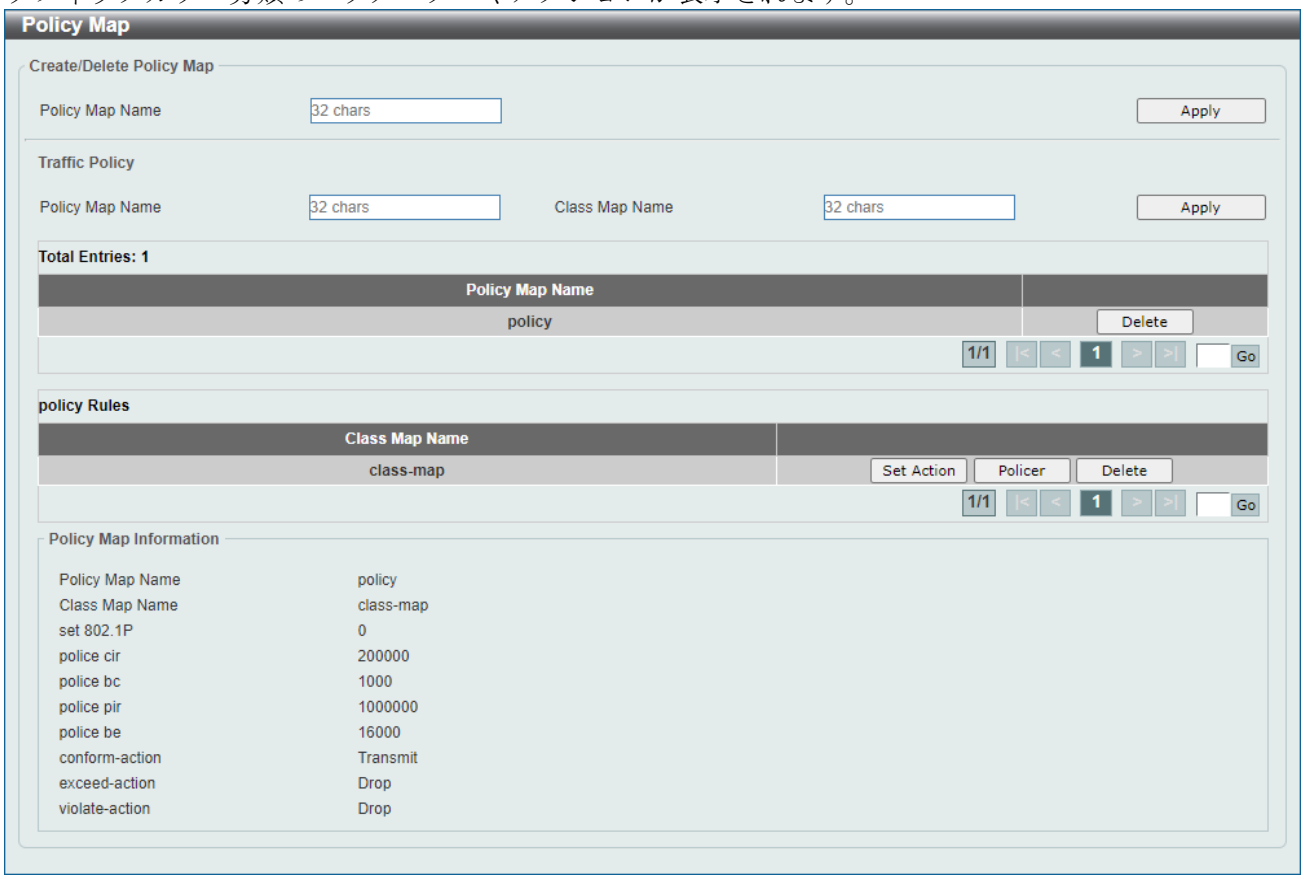
Traffic Policy の各項目の説明を以下に示します。

パラメーター	説明
Policy Map Name	ポリシーマップ名を 32 文字以内で入力します。
Class Map Name	クラスマップ名を 32 文字以内で入力します。

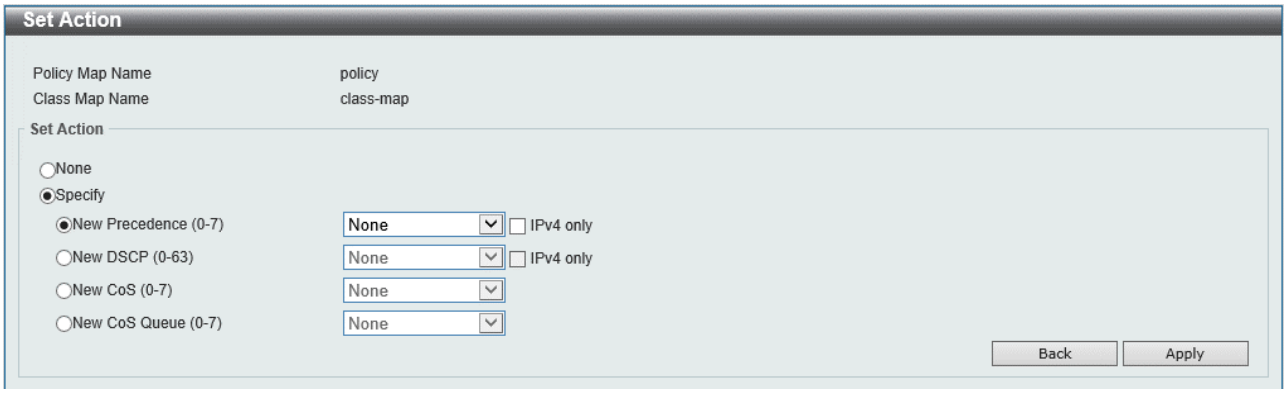
設定を適用するには、Apply ボタンをクリックします。
ポリシーマップを削除するには、Delete ボタンをクリックします。

ポリシーマップのテーブル上でいずれかのポリシーマップの行をクリックすると、ポリシーマップ上で登録したすべてのクラスマップが表示されます。
トラフィックに対する追加のアクションを設定するには、Set Action ボタンをクリックします。
ポリシングの設定を登録するには、Policer ボタンをクリックします。

表示されたクラスマップのテーブル上でいずれかのクラスマップの行をクリックすると、登録したトラフィックカラー分類のパラメーターやアクションが表示されます。



Set Action ボタンをクリックすると、以下に示す画面が表示されます。

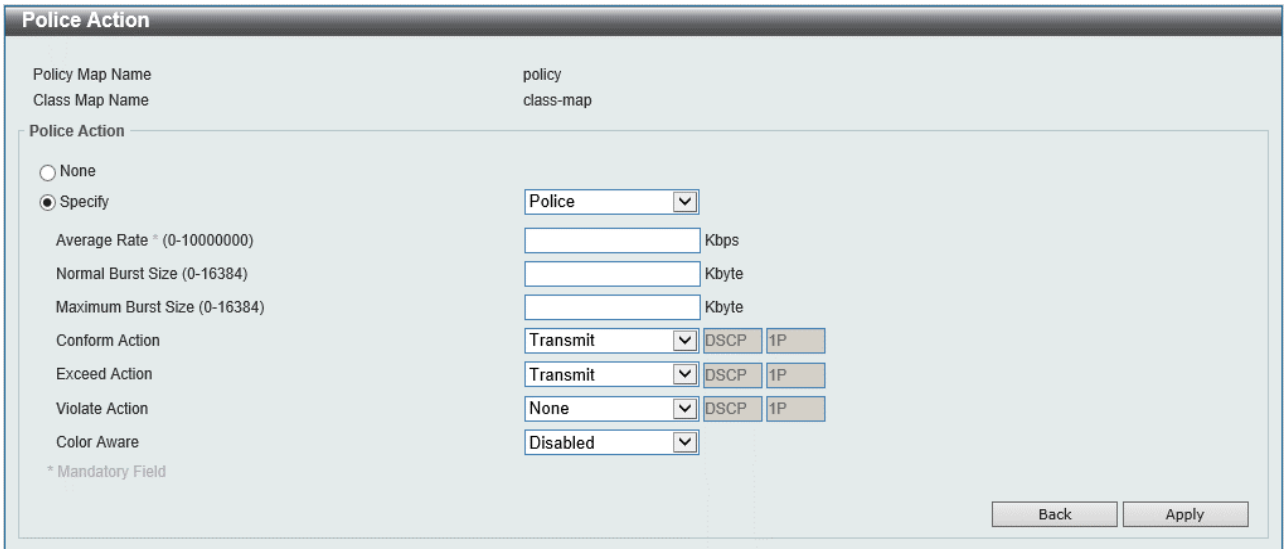


Set Action 画面の各項目の説明を以下に示します。

パラメーター	説明
None	アクションを削除する場合に選択します。
Specify	アクションを登録する場合に選択します。
New Precedence	ToS 値の書き換えを行います。ToS 値を 0～7 から選択します。 IPv4 パケットのみを対象とする場合は、IPv4 only をチェックします。
New DSCP	DSCP 値の書き換えを行います。DSCP 値を 0～63 から選択します。 IPv4 パケットのみを対象とする場合は、IPv4 only をチェックします。
New CoS	CoS 値の書き換えを行います。CoS 値を 0～7 から選択します。 この設定は、装置内部の CoS の決定とキューイングの動作に影響します。
New Cos Queue	転送するハードウェアキューを直接指定します。キュー値を 0～7 から選択します。この設定はキューイングの動作に影響しますが、リマーキングは行いません。

前の画面に戻るには、Back ボタンをクリックします。
設定を適用するには、Apply ボタンをクリックします。

Policer ボタンをクリックすると、以下に示す画面が表示されます。



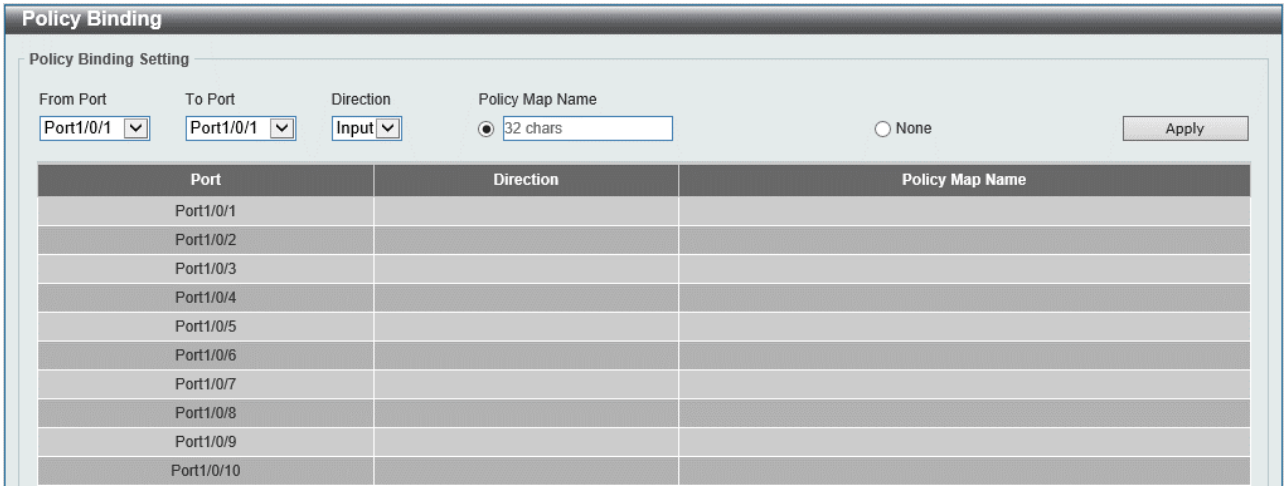
Police Action 画面の各項目の説明を以下に示します。

パラメーター	説明
None	ポリサーをクリアする場合に選択します。
Specify	ポリサーを適用する場合に選択し、ポリサーの設定方法をプルダウンメニューから選択します。Police の場合、1 レート方式のトラフィック分類パラメーターを個別に指定します。Police CIR の場合、2 レート方式のトラフィック分類パラメーターを個別に指定します。Police Aggregate の場合、集約ポリサーを指定します。
Average Rate	平均レートを 0～10000000（Kbps）の範囲で入力します。
Normal Burst Size	通常バーストサイズを 0～16384（キロバイト）の範囲で入力します。
Maximum Burst Size	最大バーストサイズを 0～16384（キロバイト）の範囲で入力します。
CIR	CIR の値を 0～10000000（Kbps）の範囲で入力します。
Confirm Burst	標準バーストサイズを 0～16384（キロバイト）の範囲で入力します。
PIR	PIR の値を 0～10000000（Kbps）の範囲で入力します。
Peak Burst	最大バーストサイズを 0～16384（キロバイト）の範囲で入力します。
Aggregate Policer Name	集約ポリサーを入力します。
Conform Action	グリーントラフィックのフレームで実行するアクションを指定します。 • Drop：フレームを破棄します。 • Set-DSCP-Transmit：指定した DSCP 値に書き換えます。 • Set-1P-Transmit：指定した CoS 値に書き換えます。 • Transmit：フレームをそのまま処理します。 • Set-DSCP-1P： 指定した DSCP 値と CoS 値に書き換えます。
Exceed Action	イエロートラフィックのフレームで実行するアクションを指定します。 指定可能なアクションは Conform Action と同じです。
Violate Action	レッドトラフィックのフレームで実行するアクションを指定します。 None 以外の指定可能なアクションは Conform Action と同じです。 • None：このアクションを指定した場合、レッドトラフィックとして分類されることはなく、イエロートラフィックとして処理します。
Color Aware	カラーモードを以下のどちらかから選択します。 • Enabled：カラーアウェアモードに指定します。 • Disabled：カラーブラインドモードに指定します。

前の画面に戻るには、Back ボタンをクリックします。
設定を適用するには、Apply ボタンをクリックします。

7.2.9 Policy Binding

Policy Binding 画面では、物理ポートにポリシーマップを割り当てます。
本画面を表示するには、QoS > Advanced Settings > Policy Binding をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートの範囲を選択します。
Direction	方向オプションを選択します。Input のみ選択できます。
Policy Map Name	ポリシーマップ名を 32 文字以内で入力します。 ポリシーマップの割り当てを解除するには None を選択します。

設定を適用するには、Apply ボタンをクリックします。

8 ACL

ACL メニューでは、アクセスコントロールリスト（ACL）の登録を行います。
ACL は、フレームの情報から物理ポートやその他のモジュールへのアクセスを制御する機能です。検査するフレームの種類とフレームの検査範囲を定めた ACL プロファイルと、ACL プロファイル上に登録した ACL ルールによってアクセス制御ポリシーを構成し、ACL プロファイルをモジュールに割り当てることでステートレスのアクセス制御を提供します。

ACL の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
8.1	ACL Configuration Wizard	ACL 構成ウィザードを開始
8.2	ACL Access List	ACL プロファイル、ACL ルールの作成と編集
8.3	ACL Interface Access Group	ACL の物理ポートへの割り当て
8.4	ACL VLAN Access Map	VLAN アクセスマップの作成
8.5	ACL VLAN Filter	VLAN フィルターの設定

■ACL プロファイル
モジュールで必要となる ACL のアクセス制御は、ネットワークポリシーによって異なります。ステートレスのアクセス制御では、フレームの送信元と宛先 IP アドレスに基づいてアクセスの許可または拒否を行うのが一般的ですが、通信プロトコルや MAC アドレスなどの情報を用いることもあります。ACL プロファイルでは、そのようなネットワークポリシーに対して、検査するフレームの種類や、フレームの検査範囲を定める ACL 種別を指定します。
本装置で指定できる ACL の種別は以下の通りです。

- 標準/拡張 IP ACL
- 標準/拡張 IPv6 ACL
- 拡張 MAC ACL
- 拡張エキスパート ACL

■ACL 種別ごとの検査範囲と適用可能なモジュール
接頭辞が「拡張」の ACL では、「標準」と比べて検査範囲が広く、細かいフレームの合致条件を指定できますが、適用できるモジュールが限定されます。接頭辞が「標準」の ACL では、送信元や宛先 IP アドレスといった要点に絞った検査を行います。

「IP ACL」、「IPv6 ACL」、「MAC ACL」は、フレームの検査対象を示します。「IP ACL」では IPv4 パケットを、「IPv6 ACL」では IPv6 パケットを、「MAC ACL」では原則として非 IP パケットを検査対象とします。
「拡張エキスパート ACL」は、「拡張 IP ACL」と「拡張 MAC ACL」のハイブリッドであり、IPv4 パケットを検査対象として、送信元、宛先 MAC アドレス、IP アドレスなど、広い範囲を検査できます。
ACL 種別や種類(標準/拡張)によって適用可能なモジュールが異なります。

■ACL ルール
ACL ルールは、フレームの合致する条件と、合致した場合のアクションを定めたものです。合致条件は、ACL 種別に基づいて定めることができます。たとえば、標準 IP ACL の場合、特定の送信元や宛先 IP アドレスを合致条件に指定できますが、特定の MAC アドレスは合致条件に指定できません。

ACL ルールで指定するアクションは、物理ポート以外のモジュールに適用する ACL プロファイル上に登録するルールの場合は許可（**permit**）のみを使用します。これらのモジュールでは、ACL のポリシーは合致条件のみ使用され、合致した場合のアクションは各モジュールで制御します。たとえば、SNMP エージェント機能に ACL を適用する場合、ACL ルールの条件に合致する SNMP マネージャーのアクセスを許可します。
物理ポートに適用する ACL プロファイルでは、許可（**permit**）と拒否（**deny**）のルールの組み合わせでポリシーを構成し、物理ポートでの合致条件とアクションは ACL ルールに従います。

■ACL による VLAN フィルター
VLAN で ACL によるアクセス制御を行う場合、複数の ACL プロファイルを組み込んだ VLAN アクセスマップを作成し、VLAN に適用します。VLAN アクセスマップは、マッチ条件とアクションを定めた複数のサブマップでポリシーを定義され、マッチ条件で ACL プロファイルを適用します。ここで ACL のポリシーは合致条件にのみ使用され、合致した場合のアクションはサブマップで規定した動作に従います。

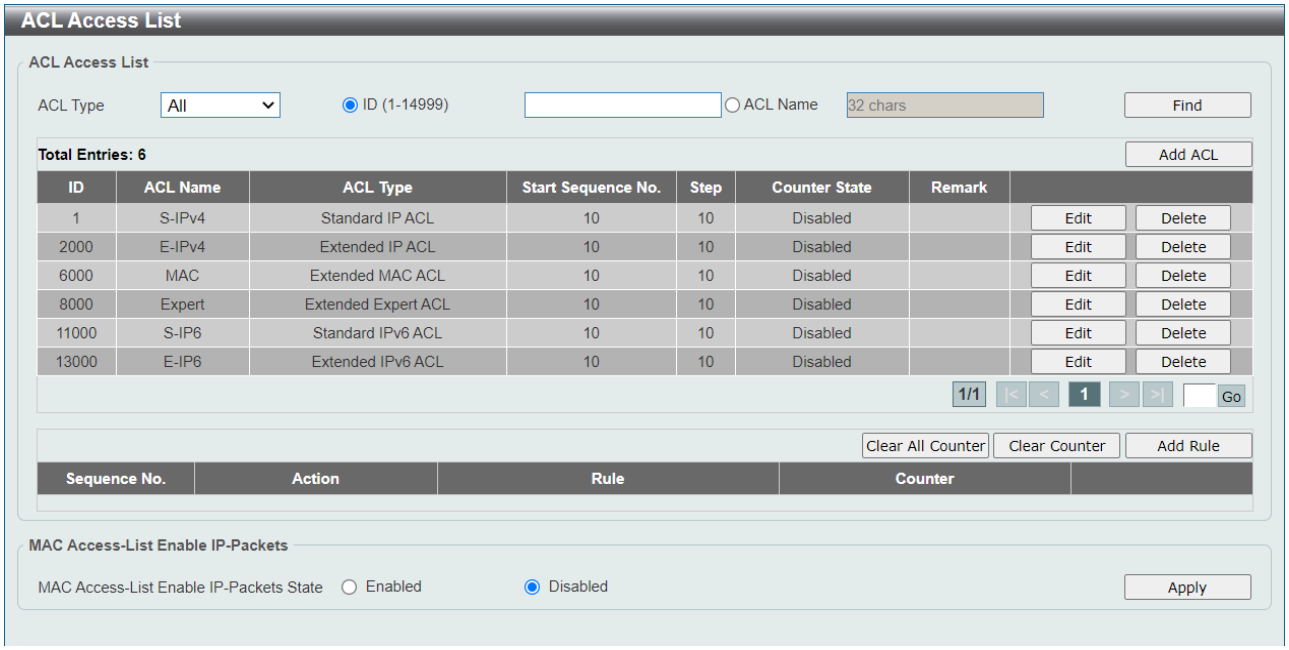
■適用 ACL プロファイル数
単一の物理ポートに対して適用可能な ACL プロファイル数は、ACL 種別ごと（接頭辞は区別しません）に 1 個です。たとえば、「標準 IP ACL」と「拡張 IPv6 ACL」のプロファイルをそれぞれ 1 個登録することはできますが、「標準 IP ACL」を 2 個登録することや、「標準 IP ACL」と「拡張 IP ACL」を同時に登録することはできません。

8.1 ACL Configuration Wizard

ACL Configuration Wizard 画面では、対話的な操作により ACL プロファイルの新規作成や ACL ルールの追加を行うことができる、ACL 構成ウィザードを使用することができます。ACL 構成ウィザードを使用すると、プロファイルやルールの構成を意識することなく、所定の ACL ルールが登録された ACL プロファイルの作成や物理インターフェースへの割り当てなどを行うことができます。

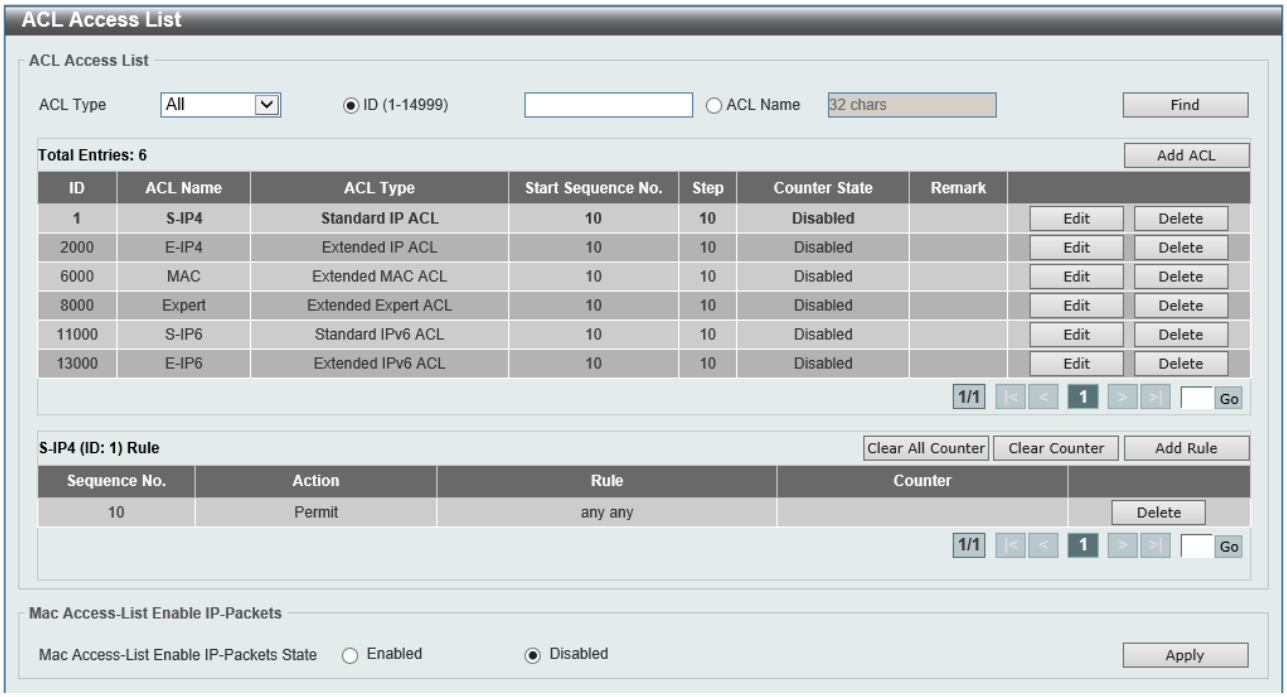
8.2 ACL Access List

ACL Access List 画面では、ACL プロファイルと ACL ルールの登録、編集を行うことができます。
本画面を表示するには、**ACL > ACL Access List** をクリックします。



本画面では、2 個のテーブルが表示されます。上のテーブルには、登録済みの ACL プロファイルが表示されます。下のテーブルには、ACL プロファイルに登録されている ACL ルールが表示されます。本画面に移行した時点では ACL ルールのテーブルには何も表示されておらず、ACL プロファイルテーブルでいずれかの ACL プロファイルの行をクリックすると、該当する ACL ルールが表示されます。

以下は、ACL プロファイルのテーブル上で一番上の行をクリックした例です。



ACL Access List の各項目の説明を以下に示します。

パラメーター	説明
ACL Type	検索する ACL プロファイルの ACL 種別（**All** / **IP ACL** / **IPv6 ACL** / **MAC ACL** / **Expert ACL**）を選択します。
ID	ACL プロファイルを ACL ID で検索する場合に選択します。また、右のボックスに ACL ID を 1～14999 の範囲で入力します。
ACL Name	ACL プロファイルを ACL 名で検索する場合に選択します。また、右のボックスに ACL 名を 32 文字以内で入力します。

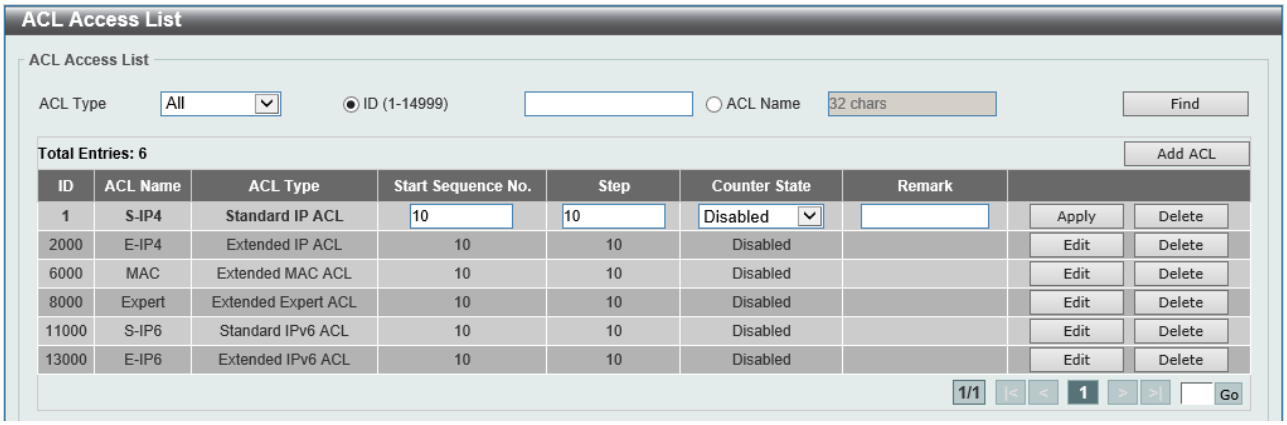
入力した情報で ACL プロファイルを検索するには、**Find** ボタンをクリックします。
ACL プロファイルを作成するには、**Add ACL** ボタンをクリックします。
ACL プロファイルの設定を編集するには、ACL プロファイルテーブルの **Edit** ボタンをクリックします。
ACL プロファイルを削除するには、ACL プロファイルテーブルの **Delete** ボタンをクリックします。
ACL ルールのすべてのカウンターをクリアするには、**Clear All Counter** ボタンをクリックします。
表示されている ACL ルールのカウンターをクリアするには、**Clear Counter** ボタンをクリックします。
選択した ACL プロファイルに ACL ルールを登録するには、**Add Rule** ボタンをクリックします。
ACL ルールを削除するには、ACL ルールテーブルの **Delete** ボタンをクリックします。

Mac Access-List Enable IP-Packets の各項目の説明を以下に示します。

パラメーター	説明
Mac Access-List Enable IP-Packets State	拡張 MAC ACL の検査対象を IPv4 パケットおよび IPv6 パケットまで広げる機能の状態を選択します。 本設定が無効（**Disabled**）の場合、拡張 MAC ACL で検査対象となるのは非 IP パケットのみです。有効（**Enabled**）の場合、IPv4 パケットや IPv6 パケットも検査対象となります。

設定を適用するには、**Apply** ボタンをクリックします。

ACL プロファイルテーブルにある **Edit** ボタンをクリックすると、該当する行の ACL プロファイルのパラメーターを編集できます。

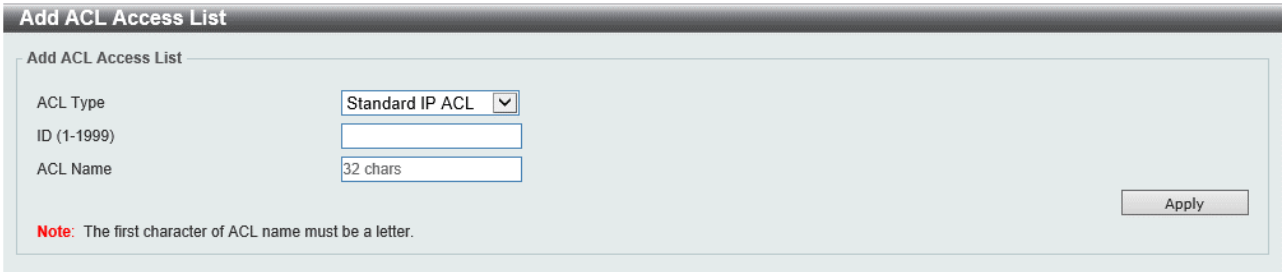


Edit ボタンをクリックした後の各項目の説明を以下に示します。

パラメーター	説明
Start Sequence No.	ACL ルール登録時にシーケンス番号を自動採番する場合の開始シーケンス番号を入力します。
Step	ACL ルールのシーケンス番号を自動採番する場合の増分値を 1～32 の範囲で入力します（デフォルト：10）。 たとえば、開始シーケンス番号が 20 で増分値が 5 の場合、後続のシーケンス番号は 25、30、35、40 となります。
Counter State	ACL のカウンターの状態（Enabled / Disabled）を選択します。
Remark	ACL プロファイルの説明を入力します。

設定を適用するには、Apply ボタンをクリックします。

Add ACL ボタンをクリックすると、以下に示す ACL プロファイル作成画面が表示されます。



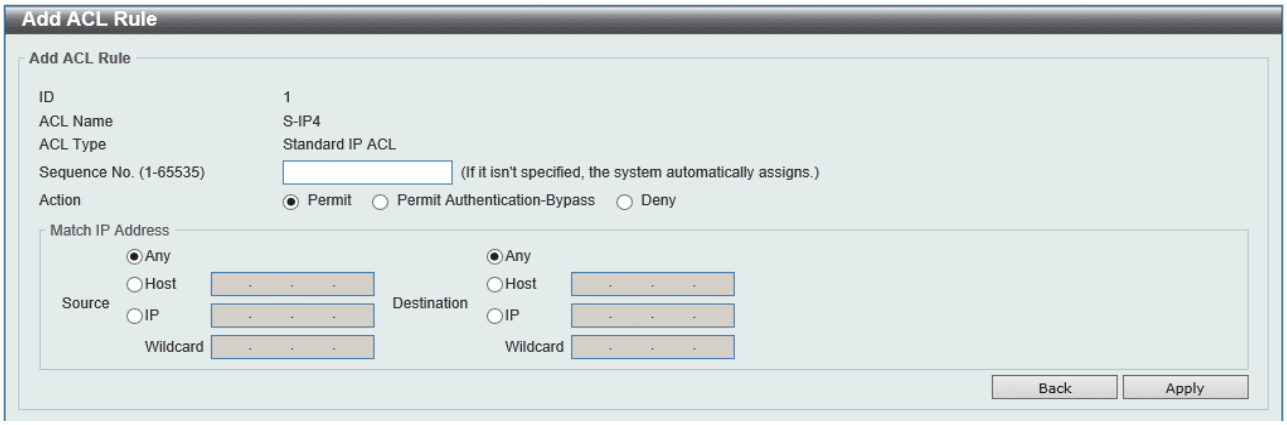
Add ACL Access List の各項目の説明を以下に示します。

パラメーター	説明
ACL Type	ACL の種別（Standard IP ACL / Extended IP ACL / Standard IPv6 ACL / Extended IPv6 ACL / Extended MAC ACL / Extended Expert ACL）を選択します。
ID	ACL の ID を入力します。 • Standard IP ACL の場合、1～1999 の範囲で入力します。 • Extended IP ACL の場合、2000～3999 の範囲で入力します。 • Standard IPv6 ACL の場合、11000～12999 の範囲で入力します。 • Extended IPv6 ACL の場合、13000～14999 の範囲で入力します。 • Extended MAC ACL の場合、6000～7999 の範囲で入力します。 • Extended Expert ACL の場合、8000～9999 の範囲で入力します。
ACL Name	ACL 名を 32 文字以内で入力します。

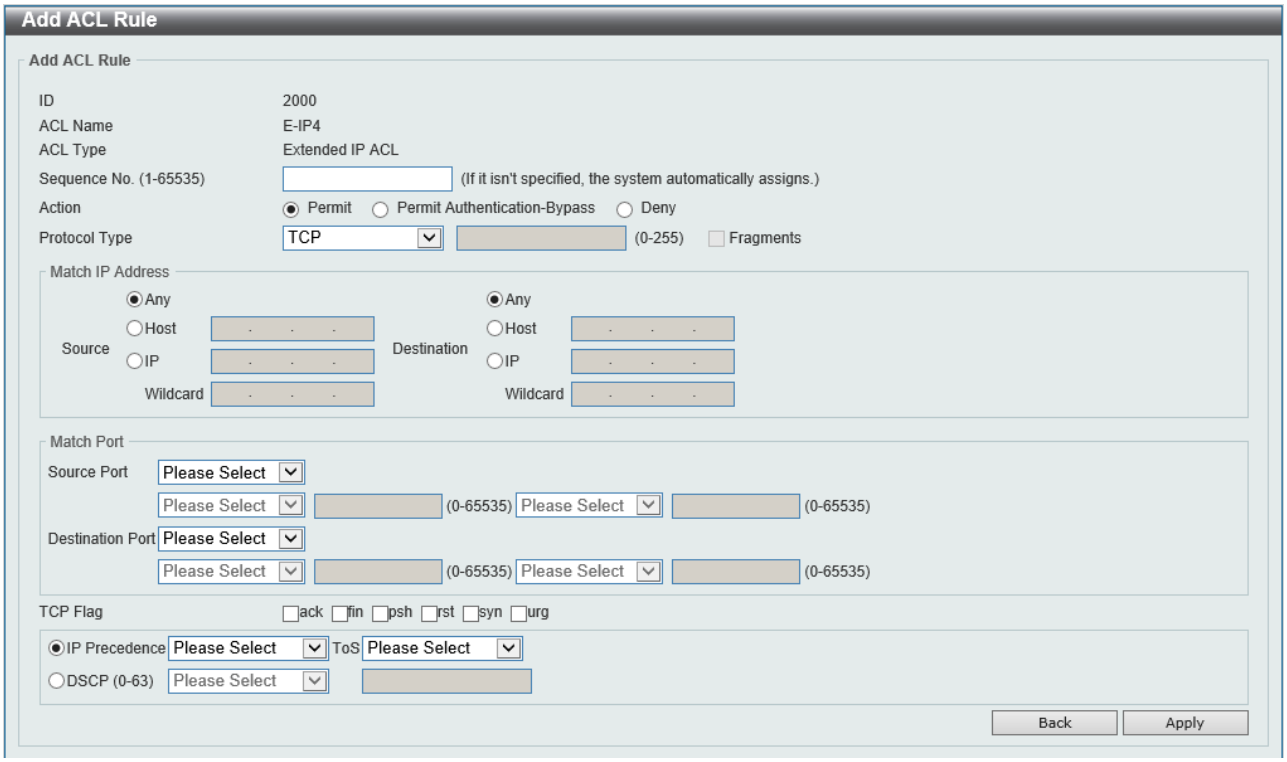
設定を適用するには、Apply ボタンをクリックします。

8.2.1 IP ACL

ACL プロファイルテーブルで標準 IP ACL が選択された状態で **Add Rule** ボタンをクリックすると、以下に示す ACL ルール登録画面が表示されます。



また、ACL プロファイルテーブルで拡張 IP ACL が選択された状態で **Add Rule** ボタンをクリックすると、以下に示す ACL ルール登録画面が表示されます。



標準 IP ACL のルールでは、送信元および宛先の IP アドレスのみで条件を指定します。拡張 IP ACL では、さらに細かく条件を定めることができます。

標準および拡張 IP ACL ルール登録画面で、プロトコルに依存しない項目の説明を以下に示します。

パラメーター	説明
Sequence No.	ACL ルールのシーケンス番号を 1～65535 の範囲で入力します。指定しない場合、自動採番のルールに従って自動的に生成します。
Action	すべての条件に合致した IPv4 パケットに対するアクション（**Permit** / **Permit Authentication-Bypass** / **Deny**）を選択します。
Protocol Type	拡張 IP ACL の場合に表示されます。 条件とするプロトコルをドロップダウンリストから選択します。手動でプロトコル番号を指定する場合、**Protocol ID** を選択します。**None** を選択した場合、プロトコルを判定条件としません。 • **Fragments**：フラグメントされたパケットを指定します。
Source	送信元 IPv4 アドレスの条件を設定します。また、条件を指定するための IPv4 アドレスやワイルドカードマスクを入力します。 • **Any**：すべての送信元ホストを合致条件とします。 • **Host**：指定した送信元 IPv4 アドレスを条件とします。 • **IP**：指定した送信元 IPv4 アドレスグループを条件とします。IPv4 アドレスとワイルドカードマスクの組み合わせで指定します。 　○ **Wildcard**：ワイルドカードマスクを指定します。
Destination	宛先 IPv4 アドレスの条件を設定します。また、条件を指定するための IPv4 アドレスやワイルドカードマスクを入力します。 • **Any**：すべての宛先ホストを合致条件とします。 • **Host**：指定した宛先 IPv4 アドレスを条件とします。 • **IP**：指定した宛先 IPv4 アドレスグループを条件とします。IPv4 アドレスとワイルドカードマスクの組み合わせで指定します。 　○ **Wildcard**：ワイルドカードマスクを指定します。
IP Precedence	拡張 IP ACL の場合に表示されます。 IP Precedence 値の条件を（**routine** (0) / **priority** (1) / **immediate** (2) / **flash** (3) / **flash-override** (4) / **critical** (5) / **internet** (6) / **network** (7)）で指定できます。選択しない場合、IP Precedence 値を判定条件としません。
ToS	拡張 IP ACL の場合に表示されます。 ToS 値の条件を（**normal** (0) / **min-monetary-cost** (1) / **max-reliability** (2) / **max-throughput** (4) / **min-delay** (8)）で指定できます。選択しない場合、ToS 値を判定条件としません。
DSCP	拡張 IP ACL の場合に表示されます。 DSCP 値の条件を（**default** (0) / **af11** (10) / **af12** (12) / **af13** (14) / **af21** (18) / **af22** (20) / **af23** (22) / **af31** (26) / **af32** (28) / **af33** (30) / **af41** (34) / **af42** (36) / **af43** (38) / **cs1** (8) / **cs2** (16) / **cs3** (24) / **cs4** (32) / **cs5** (40) / **cs6** (48) / **cs7** (56) / **ef** (46)）で指定できます。選択しない場合、手動で DSCP 値の条件を指定できます。DSCP 値が指定されていない場合、DSCP 値を判定条件としません。

