

ApresiaLightGM300 シリーズ

Ver. 3.00

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
-	2025年02月14日	新規制定

目次

制定・改訂履歴表.....	1
目次	2
1 はじめに	5
1.1 本文中の表記について.....	7
1.2 初期 IP アドレスの設定.....	8
2 Web UI について.....	9
2.1 Web UI の接続方法.....	9
2.2 Web UI の画面説明.....	10
2.3 デバイス情報.....	11
2.4 メニューの内容	12
2.5 本書での説明の記載内容について	13
3 System	14
3.1 System Information Settings.....	14
3.2 Peripheral Settings	15
3.3 Port Configuration.....	16
3.4 Port Redundant	21
3.5 System Log.....	24
3.6 Time and SNTP.....	29
4 Management.....	33
4.1 Command Logging.....	33
4.2 User Accounts Settings.....	34
4.3 User Accounts Encryption.....	36
4.4 Login Method	37
4.5 SNMP	39
4.6 RMON	47
4.7 Telnet/Web.....	52
4.8 Session Timeout.....	53
4.9 CPU Protection	54
4.10 Zero Touch Provision.....	56
4.11 IP Source Interface.....	57
4.12 File System.....	58
5 Layer 2 Features.....	60
5.1 FDB.....	60
5.2 VLAN.....	64
5.3 VLAN Tunnel	69
5.4 STP	72
5.5 MMRP Plus Settings	78
5.6 Loop Detection	81
5.7 Loop Detection Information	83

5.8 Link Aggregation	84
5.9 L2 Multicast Control.....	86
5.10 LLDP	104
6 Layer 3 Features	114
6.1 ARP.....	114
6.2 IPv6 Neighbor.....	116
6.3 Interface.....	117
6.4 IPv4 Default Route	121
6.5 IPv4 Route Table.....	122
6.6 IPv6 Default Route	123
6.7 IPv6 Route Table.....	124
7 QoS.....	125
7.1 Basic Settings	125
7.2 Advanced Settings	130
8 ACL.....	143
8.1 ACL Configuration Wizard.....	143
8.2 ACL Access List.....	161
8.3 ACL Interface Access Group	177
8.4 ACL VLAN Access Map	178
8.5 ACL VLAN Filter.....	180
8.6 ACL Resource Reserved Group	181
8.7 ACL Resource Reserved Priority.....	182
9 Security	183
9.1 Port Security.....	183
9.2 802.1X.....	186
9.3 Access Defender	189
9.4 AAA	195
9.5 RADIUS	204
9.6 TACACS.....	208
9.7 DHCP Snooping	211
9.8 BPDU Guard	214
9.9 MAC Authentication.....	215
9.10 Web Authentication	217
9.11 Network Access Authentication.....	220
9.12 Trusted Host	223
9.13 Traffic Segmentation Settings.....	224
9.14 Storm Control.....	225
9.15 SSH.....	228
9.16 SSL.....	231
10 DDM.....	233
10.1 DDM Voltage Threshold	233

10.2 DDM Bias Current Threshold.....	234
10.3 DDM TX Power Threshold.....	235
10.4 DDM RX Power Threshold.....	236
10.5 DDM Status	237
11 Monitoring	238
11.1 Utilization.....	238
11.2 Statistics.....	239
11.3 Mirror Settings	243
11.4 Device Environment.....	245
12 Green	246
12.1 EEE	246
13 Alarm	247
13.1 Alarm Settings.....	247
13.2 Alarm Debug.....	249
14 Save.....	250
14.1 Write Memory.....	250
15 Tools	251
15.1 Firmware Upgrade & Backup	251
15.2 Configuration Restore & Backup.....	255
15.3 Tech-support.....	259
15.4 Log Backup.....	261
15.5 Restore & Backup.....	263
15.6 AAA-local-db Download & Backup.....	268
15.7 SSL Files Download & Backup	270
15.8 CSR Files Backup	273
15.9 Ping.....	275
15.10 Trace Route.....	277
15.11 Reset.....	279
15.12 Reboot System	280