設定を適用するには、**Apply** ボタンをクリックします。

前の画面に戻るには、**Back** ボタンをクリックします。

送信元や宛先 IP アドレスをグループ（IP）で指定した場合、IPv4 アドレスの比較する部分をワイルドカードマスクで指定します。ワイルドカードマスクのビットマップ値が 0 に該当する部分が比較対象となり、ビットマップ値が 1 に該当する部分は比較されません。たとえば、ワイルドカードマスクが 0.0.0.255 の場合、IPv4 パケットの送信元または宛先 IP アドレスの先頭 3 オクテットのみが比較されます。

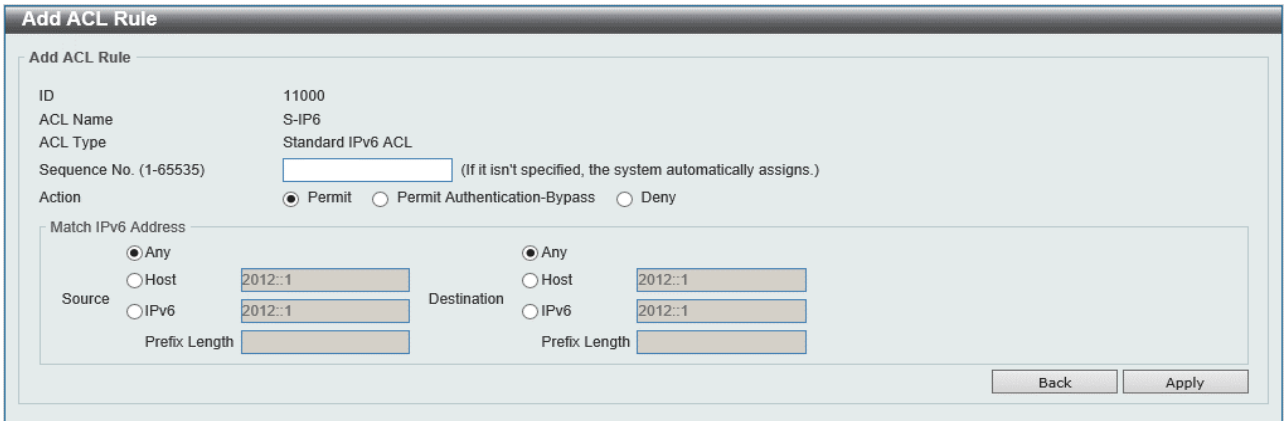
拡張 IP ACL の画面では、プロトコル条件（Protocol Type）の指定によって表示または非表示に切り替わる項目があります。各項目の説明を以下に示します。

パラメーター	説明
Source Port	プロトコル条件が TCP または UDP の場合のみ表示されます。 送信元 TCP/UDP ポート番号の条件を設定します。また、条件を指定するためのポート番号を入力します。ドロップダウンリストで上位プロトコルを選択すると、ウェルノウンポートが自動的に入力されます。条件を指定しない場合、送信先 TCP/UDP ポート番号を判定条件としません。 • =：指定したポート番号と一致する場合を条件とします。 • ＞：指定したポート番号より大きい場合を条件とします。 • ＜：指定したポート番号より小さい場合を条件とします。 • ≠：指定したポート番号と一致しない場合を条件とします。 • Range：条件となるポート番号を、開始ポート番号と終了ポート番号の範囲で指定します。
Destination Port	プロトコル条件が TCP または UDP の場合のみ表示されます。 宛先 TCP/UDP ポート番号の条件を設定します。また、条件を指定するためのポート番号を入力します。ドロップダウンリストで上位プロトコルを選択すると、ウェルノウンポートが自動的に入力されます。条件を指定しない場合、宛先 TCP/UDP ポート番号を判定条件としません。 ポート番号の条件の指定方法（= / ＞ / ＜ / ≠ / Range）は、Source Port と同じです。
Specify ICMP Message Type	プロトコル条件が ICMP の場合のみ表示されます。 ICMP メッセージの条件をメッセージの種類で指定します。メッセージタイプやメッセージコードは自動的に入力されます。指定しない場合、メッセージタイプとメッセージコードを手動で入力できます。
ICMP Message Type	プロトコル条件が ICMP の場合のみ表示されます。 ICMP メッセージタイプの条件を設定します。指定されていない場合、ICMP メッセージの種類を判定条件としません。
Message Code	プロトコル条件が ICMP の場合のみ表示されます。 ICMP メッセージコードの条件を設定します。指定されていない場合、ICMP メッセージコードを判定条件としません。
TCP Flag	プロトコル条件が TCP の場合のみ表示されます。 TCP フラグ（ack / fin / psh / rst / syn / urg）を判定条件とします。チェックされていない TCP フラグは判定条件としません。

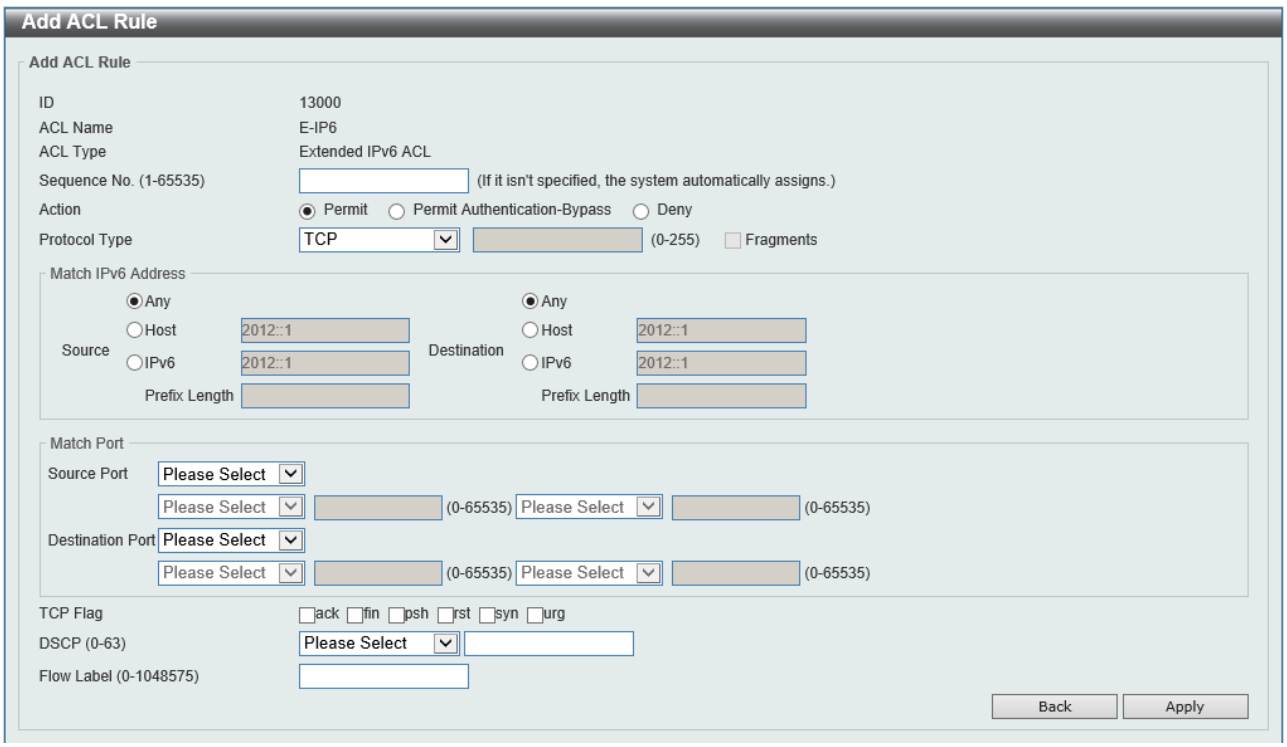
設定を適用するには、Apply ボタンをクリックします。
前の画面に戻るには、Back ボタンをクリックします。

8.2.2 IPv6 ACL

ACL プロファイルテーブルで標準 IPv6 ACL が選択された状態で **Add Rule** ボタンをクリックすると、以下に示す ACL ルール登録画面が表示されます。



また、ACL プロファイルテーブルで拡張 IPv6 ACL が選択された状態で **Add Rule** ボタンをクリックすると、以下に示す ACL ルール登録画面が表示されます。



標準 IPv6 ACL のルールでは、送信元および宛先の IPv6 アドレスのみで条件を指定します。拡張 IP ACL では、さらに細かく条件を定めることができます。

標準および拡張 IPv6 ACL ルール登録画面で、プロトコルに依存しない項目の説明を以下に示します。

パラメーター	説明
Sequence No.	ACL ルールのシーケンス番号を 1～65535 の範囲で入力します。指定しない場合、自動採番のルールに従って自動的に生成します。
Action	すべての条件に合致した IPv6 パケットに対するアクション（**Permit** / **Permit Authentication-Bypass** / **Deny**）を選択します。
Protocol Type	拡張 IPv6 ACL の場合に表示されます。 条件とするプロトコルをドロップダウンリストから選択します。手動でプロトコル番号を指定する場合、**Protocol ID** を選択します。**None** を選択した場合、プロトコルを判定条件としません。 • **Fragments**：フラグメントされたパケットを指定します。
Source	送信元 IPv6 アドレスの条件を設定します。また、条件を指定するための IPv6 アドレスやプレフィックス長を入力します。 • **Any**：すべての送信元ホストを合致条件とします。 • **Host**：指定した送信元 IPv6 アドレスを条件とします。 • **IPv6**：指定した送信元 IPv6 アドレスグループを条件とします。IPv6 アドレスとプレフィックス長の組み合わせで指定します。 　○ **Prefix Length**：プレフィックス長を入力します。
Destination	宛先 IPv6 アドレスの条件を設定します。また、条件を指定するための IPv6 アドレスやプレフィックス長を入力します。 • **Any**：すべての宛先ホストを合致条件とします。 • **Host**：指定した宛先 IPv6 アドレスを条件とします。 • **IPv6**：指定した宛先 IPv6 アドレスグループを条件とします。IPv6 アドレスとプレフィックス長の組み合わせで指定します。 　○ **Prefix Length**：プレフィックス長を入力します。
DSCP	拡張 IPv6 ACL の場合に表示されます。 DSCP 値の条件を（**default**（0）/ **af11**（10）/ **af12**（12）/ **af13**（14）/ **af21**（18）/ **af22**（20）/ **af23**（22）/ **af31**（26）/ **af32**（28）/ **af33**（30）/ **af41**（34）/ **af42**（36）/ **af43**（38）/ **cs1**（8）/ **cs2**（16）/ **cs3**（24）/ **cs4**（32）/ **cs5**（40）/ **cs6**（48）/ **cs7**（56）/ **ef**（46））で指定できます。選択しない場合、手動で DSCP 値を指定できます。DSCP 値が指定されていない場合、DSCP 値を判定条件としません。
Flow Label	拡張 IPv6 ACL の場合に表示されます。 フローラベル値（0～1048575）の条件を入力します。指定しない場合はフローラベル値を判定条件としません。

設定を適用するには、**Apply** ボタンをクリックします。

前の画面に戻るには、**Back** ボタンをクリックします。

拡張 IPv6 ACL の画面では、プロトコル条件（**Protocol Type**）の指定によって表示または非表示に切り替わる項目があります。各項目の説明を以下に示します。

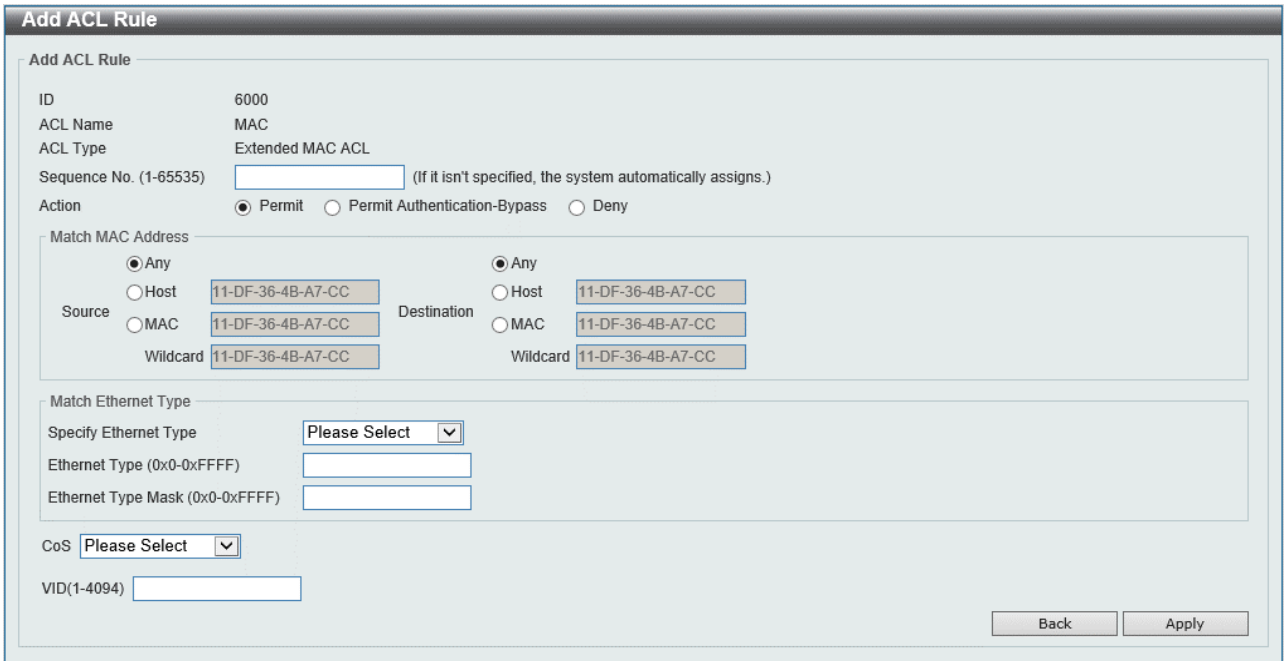
パラメーター	説明
Source Port	プロトコル条件が **TCP** または **UDP** の場合のみ表示されます。 送信元 TCP/UDP ポート番号の条件を設定します。また、条件を指定するためのポート番号を入力します。ドロップダウンリストで上位プロトコルを選択すると、ウェルノウンポートが自動的に入力されます。条件を指定しない場合、送信先 TCP/UDP ポート番号を判定条件としません。 • =：指定したポート番号と一致する場合を条件とします。 • ＞：指定したポート番号より大きい場合を条件とします。 • ＜：指定したポート番号より小さい場合を条件とします。 • ≠：指定したポート番号と一致しない場合を条件とします。 • **Range**：条件となるポート番号を、開始ポート番号と終了ポート番号の範囲で指定します。
Destination Port	プロトコル条件が **TCP** または **UDP** の場合のみ表示されます。 宛先 TCP/UDP ポート番号の条件を設定します。また、条件を指定するためのポート番号を入力します。ドロップダウンリストで上位プロトコルを選択すると、ウェルノウンポートが自動的に入力されます。条件を指定しない場合、宛先 TCP/UDP ポート番号を判定条件としません。 ポート番号の条件の指定方法（= / ＞ / ＜ / ≠ / **Range**）は、**Source Port** と同じです。
TCP Flag	プロトコル条件が **TCP** の場合のみ表示されます。 TCP フラグ（**ack** / **fin** / **psh** / **rst** / **syn** / **urg**）を判定条件とします。チェックされていない TCP フラグは判定条件としません。
Specify ICMP Message Type	プロトコル条件が **ICMP** の場合のみ表示されます。 ICMP メッセージの条件をメッセージの種類で指定します。メッセージタイプやメッセージコードは自動的に入力されます。指定しない場合、メッセージタイプとメッセージコードを手動で入力できます。
ICMP Message Type	プロトコル条件が **ICMP** の場合のみ表示されます。 ICMP メッセージタイプの条件を設定します。指定されていない場合、ICMP メッセージの種類を判定条件としません。
Message Code	プロトコル条件が **ICMP** の場合のみ表示されます。 ICMP メッセージコードの条件を設定します。指定されていない場合、ICMP メッセージコードを判定条件としません。

設定を適用するには、**Apply** ボタンをクリックします。

前の画面に戻るには、**Back** ボタンをクリックします。

8.2.3 拡張 MAC ACL

ACL プロファイルテーブルで拡張 MAC ACL が選択された状態で **Add Rule** ボタンをクリックすると、以下に示す ACL ルール登録画面が表示されます。



本画面の各項目の説明を以下に示します。

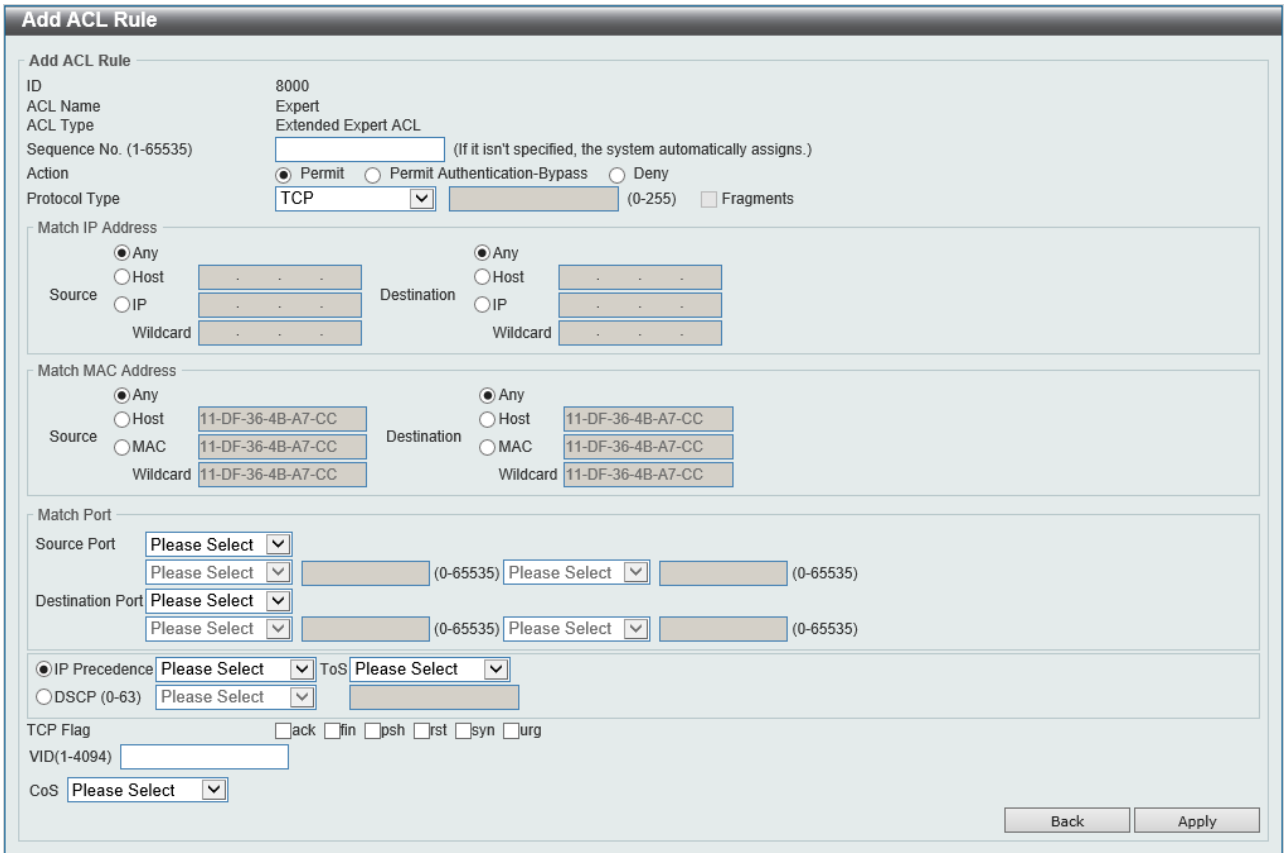
パラメーター	説明
Sequence No.	ACL ルールのシーケンス番号を 1～65535 の範囲で入力します。指定しない場合、自動採番のルールに従って自動的に生成します。
Action	すべての条件に合致したフレームに対するアクション（Permit / Permit Authentication-Bypass / Deny）を選択します。
Source	送信元 MAC アドレスの条件を設定します。また、条件を指定するための MAC アドレスやワイルドカードマスクを入力します。 • Any：すべての送信元ホストを合致条件とします。 • Host：指定した送信元 MAC アドレスを条件とします。 • MAC：指定した送信元 MAC アドレスのグループを条件とします。MAC アドレスとワイルドカードマスクの組み合わせで指定します。 　○ Wildcard：ワイルドカードマスクを指定します。
Destination	宛先 MAC アドレスの条件を設定します。また、条件を指定するための MAC アドレスやワイルドカードマスクを入力します。 • Any：すべての宛先ホストを合致条件とします。 • Host：指定した宛先 MAC アドレスを条件とします。 • MAC：指定した宛先 MAC アドレスのグループを条件とします。MAC アドレスとワイルドカードマスクの組み合わせで指定します。 　○ Wildcard：ワイルドカードマスクを指定します。
Specify Ethernet Type	イーサネットタイプの条件を（aarp / appletalk / decent-iv / etype-6000 / etype-8042 / lat / lavc-sca / mop-console / mop-dump / vines-echo / vines-ip / xns-idp / arp）で指定できます。選択しない場合、イーサネットタイプとマスクを手動で入力できます。
Ethernet Type	イーサネットタイプの条件を 16 進数値の 0x0～0xFFFF（0x は入力する必要はありません）の範囲で入力します。指定しない場合、イーサネットタイプを判定条件としません。
Ethernet Type Mask	イーサネットタイプのマスクを 16 進数値の 0x0～0xFFFF（0x は入力する必要はありません）の範囲で入力します。指定しない場合、イーサネットタイプが指定されている場合は 0x0 として処理されます。
CoS	CoS 値の条件を指定します。指定しない場合、CoS 値を判定条件としません。
VID	VLAN ID の条件を VLAN ID で指定します。

設定を適用するには、Apply ボタンをクリックします。

前の画面に戻るには、Back ボタンをクリックします。

8.2.4 拡張エキスパート ACL

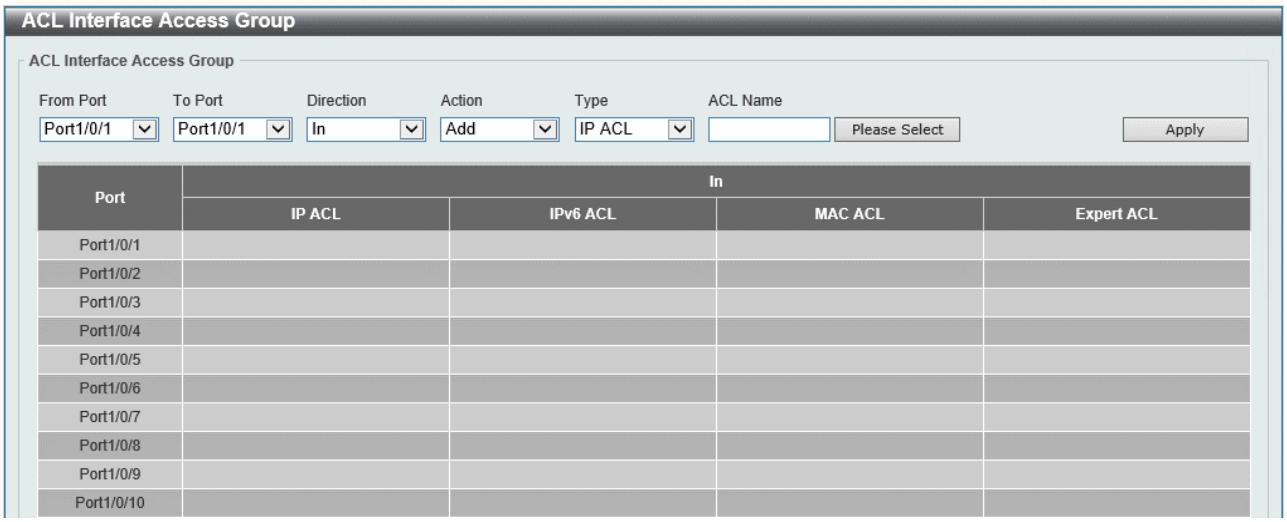
ACL プロファイルテーブルで拡張エキスパート ACL が選択された状態で **Add Rule** ボタンをクリックすると、以下に示す ACL ルール登録画面が表示されます。



拡張エキスパート ACL のルールで設定する項目は、拡張 IP ACL の内容に拡張 MAC ACL の内容を追加したものです。各設定項目の説明は IP ACL および拡張 MAC ACL の項をご参照ください。

8.3 ACL Interface Access Group

ACL Interface Access Group 画面では、登録した ACL を物理ポートに適用できます。
本画面を表示するには、ACL > ACL Interface Access Group をクリックします。

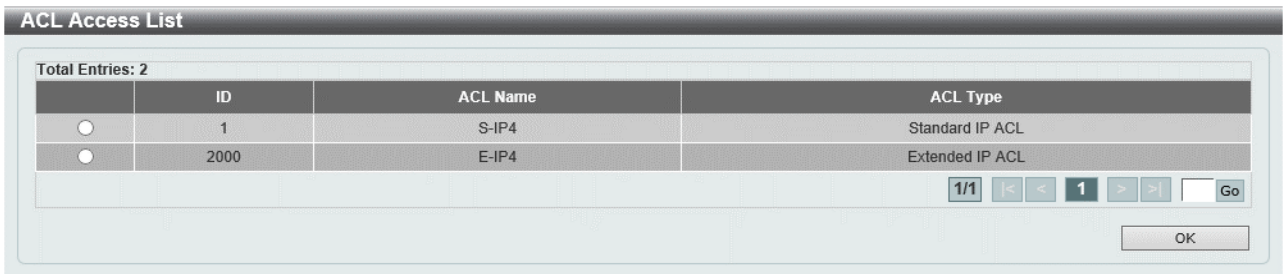


本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートの範囲を選択します。
Direction	ACL を適用する方向を選択します。In のみ選択できます。
Action	実行するアクション（Add / Delete）を選択します。
Type	適用する ACL の種別（IP ACL / IPv6 ACL / MAC ACL / Expert ACL）を選択します。
ACL Name	ACL 名を 32 文字以内で入力します。または、Please Select ボタンをクリックし、リストから既存の ACL を選択します。

設定を適用するには、Apply ボタンをクリックします。

Please Select ボタンをクリックすると、登録済みの ACL のリストが表示されます。以下は、IP ACL の一覧を表示した例です。

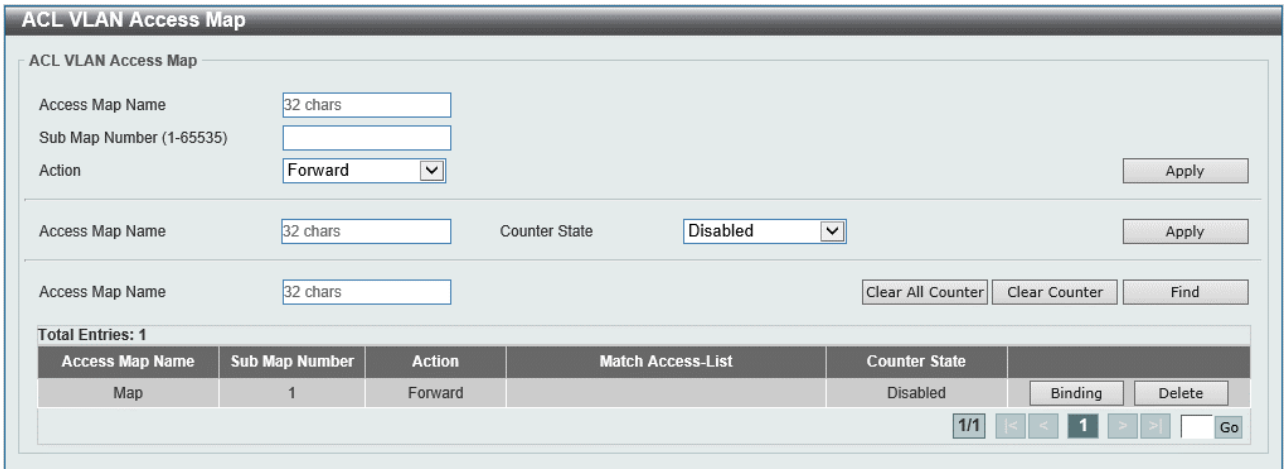


適用する ACL を選択するには、ラジオボタンをクリックします。
選択した ACL を適用するには、OK ボタンをクリックします。

8.4 ACL VLAN Access Map

ACL VLAN Access Map 画面では、VLAN アクセスマップを設定します。
VLAN アクセスマップは、ACL で VLAN のアクセス制御を行うために作成するプロファイルで、ACL ルールに基づく合致条件と、合致した場合のアクションを定めた複数のサブマップによってポリシーが定義されます。VLAN フィルターで VLAN アクセスマップを VLAN に割り当てることでアクセス制御を提供します。

本画面を表示するには、**ACL > ACL VLAN Access Map** をクリックします。

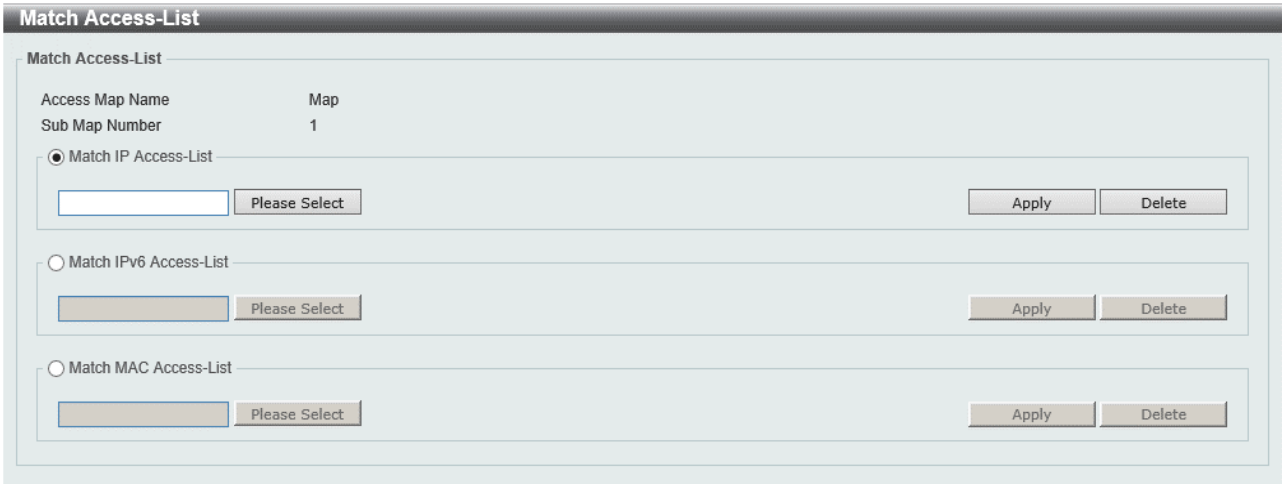


本画面の各項目の説明を以下に示します。

パラメーター	説明
Access Map Name	VLAN アクセスマップ名を 32 文字以内で入力します。
Sub Map Number	サブマップ番号を 1～65535 の範囲で入力します。
Action	実行するアクション（Forward / Drop / Redirect）を選択します。 Redirect を選択した場合は、リダイレクト先のインターフェースをドロップダウンリストで選択します。
Counter State	カウンター機能の状態（Enabled / Disabled）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。
すべての VLAN アクセスマップのカウンター情報をクリアするには、**Clear All Counter** ボタンをクリックします。
表示されている VLAN アクセスマップのカウンター情報をクリアするには、**Clear Counter** ボタンをクリックします。
入力した情報で VLAN アクセスマップを検索するには、**Find** ボタンをクリックします。
ACL プロファイルと VLAN アクセスマップを関連付けるには、**Binding** ボタンをクリックします。
VLAN アクセスマップを削除するには、**Delete** ボタンをクリックします。

Binding ボタンをクリックすると、以下に示す画面が表示されます。

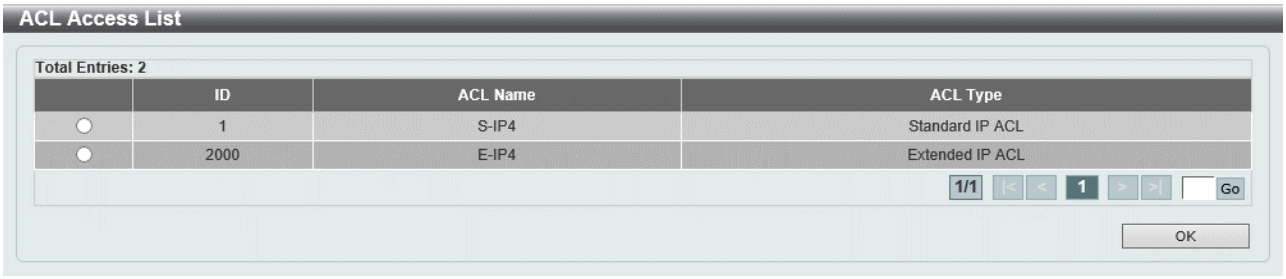


Match Access-List の各項目の説明を以下に示します。

パラメーター	説明
Match IP ACL	適用する IP ACL が表示されます。
Match IPv6 ACL	適用する IPv6 ACL が表示されます。
Match MAC ACL	適用する MAC ACL が表示されます。

適用する ACL を選択する画面に移動するには、**Please Select** ボタンをクリックします。
設定を適用するには、**Apply** ボタンをクリックします。
関連付ける ACL 情報を削除するには、**Delete** ボタンをクリックします。

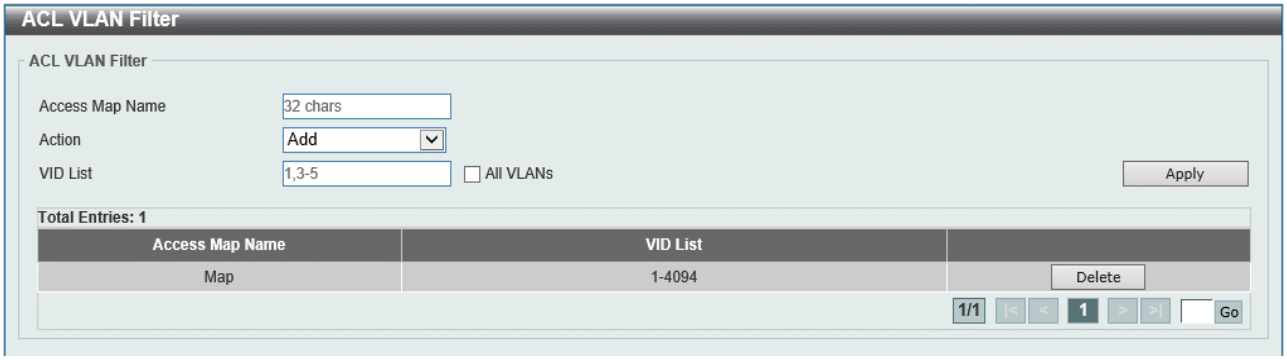
Please Select ボタンをクリックすると、以下に示す画面が表示されます。



VLAN アクセスマップに関連付ける ACL を選択するには、ラジオボタンをクリックします。
選択したアクセスリストを適用するには、**OK** ボタンをクリックします。

8.5 ACL VLAN Filter

ACL VLAN Filter 画面では、VLAN フィルターを設定します。登録した VLAN アクセスマップを VLAN に割り当てることができます。
本画面を表示するには、**ACL > ACL VLAN Filter** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Access Map Name	VLAN アクセスマップ名を 32 文字以内で入力します。
Action	実行するアクション（**Add** / **Delete**）を選択します。
VID List	適用する VLAN を VLAN ID のリストで指定します。 装置に設定されているすべての VLAN に適用するには、**All VLANs** をチェックします。

設定を適用するには、**Apply** ボタンをクリックします。
VLAN フィルターを削除するには、**Delete** ボタンをクリックします。

9 Security

Security メニューでは、ポートアクセス制御やネットワーク認証など、セキュリティーに関連する設定を行います。
Security の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.1	Port Security	ポートセキュリティー機能の設定
9.2	802.1X	IEEE802.1X 認証の設定
9.3	AAA	AAA モジュールの設定
9.4	RADIUS	RADIUS サーバーの登録
9.5	TACACS	TACACS+サーバーの登録
9.6	DHCP Snooping	DHCP スヌーピングの設定
9.7	MAC Authentication	MAC アドレス認証の設定
9.8	Web Authentication	Web 認証の設定
9.9	Network Access Authentication	ポートアクセス認証全般の設定とローカルユーザーデータベースの登録
9.10	Trusted Host	アプリケーションのトラストホストの設定
9.11	Traffic Segmentation Settings	トラフィックセグメンテーションの設定
9.12	Storm Control	ストーム制御機能の設定
9.13	SSH	SSH サーバー機能や SSH ユーザーの設定
9.14	SSL	SSL 機能の設定

9.1 Port Security

Port Security サブメニューでは、ポートセキュリティー機能の設定を行います。
ポートセキュリティー機能では、ポート単位で最大接続数を制限します。ポートセキュリティーを有効にしたポートでクライアントからのフレームを受信すると、装置はポートセキュリティーの管理テーブル上に MAC アドレスを記録します。管理テーブル上で単一ポートの所属 MAC アドレス数が最大接続数に達した状態で、未登録のクライアントからのフレームを受信すると「違反」状態になり、該当するクライアントの通信を「信頼できない通信」として扱います。

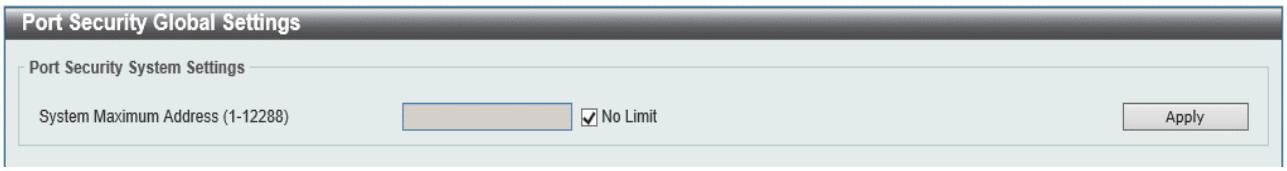
ポートセキュリティー機能の状態や、「違反」状態になった場合のポートのアクション、管理テーブル上の MAC アドレス情報の有効期限などは、ポート単位で設定できます。

Port Security の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.1.1	Port Security Global Settings	ポートセキュリティー機能のグローバル設定
9.1.2	Port Security Port Settings	ポートセキュリティー機能のポート単位の設定
9.1.3	Port Security Address Entries	ポートセキュリティーの情報表示と操作

9.1.1 Port Security Global Settings

Port Security Global Settings 画面では、ポートセキュリティー機能のシステム全体での最大登録 MAC アドレス数を設定します。
本画面を表示するには、Security > Port Security > Port Security Global Settings をクリックします。