1 はじめに

■本書の目的

本書は、Web ブラウザーを使用して ApresiaLightGM300 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。また、Web UI で設定する主要な機能の概略を説明します。

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、ApresiaLightGM300 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。

1 はじめに

■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	<p>以下の UI を示します。</p> <ul style="list-style-type: none"> 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 <p>例) File メニューを開き、Cancel を選択します。</p> <p>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。</p>
斜体	<p>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を示します。</p> <p>例) <i>filename</i></p> <p>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。</p>
メニュー名 > メニューオプション	<p>メニュー構造を示します。</p> <p>例) Device > Port > Port Properties</p> <p>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。</p>
頭文字の大文字	<p>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。</p> <p>例) Enter を押します。</p>



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。

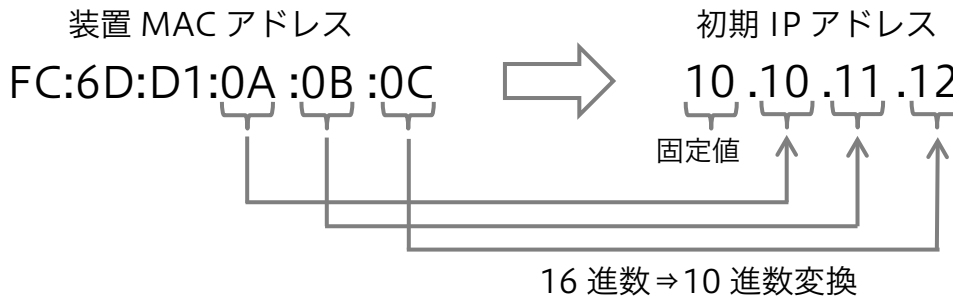
1.2 初期 IP アドレスの設定

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 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 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。