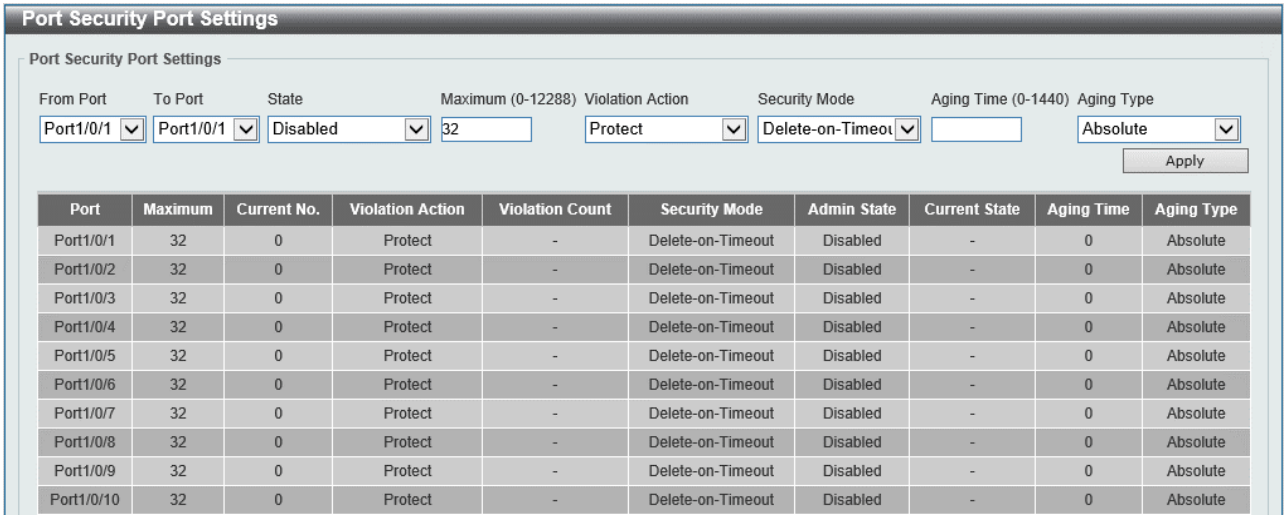
本画面の各項目の説明を以下に示します。

パラメーター	説明
System Maximum Address	接続を許可する MAC アドレスの最大数を 1～12288 の範囲で入力します。制限しない場合は、No Limit をチェックします。

設定を適用するには、Apply ボタンをクリックします。

9.1.2 Port Security Port Settings

Port Security Port Settings 画面では、ポート単位でポートセキュリティーの設定を行います。
本画面を表示するには、Security > Port Security > Port Security Port Settings をクリックします。



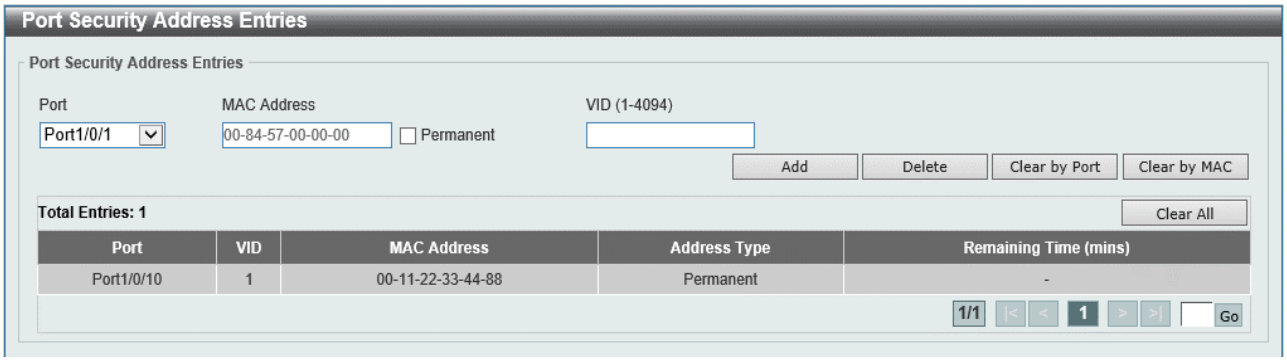
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
State	ポートセキュリティー機能の状態（Enabled / Disabled）を選択します。
Maximum	選択したポートへの接続を許可する MAC アドレスの最大数を 0～12288 の範囲で入力します（デフォルト：32）。
Violation Action	違反状態でのアクションを以下のいずれかから選択します。 • Protect：信頼できない通信をすべて破棄します。カウンターには記録しません。 • Restrict：信頼できない通信をすべて破棄します。カウンターに計上し、システムログの記録を行います。 • Shutdown：違反状態になるとポートをシャットダウンします。システムログの記録を行います。
Security Mode	セキュリティーモードを以下のどちらかから選択します。 • Permanent：学習したエントリーは永続エントリーとなり、ユーザーが手動で削除しない限り削除されません。このエントリーは設定ファイルに記録されます。 • Delete-on-Timeout：学習したエントリーは期限付きエントリーとなります。期限付きエントリーは失効すると自動的に削除されます。
Aging Time	エントリーのエージング時間を 0～1440（分）の範囲で入力します。0 の場合は期限付きであっても失効しません。
Aging Type	エントリーの失効モードを以下から選択します。 • Absolute：指定した時間で自動失効してエントリーを削除します。 • Inactivity：指定した期間内に該当するクライアントからフレームを受信しない場合にエントリーを削除します。

設定を適用するには、Apply ボタンをクリックします。

9.1.3 Port Security Address Entries

Port Security Address Entries 画面では、ポートセキュリティーの管理テーブルの表示や、エントリーの手動登録および削除を行います。
本画面を表示するには、Security > Port Security > Port Security Address Entries をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Port	エントリーを追加、削除するポートを選択します。
MAC Address	エントリーを追加、削除する MAC アドレスを入力します。永続エントリーを登録する場合は、Permanent をチェックします。
VID	VLAN ID を入力します。範囲は 1～4094 です。

入力した情報でポートセキュリティーエントリーを追加するには、Add ボタンをクリックします。
入力した情報でポートセキュリティーエントリーを削除するには、Delete ボタンをクリックします。
選択したポートのポートセキュリティーエントリーのカウンターをクリアするには、Clear by Port ボタンをクリックします。
入力した MAC アドレスのポートセキュリティーエントリーのカウンターをクリアするには、Clear by MAC ボタンをクリックします。
すべてのポートセキュリティーエントリーのカウンターをクリアするには、Clear All ボタンをクリックします。

9.2 802.1X

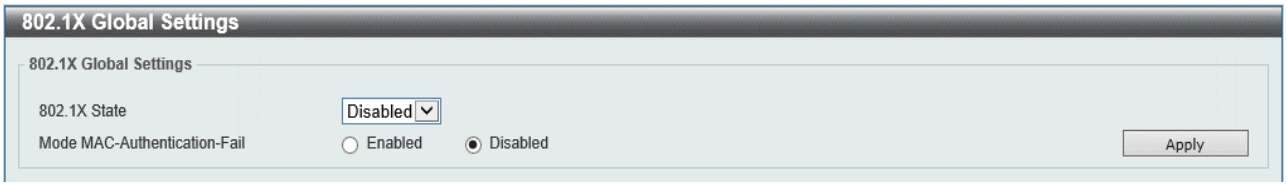
802.1X サブメニューでは、ポートアクセス認証の IEEE802.1X 認証（以後、IEEE802.1X 認証）の設定を行います。この機能は、IEEE802.1X 認証クライアントの認証アクセスによってポートのアクセス許可を決定します。

802.1X の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.2.1	802.1X Global Settings	IEEE802.1X 認証のグローバル設定
9.2.2	802.1X Port Settings	IEEE802.1X 認証のポート設定
9.2.3	Authentication Sessions Information	IEEE802.1X 認証のセッション情報の表示
9.2.4	Authenticator Statistics	IEEE802.1X 認証の統計情報の表示

9.2.1 802.1X Global Settings

802.1X Global Settings 画面では、IEEE 802.1X 認証のグローバル設定を行います。
本画面を表示するには、**Security > 802.1X > 802.1X Global Settings** をクリックします。



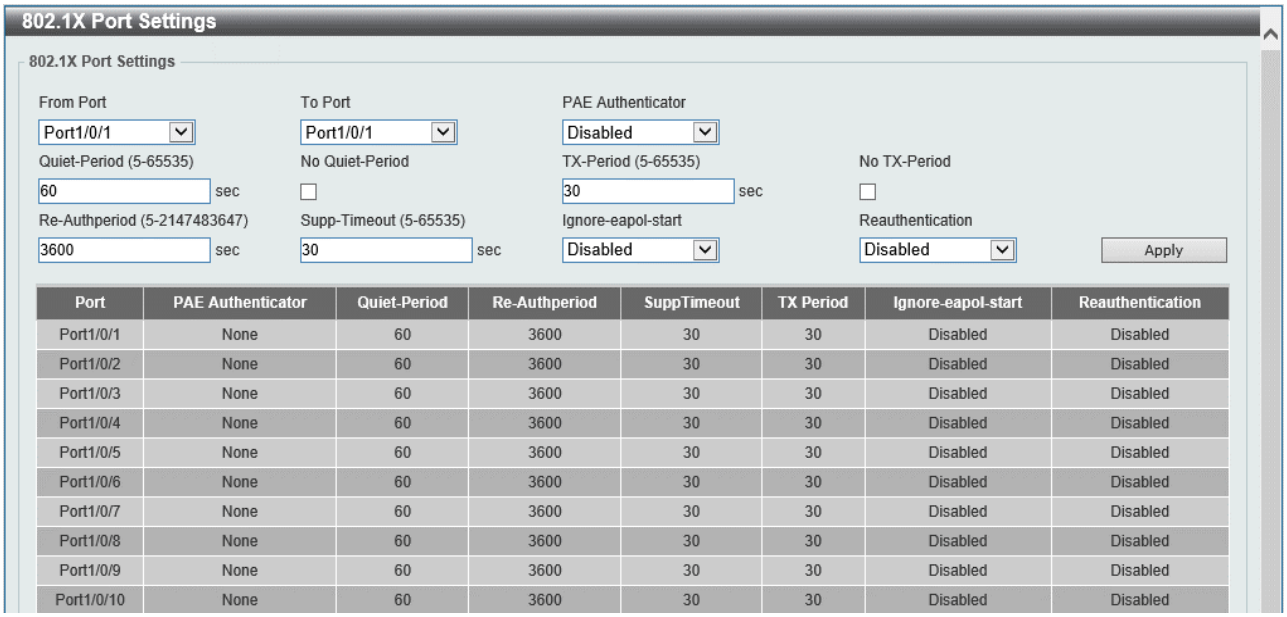
本画面の各項目の説明を以下に示します。

パラメーター	説明
802.1X State	ポートアクセス認証で IEEE 802.1X 機能の状態（**Enabled** / **Disabled**）を選択します。
Mode MAC-Authentication-Fail	MAC 認証機能と併用した際に、MAC 認証を先行して実施し、失敗した際に IEEE 802.1X 認証を実施する機能の状態（**Enabled** / **Disabled**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

9.2.2 802.1X Port Settings

802.1X Port Settings 画面では、ポート単位での IEEE 802.1X 認証の設定を行います。
本画面を表示するには、Security > 802.1X > 802.1X Port Settings をクリックします。



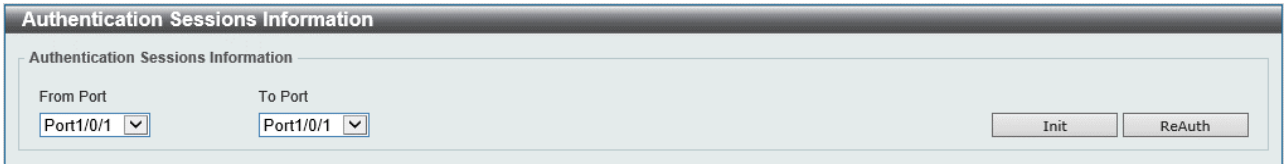
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
PAE Authenticator	IEEE 802.1X 認証機能の状態（Enabled / Disabled）を選択します。
Quiet-Period	認証失敗時のブロック時間を 5～65535（秒）の範囲で入力します。
No Quiet-Period	認証失敗時にブロック時間を設けない場合にチェックします。
TX-Period	EAP-Request/Identity を送信する間隔を 5～65535（秒）の範囲で入力します。
No TX-Period	定期的な EAP-Request/Identity を送信しない場合にチェックします。
Re-Authperiod	再認証期間を 5～2147483647（秒）の範囲で入力します。
Supp-Timeout	EAP-Request/Identity の応答待ち時間を 5～65535（秒）の範囲で入力します。
Ignore-eapol-start	EAPOL-Start に応答しない機能の状態（Enabled / Disabled）を選択します。
Reauthentication	再認証機能の状態（Enabled / Disabled）を選択します。

設定を適用するには、Apply ボタンをクリックします。

9.2.3 Authentication Sessions Information

Authentication Sessions Information 画面は、IEEE802.1X 認証のセッション情報を表示します。
本画面を表示するには、Security > 802.1X > Authentication Sessions Information をクリックします。



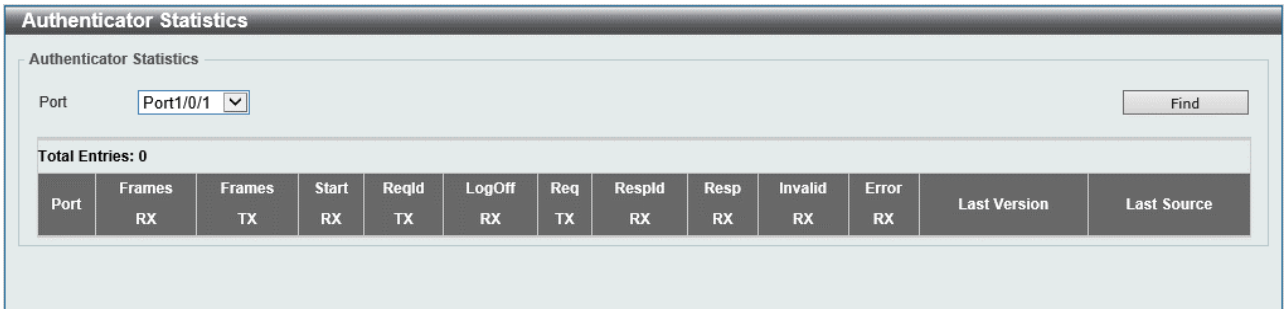
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。

選択したポートの認証セッションを初期化するには、Init ボタンをクリックします。
選択したポートの認証セッションで再認証するには、ReAuth ボタンをクリックします。

9.2.4 Authenticator Statistics

Authenticator Statistics 画面では、IEEE 802.1X 認証の統計情報を表示します。
本画面を表示するには、Security > 802.1X > Authenticator Statistics をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Port	ポート番号を選択します。

選択したポートの統計情報を検索して表示するには、Find ボタンをクリックします。

9.3 AAA

AAA サブメニューでは、AAA モジュールの機能に関する設定を行います。
AAA は、物理ポートやモジュールへのユーザーのアクセスに対して、ユーザーの認証（Authentication）、権限の指定（Authorization）、およびサービス利用状況の記録（Accounting）などに関する機能を提供するフレームワークで、ポートアクセス認証は AAA モジュールで提供される機能によって実現します。

AAA の下にあるサブメニューの一覧を以下の表に示します。

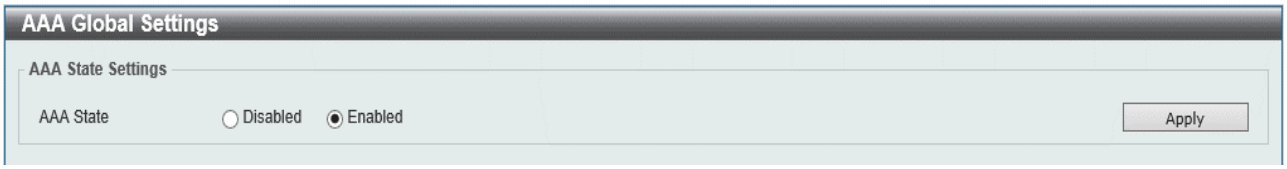
項番	メニュー名	概要
9.3.1	AAA Global Settings	AAA モジュールのグローバル設定
9.3.2	Application Authentication Settings	AAA モジュールでの CLI のログイン認証方式設定
9.3.3	Application Accounting Settings	CLI のアカウンティング方式設定
9.3.4	Authentication Settings	各認証処理でのメソッドリスト設定
9.3.5	Accounting Settings	アカウンティングのメソッドリスト設定

本装置で AAA モジュールによる認証と認可に対応する機能は、ポートアクセス認証と CLI のログイン認証です。AAA モジュールが有効になると、装置の CLI のログイン時の認証処理は AAA モジュールによって実行されます。
また、AAA モジュールでは、ネットワーク利用状況（Network アカウンティング）、システムイベント（System アカウンティング）、CLI のコマンド発行（Command アカウンティング）、および CLI のログイン／ログアウト（Exec アカウンティング）のアカウンティング要求に対応します。

AAA サブメニューで設定する内容は、AAA モジュールのグローバル設定と、AAA の各機能の処理での照会先と照会順番を定めるメソッドリストです。メソッドリスト Method1～4 で指定された順番に照会が行われます。

9.3.1 AAA Global Settings

AAA Global Settings 画面では、AAA モジュールのグローバル設定を行います。
本画面を表示するには、**Security > AAA > AAA Global Settings** をクリックします。



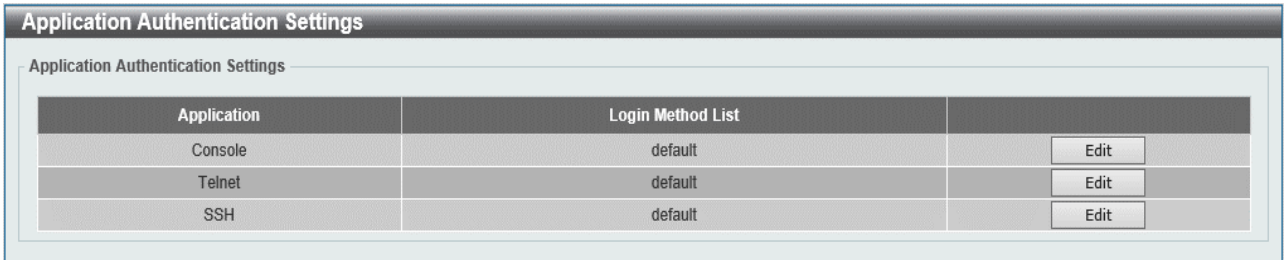
本画面の各項目の説明を以下に示します。

パラメーター	説明
AAA State	AAA モジュールの状態（**Enabled** / **Disabled**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

9.3.2 Application Authentication Settings

Application Authentication Settings 画面では、CLI のログイン認証の認証方式を設定します。認証方式は各ライン種別で指定可能です。
本画面を表示するには、**Security** > **AAA** > **Application Authentication Settings** をクリックします。



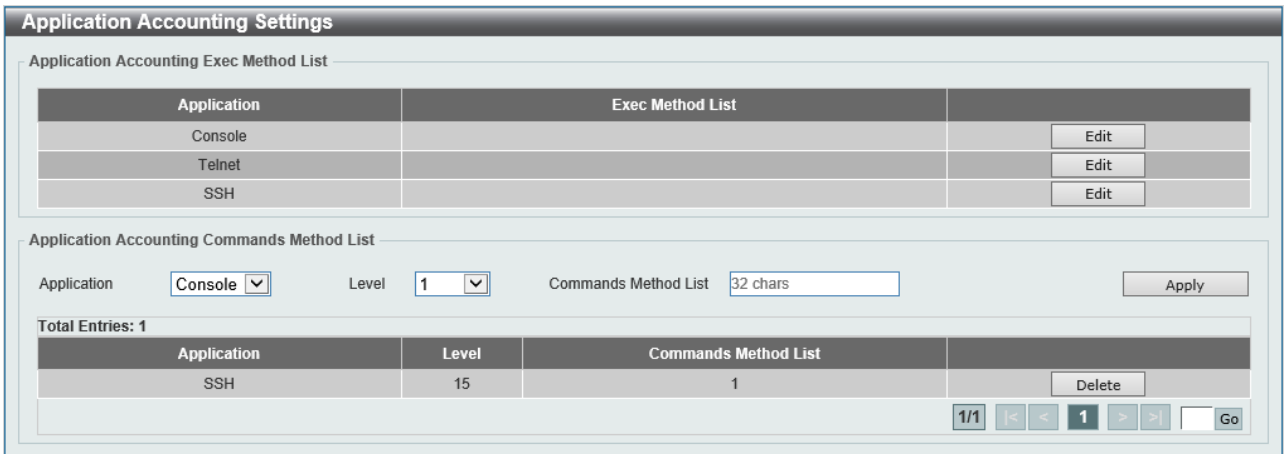
本画面の各項目の説明を以下に示します。

パラメーター	説明
Login Method List	ログイン認証のメソッドリストのプロファイルを入力します。指定するプロファイルは Secutiry > AAA > Authentication Settings の AAA Authentication Exec タブで登録したプロファイルです。

ログイン認証方式を再設定するには、**Edit** ボタンをクリックします。
設定を適用するには、**Apply** ボタンをクリックします。

9.3.3 Application Accounting Settings

Application Accounting Settings 画面では、CLI の Exec アカウンティングと Command アカウンティングの方式を設定します。
本画面を表示するには、**Security** > **AAA** > **Application Accounting Settings** をクリックします。



上のテーブルは、各ライン種別での Exec アカウンティングの方式を表示しています。**Edit** ボタンをクリックすると、Exec アカウンティング方式を編集できます。

編集画面での各項目の説明を以下に示します。

パラメーター	説明
Exec Method List	Exec アカウンティングのプロファイルを入力します。指定するプロファイルは Secutiry > AAA > Accounting Settings の AAA Accounting Exec タブで登録したプロファイルです。

設定を適用するには、Apply ボタンをクリックします。

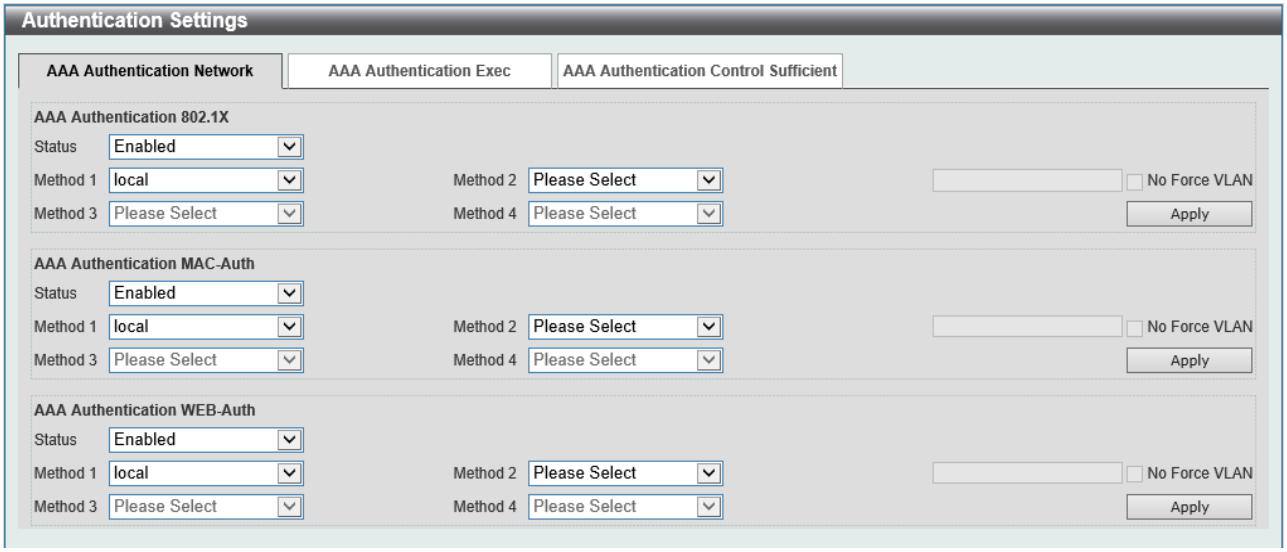
Application Accounting Commands Method List では、Command アカウンティングの方式を設定します。
各項目の説明を以下に示します。

パラメーター	説明
Application	Command アカウンティングの設定を適用するライン種別（Console / Telnet / SSH）を選択します。
Level	Command アカウンティングの方式を適用する特権レベルを 1～15 から選択します。特権レベルに応じて異なるアカウンティング方式を指定できます。
Commands Method List	Command アカウンティングのプロファイルを入力します。指定するプロファイルは Secutiry > AAA > Accounting Settings の AAA Accounting Commands タブで登録したプロファイルです。

設定を適用するには、Apply ボタンをクリックします。
Command アカウンティングの設定を削除するには、Delete ボタンをクリックします。

9.3.4 Authentication Settings

Authentication Settings 画面では、ポートアクセス認証の認証方式を設定します。また、CLI でのログイン認証のメソッドリストのプロファイルを登録します。
本画面を表示するには、Security > AAA > Authentication Settings をクリックします。



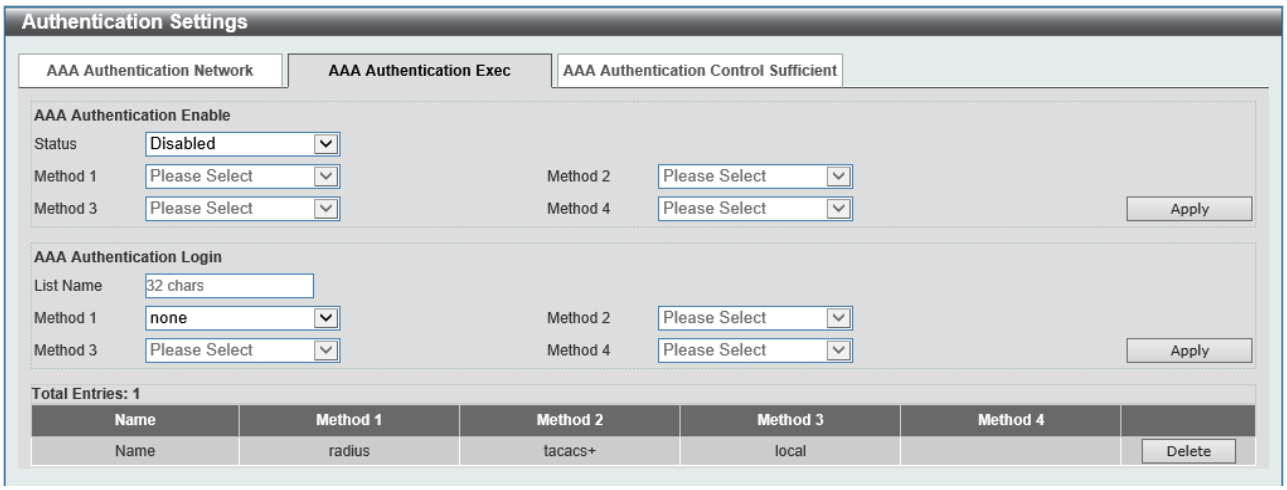
本画面には、AAA Authentication Network タブ、AAA Authentication Exec タブ、および AAA Authentication Control Sufficient タブがあります。

AAA Authentication Network タブでは、ポートアクセス認証（IEEE802.1X 認証、MAC 認証、Web 認証）でのメソッドリストを設定します。各項目の説明を以下に示します。

パラメーター	説明
Status	**Disabled** を選択すると、メソッドリストがクリアされます。
Method 1 ～ Method 4	各メソッドの照会方法を以下のいずれかから選択します。 • **local**：ローカルデータベースで認証します。 • **force**：他のメソッドの認証処理によって先行して認証を拒否されているユーザーを除き、認証を許可します。通常、この方法はメソッドリストの最後に使用します。ユーザーに割り当てる VLAN の VLAN ID をテキストボックスに入力します。VLAN を割り当てない場合は、**No Force VLAN** をチェックします。 • **group**：指定したサーバーグループに照会を行います。右のボックスにサーバーグループ名を 32 文字以内で入力します。 • **radius**：サーバーグループ「radius」に照会を行います。

設定を適用するには、**Apply** ボタンをクリックします。

AAA Authentication Exec タブでは、ログイン認証と Enable 認証でのメソッドリストを設定します。



AAA Authentication Enable では Enable 認証での設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Status	CLI で特権実行モードに遷移する際の認証(Enable 認証)の状態（**Enabled** / **Disabled**）を選択します。
Method 1 ～ Method 4	各メソッドの照会方法を以下のいずれかから選択します。 • **none**：他のメソッドの認証処理によって先行して認証を拒否されているユーザーを除き、認証を許可します。通常、この方法はメソッドリストの最後に使用します。 • **enabled**：ローカルデータベースのパスワードを使用します。 • **group**：指定したサーバーグループに照会を行います。右のボックスにサーバーグループ名を 32 文字以内で入力します。 • **radius**：サーバーグループ「radius」に照会します。 • **tacacs+**：サーバーグループ「tacacs+」に照会します。

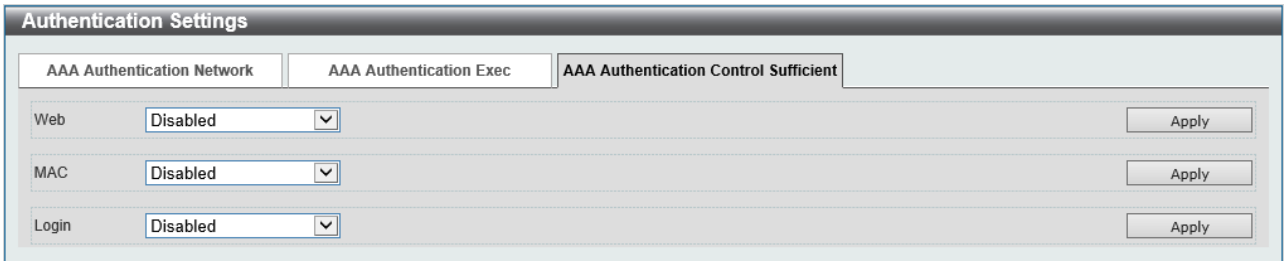
設定を適用するには、**Apply** ボタンをクリックします。

AAA Authentication Login では、ログイン認証のメソッドリストのプロファイルを登録します。各項目の説明を以下に示します。

パラメーター	説明
List Name	ログイン認証のメソッドリストのプロファイル名を入力します。
Method 1 ～ Method 4	各メソッドの照会方法を以下のいずれかから選択します。 • **none**：他のメソッドの認証処理によって先行して認証を拒否されているユーザーを除き、認証を許可します。通常、この方法はメソッドリストの最後に使用します。 • **enabled**：ローカルデータベースで認証します。 • **group**：指定したサーバーグループに照会を行います。右のボックスにサーバーグループ名を 32 文字以内で入力します。 • **radius**：サーバーグループ「radius」に照会します。 • **tacacs+**：サーバーグループ「tacacs+」に照会します。

設定を適用するには、**Apply** ボタンをクリックします。
登録したメソッドリストのプロファイルを削除するには、**Delete** ボタンをクリックします。

AAA Authentication Control Sufficient タブをクリックすると、以下に示す画面が表示されます。



AAA モジュールの認証では、規定したメソッドリストの順番で登録したメソッドを実行します。デフォルトの動作では、いずれかのメソッドで認証が拒否された場合は認証失敗となり、以降のメソッドは実行されません。**AAA Authentication Control Sufficient** の設定を **Enabled** にすると、総当たりでメソッドを実行し、認証が拒否されても引き続き以降のメソッドで認証処理が行われます。

本画面の各項目の説明を以下に示します。

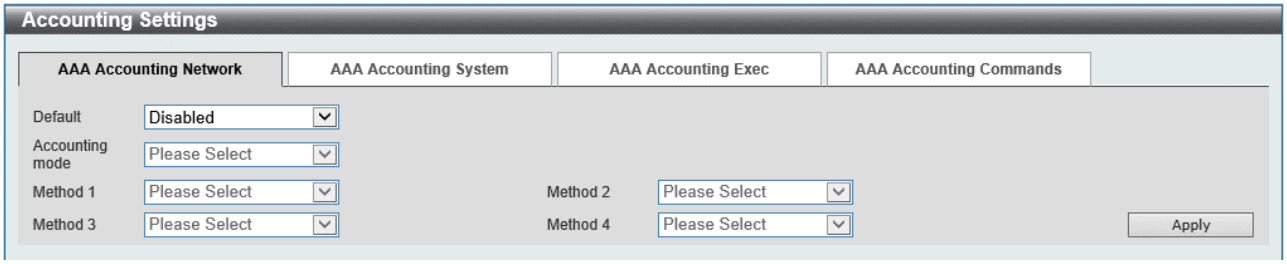
パラメーター	説明
Web	**Enabled** を選択すると、Web 認証の認証処理をメソッドリストの総当たりで実行します。
MAC	**Enabled** を選択すると、MAC 認証の認証処理をメソッドリストの総当たりで実行します。
Login	**Enabled** を選択すると、ログイン認証の認証処理をメソッドリストの総当たりで実行します。

設定を適用するには、**Apply** ボタンをクリックします。

9.3.5 Accounting Settings

Accounting Settings 画面では、Network アカウンティングと System アカウンティングの方式を設定します。また、CLI の Exec アカウンティングと Command アカウンティングのメソッドリストのプロファイルを登録します。

本画面を表示するには、**Security** > **AAA** > **Accounting Settings** をクリックします。



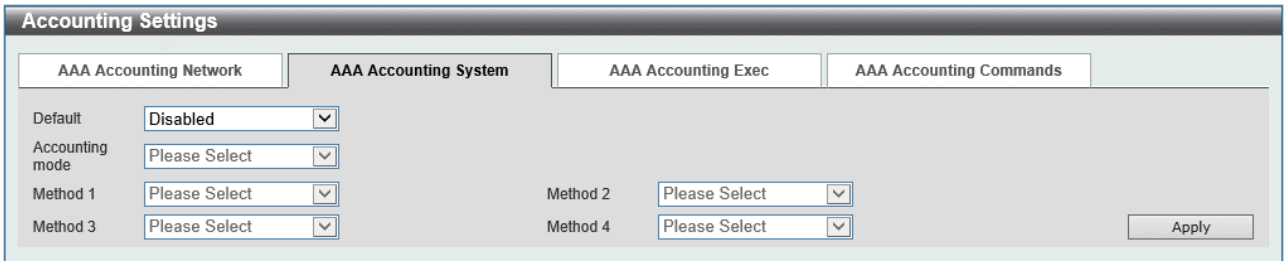
本画面には、**AAA Accounting Network** タブ、**AAA Accounting System** タブ、**AAA Accounting Exec** タブ、および **AAA Accounting Commands** タブがあります。

AAA Accounting Network タブでは、Network アカウンティングのモードやメソッドリストを設定します。各項目の説明を以下に示します。

パラメーター	説明
Default	**Enabled** を選択すると、以下の各項目で設定したモードとメソッドリストで Network アカウンティングが有効になります。
Accounting mode	Network アカウンティングのモードを以下のいずれかから選択します。 • **none**：Network アカウンティングの処理を行いません。 • **start-stop**：Network アカウンティングを有効にし、アクセスの開始時と終了時にアカウンティングメッセージを送信します。アカウンティング開始メッセージでアカウンティングが有効になるかどうかに関わらず、ユーザーはネットワークにアクセスできます。 • **stop-only**：Network アカウンティングを有効にし、アクセス終了時にアカウンティングメッセージを送信します。
Method 1 ～ Method 4	各メソッドの照会方法（**group** / **radius** / **tacacs+**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

AAA Accounting System タブでは System アカウンティングのメソッドリストを設定します。以下に示す画面が表示されます。

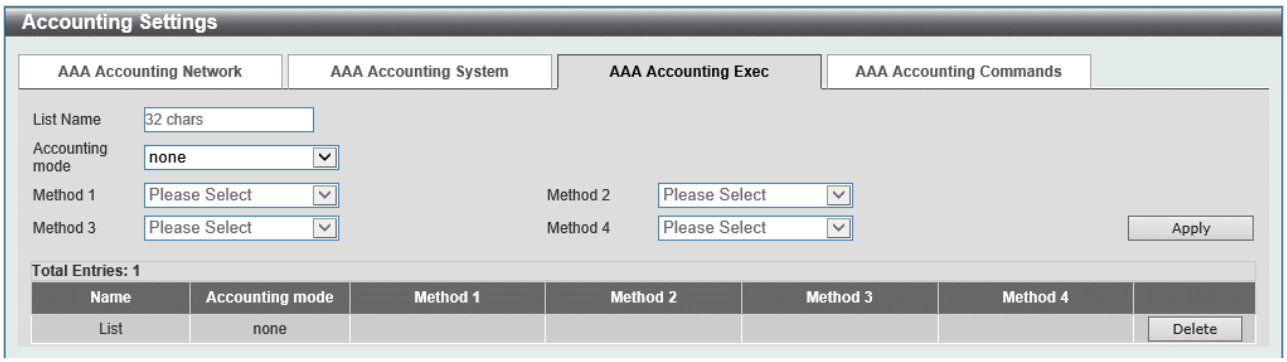


本画面の各項目の説明を以下に示します。

パラメーター	説明
Default	Enabled を選択すると、以下の各項目で設定したモードとメソッドリストで System アカウンティングが有効になります。
Accounting mode	System アカウンティングモードを以下のいずれかから選択します。 • none：System アカウンティングの処理を行いません • start-stop：System アカウンティングを有効にします。
Method 1 ～ Method 4	各メソッドの照会方法（group / radius / tacacs+）を選択します。

設定を適用するには、Apply ボタンをクリックします。

AAA Accounting Exec タブでは、Exec アカウンティングのメソッドリストのプロファイルを登録します。以下に示す画面が表示されます。

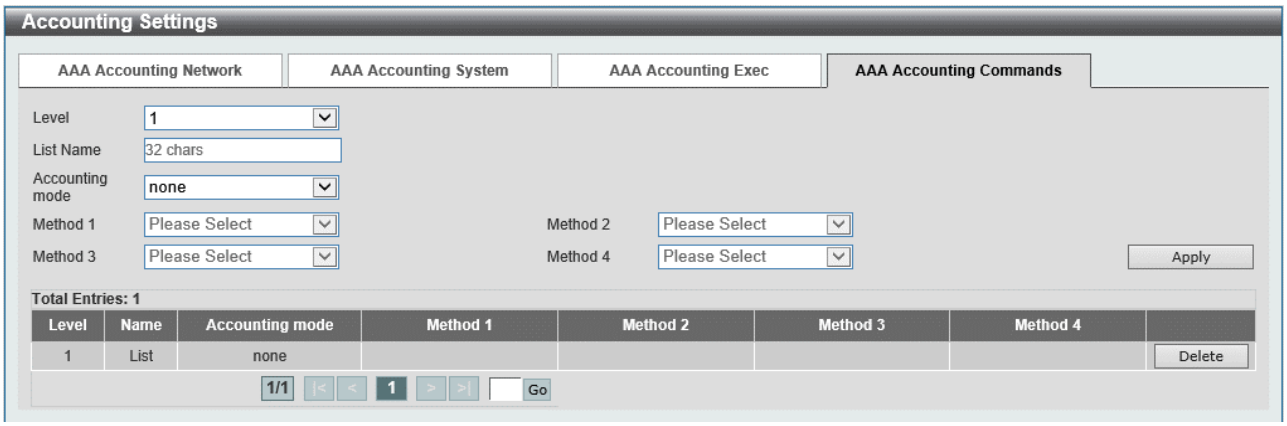


本画面の各項目の説明を以下に示します。

パラメーター	説明
List Name	Exec アカウンティングのメソッドリストのプロファイル名を入力します。
Accounting mode	Exec アカウンティングのモードを以下のどちらかから選択します。 • none：Exec アカウンティングの処理を行いません。 • start-stop：Exec アカウンティングを有効にします。
Method 1 ～ Method 4	各メソッドの照会方法（group / radius / tacacs+）を選択します。

設定を適用するには、Apply ボタンをクリックします。
登録したメソッドリストのプロファイルを削除するには、Delete ボタンをクリックします。

AAA Accounting Commands タブでは Command アカウンティングのメソッドリストのプロファイルを登録します。以下に示す画面が表示されます。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Level	特権レベルを 1～15 から選択します。指定した特権レベルで使用可能なコマンドが対象になります。
List Name	Command アカウンティングのメソッドリストのプロファイル名を入力します。
Accounting mode	Command アカウンティングのモードを以下のどちらかから選択します。 • **none**：Command アカウンティングの処理を行いません。 • **start-stop**：Command アカウンティングを有効にします。
Method 1 ～ Method 4	各メソッドの照会方法（**group** / **radius** / **tacacs+**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。
登録したメソッドリストのプロファイルを削除するには、**Delete** ボタンをクリックします。

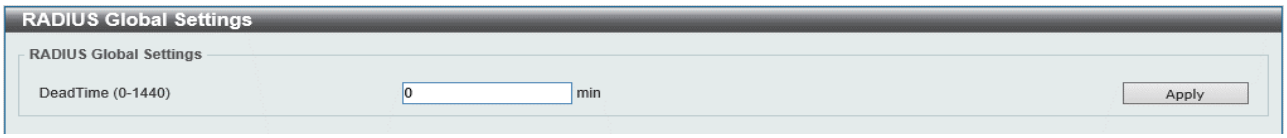
9.4 RADIUS

RADIUS サブメニューでは、RADIUS サーバーの設定を行います。
RADIUS の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.4.1	RADIUS Global Settings	RADIUS サーバーに関するグローバル設定
9.4.2	RADIUS Server Settings	RADIUS サーバーの登録
9.4.3	RADIUS Group Server Settings	RAIDUS サーバーグループの登録
9.4.4	RADIUS Statistic	RADIUS 統計情報の表示

9.4.1 RADIUS Global Settings

RADIUS Global Settings 画面では、RADIUS サーバーに関するグローバル設定を行います。
本画面を表示するには、Security > RADIUS > RADIUS Global Settings をクリックします。



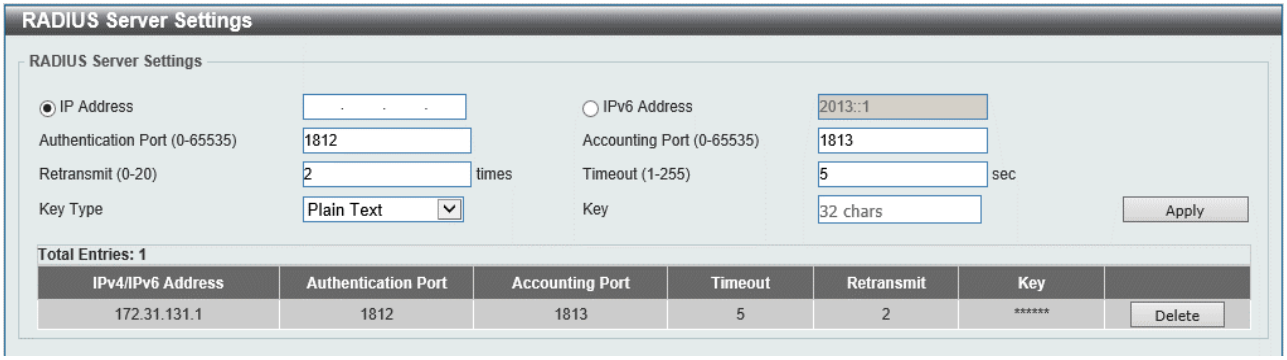
本画面の各項目の説明を以下に示します。

パラメーター	説明
DeadTime	RADIUS サーバーのデッドタイムを 0～1440（分）の範囲で入力します。このパラメーターは、認証問い合わせに対して RADIUS サーバーから応答がない場合に、RADIUS サーバーをダウンとみなす期間を示します。ダウンとみなされた RADIUS サーバーに対する認証問い合わせは、デッドタイマーが満了するまでは見送られます。複数の RADIUS サーバーを照会先に登録している場合に、サーバーダウン発生時に問い合わせをキャンセルすることで、認証処理プロセスを改善します。0 が設定された場合は、デッドタイマーによる処理は行いません。

設定を適用するには、Apply ボタンをクリックします。

9.4.2 RADIUS Server Settings

RADIUS Server Settings 画面では、RADIUS サーバーを登録します。
本画面を表示するには、Security > RADIUS > RADIUS Server Settings をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
IP Address	RADIUS サーバーの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバーの IPv6 アドレスを入力します。
Authentication Port	RADIUS 認証の UDP ポート番号を 0～65535 の範囲で入力します。 認証を使用しない場合は、0 を入力します。
Accounting Port	アカウンティングの UDP ポート番号を 0～65535 の範囲で入力します。 アカウンティングを使用しない場合は、0 を入力します。
Retransmit	再送処理の回数を 0～20 の範囲で入力します（デフォルト：2）。 再送を行わない場合は、0 を入力します。
Timeout	RADIUS サーバーの応答待ち時間を 1～255（秒）の範囲で入力します。
Key Type	共有鍵の入力タイプ（Plain Text / Encrypted）を選択します。
Key	RADIUS サーバーとの通信に使用する共有鍵を登録します。Key Type で選択した入力タイプに応じて入力します。

設定を適用するには、Apply ボタンをクリックします。
RADIUS サーバーを削除するには、Delete ボタンをクリックします。

9.4.3 RADIUS Group Server Settings

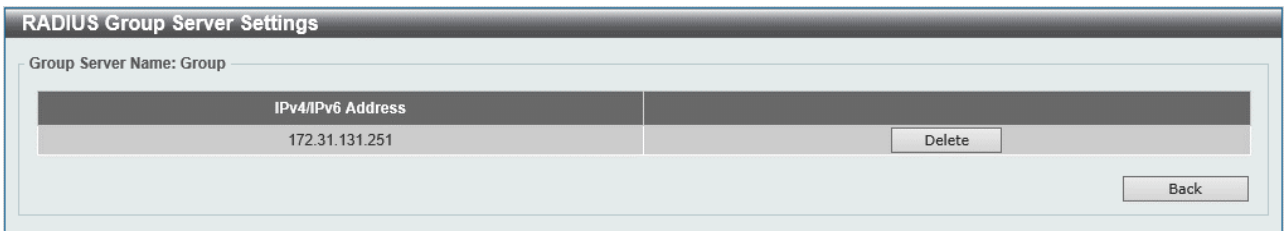
RADIUS Group Server Settings 画面では、RADIUS サーバーグループを設定します。
本画面を表示するには、**Security** > **RADIUS** > **RADIUS Group Server Settings** をクリックします。

本画面の各項目の説明を以下に示します。

パラメーター	説明
Group Server Name	RADIUS サーバーグループ名を 32 文字以内で入力します。
IP Address	追加する RADIUS サーバーの IPv4 アドレスを入力します。
IPv6 Address	追加する RADIUS サーバーの IPv6 アドレスを入力します。

入力した情報で RADIUS サーバーグループや RADIUS サーバーを追加するには、**Add** ボタンをクリックします。
RADIUS サーバーグループの詳細を表示するには、**Detail** ボタンをクリックします。
RADIUS サーバーグループを削除するには、**Delete** ボタンをクリックします。

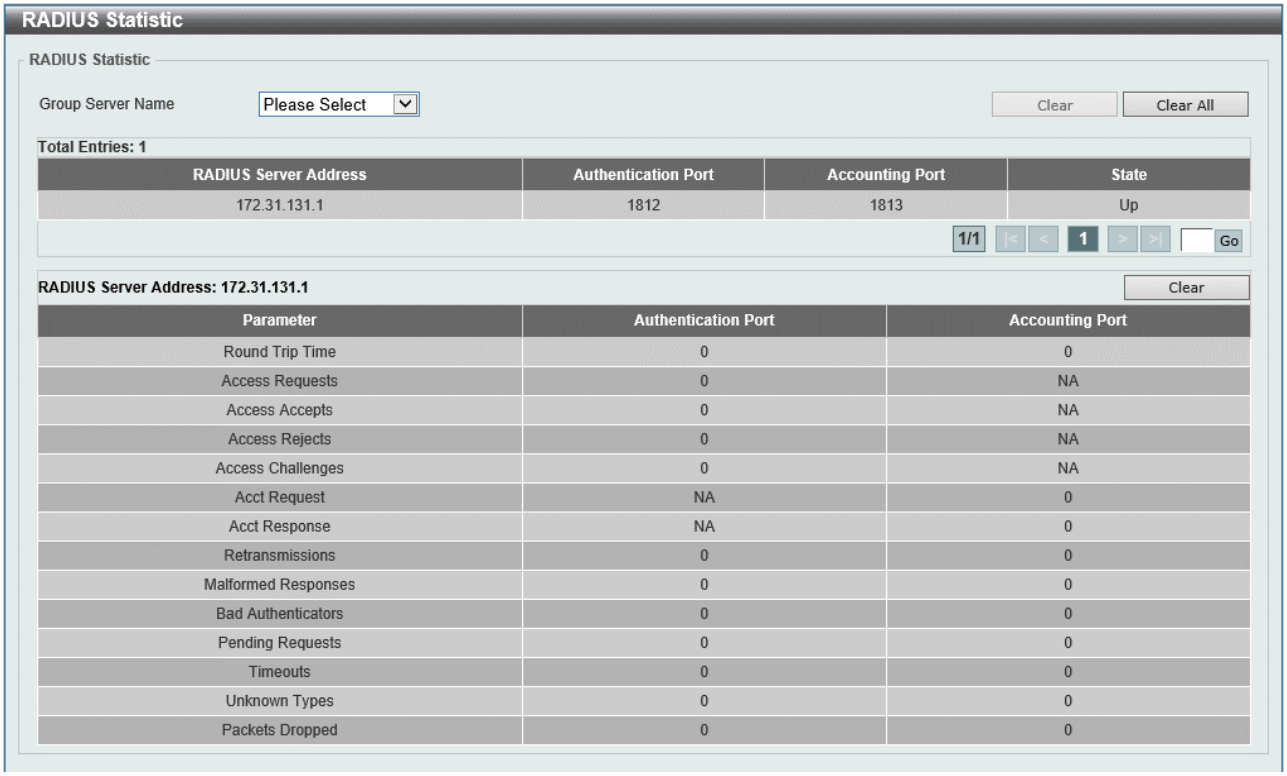
Detail ボタンをクリックすると、次のページが表示されます。



RADIUS サーバーグループから RADIUS サーバーを削除するには、**Delete** ボタンをクリックします。
前の画面に戻るには、**Back** ボタンをクリックします。

9.4.4 RADIUS Statistic

RADIUS Statistic 画面では、RADIUS 統計情報を表示およびクリアします。
本画面を表示するには、Security > RADIUS > RADIUS Statistic をクリックします。



本画面では、RADIUS サーバー一覧を表示するテーブルと、認証およびアカウンティングの統計情報を表示するテーブルの 2 種類が表示されます。RADIUS サーバー一覧のテーブル上で RADIUS サーバーの行をクリックすると、統計情報表示テーブルで該当するサーバーの統計情報が表示されます。

本画面の各項目の説明を以下に示します。

パラメーター	説明
Group Server Name	RADIUS グループサーバー名を選択します。

選択した RADIUS サーバーグループの統計情報をクリアするには、ドロップダウンリストの行の右端の Clear ボタンをクリックします。
すべての RADIUS サーバーの統計情報をクリアするには、Clear All ボタンをクリックします。
特定の RADIUS サーバーの統計情報をクリアするには、統計情報テーブルの Clear ボタンをクリックします。

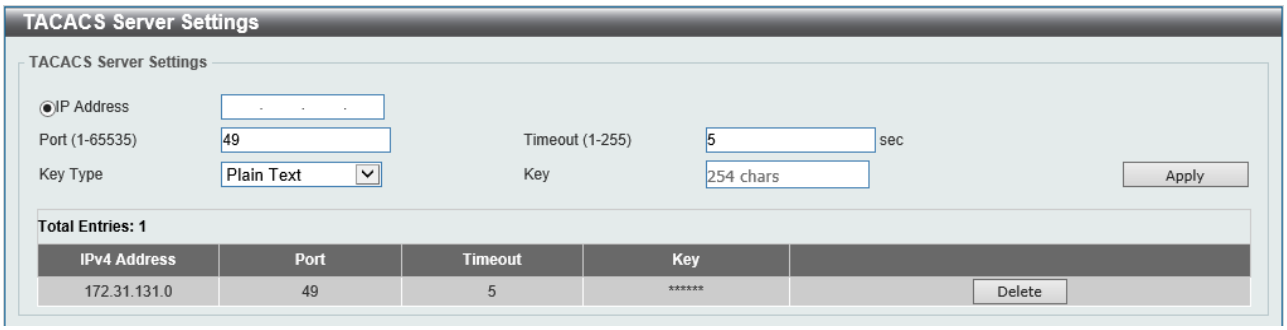
9.5 TACACS

TACACS サブメニューでは、TACACS+サーバーの設定を行います。
TACACS の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.5.1	TACACS Server Settings	TACACS+サーバーの登録
9.5.2	TACACS Group Server Settings	TACACS+サーバーグループの登録
9.5.3	TACACS Statistic	TACACS+統計情報の表示

9.5.1 TACACS Server Settings

TACACS Server Settings 画面では、TACACS+サーバーを登録します。
本画面を表示するには、Security > TACACS > TACACS Server Settings をクリックします。



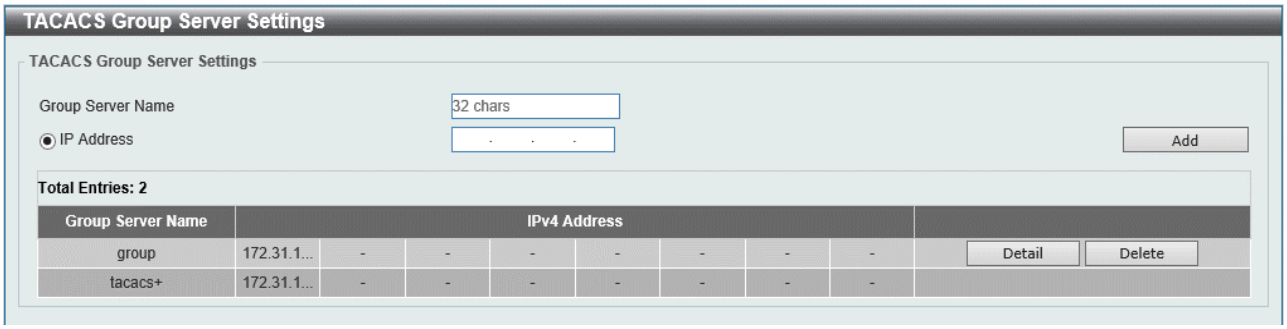
本画面の各項目の説明を以下に示します。

パラメーター	説明
IP Address	TACACS+サーバーの IPv4 アドレスを入力します。
Port	TACACS+で使用する TCP ポート番号を 1～65535 の範囲で入力します。
Timeout	TACACS+サーバーの応答待ち時間を 1～255（秒）の範囲で入力します。
Key Type	共有鍵の入力タイプ（Plain Text / Encrypted）を選択します。
Key	TACACS+サーバーとの通信に使用する共有鍵キーを登録します。Key Type で選択した入力タイプに応じて入力します。

設定を適用するには、Apply ボタンをクリックします。
TACACS+サーバーを削除するには、Delete ボタンをクリックします。

9.5.2 TACACS Group Server Settings

TACACS Group Server Settings 画面では、TACACS+サーバーグループを設定します。
本画面を表示するには、**Security** > **TACACS** > **TACACS Group Server Settings** をクリックします。

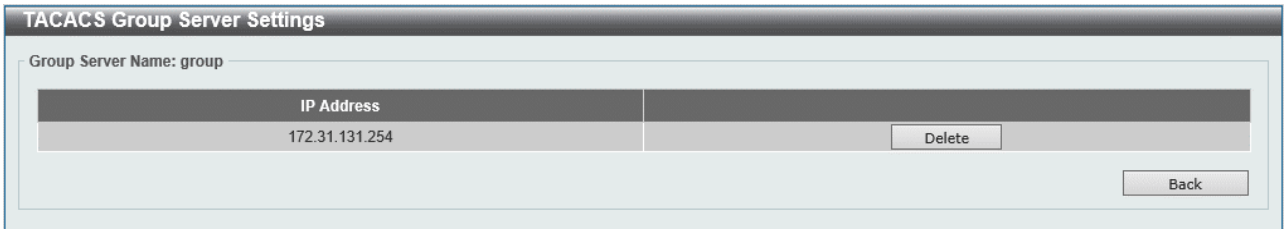


本画面の各項目の説明を以下に示します。

パラメーター	説明
Group Server Name	TACACS+サーバーグループ名を 32 文字以内で入力します。
IP Address	TACACS+サーバーの IPv4 アドレスを入力します。

入力した情報で TACACS+サーバーグループや TACACS+サーバーを追加するには、**Add** ボタンをクリックします。
TACACS+サーバーグループ詳細を表示するには、**Detail** ボタンをクリックします。
TACACS+サーバーグループを削除するには、**Delete** ボタンをクリックします。

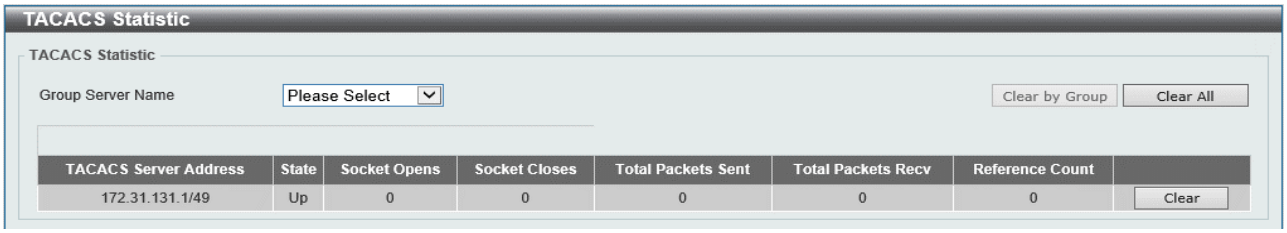
Detail ボタンをクリックすると、以下に示す画面が表示されます。



TACACS+サーバーを削除するには、**Delete** ボタンをクリックします。
前の画面に戻るには、**Back** ボタンをクリックします。

9.5.3 TACACS Statistic

TACACS Statistic 画面では、TACACS+統計情報を表示およびクリアします。
本画面を表示するには、Security > TACACS > TACACS Statistic をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Group Server Name	TACACS グループサーバー名を選択します。

選択した TACACS+サーバーグループの統計情報をクリアするには、Clear by Group ボタンをクリックします。
すべての TACACS+サーバーグループの統計情報をクリアするには、Clear All ボタンをクリックします。
特定の TACACS+サーバーの統計情報をクリアするには、Clear ボタンをクリックします。

9.6 DHCP Snooping

DHCP Snooping サブメニューでは、DHCP スヌーピング機能の設定を行います。
DHCP スヌーピングは、接続する端末が IP アドレスを取得するための DHCP パケットのやり取りをモニタリングし、正常に取得した端末のみ通信を許可する機能です。端末情報はバインディングデータベースというテーブルに登録され、DHCP スヌーピングが動作するポートではバインディングデータベースを参照して通信の可否を決定します。

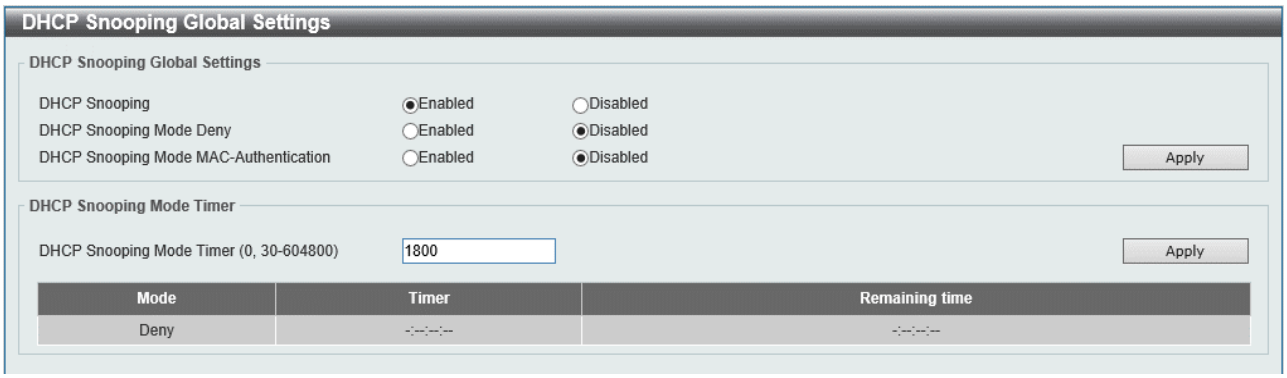
運用中の装置に対して DHCP スヌーピングを有効に切り替えてフィルタリングを動作させると、その時点ではバインディングデータベースに登録がないため、IP アドレスの再取得が行われるまですべての端末の通信が遮断されます。これを回避するために、一定期間 DHCP パケットのモニタリングのみを実施してフィルタリングを行わない「PERMIT モード」を使用できます。PERMIT モードは所定のタイマーで DENY モードに切り替わり、それ以降はフィルタリングが行われます。

DHCP Snooping の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.6.1	DHCP Snooping Global Settings	DHCP スヌーピング機能のグローバル設定
9.6.2	DHCP Snooping Binding Entry	バインディングデータベースの登録
9.6.3	DHCP Snooping Interface	DHCP スヌーピング機能のポート設定
9.6.4	DHCP Snooping Static Entry	スタティックエントリーの登録

9.6.1 DHCP Snooping Global Settings

DHCP Snooping Global Settings 画面では、DHCP スヌーピング機能全体に関する項目を設定します。
本画面を表示するには、**Security > DHCP Snooping > DHCP Snooping Global Settings** をクリックします。



DHCP Snooping Global Settings の各項目の説明を以下に示します。

パラメーター	説明
DHCP Snooping	DHCP スヌーピングの状態（Enabled / Disabled）を選択します。
DHCP Snooping Mode Deny	このパラメーターが Disabled の場合、DHCP スヌーピング機能の起動時には PERMIT モードで動作します。このパラメーターが Enabled の場合、最初から DENY モードで動作します。
DHCP Snooping Mode MAC-Authentication	このパラメーターが Enabled の場合、MAC 認証を併用するポートで先行して MAC 認証を実施し、成功した後で DHCP スヌーピングによる制御を行います。Disabled の場合、双方の機能は連動しません。

設定を適用するには、Apply ボタンをクリックします。

DHCP Snooping Mode Timer の各項目の説明を以下に示します。

パラメーター	説明
DHCP Snooping Mode Timer	PERMIT モードから DENY モードに切り替わるまでの時間（秒）を 30～604800 の範囲で指定します。0 の場合は切り替えが行われません。

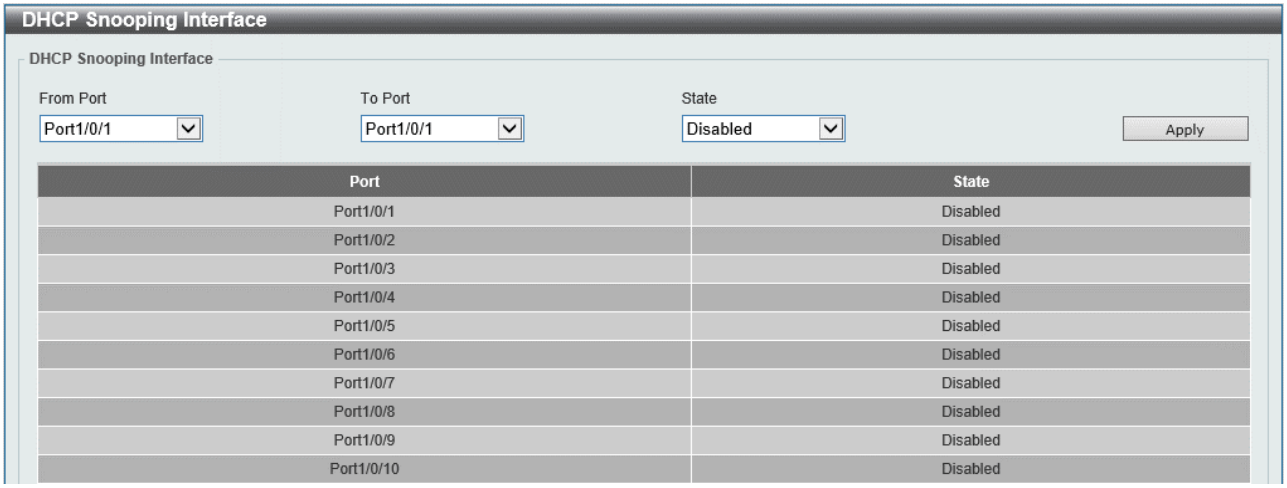
設定を適用するには、Apply ボタンをクリックします。

9.6.2 DHCP Snooping Binding Entry

DHCP Snooping Binding Entry 画面では、バインディングデータベースを表示します。
本画面を表示するには、Security > DHCP Snooping > DHCP Snooping Binding Entry をクリックします。

9.6.3 DHCP Snooping Interface

DHCP Snooping Interface 画面では、物理ポート単位で DHCP スヌーピングの動作を設定します。
本画面を表示するには、Security > DHCP Snooping > DHCP Snooping Interface をクリックします。



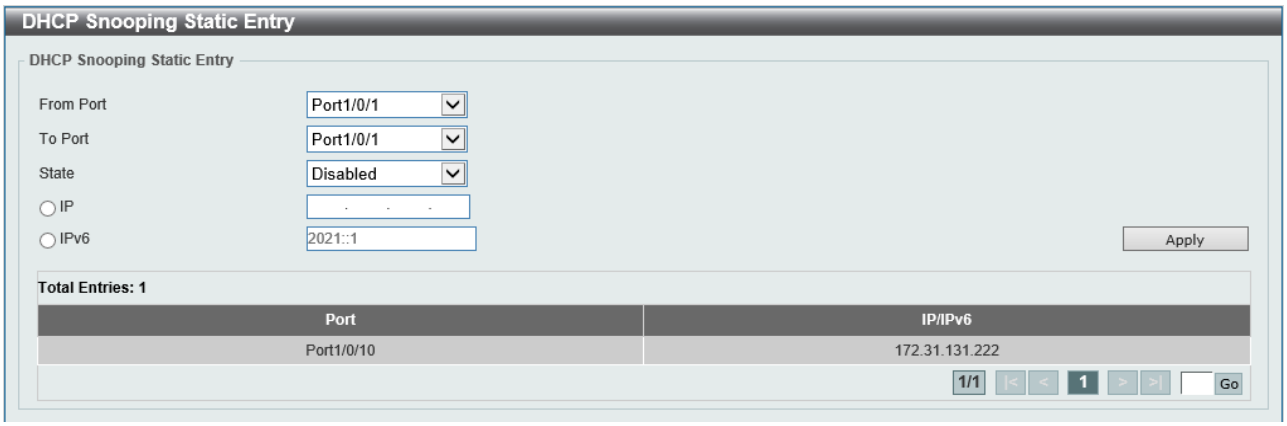
本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
State	DHCP スヌーピング機能の状態（Enabled / Disabled）を選択します。

設定を適用するには、Apply ボタンをクリックします。

9.6.4 DHCP Snooping Static Entry

DHCP Snooping Static Entry 画面では、DHCP スヌーピングのスタティックエントリーを設定します。
本画面を表示するには、Security > DHCP Snooping > DHCP Snooping Static Entry をクリックします。



本画面の各項目の説明を以下に示します。

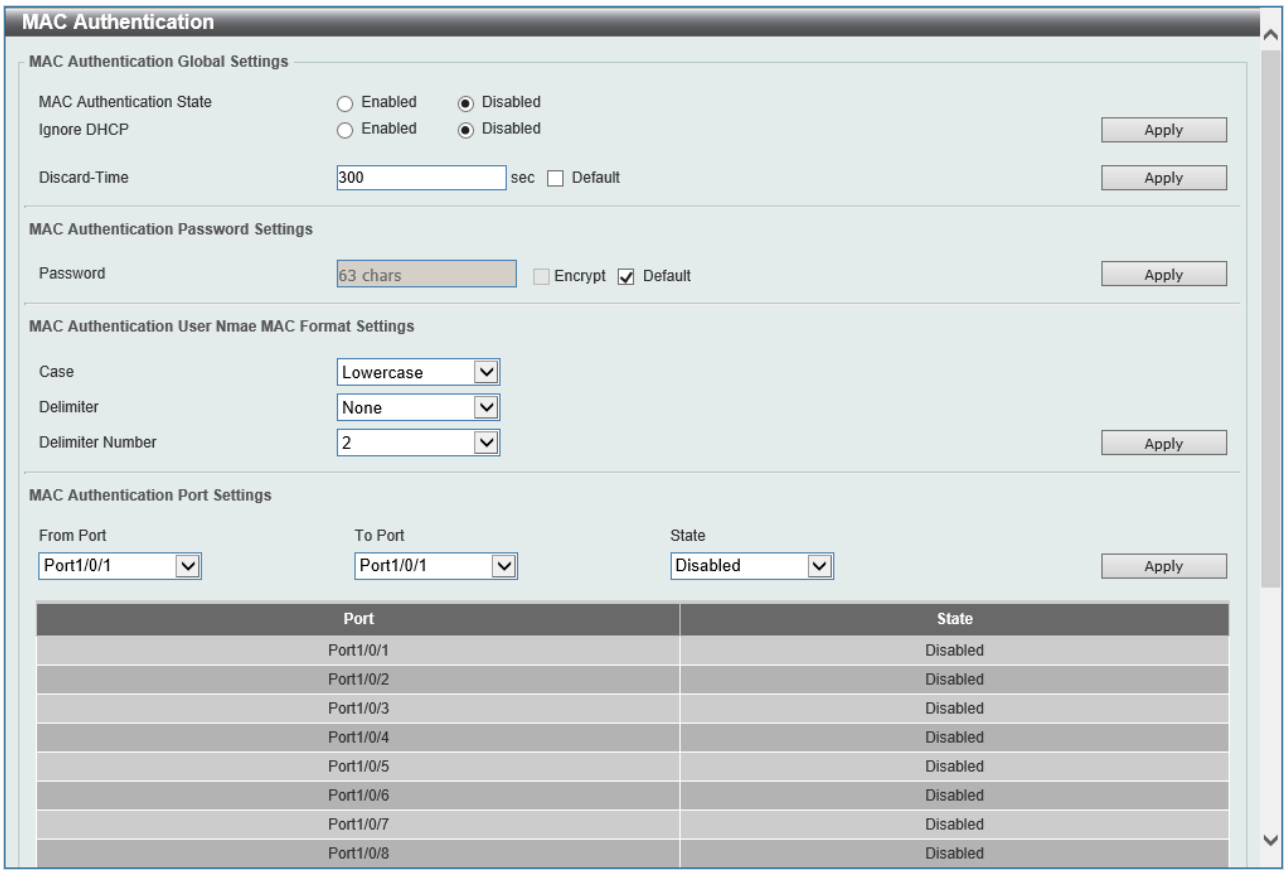
パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
State	スタティックエントリーを登録する場合は Enabled を選択します。削除する場合は Disabled を選択します。
IP	スタティックエントリーの IPv4 アドレスを入力します。
IPv6	スタティックエントリーの IPv6 アドレスを入力します。

スタティックエントリーの追加、削除を行うには、Apply ボタンをクリックします。

9.7 MAC Authentication

MAC Authentication 画面では、ポートアクセス認証の MAC アドレスベース認証（以後、MAC 認証）を設定します。

本画面を表示するには、**Security** > **MAC Authentication** をクリックします。



MAC Authentication Global Settings の各項目の説明を以下に示します。

パラメーター	説明
MAC Authentication State	MAC 認証機能のグローバル状態（**Enabled** / **Disabled**）を選択します。**Enabled** の場合、MAC 認証機能が有効になります。
Ignore DHCP	このパラメーターが **Enabled** の場合、DHCP パケットは MAC 認証のアクセス制御の対象にはなりません。**Disabled** の場合は、DHCP パケットもアクセス制御の対象に含まれます。
Discard-Time	MAC 認証の認証ブロック時間を 300～86400 秒の範囲で指定します。デフォルト値（300 秒）に戻す場合は、**Default** をチェックします。MAC 認証に失敗した端末は Discard 状態として登録され、本パラメーターで指定するブロック時間が満了するまで、認証を行いません。

設定を適用するには、**Apply** ボタンをクリックします。

MAC Authentication Password Settings の各項目の説明を以下に示します。

パラメーター	説明
Password	MAC 認証のパスワードを設定します。本パラメーターで **Default** がチェックされている状態では、MAC 認証のパスワードは MAC アドレス自体を使用します。**Default** がチェックされていない場合、共通パスワードと呼ばれるすべての MAC アドレスで共通のパスワードを使用します。使用する共通パスワードは、**Encrypt** がチェックされている場合は暗号化方式で、**Encrypt** がチェックされていない場合は平文で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

MAC Authentication User Name MAC Format Settings の各項目の説明を以下に示します。

パラメーター	説明
Case	MAC 認証の照会で使用するユーザー名の文字形式（**Lowercase** / **Uppercase**）を選択します。**Lowercase** の場合は MAC アドレスのアルファベットがすべて小文字になり、**Uppercase** では大文字になります。
Delimiter	MAC 認証の照会でのユーザー名の MAC アドレスの区切り文字（**Hyphen** / **Colon** / **Dot** / **None**）を選択します。**Hyphen** はハイフン「-」を、Colon ではコロン「:」を、**Dot** ではドット「.」を使用します。**None** は区切り文字を使用しません。
Delimiter Number	使用する区切り文字の数（**1** / **2** / **5**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

MAC Authentication Port Settings の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
State	選択したポートの MAC 認証の状態（**Enabled** / **Disabled**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

9.8 Web Authentication

Web Authentication サブメニューでは、ポートアクセス認証の Web ブラウザーによる認証（以後、Web 認証）の設定を行います。

Web 認証機能を使用すると、装置が未認証端末からの外部 Web サイトへのアクセスを検知した場合に、そのトラフィックを終端します。Web 認証リダイレクトオプションを使用すると、未認証端末との間に一種のなりすましによる偽装セッションを確立し、HTTP リダイレクトで Web 認証を行うための認証サイトに誘導します。
未認証端末は、Web ブラウザーの直接アクセス、または Web 認証リダイレクトオプションを用いた HTTP リダイレクトによる誘導によって認証サイトにアクセスし、認証に成功するまではポートへのアクセスが制限されます。

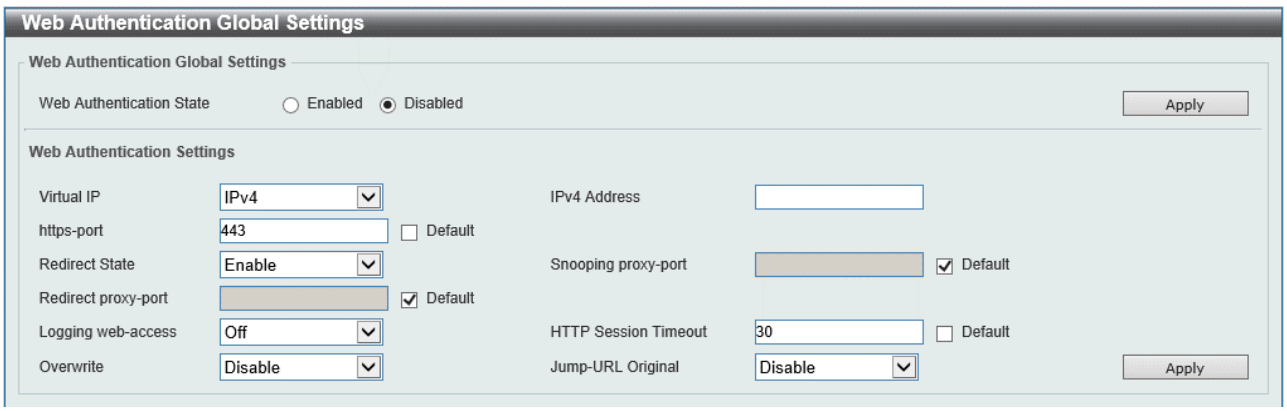
Web 認証の認証サイトには、外部サーバーの Web 認証ポータル、または装置内部の Web 認証ポータルを使用します。装置内部の Web 認証ポータルは、設定した仮想 IP アドレスに紐付けられた疑似的な Web サイトです。未認証端末が仮想 IP アドレスにアクセスする際、仮想 IP アドレスが同一ネットワーク上に存在しない場合には、デフォルトゲートウェイを中継ターゲットにしてトラフィックを送信します。装置は、このトラフィックを傍受し、仮想 IP アドレスを使用した疑似セッションを確立することで、未認証端末に対して認証ポータルを提供します。

Web Authentication の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.8.1	Web Authentication Global Settings	Web 認証のグローバル設定
9.8.2	Web Authentication Port Settings	Web 認証のポート設定

9.8.1 Web Authentication Global Settings

Web Authentication Global Settings 画面では、Web 認証機能のグローバル設定を行います。
本画面を表示するには、**Security > Web Authentication > Web Authentication Global Settings** をクリックします。



Web Authentication Global Settings の各項目の説明を以下に示します。

パラメーター	説明
Web Authentication State	Web 認証機能のグローバル設定（**Enabled** / **Disabled**）を選択します。**Enabled** の場合、Web 認証機能が有効になります。

設定を適用するには、**Apply** ボタンをクリックします。

Web Authentication Settings の各項目の説明を以下に示します。

パラメーター	説明
Virtual IP	仮想 IP アドレスとタイプを以下のいずれかから選択します。 • **IPv4**：IPv4 アドレスを使用する場合に選択します。 　○ **IPv4 Address**：仮想 IPv4 アドレスを入力します。 • **IPv6**：IPv6 アドレスを使用する場合に選択します。 　○ **IPv6 Address**：仮想 IPv6 アドレスを入力します。 • **URL**：仮想 URL を使用する場合に選択します。 　○ **Virtual URL**：仮想 URL を入力します。
https-port	HTTPS の TCP ポート番号を入力します。デフォルト（443）に戻す場合は、**Default** をチェックします。
Redirect State	Web 認証リダイレクトの状態を以下のいずれかから選択します。 • **Disabled**：Web 認証リダイレクトを無効にします。 • **Disabled HTTP**：HTTP の Web 認証リダイレクトを無効にします。 • **Disabled HTTPS**：HTTPS の Web 認証リダイレクトを無効にします。 • **Enabled**：HTTP/HTTPS の Web 認証リダイレクトを有効にします。
Snooping proxy-port	HTTP プロキシのプロキシポート番号を入力します。このパラメーターを設定すると、HTTP 通信の検知や装置内部の Web 認証ポータルの待ち受けを、指定したポート番号でも行います。デフォルト（0:指定しない）に戻す場合は、**Default** をチェックします。
Redirect proxy-port	HTTP プロキシのプロキシポート番号を入力します。このパラメーターを設定すると、指定したポート番号での HTTP 通信を検知します。認証トラフィックの識別は行わないため、認証ポータルへのアクセスはプロキシを経由しない通信である必要があります。デフォルト（0:指定しない）に戻す場合は、**Default** をチェックします。
Logging web-access	このパラメーターが **On** の場合、Web 認証のアクセスログを有効になります。Web ブラウザー側が複数にセッション確立を試みた結果、同時に多数のログが表示されることがあります。**Off** の場合はアクセスログが記録されません。
HTTP Session Timeout	Web 認証ポータルの HTTP セッションタイムアウト時間を 5～60 秒の範囲で指定します。デフォルト（30 秒）に戻す場合は、**Default** をチェックします。
Overwrite	このパラメーターが **Enabled** の場合、認証済みのクライアントから別の Web 認証処理が行われた場合に上書きで処理します。**Disabled** の場合は上書きを行いません。
Jump-URL Original	このパラメーターが **Enabled** の場合、認証前にアクセスした URL にジャンプします。**Disabled** の場合はジャンプしません。