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

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。



Connect to 10.85.104.32

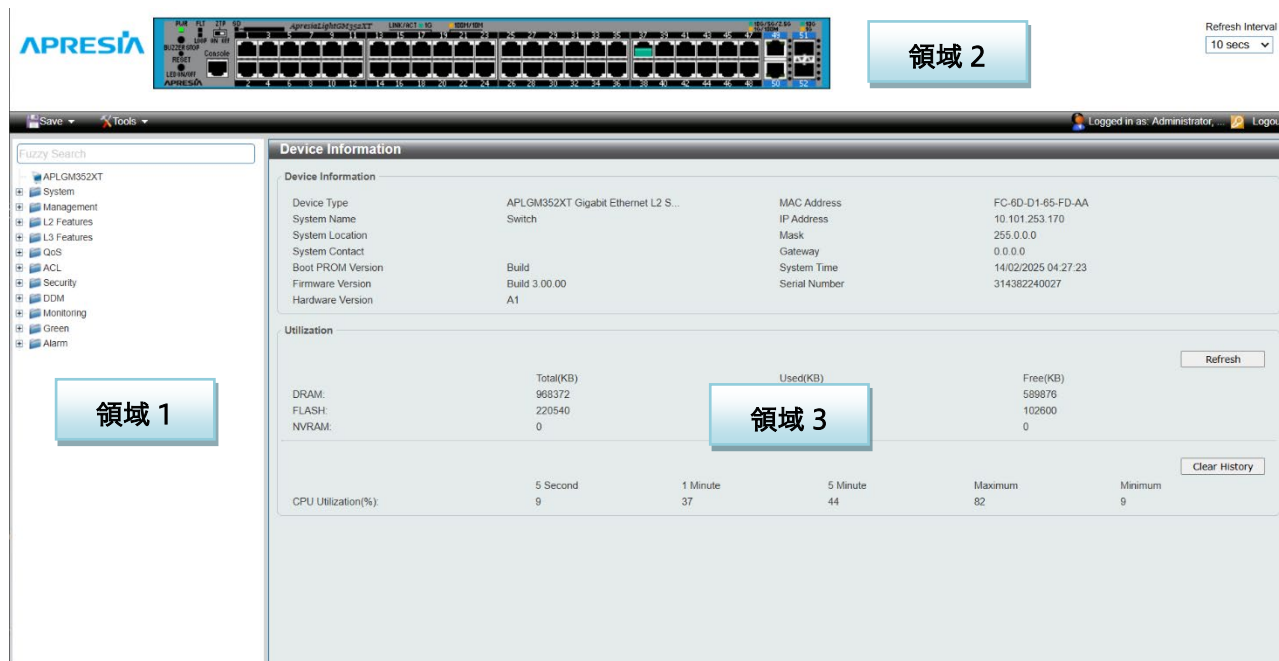
User Name

Password

Login Reset

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)	<p>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。</p> <p>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。</p> <p>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。</p>
領域 2 (フロントパネルビュー)	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
領域 3 (メイン画面)	<p>ログイン直後は、Device Information 画面が表示されます。</p> <p>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。</p>

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 **APLGM352XT**)をクリックします。

Device Information					
Device Information					
Device Type	APLGM352XT Gigabit Ethernet L2 S...	MAC Address	FC-6D-D1-65-FD-AA		
System Name	Switch	IP Address	10.101.253.170		
System Location		Mask	255.0.0.0		
System Contact		Gateway	0.0.0.0		
Boot PROM Version	Build	System Time	14/02/2025 04:27:23		
Firmware Version	Build 3.00.00	Serial Number	314382240027		
Hardware Version	A1				
Utilization					
	Total(KB)	Used(KB)	Free(KB)		<input type="button" value="Refresh"/>
DRAM:	968372	378496	589876		
FLASH:	220540	117940	102600		
NVRAM:	0	0	0		
<input type="button" value="Clear History"/>					
CPU Utilization(%)	5 Second	1 Minute	5 Minute	Maximum	Minimum
	9	37	44	82	9

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

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	Layer 2 Features	レイヤー2 の機能に関する設定
6	Layer 3 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。

The screenshot shows the 'Policy Map' configuration page. It has a header 'Policy Map' and a sub-header 'Create/Delete Policy Map'. Below this is a form with a 'Policy Map Name' field (32 chars) and an 'Apply' button. The next section is 'Traffic Policy', which has a 'Policy Map Name' field (32 chars), a 'Class Map Name' field (32 chars), and an 'Apply' button. Below that is a table titled 'Total Entries: 2' with two rows: 'Policy' and 'Policy_vlan', each with a 'Delete' button. At the bottom of this table is a pagination control showing '1/1' and a 'Go' button. The final section is 'Class Rules' with a table header 'Class Map Name'.

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。

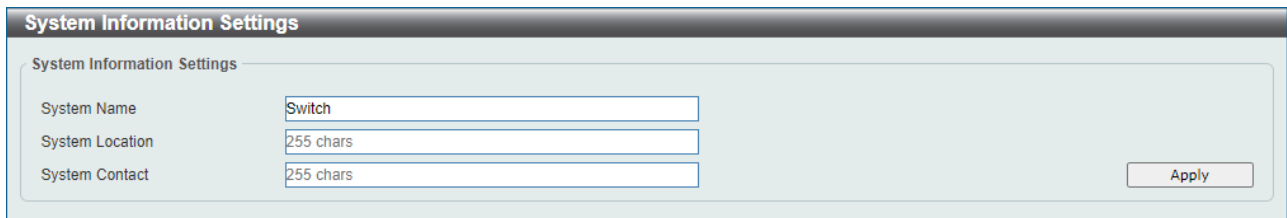
表示された画面には、現在の設定情報や状態を表示するテーブルが含まれる場合があります。テーブルには表示できる行数のサイズが決められており、それを越えたエントリが存在する場合は複数のページにまたがります。この場合、テーブル右下にあるページ番号ボタンをクリックするか、またはテキストボックスにページ番号を入力して **Go** ボタンをクリックすると、指定したページに移動します。

3 System

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。



The screenshot shows a web interface for 'System Information Settings'. It features three text input fields: 'System Name' containing 'Switch', 'System Location' containing '255 chars', and 'System Contact' containing '255 chars'. An 'Apply' button is positioned in the bottom right corner of the form area.