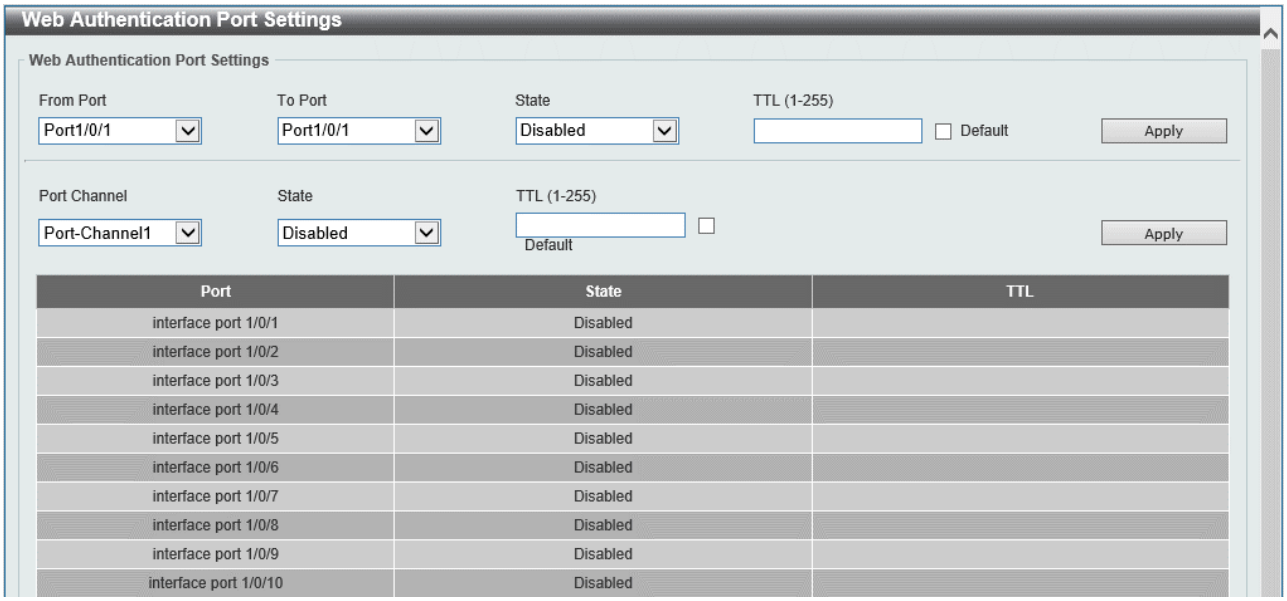
設定を適用するには、**Apply** ボタンをクリックします。

注意事項

仮想 IP が設定されていない場合、Web 認証が正しく機能しません。Web 認証を有効にする前に、Web 認証仮想 IP アドレスを設定してください。

9.8.2 Web Authentication Port Settings

Web Authentication Port Settings 画面では、物理ポート単位で Web 認証の状態を設定します。
本画面を表示するには、**Security** > **Web Authentication** > **Web Authentication Port Settings** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
State	選択したポートまたはポートチャネルの Web 認証機能の状態（**Enabled** / **Disabled**）を選択します。
TTL	このパラメーターを指定すると、TTL フィルターが有効になり、特定の TTL 値のパケットのみを Web 認証処理を可能とします。入力可能な TTL は 1～255 の範囲で、ポートあたり最大 8 個の値を登録できます。 デフォルト（指定なし）に戻す場合は、**Default** をチェックします。
Port Channel	ポートチャネルを選択します。

設定を適用するには、**Apply** ボタンをクリックします。

9.9 Network Access Authentication

Network Access Authentication サブメニューでは、ポートアクセス認証全般の動作に関する設定、ローカルユーザーデータベースの登録、および認証済みクライアント情報などのポートアクセス認証のステータスの表示などを行います。

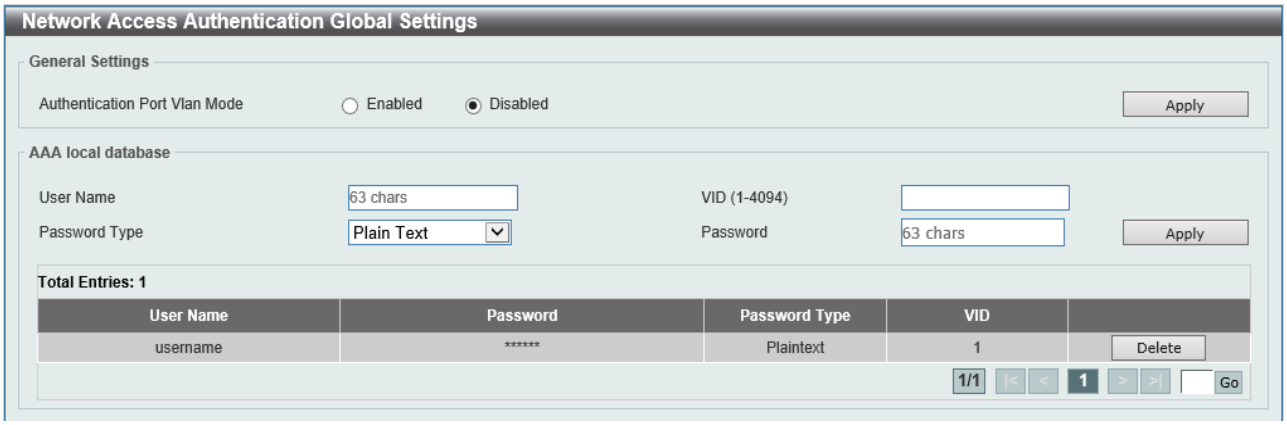
Network Access Authentication の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.9.1	Network Access Authentication Global Settings	ポートアクセス認証全般の動作に関する設定、およびローカルユーザーデータベースの登録
9.9.2	Network Access Authentication Sessions Information	ポートアクセス認証のセッション情報の表示

9.9.1 Network Access Authentication Global Settings

Network Access Authentication Global Settings 画面では、ポートアクセス認証全般の動作に関する設定や、ローカルユーザーデータベースの登録を行います。

本画面を表示するには、Security > Network Access Authentication > Network Access Authentication Global Settings をクリックします。



General Settings の各項目の説明を以下に示します。

パラメーター	説明
Authentication Port VLAN Mode	MAC 認証および IEEE802.1X 認証で動作するポート VLAN モードオプションを設定します。このパラメーターが Enabled の場合、認証属性によってダイナミックに割り当てられた VLAN をポートのアクセス VLAN またはネイティブ VLAN に変更します。この変更が行われると、異なる VLAN ID を認証属性とするホストの認証は許可されません。また、VLAN ID の認証属性を持たないホストの認証も、タグ付きフレームのみで通信を行うホストを除いて許可されません。

設定を適用するには、Apply ボタンをクリックします。

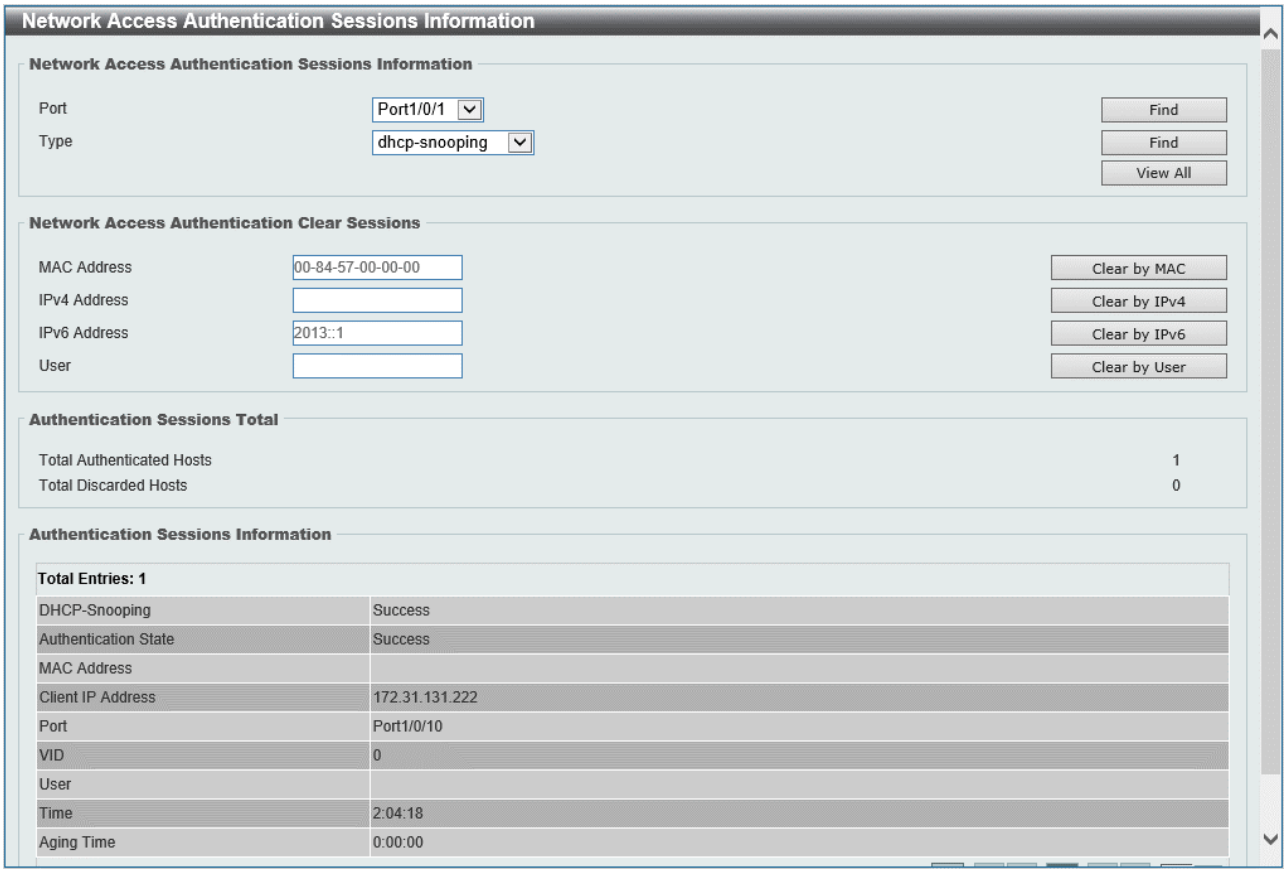
AAA local database の各項目の説明を以下に示します。

パラメーター	説明
User Name	ユーザー名を 63 文字以内で入力します。
VID	VLAN ID を 1～4094 の範囲で入力します。
Password Type	パスワードタイプ（Plain Text / Encrypted）を選択します。
Password	パスワードを入力します。

設定を適用するには、Apply ボタンをクリックします。
ネットワークアクセス認証を削除するには、Delete ボタンをクリックします。

9.9.2 Network Access Authentication Sessions Information

Network Access Authentication Sessions Information 画面では、ポートアクセス認証のセッション情報を表示します。また、認証済みホストの認証を解除します。
本画面を表示するには、Security > Network Access Authentication > Network Access Authentication Sessions Information をクリックします。



Network Access Authentication Sessions Information の各項目の説明を以下に示します。

パラメーター	説明
Port	検索するポート番号を選択します。
Type	検索するプロトコル（dhcp-snooping / disc / dot1x / mac / web）を選択します。

入力した情報でポートアクセス認証のセッション情報を検索するには、Find ボタンをクリックします。
すべてのポートアクセス認証のセッション情報を検索して表示するには、View All ボタンをクリックします。

Network Access Authentication Clear Sessions の各項目の説明を以下に示します。

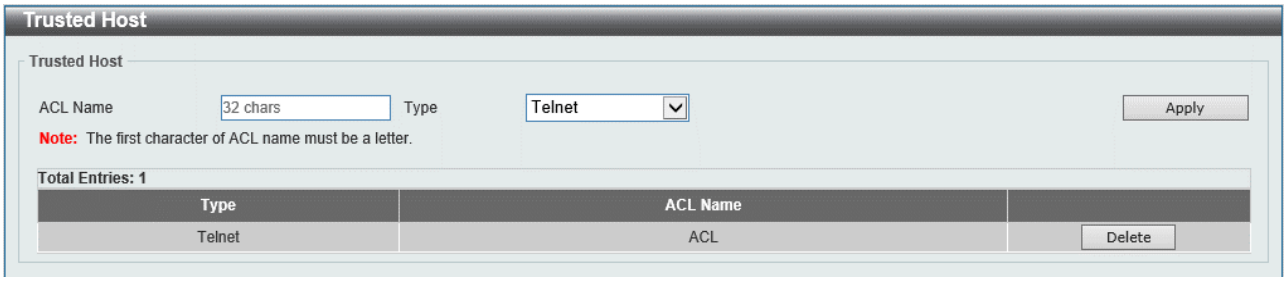
パラメーター	説明
MAC Address	ネットワークアクセス認証済みクライアントの MAC アドレスを入力します。
IPv4 Address	ネットワークアクセス認証済みクライアントの IPv4 アドレスを入力します。
IPv6 Address	ネットワークアクセス認証済みクライアントの IPv6 アドレスを入力します。
User	ネットワークアクセス認証済みクライアントのアカウントのユーザー名を入力します。

入力した MAC アドレスでポートアクセス認証のセッション情報をクリアするには、Clear by MAC ボタンをクリックします。
入力した IPv4 アドレスでポートアクセス認証のセッション情報をクリアするには、Clear by IPv4 ボタンをクリックします。
入力した IPv6 アドレスでポートアクセス認証のセッション情報をクリアするには、Clear by IPv6 ボタンをクリックします。
入力したユーザーアカウントでポートアクセス認証のセッション情報をクリアするには、Clear by User ボタンをクリックします。

9.10 Trusted Host

Trusted Host 画面では、アプリケーション（Telnet、SSH、および Ping）での装置のアクセスに対し、標準 IP ACL を使用して許可するホストを設定します。

本画面を表示するには、**Security** > **Trusted Host** をクリックします。



本画面の各項目の説明を以下に示します。

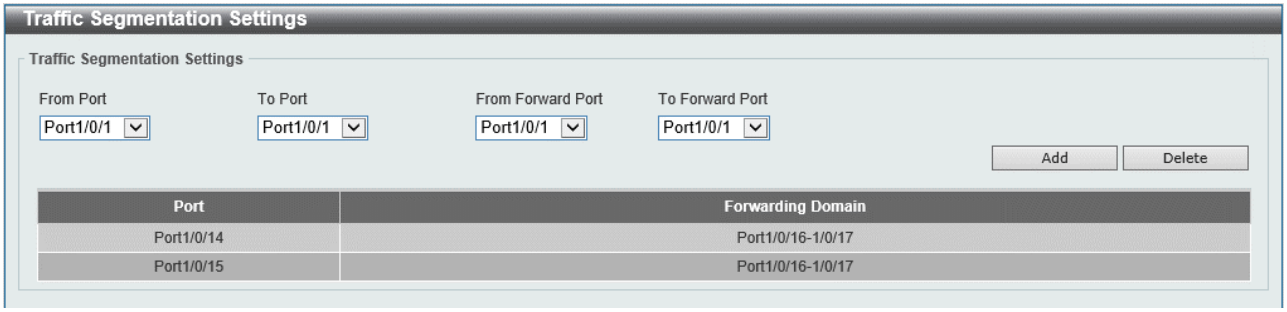
パラメーター	説明
ACL Name	適用する標準 IP ACL 名を 32 文字以内で入力します。
Type	適用するアプリケーションの種類（**Telnet** / **SSH** / **Ping**）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

トラストホストを削除するには、**Delete** ボタンをクリックします。

9.11 Traffic Segmentation Settings

Traffic Segmentation Settings 画面では、トラフィックセグメンテーションを設定します。トラフィックセグメンテーション機能は、受信したトラフィックの転送先ポートを制限できます。
本画面を表示するには、**Security** > **Traffic Segmentation Settings** をクリックします。



本画面の各項目の説明を以下に示します。

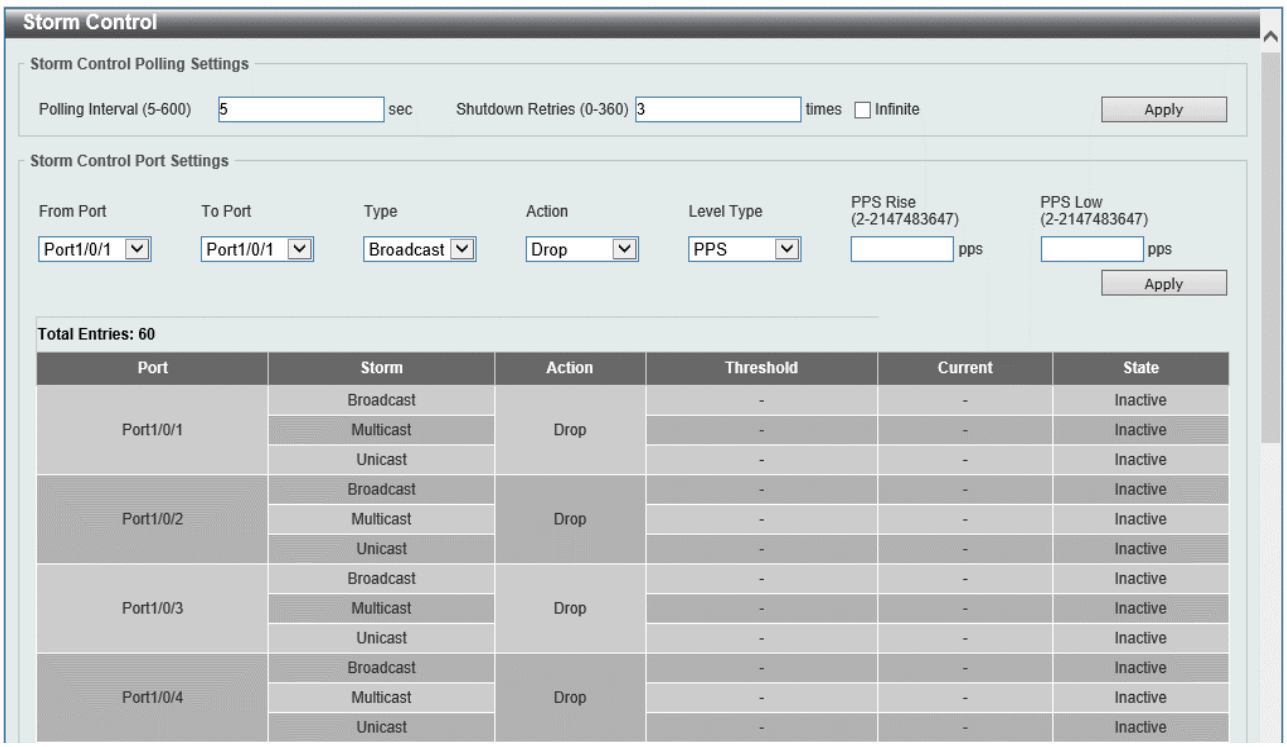
パラメーター	説明
From Port / To Port	受信ポートの範囲を選択します。
From Forward Port / To Forward Port	転送ポートの範囲を選択します。

入力した情報でトラフィックセグメンテーションを追加するには、**Add** ボタンをクリックします。
入力した情報でトラフィックセグメンテーションを削除するには、**Delete** ボタンをクリックします。

9.12 Storm Control

Storm Control 画面では、ストームコントロール機能の設定を行います。ストームコントロール機能では、ポートに所定の上限値を超える量のブロードキャストフレーム、マルチキャストフレーム、またはユニキャストフレームを受信したことを検知すると、ストーム発生状態に移行し、フレーム破棄やポートシャットダウンなどの処理を行います。ストーム発生状態の解消は、該当するトラフィック量が所定の下限値を下回ったことを検知した場合に行われます。

本画面を表示するには、Security > Storm Control をクリックします。



Storm Control Polling Settings の各項目の説明を以下に示します。

パラメーター	説明
Polling Interval	ストームコントロールのポーリング間隔を 5～600（秒）の範囲で入力します。
Shutdown Retries	Action が Shutdown の場合の、ポートシャットダウンまでの検知試行回数を 0～360 の範囲で入力します（デフォルト：3）。Infinite をチェックした場合、ポートシャットダウンは行いません。

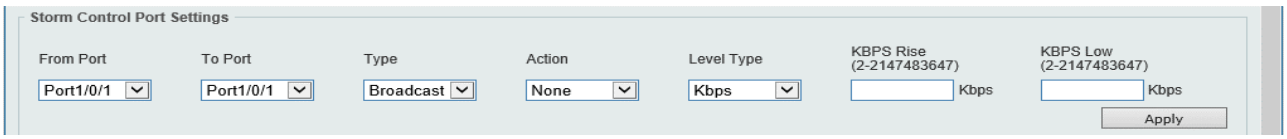
設定を適用するには、Apply ボタンをクリックします。

Storm Control Port Settings の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Type	ストームコントロールのタイプ（Broadcast / Multicast / Unicast）を選択します。 アクションがシャットダウンモードに設定されている場合、ユニキャストは既知と未知の両方のユニキャストパケットを参照します。これにより、既知と未知のユニキャストパケットが指定された上限値に達すると、ポートがシャットダウンされます。アクションがシャットダウンモード以外に設定されている場合、ユニキャストは未知のユニキャストパケットを参照します。
Action	実行するアクションを以下のいずれかから選択します。 • None：アクションを実施しません。 • Shutdown：ポートをシャットダウンします。 • Drop：上限値を超えるパケットをドロップする場合に選択します。
Level Type	ストームコントロールの上限値と下限値の基準（PPS / Kbps / Level）を選択します。
PPS Rise	Level Type が PPS の場合に表示されます。 ストームコントロールの上限値を pps（パケット/秒）で指定します。2～2147483647 の範囲で入力します。
PPS Low	Level Type が PPS の場合に表示されます。 ストームコントロールの下限値を pps で指定します。2～2147483647 の範囲で入力します。このパラメーターを指定しない場合、PPS Rise の 80%の値が使用されます。

設定を適用するには、Apply ボタンをクリックします。

Level Type で Kbps を選択した場合、Storm Control Port Settings の右 2 つの項目が以下のように変更されます。

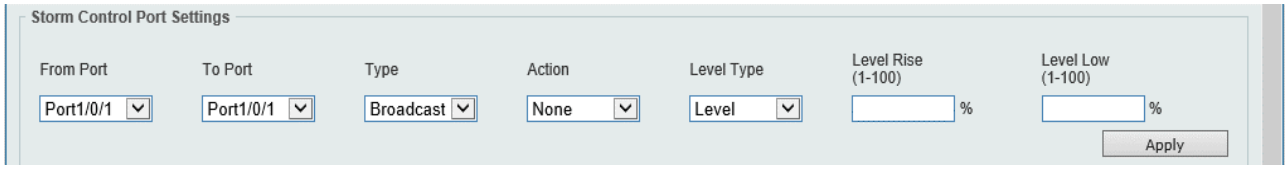


Level Type で Kbps を選択した場合の、Storm Control Port Settings の右 2 つの項目の説明を、以下に示します。

パラメーター	説明
KBPS Rise	ストームコントロールの上限値を kbps（キロビット/秒）で指定します。2～2147483647（Kbps）の範囲で入力します。
KBPS Low	ストームコントロールの下限値を kbps で指定します。2～2147483647（Kbps）の範囲で入力します。このパラメーターを指定しない場合、KBPS Rise の 80%の値が使用されます。

設定を適用するには、Apply ボタンをクリックします。

Level Type で **Level** を選択した場合、**Storm Control Port Settings** の右 2 つの項目が以下のように変更されます。



Level Type で **Level** を選択した場合の、**Storm Control Port Settings** の右 2 つの項目の説明を、以下に示します。

パラメーター	説明
Level Rise	ストームコントロールの上限値をポートの帯域に対する百分率(%)で指定します。1～100 の範囲で入力します。
Level Low	ストームコントロールの下限値をポートの帯域に対する百分率(%)で指定します。1～100 の範囲で入力します。このパラメーターを指定しない場合、**Level Rise** の 80%の値が使用されます。

設定を適用するには、**Apply** ボタンをクリックします。

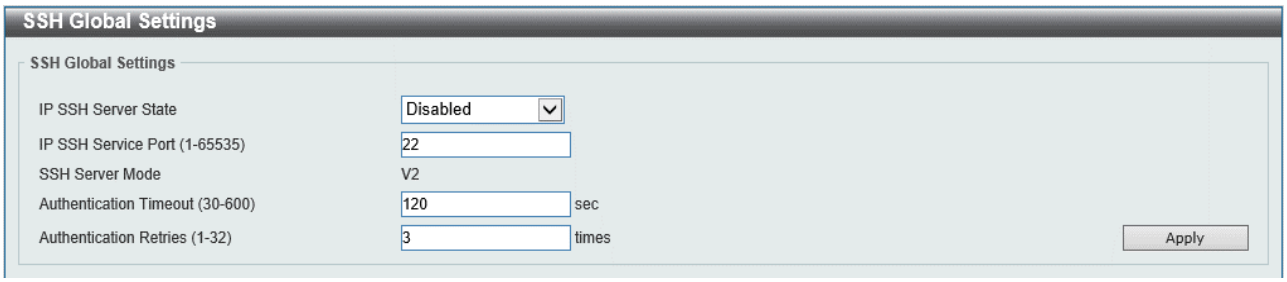
9.13 SSH

SSH サブメニューでは、CLI の SSH サーバー機能や SSH ユーザーに関する設定を行います。
SSH の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.13.1	SSH Global Settings	SSH サーバー機能のグローバル設定
9.13.2	Host Key	SSH ホスト鍵の作成
9.13.3	SSH Server Connection	SSH 接続テーブルの表示
9.13.4	SSH User Settings	SSH ユーザーの設定

9.13.1 SSH Global Settings

SSH Global Settings 画面では、SSH サーバー機能全般の設定を行います。
本画面を表示するには、Security > SSH > SSH Global Settings をクリックします。



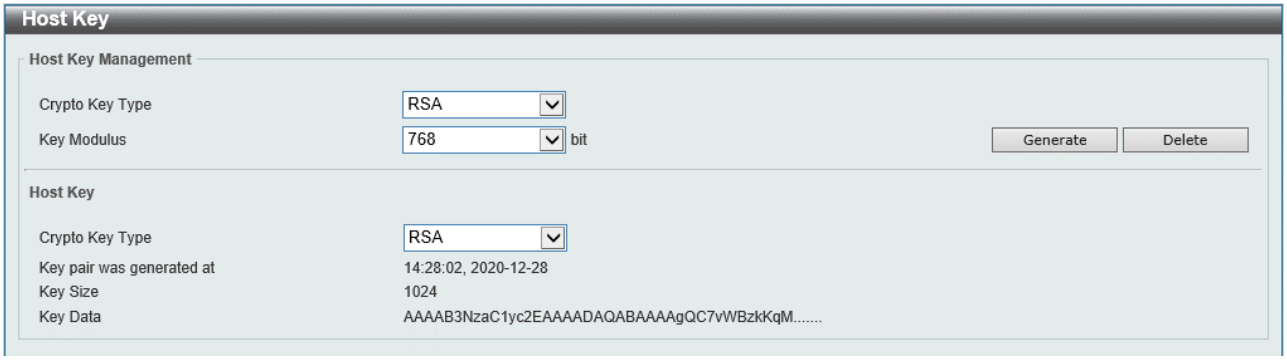
本画面の各項目の説明を以下に示します。

パラメーター	説明
IP SSH Server State	SSH サーバー機能の状態（Enabled / Disabled）を選択します。
IP SSH Service Port	SSH 接続の TCP ポート番号を 1～65535 の範囲で入力します。
Authentication Timeout	SSH の認証タイムアウトを 30～600（秒）の範囲で入力します。
Authentication Retries	SSH の認証再試行回数を 1～32 の範囲で入力します。

設定を適用するには、Apply ボタンをクリックします。

9.13.2 Host Key

Host Key 画面では、SSH ホスト鍵を表示および生成します。
本画面を表示するには、Security > SSH > Host Key をクリックします。



Host Key Management の各項目の説明を以下に示します。

パラメーター	説明
Crypto Key Type	生成するホスト鍵の暗号タイプ（RSA / DSA）を選択します。
Key Modulus	ホスト鍵の鍵長を以下のいずれかから選択します。 • 360 ビット • 512 ビット • 768 ビット • 1024 ビット • 2048 ビット

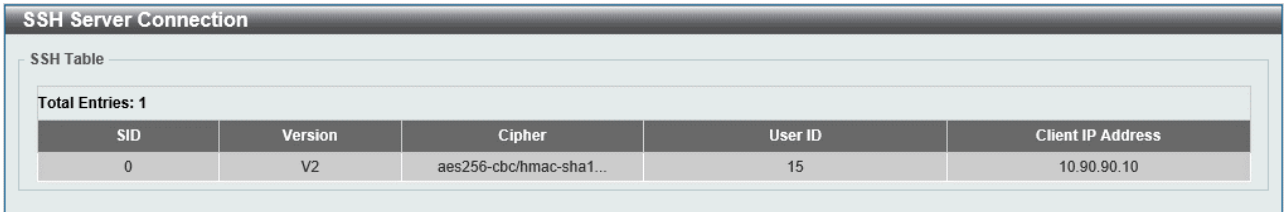
選択した内容でホストキーを生成するには、Generate ボタンをクリックします。
選択した内容でホストキーを削除するには、Delete ボタンをクリックします。

Host Key の各項目の説明を以下に示します。

パラメーター	説明
Crypto Key Type	表示する SSH ホスト鍵の暗号タイプ（RSA / DSA）を選択します。

9.13.3 SSH Server Connection

SSH Server Connection 画面では、SSH サーバー接続テーブルを表示します。
本画面を表示するには、Security > SSH > SSH Server Connection をクリックします。



9.13.4 SSH User Settings

SSH User Settings 画面では、SSH ユーザーを設定および表示します。
本画面を表示するには、Security > SSH > SSH User Settings をクリックします。

本画面の各項目の説明を以下に示します。

パラメーター	説明
User Name	SSH 接続のユーザー名を 32 文字以内で入力します。入力する SSH ユーザーは、別途ユーザーアカウントに登録されている必要があります。
Authentication Method	認証方法を以下のいずれかから選択します。 • Password：パスワード認証方式を使用します。ローカルユーザーアカウントのパスワードを使用します。 • Public Key：公開鍵認証方式を使用します。 　○ Key File：公開鍵ファイル名と場所を 779 文字以内で入力します。 • Host-based：ホストベース認証方式を使用します。 　○ Host Name：ホスト名を 255 文字以内で入力します。 　○ IPv4 Address：IPv4 アドレスを指定する場合、ラジオボタンをクリックし、右のボックスに SSH クライアントの IPv4 アドレスを入力します。 　○ IPv6 Address：IPv6 アドレスを指定する場合、ラジオボタンをクリックし、右のボックスに SSH クライアントの IPv6 アドレスを入力します。

設定を適用するには、Apply ボタンをクリックします。

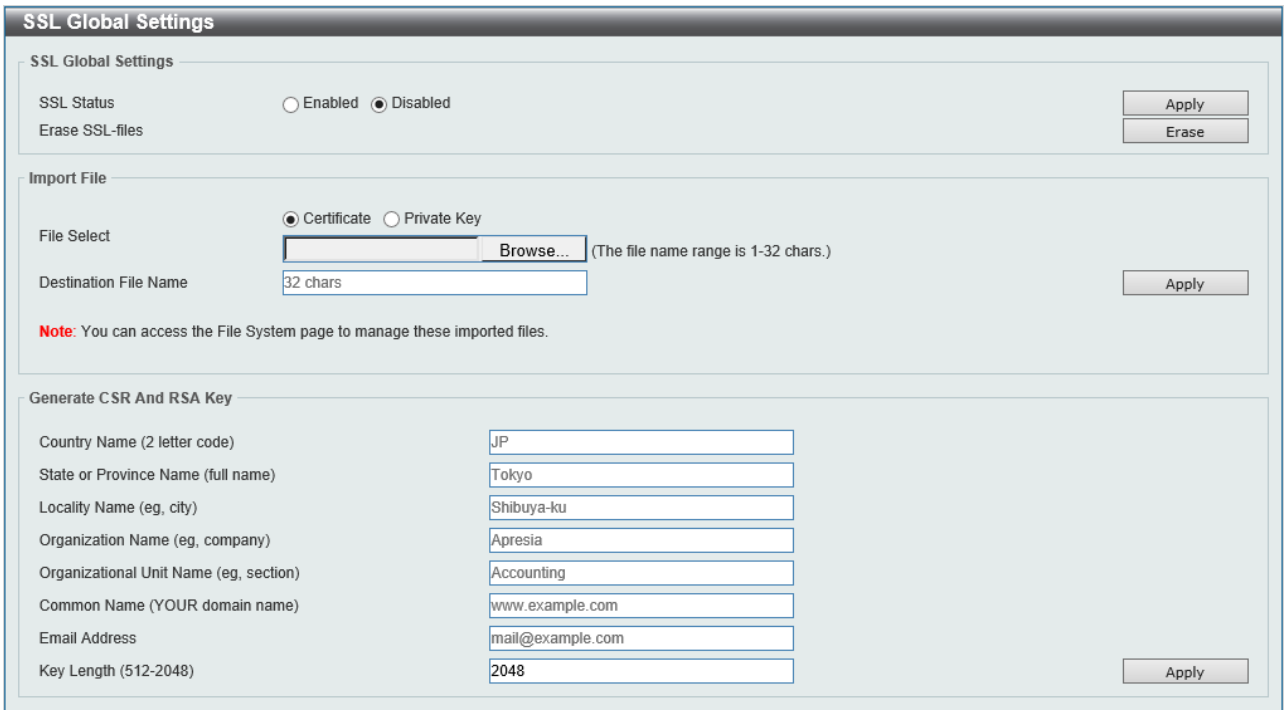
9.14 SSL

SSL サブメニューでは、SSL 機能に関する設定を行います。
SSL の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
9.14.1	SSL Global Settings	SSL 機能のグローバル設定
9.14.2	SSL Information	SSL の証明書や CSR 情報の表示

9.14.1 SSL Global Settings

SSL Global Settings 画面では、SSL 機能の設定を行います。
本画面を表示するには、Security > SSL > SSL Global Settings をクリックします。



SSL Global Settings の各項目の説明を以下に示します。

パラメーター	説明
SSL Status	SSL 機能の状態（Enabled / Disabled）を選択します。

設定を適用するには、Apply ボタンをクリックします。
SSL ポリシーファイルを消去するには、Erase ボタンをクリックします。なお、SSL または Web 認証が有効な場合は、SSL ポリシーは消去できません。

Import File の各項目の説明を以下に示します。

パラメーター	説明
File Select	読み込むファイルの種類（Certificate / Private Key）を選択します。 ファイルの種類を選択した後、Browse ボタンをクリックしてローカル PC 上のファイルを選択します。
Destination File Name	宛先ファイル名を 32 文字以内で入力します。

設定を適用するには、Apply ボタンをクリックします。

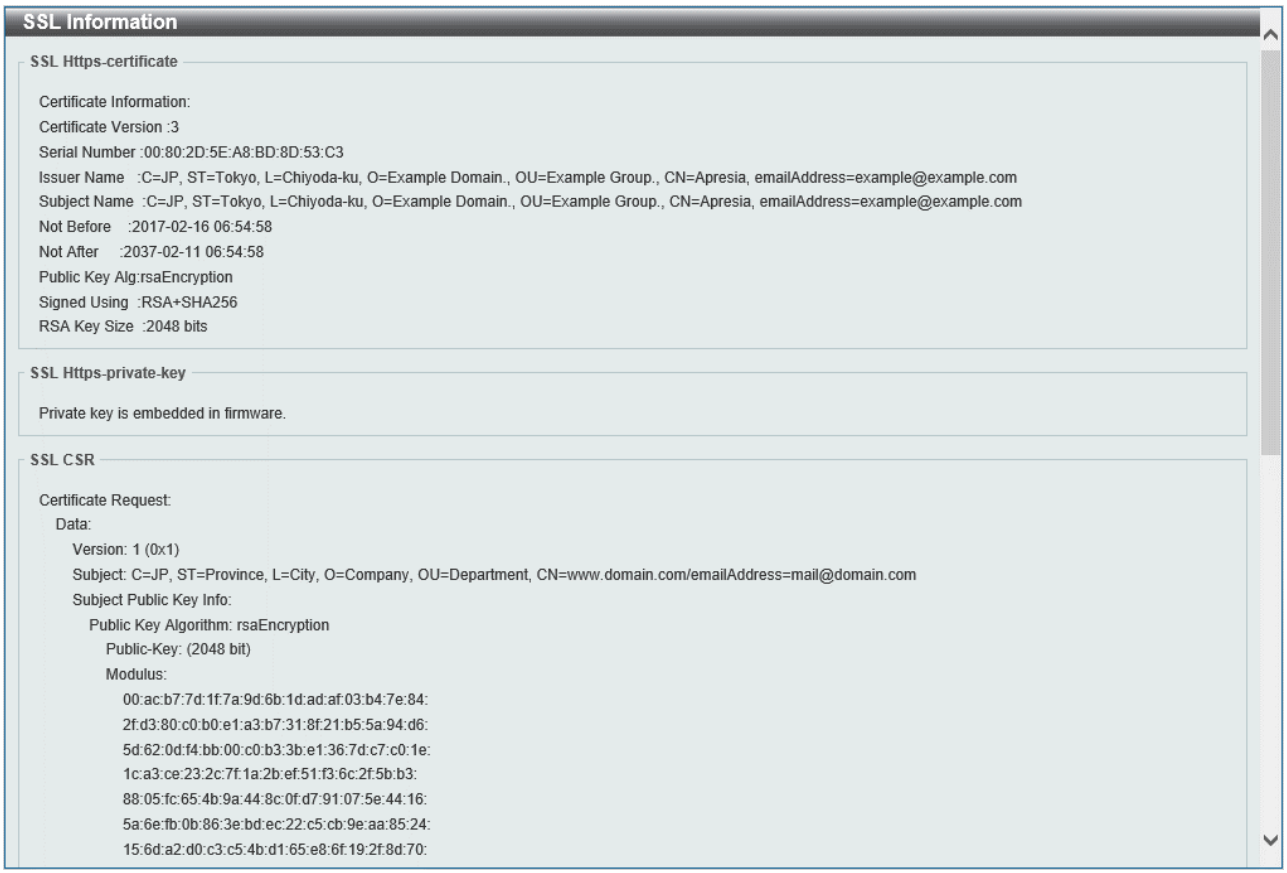
Generate CSR And RSA Key の各項目の説明を以下に示します。

パラメーター	説明
Country Name	国コードを 2 文字で入力します。日本の国コードは JP です。
State or Province Name	都道府県名を入力します。
Locality Name	地域（市）名を入力します。
Organization Name	組織名（会社名）を入力します。
Organization Unit Name	組織単位（部門）名を入力します。
Common Name	ドメイン名を入力します。
Email Address	連絡先のメールアドレスを入力します。
Key Length	CSR/RSA キーの長さを 512～2048 の範囲で入力します。

設定を適用するには、Apply ボタンをクリックします。

9.14.2 SSL Information

SSL Information 画面では、SSL の証明書および CSR 情報を表示します。
本画面を表示するには、Security > SSL > SSL Information をクリックします。



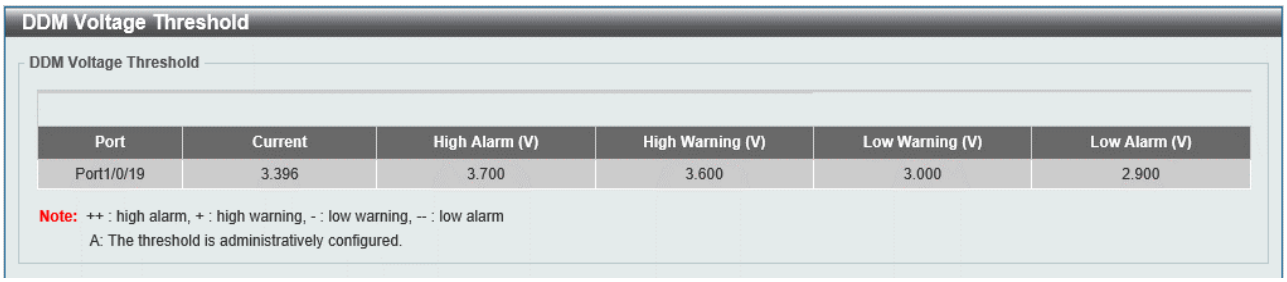
10 DDM

DDM メニューでは、SFP ポートでのデジタル診断監視（以後、DDM）の情報を確認できます。
DDM の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
10.1	DDM Voltage Threshold	DDM 電圧しきい値の表示
10.2	DDM Bias Current Threshold	DDM バイアス電流しきい値の表示
10.3	DDM TX Power Threshold	DDM 送信電力しきい値の表示
10.4	DDM RX Power Threshold	DDM 受信電力しきい値の表示
10.5	DDM Status	DDM の状態表示

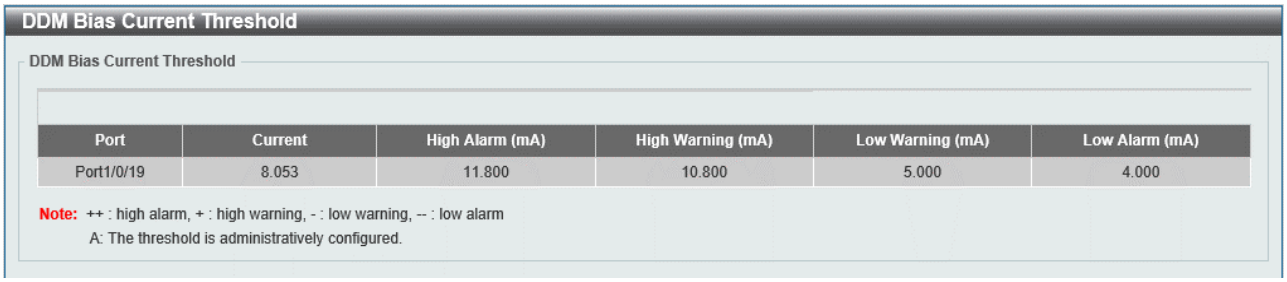
10.1 DDM Voltage Threshold

DDM Voltage Threshold 画面では、DDM 電圧しきい値の情報を表示します。
本画面を表示するには、**DDM > DDM Voltage Threshold** をクリックします。



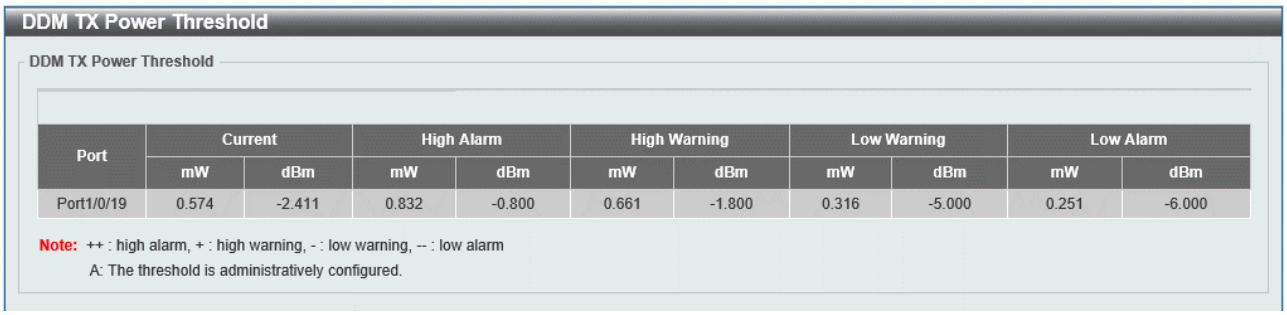
10.2 DDM Bias Current Threshold

DDM Bias Current Threshold 画面では、DDM バイアス電流しきい値の情報を表示します。
本画面を表示するには、DDM > DDM Bias Current Threshold をクリックします。



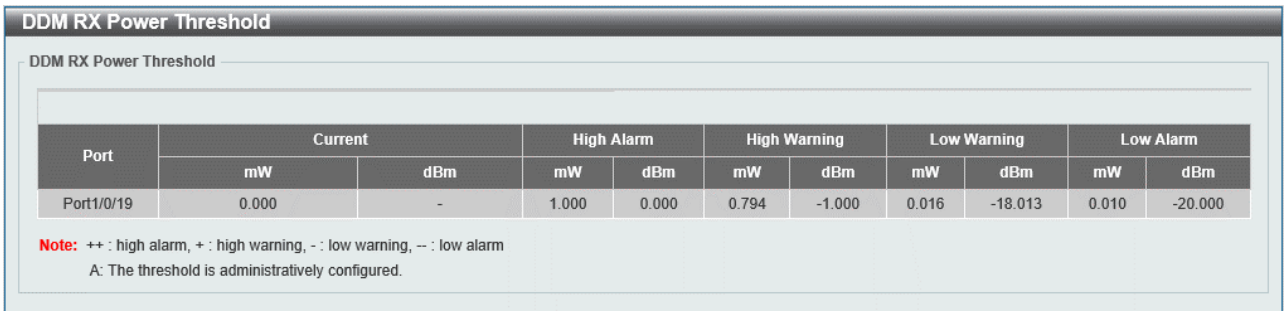
10.3 DDM TX Power Threshold

DDM TX Power Threshold 画面では、DDM TX 電力しきい値の情報を表示します。
本画面を表示するには、DDM > DDM TX Power Threshold をクリックします。



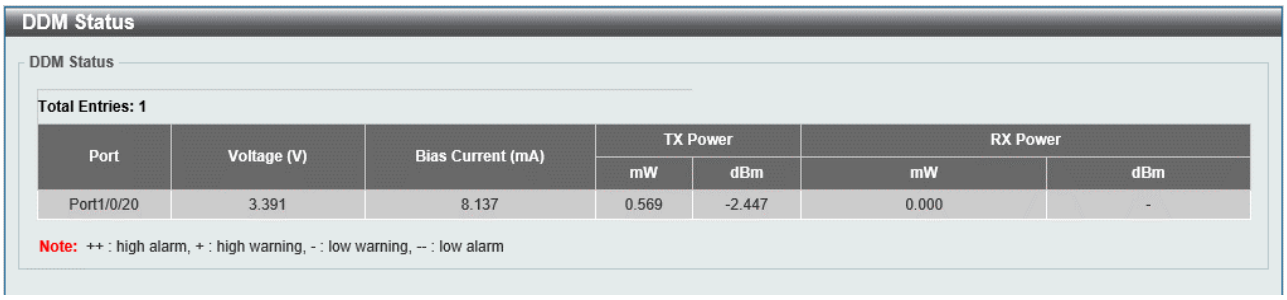
10.4 DDM RX Power Threshold

DDM RX Power Threshold 画面では、DDM RX 電力しきい値の情報を表示します。
本画面を表示するには、DDM > DDM RX Power Threshold をクリックします。



10.5 DDM Status

DDM Status 画面では、DDM ステータス情報を表示します。
本画面を表示するには、DDM > DDM Status をクリックします。



11 Monitoring

Monitoring メニューでは、装置のハードウェア状態の監視に関する設定を行います。また、ポートミラーリングの設定を行います。
Monitoring の下にあるサブメニューの一覧を以下の表に示します。

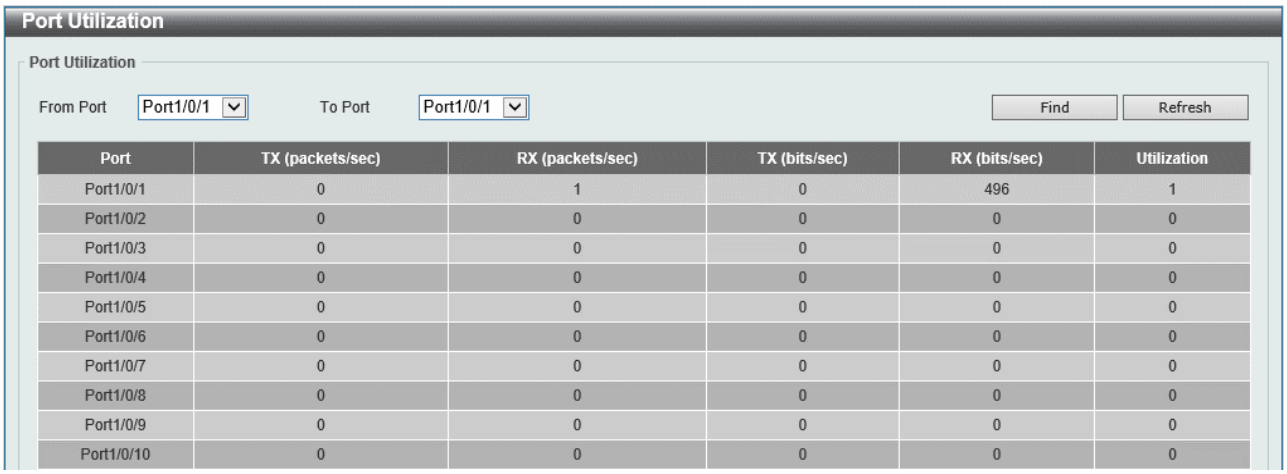
項番	メニュー名	概要
11.1	Utilization	ハードウェアの使用率情報の表示
11.2	Statistics	統計情報の表示
11.3	Mirror Settings	ポートミラーリングの設定
11.4	Device Environment	デバイス環境情報の表示

11.1 Utilization

Utilization サブメニューでは、物理ポートなどのハードウェアの使用率の情報を表示します。

11.1.1 Port Utilization

Port Utilization 画面では、ポート使用率の一覧を表示します。
本画面を表示するには、Monitoring > Utilization > Port Utilization をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。

入力／選択した情報でポート使用率のエントリーを検索するには、Find ボタンをクリックします。
一覧に表示されているポート使用率の情報を更新するには、Refresh ボタンをクリックします。

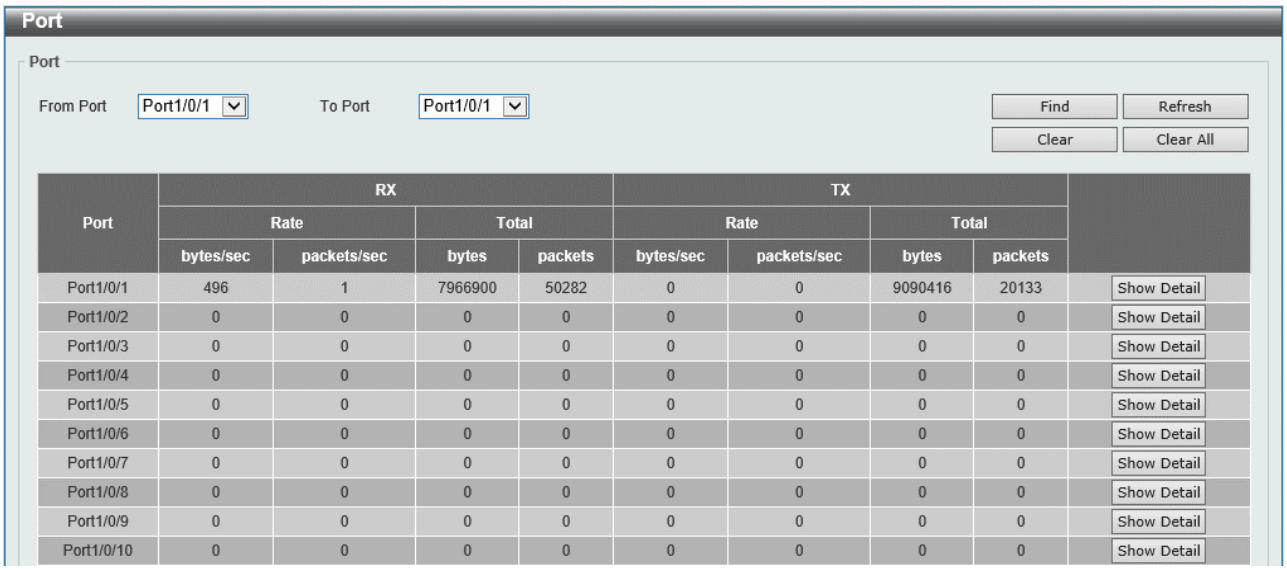
11.2 Statistics

Statistics サブメニューでは、ポートでの統計情報に関する情報を表示します。
Statistics の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
11.2.1	Port	ポートの帯域利用状況や統計情報の表示
11.2.2	Port Counters	パケット統計カウンターの概要情報の表示
11.2.3	Counters	パケット統計カウンターの詳細情報の表示

11.2.1 Port

Port 画面では、物理ポートの帯域利用状況や統計情報の概要情報を表示します。
本画面を表示するには、Monitoring > Statistics > Port をクリックします。

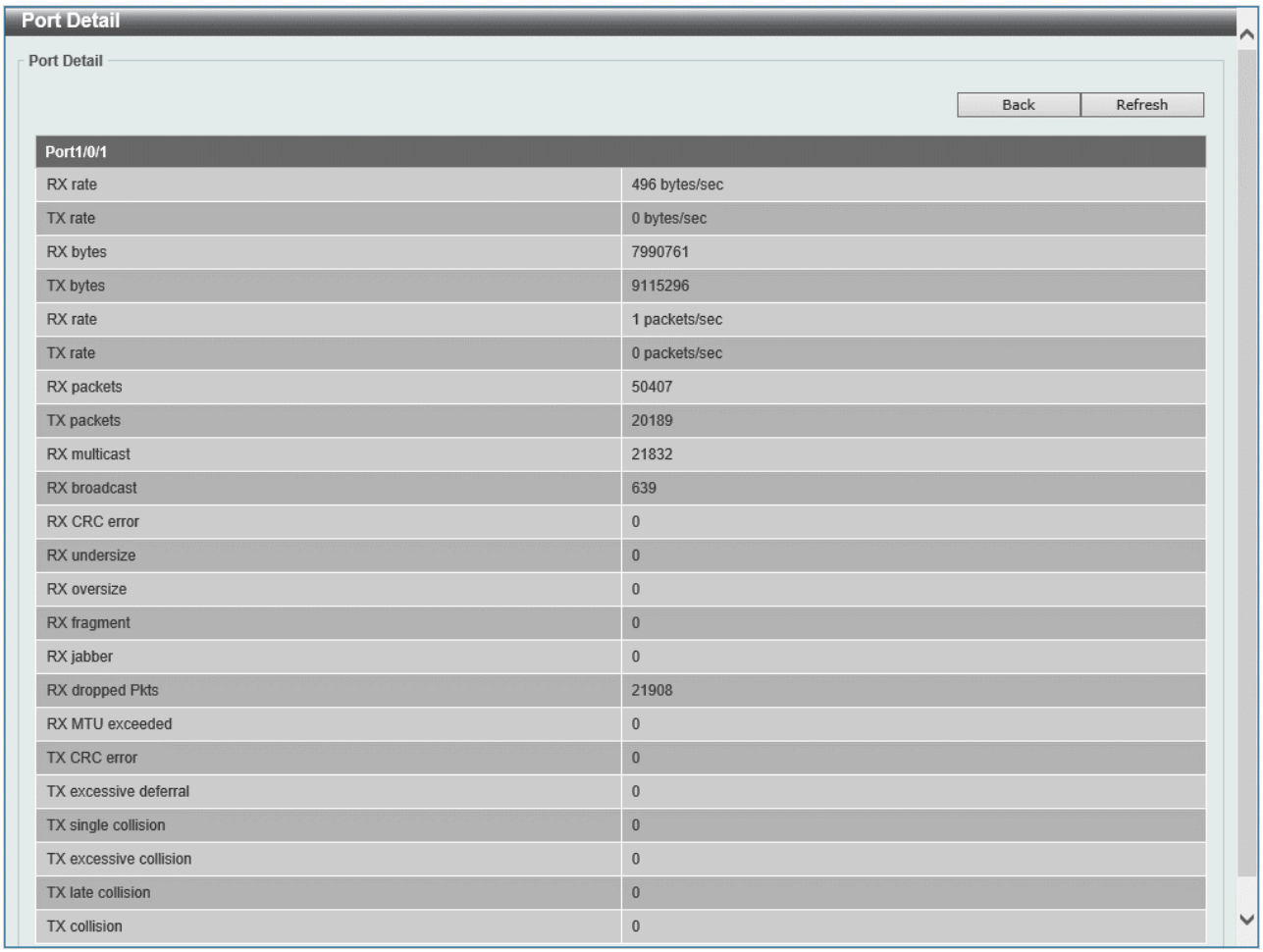


本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。

選択したポートの統計情報を検索するには、Find ボタンをクリックします。
表示されているポートの統計情報を更新するには、Refresh ボタンをクリックします。
選択したポートの統計情報をクリアするには、Clear ボタンをクリックします。
すべてのポートの統計情報をクリアするには、Clear All ボタンをクリックします。
ポート統計情報の詳細を表示するには、Show Detail ボタンをクリックします。

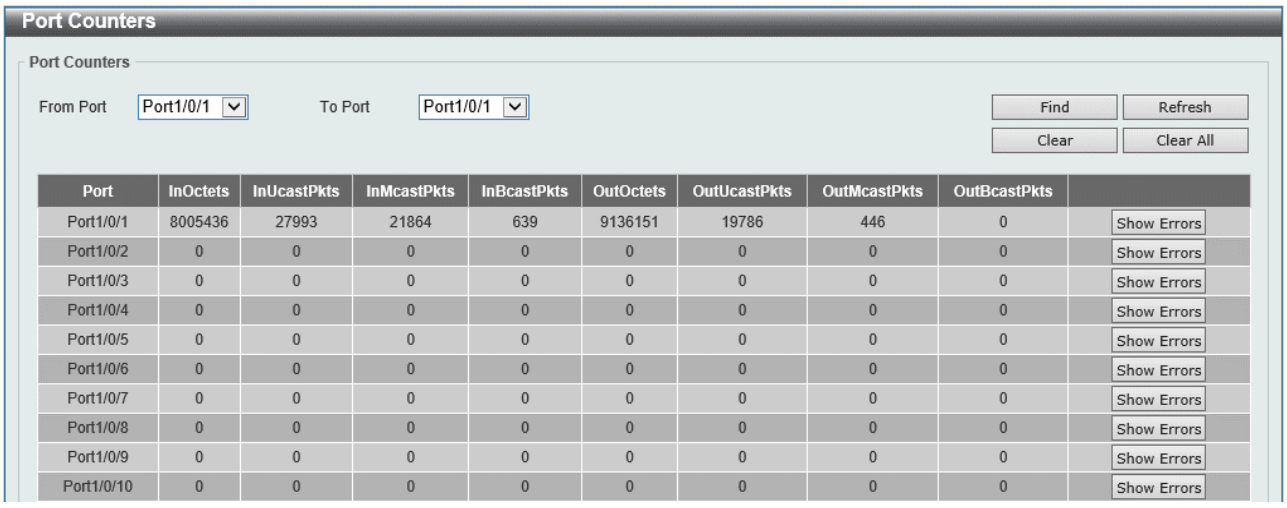
Show Detail ボタンをクリックすると、以下に示す画面が表示されます。



前の画面に戻るには、Back ボタンをクリックします。
一覧に表示されている情報を更新するには、Refresh ボタンをクリックします。

11.2.2 Port Counters

Port Counters 画面では、物理ポートでのパケット統計カウンターの概要情報を表示します。
本画面を表示するには、Monitoring > Statistics > Port Counters をクリックします。

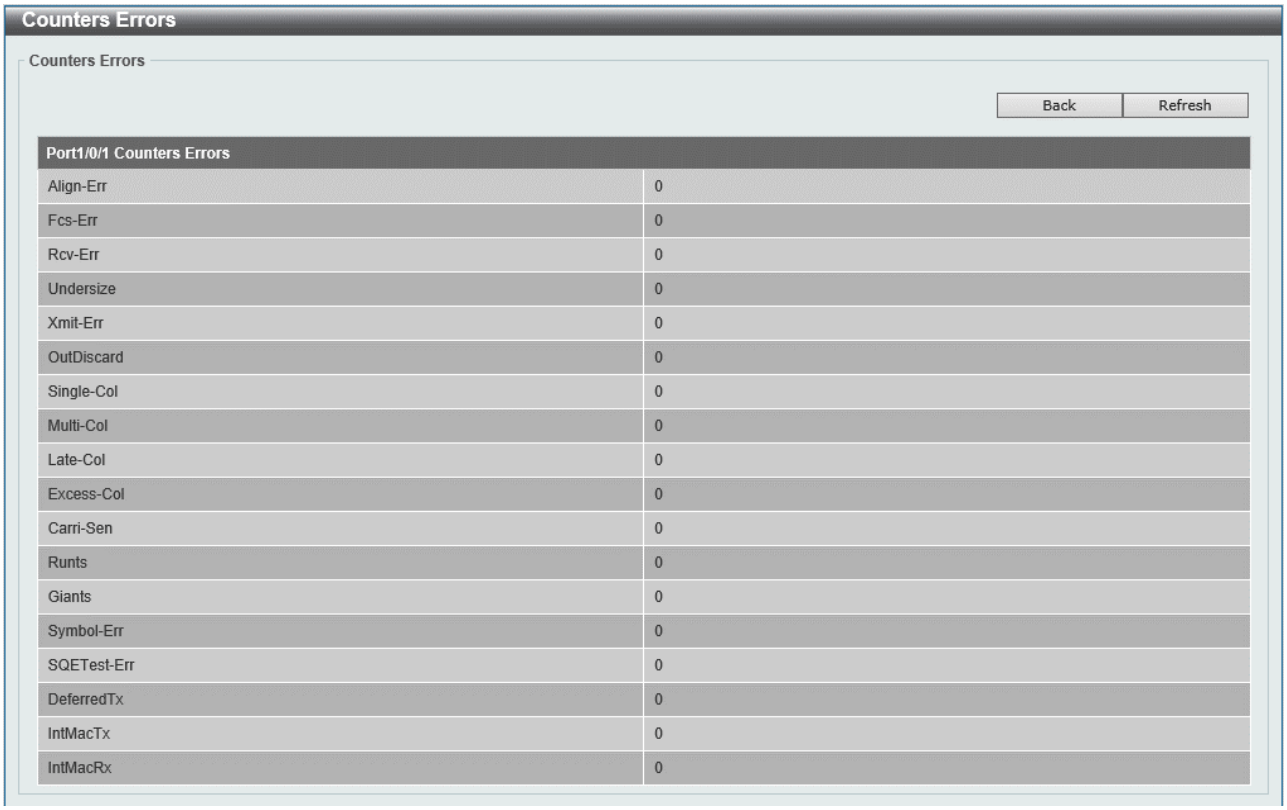


本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。

選択したポートのパケット統計カウンター情報を表示するには、Find ボタンをクリックします。
表示されているパケット統計カウンター情報を更新するには、Refresh ボタンをクリックします。
選択したポートのパケット統計カウンター情報をクリアするには、Clear ボタンをクリックします。
すべてのポートのパケット統計カウンター情報をクリアするには、Clear All ボタンをクリックします。
ポートで検出されたエラーの数を表示するには、Show Errors ボタンをクリックします。

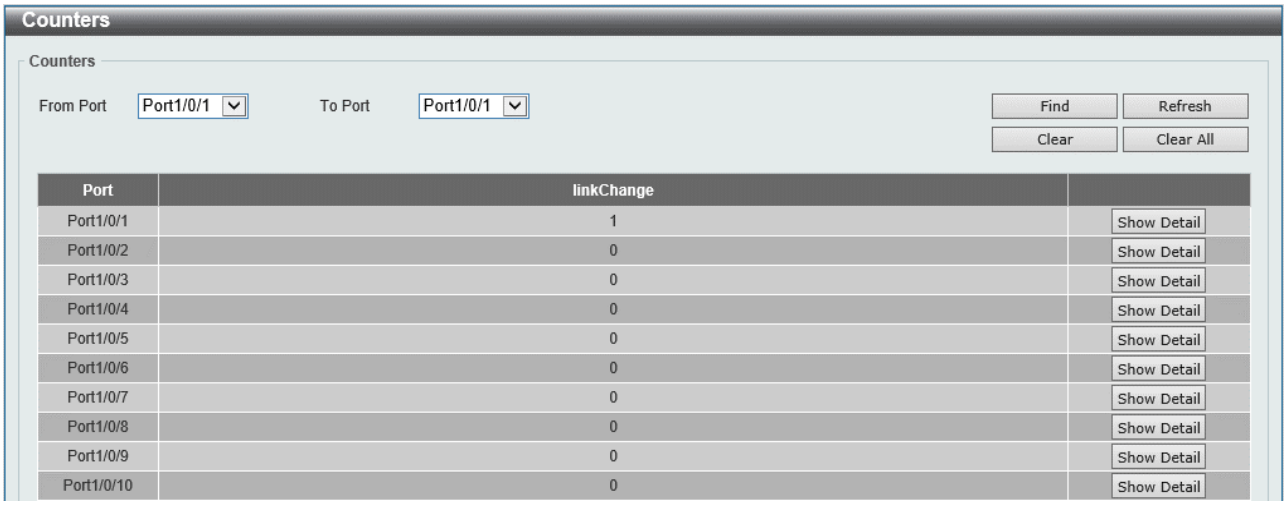
Show Errors ボタンをクリックすると、以下に示す画面が表示されます。



前の画面に戻るには、Back ボタンをクリックします。
一覧に表示されている情報を更新するには、Refresh ボタンをクリックします。

11.2.3 Counters

Counters 画面では、物理ポートのパケット統計カウンターの詳細情報を表示します。
本画面を表示するには、Monitoring > Statistics > Counters をクリックします。

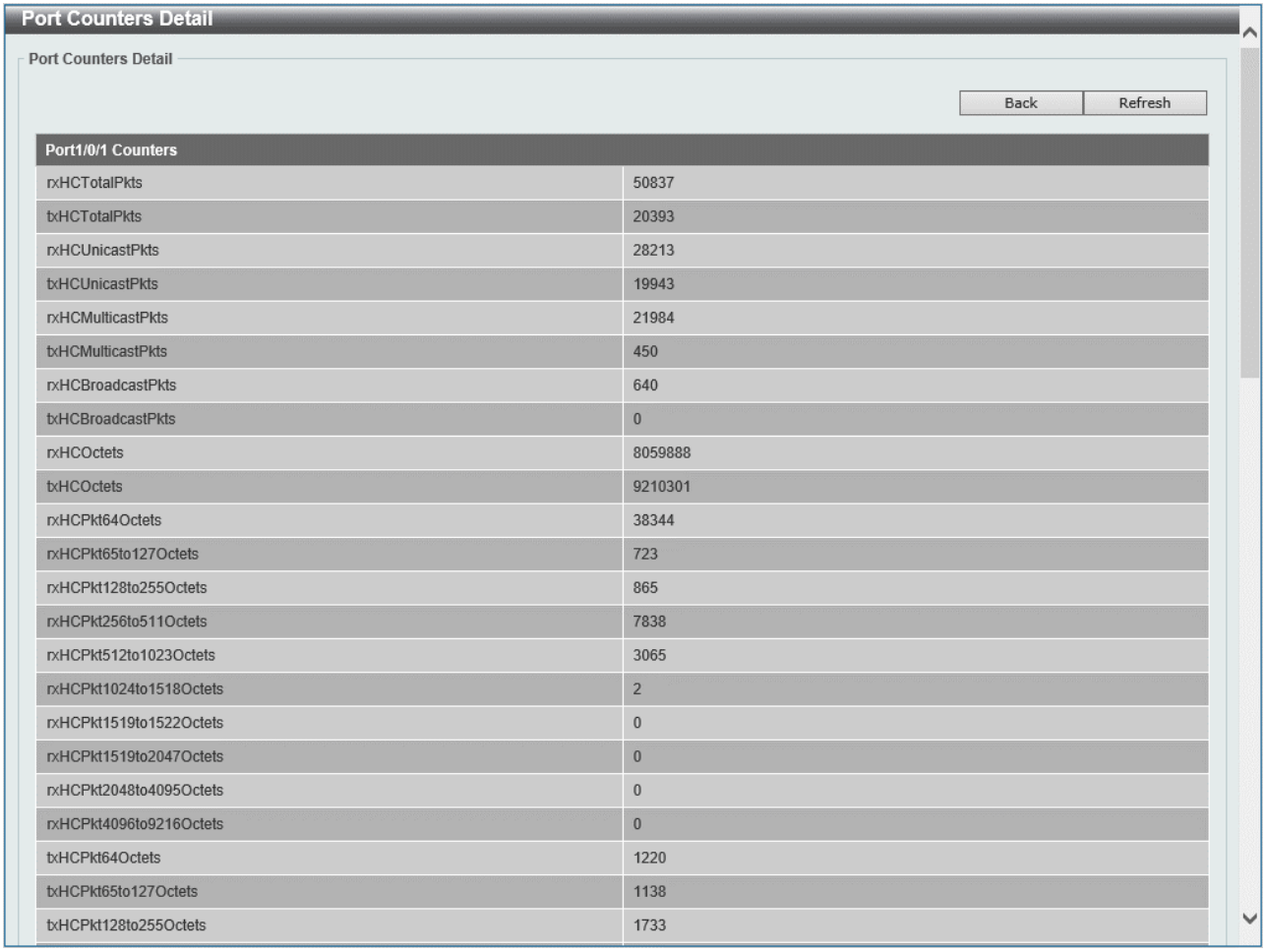


本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。

選択したポートのパケット統計カウンター情報を検索するには、Find ボタンをクリックします。
表示されているパケット統計カウンター情報を更新するには、Refresh ボタンをクリックします。
選択したポートのパケット統計カウンター情報をクリアするには、Clear ボタンをクリックします。
すべてのポートのパケット統計カウンター情報をクリアするには、Clear All ボタンをクリックします。
パケット統計カウンター情報の詳細情報を表示するには、Show Detail ボタンをクリックします。

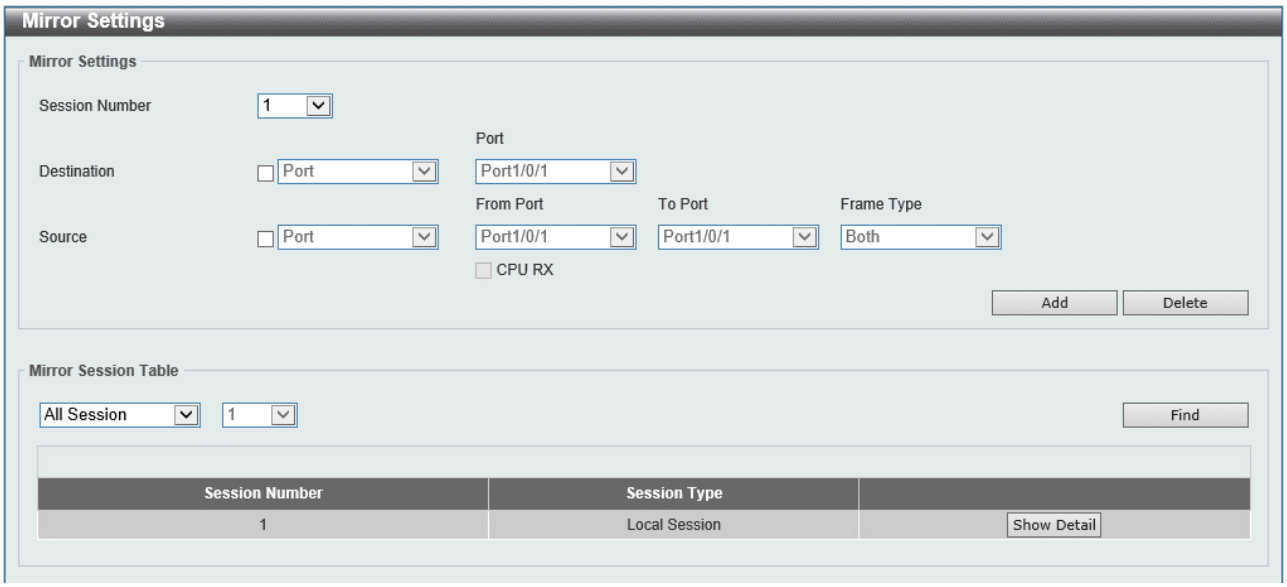
Show Detail ボタンをクリックすると、以下に示す画面が表示されます。



前の画面に戻るには、**Back** ボタンをクリックします。
表示されている情報を更新するには、**Refresh** ボタンをクリックします。

11.3 Mirror Settings

Mirror Settings 画面では、ポートミラーリングを設定します。
本画面を表示するには、Monitoring > Mirror Settings をクリックします。



Mirror Settings の各項目の説明を以下に示します。

パラメーター	説明
Session Number	ミラーリングの識別セッション番号を 1～4 から選択します。
Destination	宛先ポート番号を指定する場合にチェックします。 • Port：宛先ポートを選択します。
Source	送信元ポート番号または ACL を指定する場合にチェックします。 • Port：送信元ポートを設定する場合に選択します。 o From Port / To Port：送信元ポートの範囲を選択します。 o Frame Type：ミラーリングを行うトラフィックの方向をいずれかから選択します。 ➢ Both：受信と送信の両方のトラフィックに適用します。 ➢ RX：受信トラフィックのみに適用します。 ➢ TX：送信トラフィックのみに適用します。 o CPU RX： CPU 宛のトラフィックを含める場合にチェックします。 • ACL： ACL でミラーリングを行うパケットを絞り込む場合に選択します。 o ACL Name：ミラーリングするパケットの条件として使用する ACL 名を 32 文字以内で入力します。

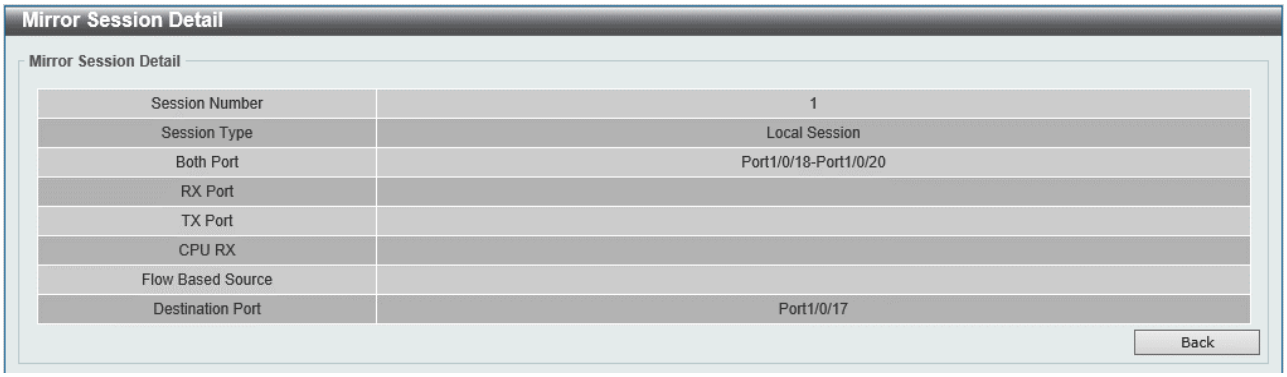
ポートミラーリングの設定を追加するには、Add ボタンをクリックします。
ポートミラーリングの設定を削除するには、Delete ボタンをクリックします。

Mirror Session Table の各項目の説明を以下に示します。

パラメーター	説明
Mirror Session Type	表示するミラーリング設定情報を以下のいずれかから選択します。 • All Session：すべての設定を表示する場合に選択します。 • Session Number：選択したセッション番号の設定のみ表示する場合に選択します。右のドロップダウンリストで、表示するセッション番号として 1～4 のいずれかを選択します。

入力した情報でポートミラーリングを検索するには、Find ボタンをクリックします。
ミラーリング設定の詳細情報を表示するには、Show Detail ボタンをクリックします。

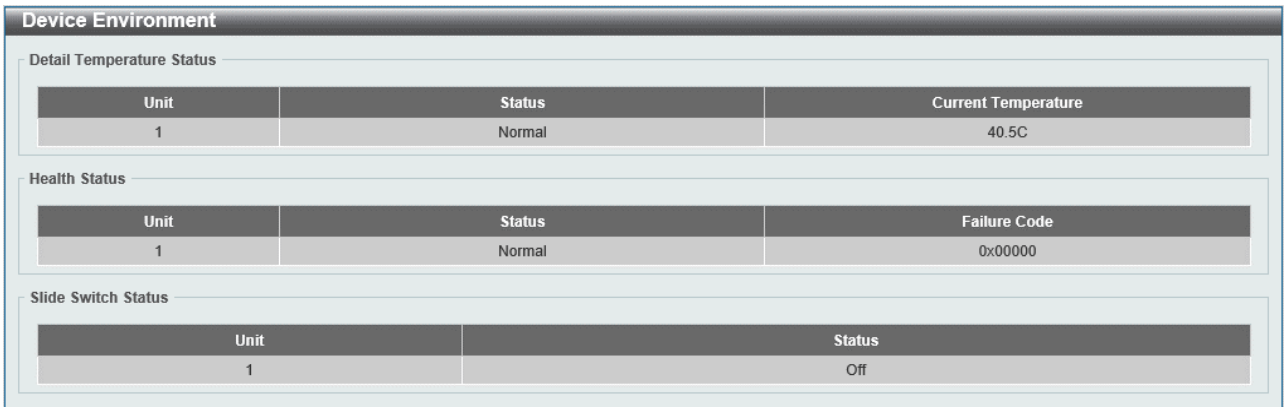
Show Detail ボタンをクリックすると、以下に示す画面が表示されます。



前の画面に戻るには、Back ボタンをクリックします。

11.4 Device Environment

Device Environment 画面では、装置のステータスや環境温度などのデバイス環境情報を表示します。
本画面を表示するには、Monitoring > Device Environment をクリックします。