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、装置の環境に関する設定を行います。
本画面を表示するには、**System > Peripheral Settings** をクリックします。

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

パラメーター	説明
Fan Trap	ファンの SNMP トラップ機能を有効または無効にします。
Temperature Trap	温度の SNMP トラップ機能を有効または無効にします。

設定を適用するには、**Apply** ボタンをクリックします。

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

パラメーター	説明
User Port LED	ポート LED 機能の状態 (Enabled / Disabled) を選択します。無効にした場合、ポートがリンクアップしてもポート LED は点灯しません。ただし、Alarm Settings で Warning LED が有効になっている場合、機能に対応した警告 LED の点滅動作は行います。

設定を適用するには、**Apply** ボタンをクリックします。

Environment Temperature Threshold Settings 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 (°C) 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 (°C) 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。以下の項で説明するサブメニューに分かれています。

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。

Port	Link Status	State	MDIX	Flow Control		Duplex	Speed	Auto Downgrade	Description
				Send	Receive				
Port1/0/1	Up	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	
Port1/0/2	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	
Port1/0/3	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	
Port1/0/4	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	
Port1/0/5	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	
Port1/0/6	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	
Port1/0/7	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	
Port1/0/8	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	
Port1/0/9	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	
Port1/0/10	Down	Enabled	Auto-MDIX	Off	Off	Auto-duplex	Auto-speed	Disabled	

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。ポートの動作速度やデュプレックスに関する設定では、該当するポートで対応していない設定を行うことはできません。各項目の説明を以下に示します。

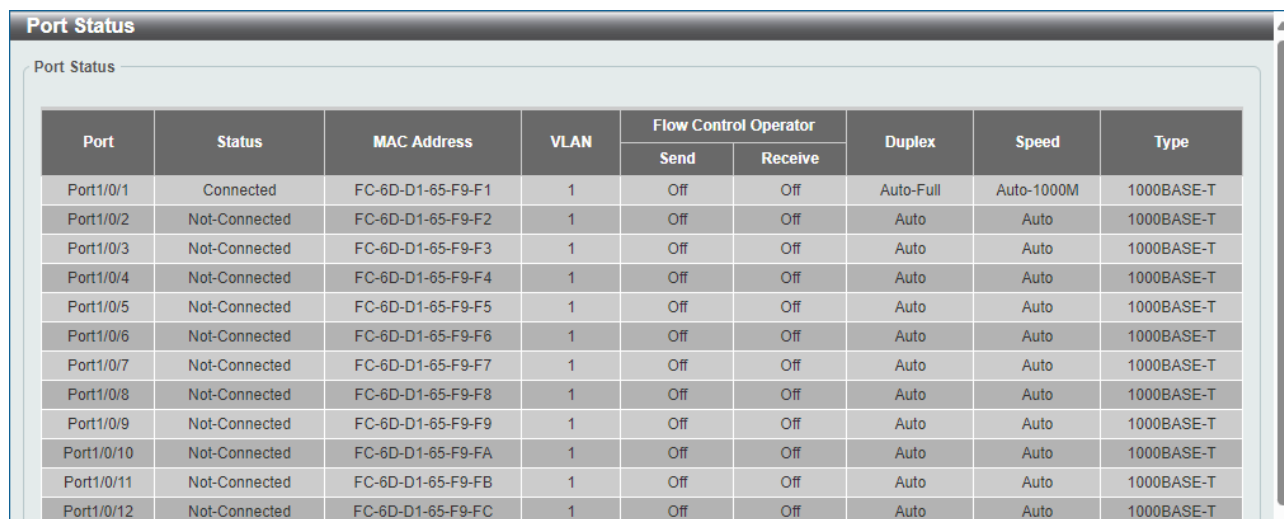
パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
State	物理ポートの状態 (Enabled / Disabled) を選択します。
MDIX	MDI/ MDIX の設定 (Auto / Normal / Cross) を選択します。
Auto Downgrade	自動ダウングレード機能の状態 (Enabled / Disabled) を選択します。
Flow Control	フロー制御の状態 (On / Off) を選択します。
Duplex	ポートのデュプレックス (Auto / Half / Full) を選択します。
Speed	ポ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。 オートネゴシエーション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ダプ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。