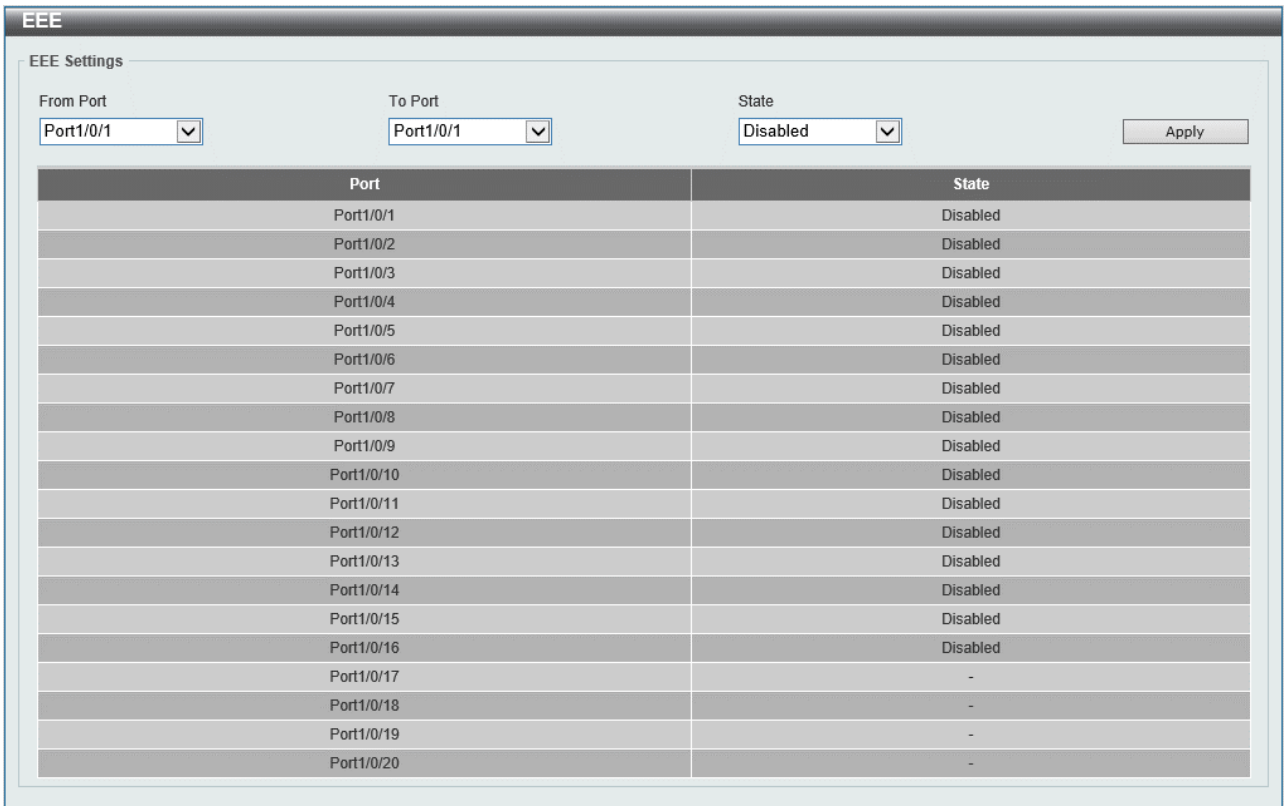


12 Green

Green メニューでは、装置のポート省電力機能に関する設定を行います。

12.1 EEE

EEE 画面は、IEEE 802.3az で規定される EEE の設定を行います。
本画面を表示するには、**Green** > **EEE** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
State	EEE の状態（Enabled / Disabled）を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

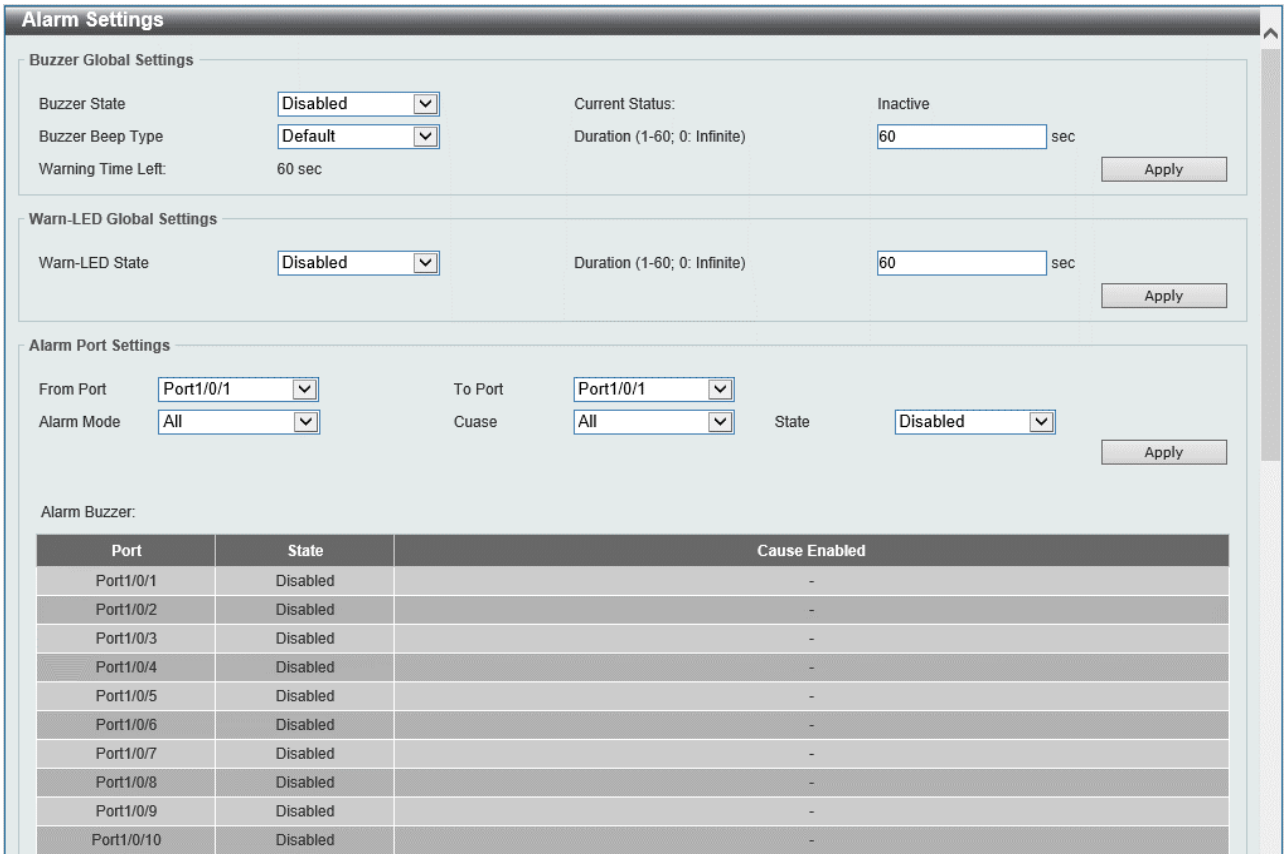
13 Alarm

Alarm メニューでは、ブザーや警告 LED による警告通知に関する設定を行います。
Alarm の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
13.1	Alarm Settings	ブザー、警告 LED の動作の設定
13.2	Alarm Debug	ブザー、警告 LED のテストの実施

13.1 Alarm Settings

Alarm Settings 画面では、ブザーおよび警告 LED のアラーム設定を行います。
本画面を表示するには、**Alarm** > **Alarm Settings** をクリックします。



Buzzer Global Settings の各項目の説明を以下に示します。

パラメーター	説明
Buzzer State	ブザー警告機能のグローバル設定（Enabled / Disabled）を選択します。
Current Status	ブザー警告機能のグローバル設定状態が表示されます。
Buzzer Beep Type	ブザー警告音のパターンを以下のいずれかから選択します。 • Default：ビープ音を 2 秒間鳴らして 2 秒間無音というパターンを繰り返す場合に選択します。 • Type 1： 2 秒間ビープ音を鳴らして 8 秒間無音というパターンを繰り返す場合に選択します。 • Type 2：ビープ音を 5 秒間鳴らして 5 秒間無音というパターンを繰り返す場合に選択します。 • Type 3：ビープ音を 8 秒間鳴らして 2 秒間無音というパターンを繰り返す場合に選択します。
Duration	ブザーの動作時間（秒）を 0～60 の範囲で入力します。0 を指定すると、警告イベント発生時にブザー音の警告が行われません。
Warning Time Left	警告イベント発生時のブザー停止までの残時間が表示されます。

設定を適用するには、Apply ボタンをクリックします。

Warn-LED Global Settings の各項目の説明を以下に示します。

パラメーター	説明
Warn-LED State	警告 LED の状態（Enabled / Disabled）を選択します。
Duration	警告 LED の動作時間（秒）を 0～60 の範囲で入力します。0 を指定すると、警告イベント発生時に警告 LED による警告が行われません。

設定を適用するには、Apply ボタンをクリックします。

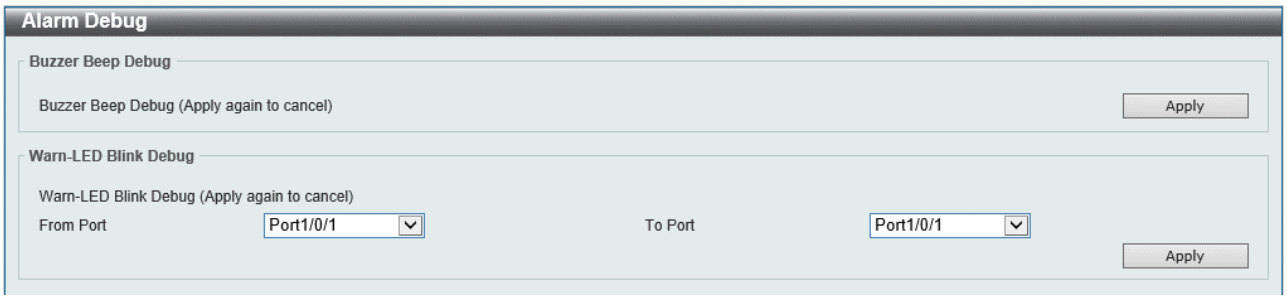
Alarm Port Settings の各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Alarm Mode	警告イベント発生時のアラームモードを以下から選択します。 • All：ブザーと警告 LED による警告を行います。 • Buzzer：ブザーによる警告を行います。 • Warning LED：警告 LED による警告を行います。
Cause	警告イベントを以下から選択します。 • All：ループ検出およびストーム発生時に警告します。 • Loop Detection：ループ検出時に警告します。 • Storm Control：ストーム発生時に警告します。
State	アラーム警告機能の状態（Enabled / Disabled）を選択します。

設定を適用するには、Apply ボタンをクリックします。

13.2 Alarm Debug

Alarm Debug 画面では、ブザーや警告 LED のテストを行うことができます。
本画面を表示するには、**Alarm > Alarm Debug** をクリックします。



Buzzer Beep Debug の各項目の説明を以下に示します。

パラメーター	説明
Buzzer Beep Debug	ブザーのテストを行います。**Apply** ボタンをクリックするたびに、鳴動と停止が切り替わります。

Warning LED Blink Debug の各項目の説明を以下に示します。

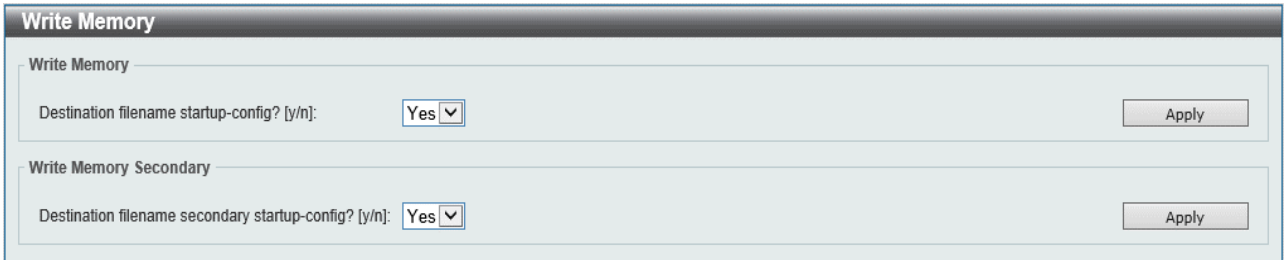
パラメーター	説明
From Port / To Port	警告 LED のテストを行います。テストする警告 LED のポートの範囲を選択し、**Apply** ボタンをクリックするたびに、オンとオフが切り替わります。

14 Save

画面上部のフロントパネルビューに表示されているツールバーに表示されている **Save** ボタンをクリックし、表示されるサブメニューの **Write Memory** をクリックすると、現在の設定を保存する画面に移行します。

14.1 Write Memory

Write Memory 画面では、現在の設定情報を起動時設定に書き込みます。
本画面を表示するには、**Save** > **Write Memory** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
Write Memory	**Yes** を選択して **Apply** ボタンをクリックすると、現在の設定情報をプライマリーの起動時設定ファイルに書き込みます。
Write Memory Secondary	**Yes** を選択して **Apply** ボタンをクリックすると、現在の設定情報をセカンダリーの起動時設定ファイルに書き込みます。

15 Tools

Tool ボタンから、イメージファイルや設定ファイルの操作を行うことができます。
Tool ボタンをクリックすると以下のサブメニューが出現します。

項番	メニュー名	概要
15.1	Firmware Upgrade & Backup	イメージファイルの操作
15.2	Configuration Restore & Backup	設定ファイルの操作
15.3	Tech-support Backup	技術サポート情報のバックアップ
15.4	Log Backup	システムログのバックアップ
15.5	Restore & Backup	一括リストアと一括バックアップ
15.6	AAA-local-db Download & Backup	AAA ローカルデータベースファイルの操作
15.7	SSL Files Download & Backup	SSL 関連ファイルの操作
15.8	CSR Files Backup	CSR 関連ファイルの操作
15.9	Ping	Ping の実行
15.10	Trace Route	Traceroute の実行
15.11	Reset	システムリセットの実行
15.12	Reboot System	システム再起動の実行

15.1 Firmware Upgrade & Backup

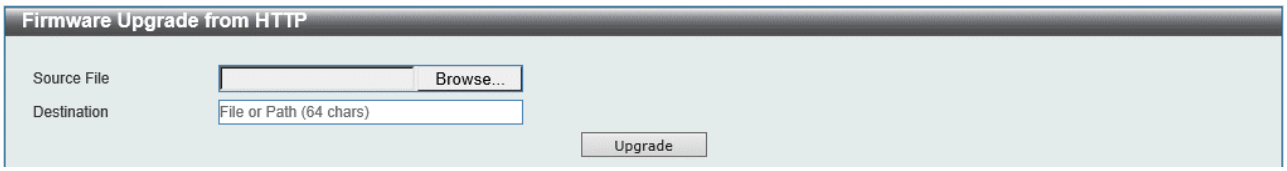
Firmware Upgrade & Backup メニューからは、イメージファイルのアップロードとダウンロードを実行します。起動するファームウェアを、装置にアップロードしたイメージファイルに更新する場合、装置の再起動が必要になります。また、アップロードしたイメージファイルが起動イメージに指定されていない場合は、**Management > File System** の画面で起動イメージを変更する必要があります。

Firmware Upgrade & Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.1.1	Firmware Upgrade from HTTP	HTTP でローカル PC からイメージファイルを取得
15.1.2	Firmware Upgrade from TFTP	TFTP サーバーからイメージファイルを取得
15.1.3	Firmware Upgrade from FTP	FTP サーバーからイメージファイルを取得
15.1.4	Firmware Backup to HTTP	HTTP でローカル PC にイメージファイルを保管
15.1.5	Firmware Backup to TFTP	TFTP サーバーにイメージファイルを保管
15.1.6	Firmware Backup to FTP	FTP サーバーにイメージファイルを保管

15.1.1 Firmware Upgrade from HTTP

Firmware Upgrade from HTTP 画面では、HTTP でローカル PC から装置にイメージファイルをアップロードします。
本画面を表示するには、**Tools** > **Firmware Upgrade & Backup** > **Firmware Upgrade from HTTP** をクリックします。



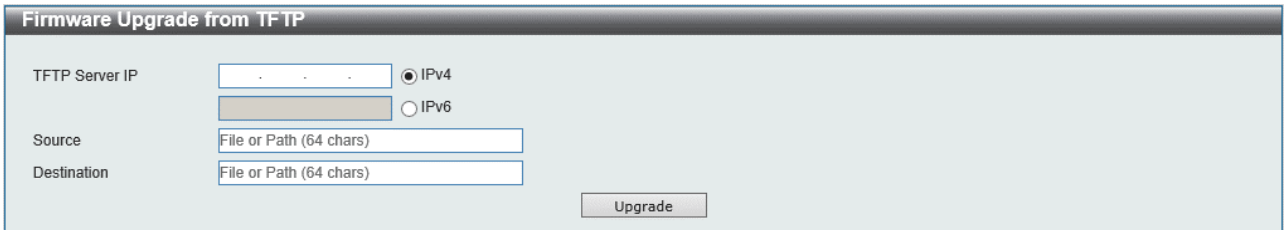
本画面の各項目の説明を以下に示します。

パラメーター	説明
Source File	**Browse** ボタンをクリックし、ローカル PC 上のイメージファイルを選択します。**Browse** ボタンの左のボックスにファイル名とパスが表示されます。
Destination	装置に保存するファイル名とパスを 64 文字以内で入力します。

イメージファイルのアップロードを開始するには、**Upgrade** ボタンをクリックします。

15.1.2 Firmware Upgrade from TFTP

Firmware Upgrade from TFTP 画面では、TFTP サーバーからイメージファイルをアップロードします。
本画面を表示するには、**Tools** > **Firmware Upgrade & Backup** > **Firmware Upgrade from TFTP** をクリックします。



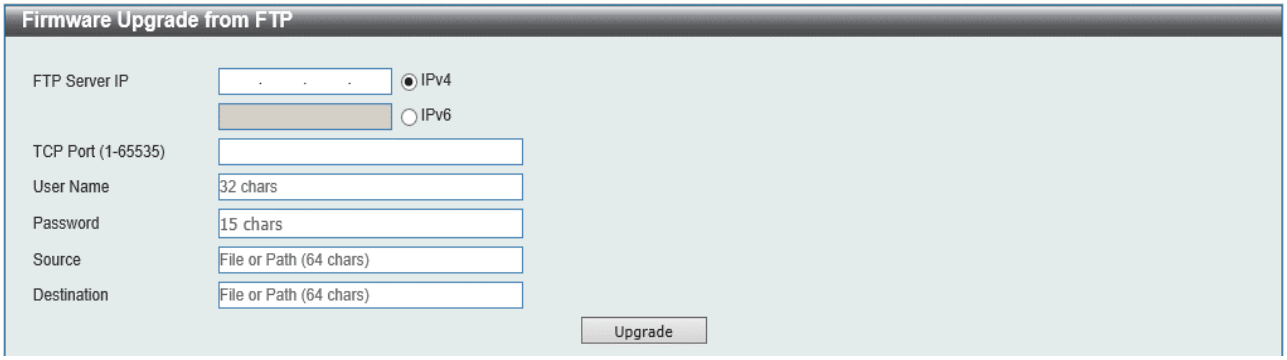
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IP アドレス、IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Source	TFTP サーバー上のファイル名とパスを 64 文字以内で入力します。
Destination	装置に保存するファイル名とパスを 64 文字以内で入力します。

イメージファイルのアップロードを開始するには、**Upgrade** ボタンをクリックします。

15.1.3 Firmware Upgrade from FTP

Firmware Upgrade from FTP 画面では、FTP サーバーからイメージファイルをアップロードします。
本画面を表示するには、**Tools > Firmware Upgrade & Backup > Firmware Upgrade from FTP** をクリックします。



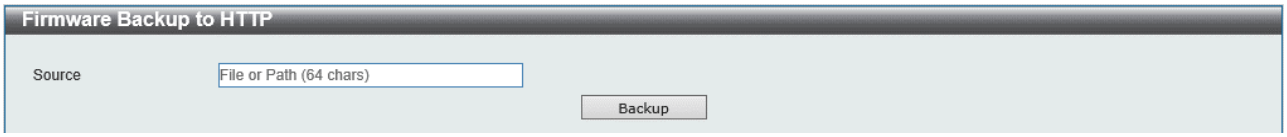
本画面の各項目の説明を以下に示します。

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1～65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Source	FTP サーバー上のファイル名とパスを 64 文字以内で入力します。
Destination	装置に保存するファイル名とパスを 64 文字以内で入力します。

イメージファイルのアップロードを開始するには、**Upgrade** ボタンをクリックします。

15.1.4 Firmware Backup to HTTP

Firmware Backup to HTTP 画面では、HTTP でローカル PC にイメージファイルをバックアップします。
本画面を表示するには、**Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP** をクリックします。



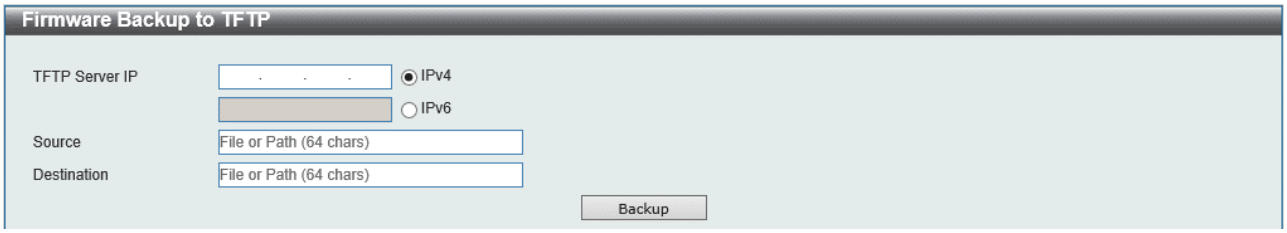
本画面の各項目の説明を以下に示します。

パラメーター	説明
Source	装置のファームウェアファイル名とパスを 64 文字以内で入力します。

イメージファイルのバックアップを開始するには、**Backup** ボタンをクリックします。

15.1.5 Firmware Backup to TFTP

Firmware Backup to TFTP 画面では、TFTP サーバーにイメージファイルをバックアップします。
本画面を表示するには、**Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP** をクリックします。



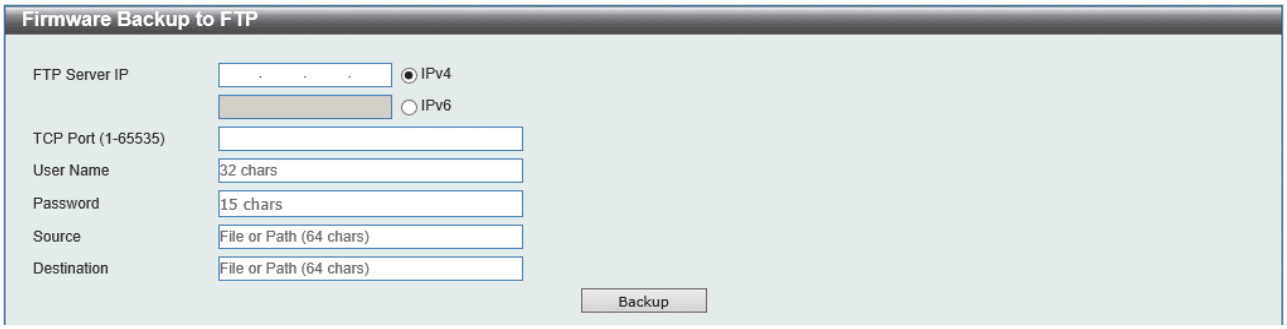
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Source	装置のイメージファイル名とパスを 64 文字以内で入力します。
Destination	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

イメージファイルのバックアップを開始するには、**Backup** ボタンをクリックします。

15.1.6 Firmware Backup to FTP

Firmware Backup to FTP 画面では、FTP サーバーにイメージファイルをバックアップします。
本画面を表示するには、**Tools > Firmware Upgrade & Backup > Firmware Backup to FTP** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（IPv4 / IPv6）を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1～65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Source	装置のイメージファイル名とパスを 64 文字以内で入力します。
Destination	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

イメージファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.2 Configuration Restore & Backup

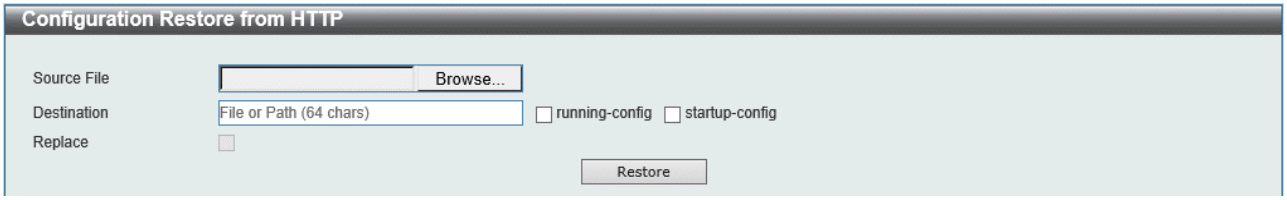
Configuration Restore & Backup メニューからは、設定ファイルのバックアップ、リストアを実行できます。

Configuration Restore & Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.2.1	Configuration Restore from HTTP	HTTP でローカル PC から設定ファイルを取得
15.2.2	Configuration Restore from TFTP	TFTP サーバーから設定ファイルを取得
15.2.3	Configuration Restore from FTP	FTP サーバーから設定ファイルを取得
15.2.4	Configuration Backup to HTTP	HTTP でローカル PC に設定ファイルを保管
15.2.5	Configuration Backup to TFTP	TFTP サーバーに設定ファイルを保管
15.2.6	Configuration Backup to FTP	FTP サーバーに設定ファイルを保管

15.2.1 Configuration Restore from HTTP

Configuration Restore from HTTP 画面では、HTTP でローカル PC から設定ファイルを復元できます。本画面を表示するには、**Tools** > **Configuration Restore & Backup** > **Configuration Restore from HTTP** をクリックします。



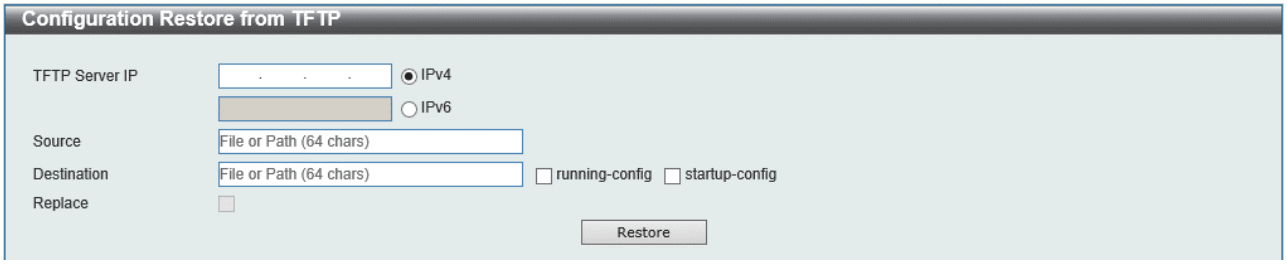
本画面の各項目の説明を以下に示します。

パラメーター	説明
Source File	テキストボックスをダブルクリックするか、**Browse** ボタンをクリックし、ローカル PC 上の設定ファイルを選択します。**Browse** ボタンの左のボックスにファイル名とパスが表示されます。
Destination	装置に保存する設定ファイル名とパスを 64 文字以内で入力します。 • **running-config** をチェックすると、現在の設定に反映します。 • **startup-config** をチェックすると、起動時設定に反映します。
Replace	装置の設定ファイルを置き換える場合にチェックします。

設定ファイルの復元を開始するには、**Restore** ボタンをクリックします。

15.2.2 Configuration Restore from TFTP

Configuration Restore from TFTP 画面では、TFTP サーバーから設定ファイルを復元します。
本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Restore from TFTP をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（IPv4 / IPv6）を指定します。
Source	TFTP サーバー上のファイル名とパスを 64 文字以内で入力します。
Destination	装置に保存する設定ファイル名とパスを 64 文字以内で入力します。 • running-config をチェックすると、現在の設定に反映します。 • startup-config をチェックすると、起動時設定に反映します。
Replace	装置の設定ファイルを置き換える場合にチェックします。

設定ファイルの復元を開始するには、Restore ボタンをクリックします。

15.2.3 Configuration Restore from FTP

Configuration Restore from FTP 画面では、FTP サーバーから設定ファイルを復元します。
本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Restore from FTP をクリックします。

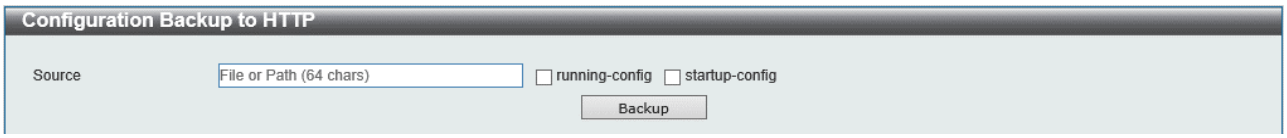
本画面の各項目の説明を以下に示します。

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（IPv4 / IPv6）を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1～65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Source	FTP サーバー上のファイル名とパスを 64 文字以内で入力します。
Destination	装置に保存する設定ファイル名とパスを 64 文字以内で入力します。 • running-config をチェックすると、現在の設定に反映します。 • startup-config をチェックすると、起動時設定に反映します。
Replace	装置の設定ファイルを置き換える場合にチェックします。

設定ファイルの復元を開始するには、Restore ボタンをクリックします。

15.2.4 Configuration Backup to HTTP

Configuration Backup to HTTP 画面では、HTTP でローカル PC に設定ファイルをバックアップします。本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Backup to HTTP をクリックします。



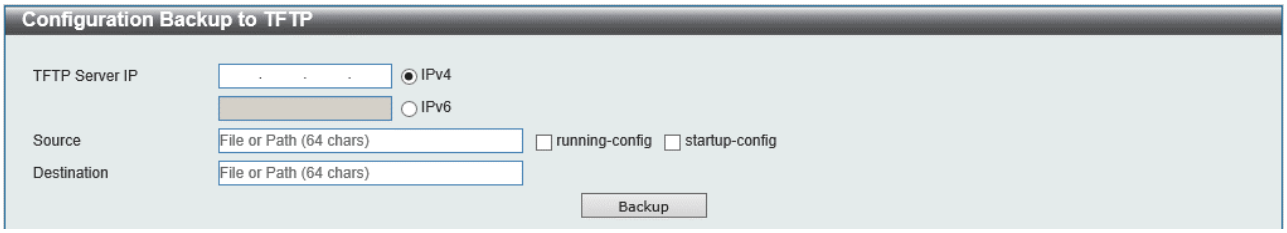
本画面の各項目の説明を以下に示します。

パラメーター	説明
Source	装置上の設定ファイル名とパスを 64 文字以内で入力します。 • running-config をチェックすると、現在の設定を取得します。 • startup-config をチェックすると、起動時設定を取得します。

設定ファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.2.5 Configuration Backup to TFTP

Configuration Backup to TFTP 画面では、TFTP サーバーに設定ファイルをバックアップします。
本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Backup to TFTP をクリックします。



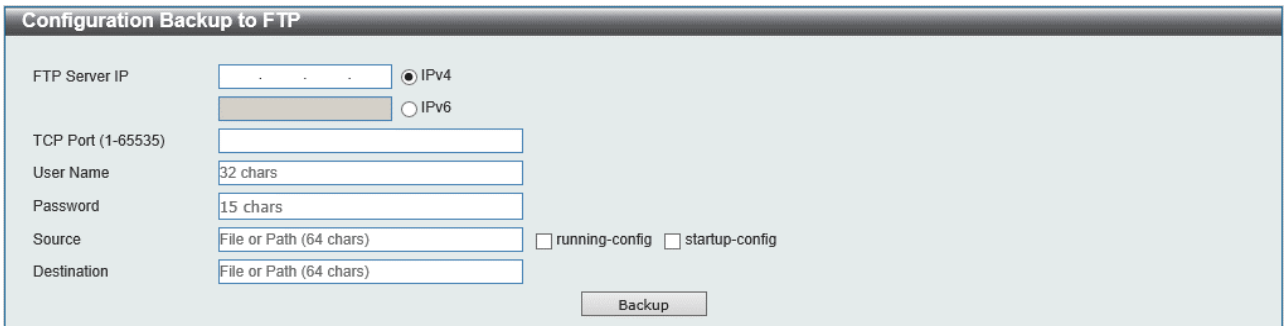
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（IPv4 / IPv6）を指定します。
Source	装置上の設定ファイル名とパスを 64 文字以内で入力します。 • running-config をチェックすると、現在の設定を取得します。 • startup-config をチェックすると、起動時設定を取得します。
Destination	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

設定ファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.2.6 Configuration Backup to FTP

Configuration Backup to FTP 画面では、FTP サーバーに設定ファイルをバックアップします。
本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Backup to FTP をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（IPv4 / IPv6）を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1～65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Source	装置上の設定ファイル名とパスを 64 文字以内で入力します。 • running-config をチェックすると、現在の設定を取得します。 • startup-config をチェックすると、起動時設定を取得します。
Destination	FTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

設定ファイルのバックアップを開始するには、Backup ボタンをクリックします。

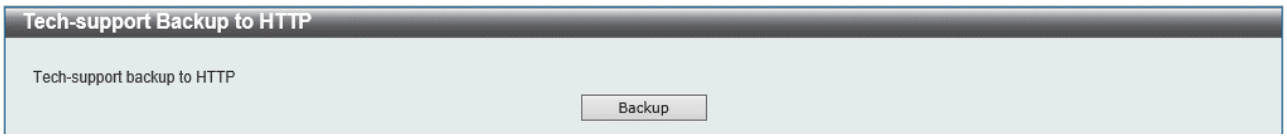
15.3 Tech-support Backup

Tech-support Backup メニューからは、技術サポート情報のバックアップを実行できます。
Tech-support Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.3.1	Tech-support Backup to HTTP	HTTP でローカル PC に技術サポート情報を保存
15.3.2	Tech-support Backup to TFTP	TFTP サーバーに技術サポート情報を保存

15.3.1 Tech-support Backup to HTTP

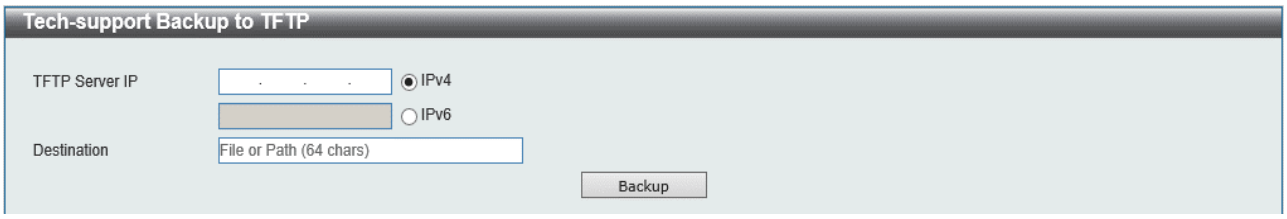
Tech-support Backup to HTTP 画面では、HTTP でローカル PC に技術サポート情報ファイルをバックアップします。
本画面を表示するには、**Tools > Tech-support Backup > Tech-support Backup to HTTP** をクリックします。



技術サポート情報ファイルのバックアップを開始するには、**Backup** ボタンをクリックします。

15.3.2 Tech-support Backup to TFTP

Tech-support Backup to TFTP 画面では、TFTP サーバーに技術サポート情報ファイルをバックアップします。
本画面を表示するには、**Tools > Tech-support Backup > Tech-support Backup to TFTP** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4 / IPv6**）を指定します。
Destination	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

技術サポート情報ファイルのバックアップを開始するには、**Backup** ボタンをクリックします。

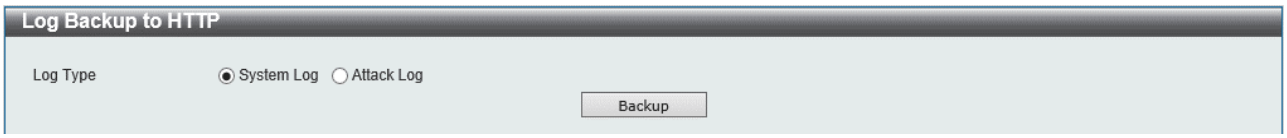
15.4 Log Backup

Log Backup メニューからは、システムログのバックアップを実行できます。
Log Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.4.1	Log Backup to HTTP	HTTP でローカル PC にシステムログを保存
15.4.2	Log Backup to TFTP	TFTP サーバーにシステムログを保存

15.4.1 Log Backup to HTTP

Log Backup to HTTP 画面では、HTTP でローカル PC にシステムログをバックアップします。
本画面を表示するには、Tools > Log Backup > Log Backup to HTTP をクリックします。



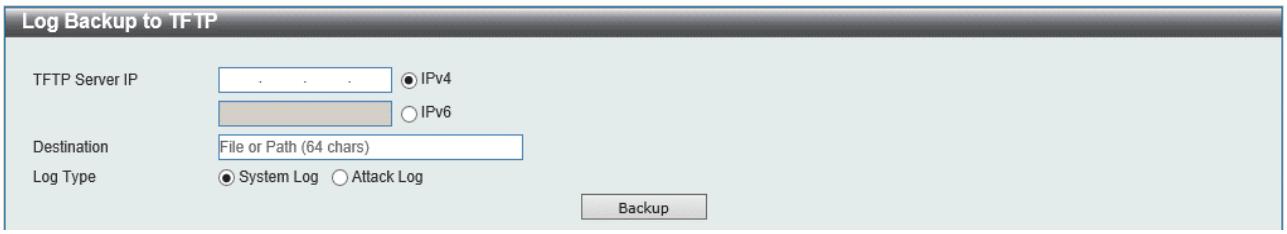
本画面の各項目の説明を以下に示します。

パラメーター	説明
Log Type	バックアップするログの種類を以下のどちらかから選択します。 • System Log を選択すると、システムログをバックアップします。 • Attack Log を選択すると、アタックログをバックアップします。

システムログのバックアップを開始するには、Backup ボタンをクリックします。

15.4.2 Log Backup to TFTP

Log Backup to TFTP 画面では、TFTP サーバーにシステムログをバックアップします。
本画面を表示するには、Tools > Log Backup > Log Backup to TFTP をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（IPv4 / IPv6）を指定します。
Destination	FTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。
Log Type	バックアップするログの種類を以下のどちらかから選択します。 • System Log を選択すると、システムログをバックアップします。 • Attack Log を選択すると、アタックログをバックアップします。

システムログのバックアップを開始するには、Backup ボタンをクリックします。

15.5 Restore & Backup

Restore & Backup メニューからは、イメージファイルや構成ファイルなどのファイル一式の一括レストアおよびバックアップを実行できます。

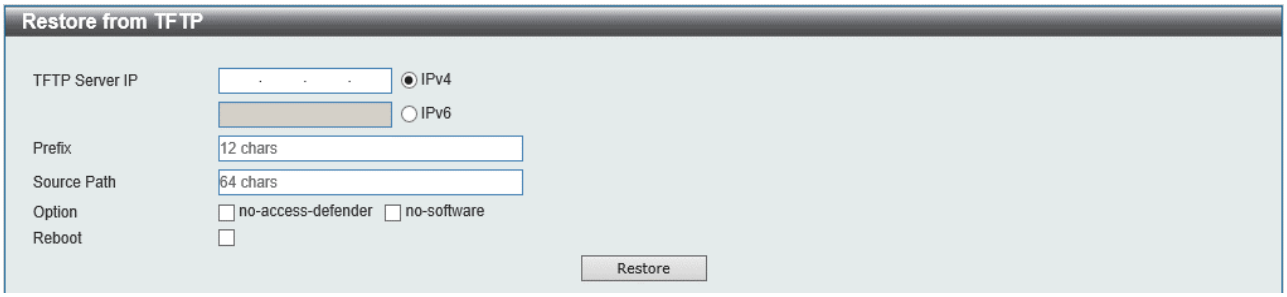
Restore & Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.5.1	Restore from TFTP	TFTP サーバーから一括レストアを実施
15.5.2	Restore from FTP	FTP サーバーから一括レストアを実施
15.5.3	Restore from SD Card	SD カードから一括レストアを実施
15.5.4	Backup to TFTP	TFTP サーバーに一括バックアップを実施
15.5.5	Backup to FTP	FTP サーバーに一括バックアップを実施
15.5.6	Backup to SD Card	SD カードに一括バックアップを実施
15.5.7	SD Card Backup Clone	SD カードにクローンファイルをバックアップ