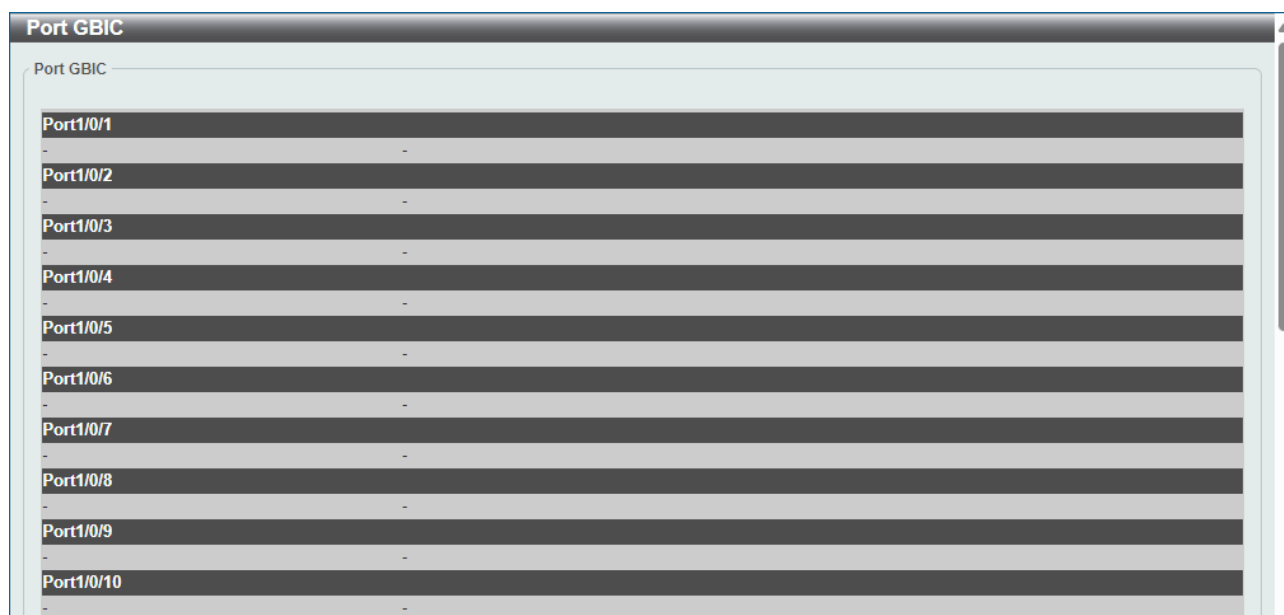
本画面を表示するには、**System > Port Configuration > Port Status** をクリックします。



Port	Status	MAC Address	VLAN	Flow Control Operator		Duplex	Speed	Type
				Send	Receive			
Port1/0/1	Connected	FC-6D-D1-65-F9-F1	1	Off	Off	Auto-Full	Auto-1000M	1000BASE-T
Port1/0/2	Not-Connected	FC-6D-D1-65-F9-F2	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/3	Not-Connected	FC-6D-D1-65-F9-F3	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/4	Not-Connected	FC-6D-D1-65-F9-F4	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/5	Not-Connected	FC-6D-D1-65-F9-F5	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/6	Not-Connected	FC-6D-D1-65-F9-F6	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/7	Not-Connected	FC-6D-D1-65-F9-F7	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/8	Not-Connected	FC-6D-D1-65-F9-F8	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/9	Not-Connected	FC-6D-D1-65-F9-F9	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/10	Not-Connected	FC-6D-D1-65-F9-FA	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/11	Not-Connected	FC-6D-D1-65-F9-FB	1	Off	Off	Auto	Auto	1000BASE-T
Port1/0/12	Not-Connected	FC-6D-D1-65-F9-FC	1	Off	Off	Auto	Auto	1000BASE-T