15.5.1 Restore from TFTP

Restore from TFTP 画面では、TFTP サーバーから一括レストアを行います。

本画面を表示するには、**Tools** > **Restore & Backup** > **Restore from TFTP** をクリックします。



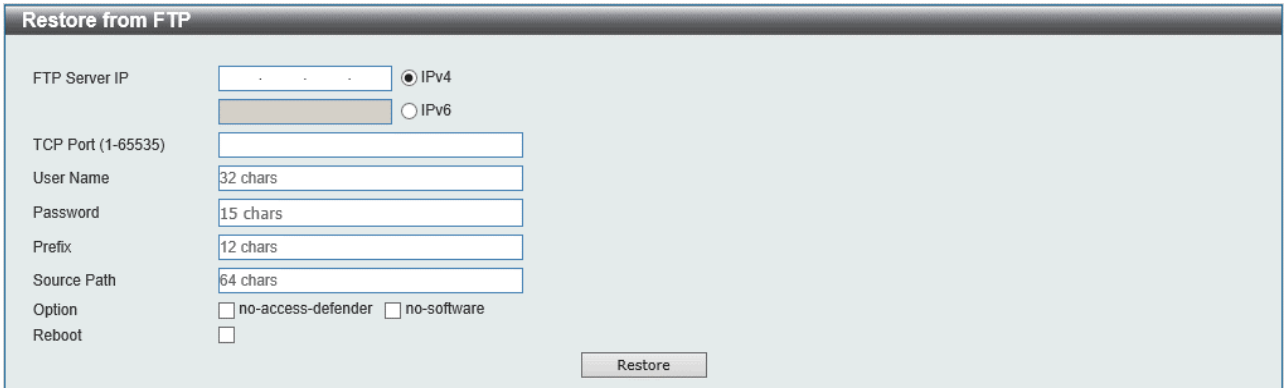
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Prefix	各ファイルに付加されたプレフィックスを 12 文字以内で入力します。
Source Path	TFTP サーバー上のファイルのパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。
Reboot	ファイルが復元された後に装置を再起動する場合にチェックします。

一括レストアを開始するには、**Restore** ボタンをクリックします。

15.5.2 Restore from FTP

Restore from FTP 画面では、FTP サーバーから一括レストアを実施します。
本画面を表示するには、**Tools** > **Restore & Backup** > **Restore from FTP** をクリックします。



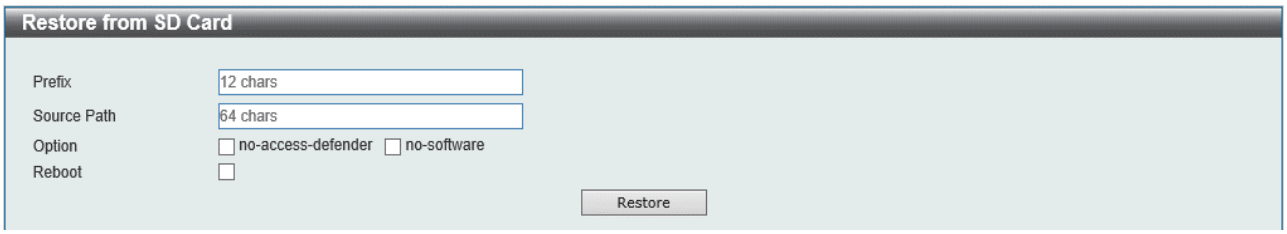
本画面の各項目の説明を以下に示します。

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1～65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Prefix	各ファイルに付加されたプレフィックスを 12 文字以内で入力します。
Source Path	FTP サーバー上のファイルパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。
Reboot	ファイルが復元された後に装置を再起動する場合にチェックします。

一括レストアを開始するには、**Restore** ボタンをクリックします。

15.5.3 Restore from SD Card

Restore from SD Card 画面では、装置に挿入した SD カードから一括レストアを実施します。
本画面を表示するには、**Tools** > **Restore & Backup** > **Restore from SD Card** をクリックします。



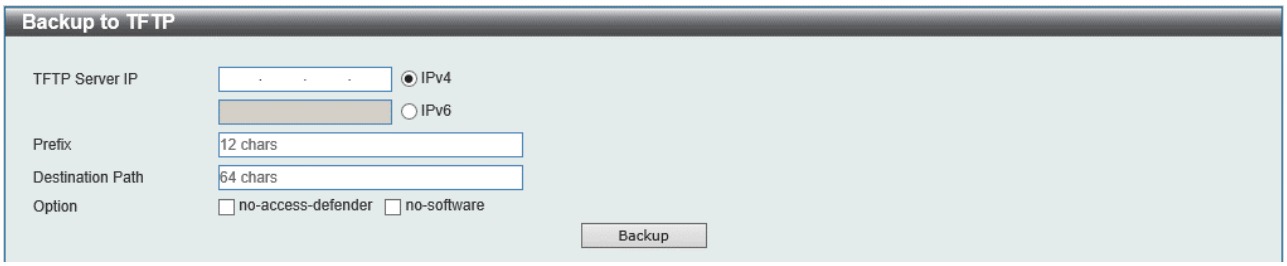
本画面の各項目の説明を以下に示します。

パラメーター	説明
Prefix	各ファイルに付加されたプレフィックスを 12 文字以内で入力します。
Source Path	SD カード上のファイルパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。
Reboot	ファイルが復元された後に装置を再起動する場合にチェックします。

一括レストアを開始するには、**Restore** ボタンをクリックします。

15.5.4 Backup to TFTP

Backup to TFTP 画面では、TFTP サーバーに一括バックアップを実施します。
本画面を表示するには、**Tools > Restore & Backup > Backup to TFTP** をクリックします。



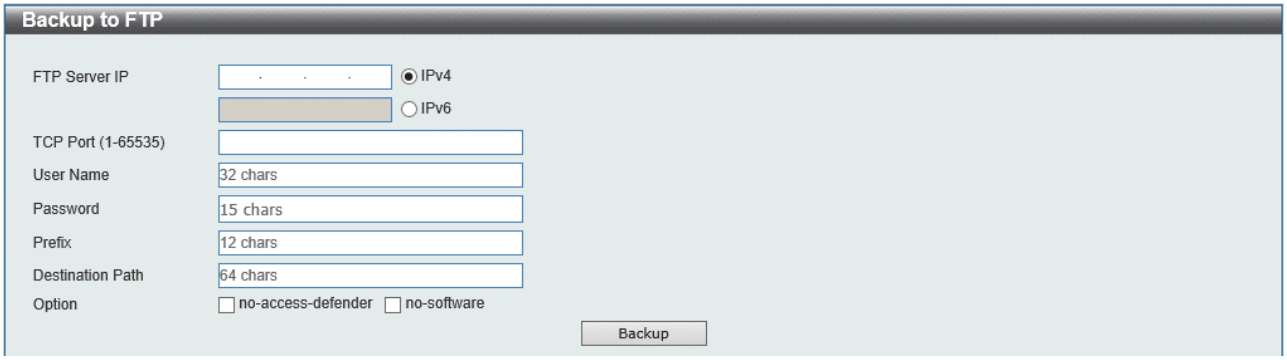
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Prefix	各ファイルに付加するプレフィックスを 12 文字以内で入力します。
Destination Path	TFTP サーバーの保存先ファイルパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。

一括バックアップを開始するには、**Backup** ボタンをクリックします。

15.5.5 Backup to FTP

Backup to FTP 画面では、FTP サーバーに一括バックアップを実施します。
本画面を表示するには、**Tools** > **Restore & Backup** > **Backup to FTP** をクリックします。



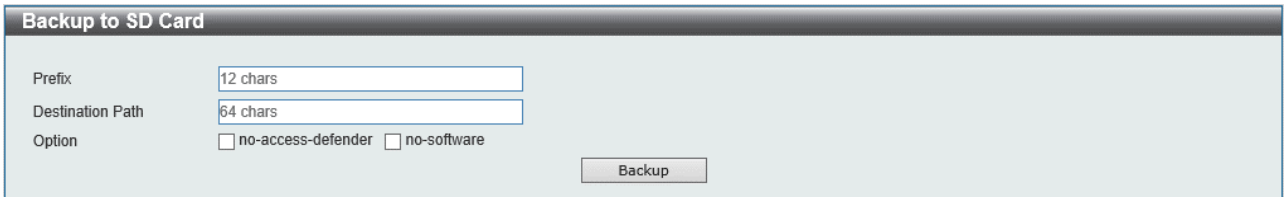
本画面の各項目の説明を以下に示します。

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1～65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Prefix	各ファイルに付加するプレフィックスを 12 文字以内で入力します。
Destination Path	FTP サーバーの保存先ファイルパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。

一括バックアップを開始するには、**Backup** ボタンをクリックします。

15.5.6 Backup to SD Card

Backup to SD Card 画面では、SD カード上のファイルを SD カード上の別の場所にバックアップします。
本画面を表示するには、**Tools** > **Restore & Backup** > **Backup to SD Card** をクリックします。



本画面の各項目の説明を以下に示します。

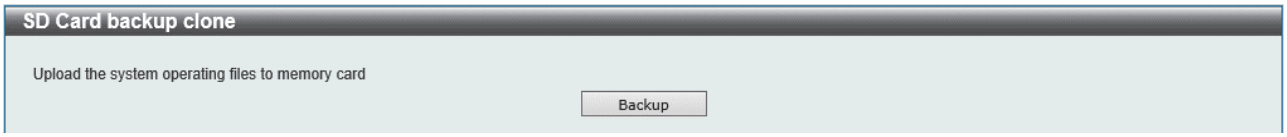
パラメーター	説明
Prefix	各ファイルに付加するプレフィックスを 12 文字以内で入力します。
Destination Path	SD カードの保存先ファイルパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。

一括バックアップを開始するには、Backup ボタンをクリックします。

15.5.7 SD Card Backup Clone

SD Card Backup Clone 画面では、クローンファイルを SD カードにバックアップします。クローンファイルは、ブート情報を含む装置の動作に必要なすべてのファイルで構成される一式のファイル群です。クローンファイルを持つ SD カードを同じ型式の別の装置に挿入して起動すると、クローンファイルを作成した装置と同じ動作をするようになります。

本画面を表示するには、Tools > Restore & Backup > SD Card Backup Clone をクリックします。



クローンファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.6 AAA-local-db Download & Backup

AAA-local-db Download & Backup メニューからは、AAA のローカルデータベースファイルのバックアップ、リストアを実行できます。

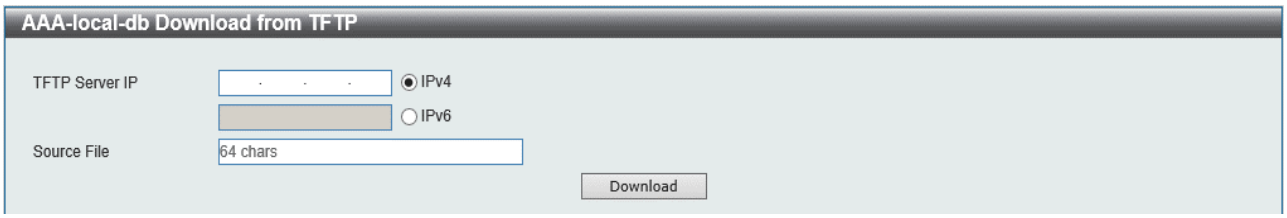
AAA-local-db Download & Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.6.1	AAA-local-db Download from TFTP	TFTP サーバーから AAA ローカルデータベースファイルをダウンロード
15.6.2	AAA-local-db Backup to TFTP	TFTP サーバーに AAA ローカルデータベースファイルをバックアップ

15.6.1 AAA-local-db Download from TFTP

AAA-local-db Download from TFTP 画面では、TFTP サーバーからローカル AAA データベースファイルをダウンロードします。

本画面を表示するには、**Tools > AAA-local-db Download & Backup > AAA-local-db Download from TFTP** をクリックします。



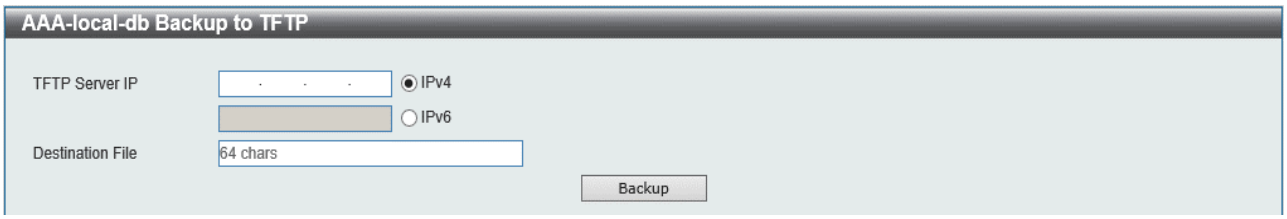
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Source File	TFTP サーバー上のファイル名とパスを 64 文字以内で入力します。

ファイルのダウンロードを開始するには、**Download** ボタンをクリックします。

15.6.2 AAA-local-db Backup to TFTP

AAA-local-db Backup to TFTP 画面では、ローカル AAA データベースファイルを TFTP サーバーにバックアップします。
本画面を表示するには、**Tools > AAA-local-db Download & Backup > AAA-local-db Backup to TFTP** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Destination File	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

ファイルのバックアップを開始するには、**Backup** ボタンをクリックします。

15.7 SSL Files Download & Backup

SSL Files Download & Backup メニューからは、SSL 関連のファイルのバックアップ、リストアを実行できます。

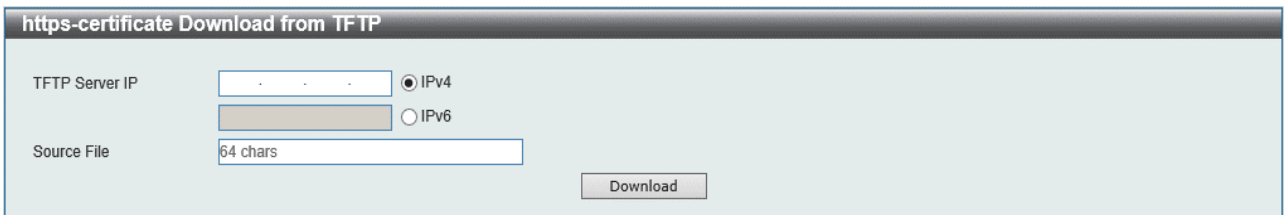
SSL Files Download & Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.7.1	https-certificate Download from TFTP	TFTP サーバーから HTTPS 証明書をダウンロード
15.7.2	https-certificate Backup to TFTP	TFTP サーバーに HTTPS 証明書をアップロード
15.7.3	https-private-key Download from TFTP	TFTP サーバーから HTTPS 秘密鍵ファイルをダウンロード
15.7.4	https-private-key Backup to TFTP	TFTP サーバーに HTTPS 秘密鍵ファイルをアップロード

15.7.1 https-certificate Download from TFTP

https-certificate Download from TFTP 画面では、TFTP サーバーから装置に HTTPS 証明書をダウンロードします。

本画面を表示するには、**Tools > SSL Files Download & Backup > https-certificate Download from TFTP** をクリックします。



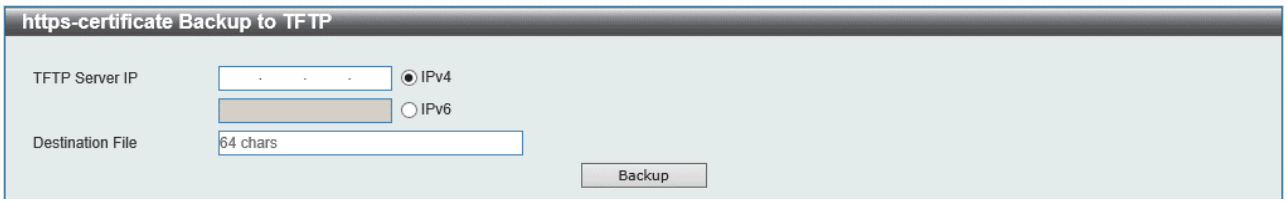
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Source File	TFTP サーバー上のファイル名とパスを 64 文字以内で入力します。

HTTPS 証明書ファイルのダウンロードを開始するには、**Download** ボタンをクリックします。

15.7.2 https-certificate Backup to TFTP

https-certificate Backup to TFTP 画面では、HTTPS 証明書を装置から TFTP サーバーにバックアップします。
本画面を表示するには、**Tools > SSL Files Download & Backup > https-certificate Backup to TFTP** をクリックします。



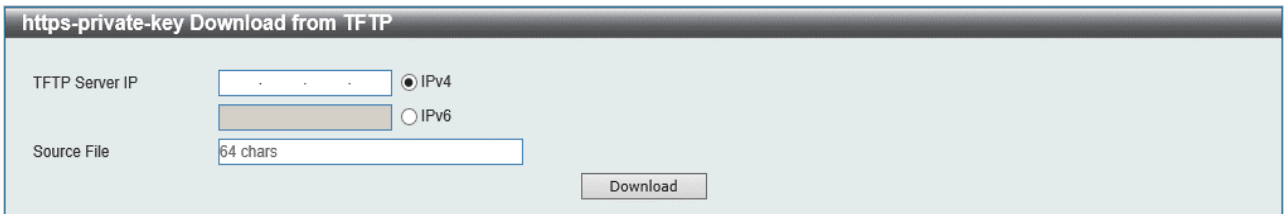
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Destination File	TFTP サーバーの宛先ファイル名とパスを 64 文字以内で入力します。

HTTPS 証明書のバックアップを開始するには、**Backup** ボタンをクリックします。

15.7.3 https-private-key Download from TFTP

https-private-key Download from TFTP 画面では、HTTPS 秘密鍵ファイルを TFTP サーバーから装置にダウンロードします。
本画面を表示するには、**Tools > SSL Files Download & Backup > https-private-key Download from TFTP** をクリックします。



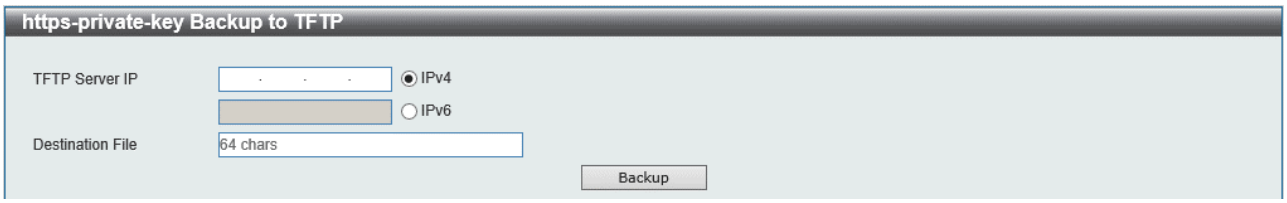
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Source File	TFTP サーバー上のファイル名とパスを 64 文字以内で入力します。

HTTPS 秘密鍵ファイルのダウンロードを開始するには、**Download** ボタンをクリックします。
なお、SSL または Web 認証が有効な場合、ダウンロードできません。

15.7.4 https-private-key Backup to TFTP

https-private-key Backup to TFTP 画面では、HTTPS 秘密鍵ファイルを装置から TFTP サーバーにバックアップします。
本画面を表示するには、**Tools > SSL Files Download & Backup > https-private-key Backup to TFTP** をクリックします。



本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Destination File	TFTP サーバーの宛先ファイル名とパスを 64 文字以内で入力します。

HTTPS 秘密鍵ファイルのバックアップを開始するには、**Backup** ボタンをクリックします。

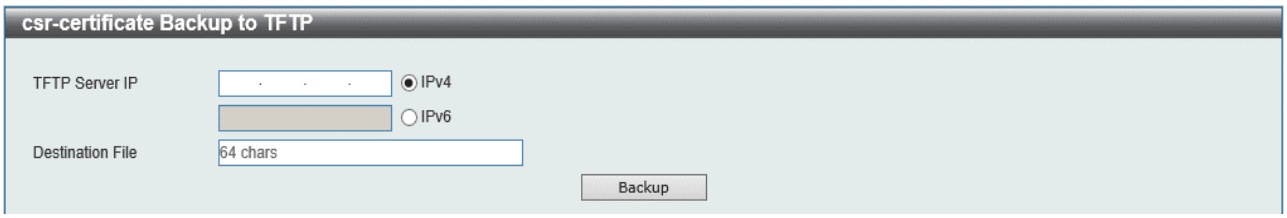
15.8 CSR Files Backup

CSR Files Backup メニューからは、CSR ファイルのバックアップを実行できます。
CSR Files Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.8.1	csr-certificate Backup to TFTP	TFTP サーバーに CSR ファイルをバックアップ
15.8.2	csr-private-key Backup to TFTP	TFTP サーバーに CSR 秘密鍵ファイルをバックアップ

15.8.1 csr-certificate Backup to TFTP

csr-certificate Backup to TFTP 画面では、装置から TFTP サーバーに CSR ファイルをバックアップします。
本画面を表示するには、**Tools > CSR Files Backup > csr-certificate Backup to TFTP** をクリックします。



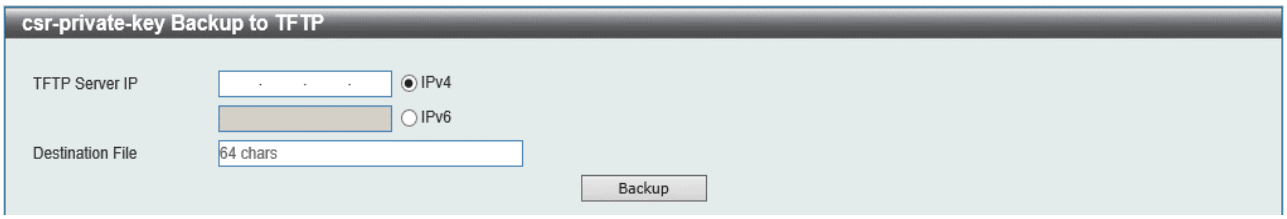
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Destination File	TFTP サーバーの宛先ファイル名とパスを 64 文字以内で入力します。

CSR ファイルのバックアップを開始するには、**Backup** ボタンをクリックします。

15.8.2 csr-private-key Backup to TFTP

csr-private-key Backup to TFTP 画面では、CSR 秘密鍵ファイルを装置から TFTP サーバーにバックアップします。
本画面を表示するには、**Tools** > **CSR Files Backup** > **csr-private-key Backup to TFTP** をクリックします。



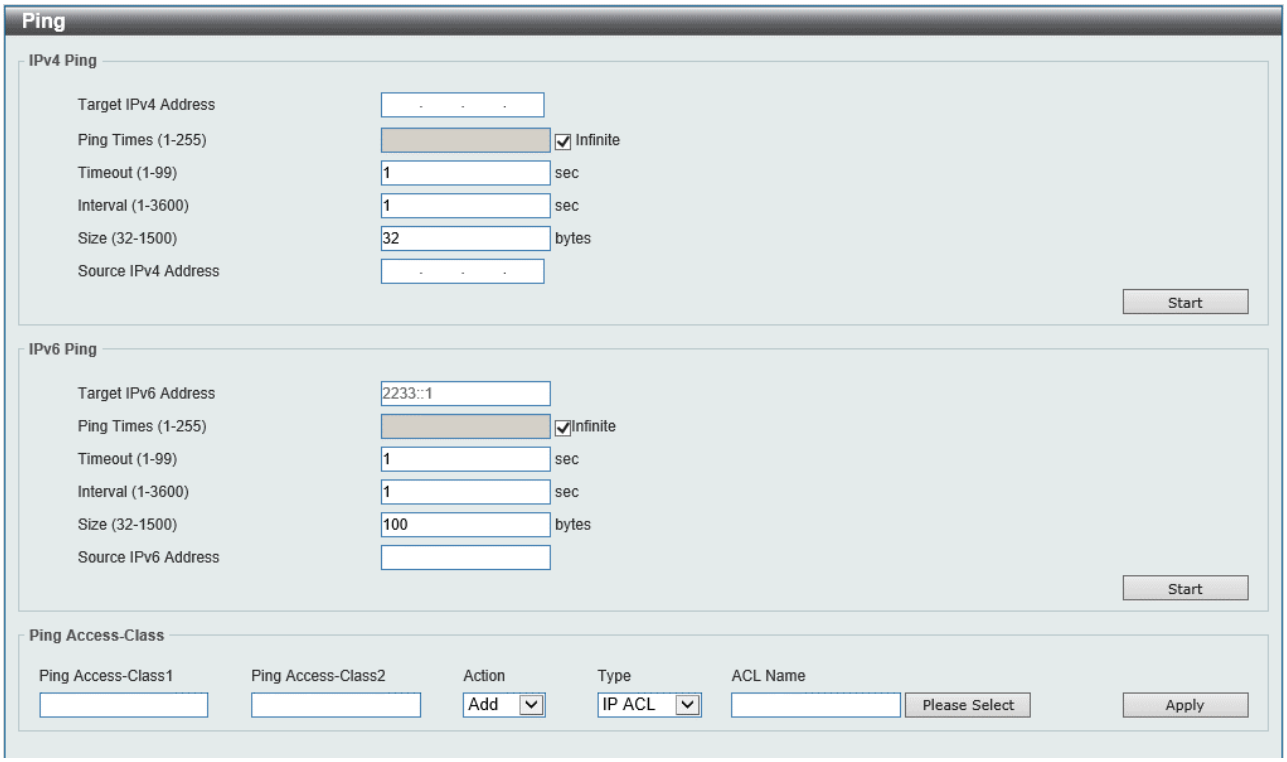
本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジオボタンで IP アドレスの形式（**IPv4** / **IPv6**）を指定します。
Destination File	TFTP サーバーの宛先ファイル名とパスを 64 文字以内で入力します。

CSR 秘密鍵ファイルのバックアップを開始するには、**Backup** ボタンをクリックします。

15.9 Ping

Ping 画面では、ネットワーク上の他のデバイスに ping を実行します。
本画面を表示するには、**Tools** > **Ping** をクリックします。



IPv4 Ping の各項目の説明を以下に示します。

パラメーター	説明
Target IPv4 Address	Ping を実行する IPv4 アドレスを入力します。
Ping Times	IPv4 アドレスへの Ping の試行回数を 1～255 の範囲で入力します。 手動で停止させるまで、指定した IPv4 アドレスに Ping を実行し続けるには、**Infinite** をチェックします。
Timeout	Ping のタイムアウトを 1～99（秒）の範囲で入力します。
Interval	Ping の送信の間隔を 1～3600（秒）入力します。
Size	Ping パケットサイズを 32～1500（バイト）の範囲で入力します。
Source IPv4 Address	送信元 IPv4 アドレスを入力します。本装置では指定する必要はありません。

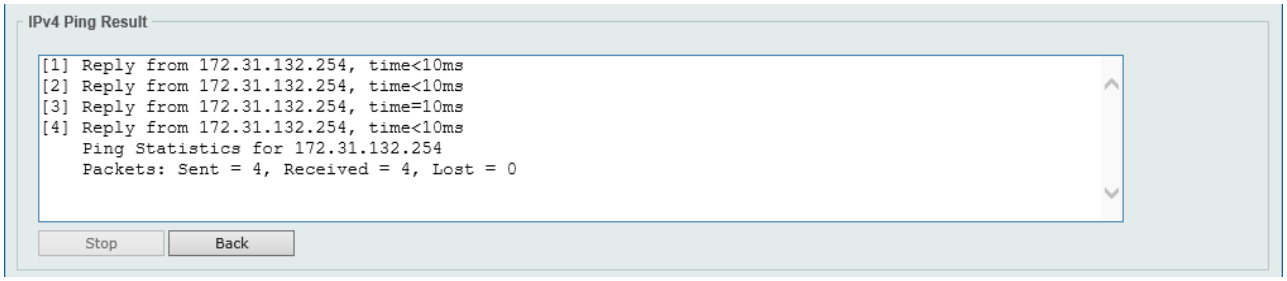
Ping を実行するには、**Start** ボタンをクリックします。

IPv6 Ping の各項目の説明を以下に示します。

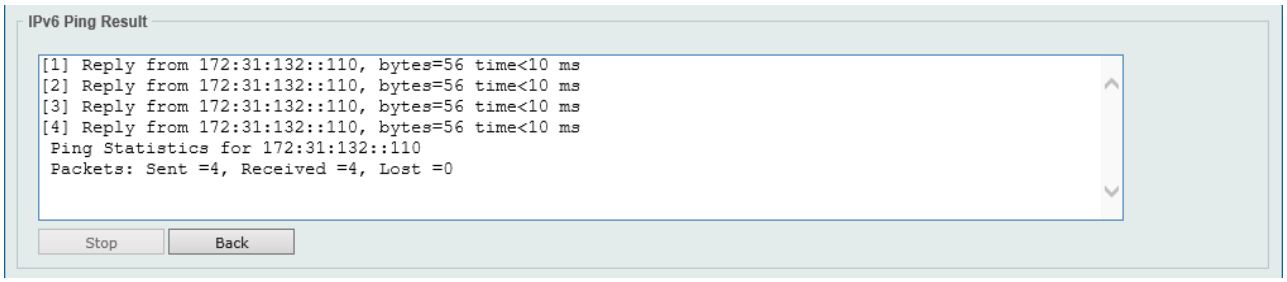
パラメーター	説明
Target IPv6 Address	Ping を実行する IPv6 アドレスを入力します。
Ping Times	IPv6 アドレスへの Ping の試行回数を 1～255 の範囲で入力します。 手動で停止させるまで指定した IPv6 アドレスに Ping を実行し続けるには、**Infinite** をチェックします。
Timeout	Ping のタイムアウトを 1～99（秒）の範囲で入力します。
Interval	Ping リクエストの間隔を 1～3600（秒）の範囲で入力します（デフォルト：1 秒）。
Size	Ping パケットサイズを 32～1500（バイト）の範囲で入力します（デフォルト：100 バイト）。
Source IPv6 Address	送信元 IPv6 アドレスを入力します。 リモートホストに送信されるパケットの送信元 IPv6 アドレスとして使用されます。

Ping を実行するには、**Start** ボタンをクリックします。

IPv4 Ping の **Start** ボタンをクリックすると、**IPv4 Ping Result** が表示されます。



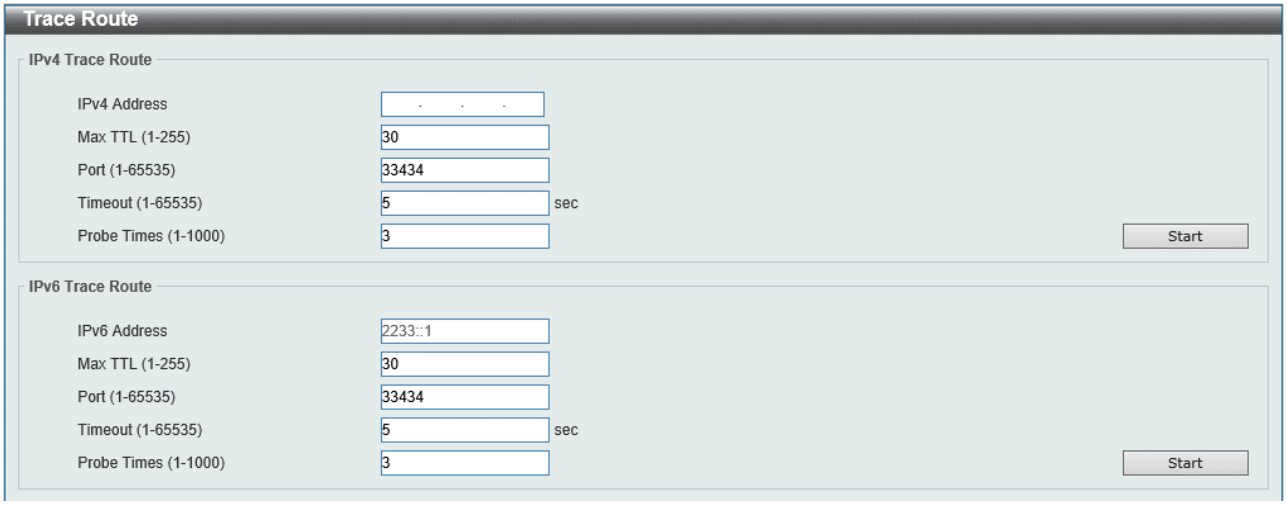
IPv6 Ping の **Start** ボタンをクリックすると、**IPv6 Ping Result** が表示されます。



Ping を停止するには、**Stop** ボタンをクリックします。
Ping 画面に戻るには、**Back** ボタンをクリックします。

15.10 Trace Route

Trace Route 画面では、ネットワーク上の他のデバイスに Traceroute を実行します。
本画面を表示するには、**Tools** > **Trace Route** をクリックします。



IPv4 Trace Route の各項目の説明を以下に示します。

パラメーター	説明
IPv4 Address	宛先の IPv4 アドレスを入力します。
Max TTL	Traceroute の最大 TTL を 1～255 の範囲で入力します。
Port	Traceroute で使用する TCP/UDP ポート番号を 1～65535 の範囲で入力します。
Timeout	Traceroute の各ホップのタイムアウトを 1～65535（秒）の範囲で入力します。
Probe Times	Traceroute のプローブ回数を 1～1000 の範囲で入力します。

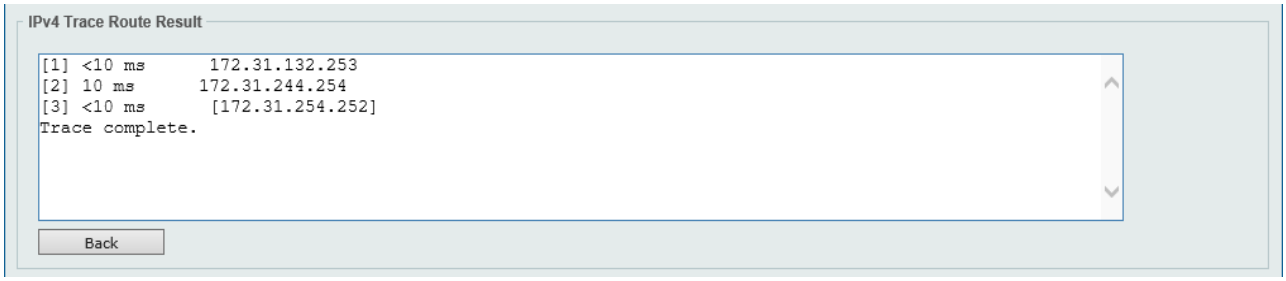
Traceroute を実行するには、**Start** ボタンをクリックします。

IPv6 Trace Route の各項目の説明を以下に示します。

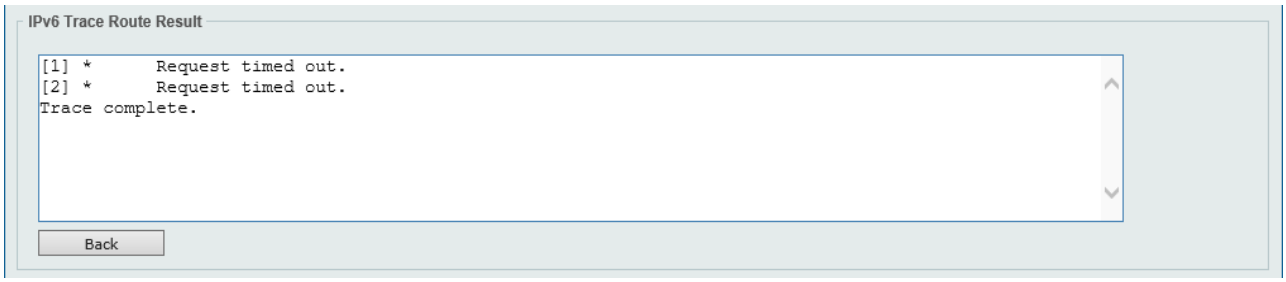
パラメーター	説明
IPv6 Address	宛先の IPv6 アドレスを入力します。
Max TTL	Traceroute の最大 TTL を 1～255 の範囲で入力します。
Port	Traceroute の TCP/UDP ポート番号を 1～65535 の範囲で入力します。
Timeout	Traceroute の各ホップのタイムアウトを 1～65535（秒）の範囲で入力します。
Probe Times	Traceroute のプローブ回数を 1～1000 の範囲で入力します（デフォルト：3）。

Traceroute を実行するには、**Start** ボタンをクリックします。

IPv4 Trace Route の **Start** ボタンをクリックすると、**IPv4 Trace Route Result** が表示されます。



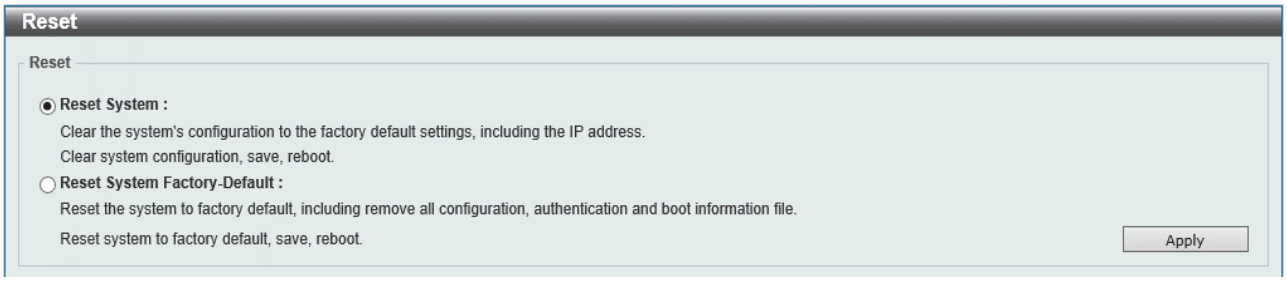
IPv6 Trace Route の **Start** ボタンをクリックすると、**IPv6 Trace Route Result** が表示されます。



Traceroute を停止して **Trace Route** 画面に戻るには、**Back** ボタンをクリックします。

15.11 Reset

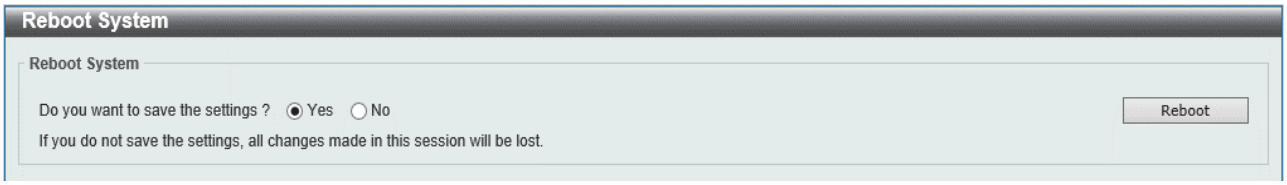
Reset 画面では、システムをリセットします。システムをリセットし、工場出荷時のデフォルト設定に戻すこともできます。
本画面を表示するには、**Tools** > **Reset** をクリックします。



システムをリセットするには、**Apply** ボタンをクリックします。

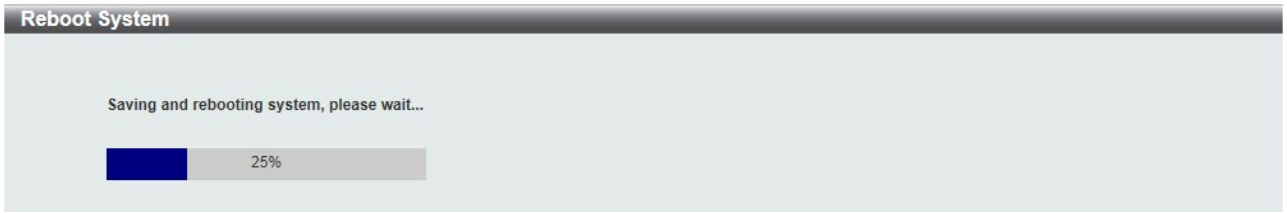
15.12 Reboot System

Reboot System 画面では、装置を再起動します。装置を再起動する前に、現在の設定を保存することもできます。
本画面を表示するには、Tools > Reboot System をクリックします。



装置の再起動では、Do you want to save the settings? で Yes を選択すると、現在の設定が起動時設定ファイルに反映されます。No を選択すると、起動時設定ファイルに反映されないため、設定変更を実施した場合に、別途設定保存の操作を実行している場合を除き、変更した内容が失われます。

装置を再起動するには、Reboot ボタンをクリックします。



ApresiaLightGM200 シリーズ Ver.2.00 SW マニュアル

2021 年 7 月 初版

APRESIA Systems 株式会社
東京都中央区築地二丁目 3 番 4 号
築地第一長岡ビル
https://www.apresiasystems.co.jp/