3.3.3 Port GBIC

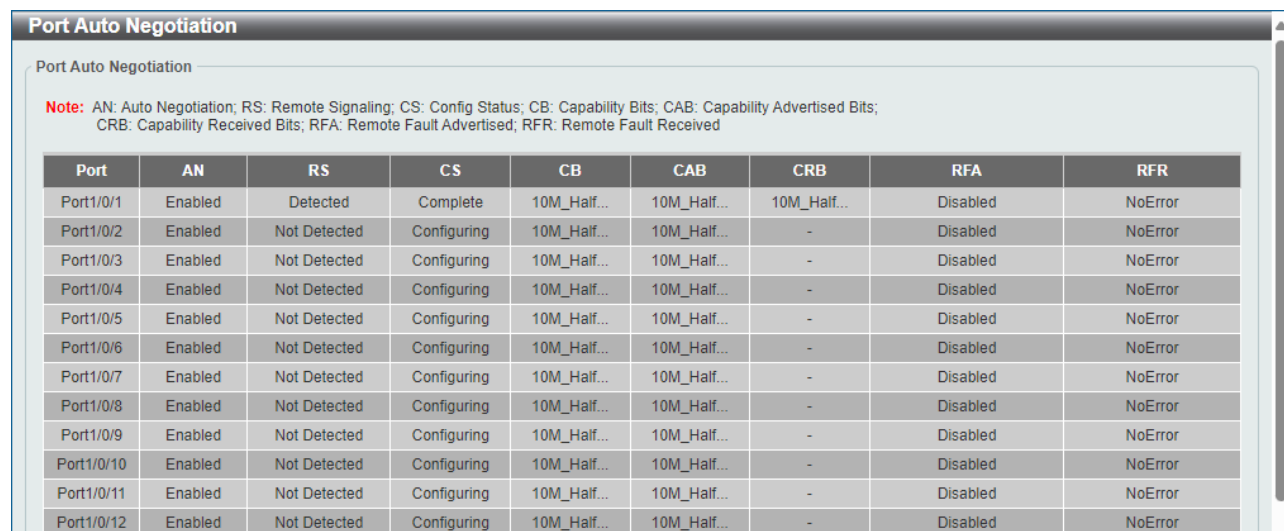
Port GBIC 画面では、装置の各 SFP ポートで検出されたモジュールの情報を確認できます。本画面を表示するには、**System > Port Configuration > Port GBIC** をクリックします。



Port	Module
Port1/0/1	-
Port1/0/2	-
Port1/0/3	-
Port1/0/4	-
Port1/0/5	-
Port1/0/6	-
Port1/0/7	-
Port1/0/8	-
Port1/0/9	-
Port1/0/10	-

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。



Note: AN: Auto Negotiation; RS: Remote Signaling; CS: Config Status; CB: Capability Bits; CAB: Capability Advertised Bits; CRB: Capability Received Bits; RFA: Remote Fault Advertised; RFR: Remote Fault Received

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	Not Detected	Configuring	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
Port1/0/11	Enabled	Not Detected	Configuring	10M_Half...	10M_Half...	-	Disabled	NoError
Port1/0/12	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。BPDU ガード機能に対しては、Attacked 状態からの自動復旧にも適用されます。

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 の原因となる機能 (All / Port Security / Storm Control / BPDU Guard / Loop Detection) 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 64~12288 (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 Port Redundant

Port Redundant サブメニューでは、ポトリダント機能の設定を行います。以下の項で説明するサブメニューに分かれています。

3.4.1 Redundant Group Preempt

Redundant Group Preempt 画面では、指定されたポトリダントグループのプリエンプトモードを設定します。

本画面を表示するには、**System > Port Redundant > Redundant Group Preempt** をクリックします。

The screenshot shows the 'Redundant Group Preempt' configuration window. At the top, there's a title bar 'Redundant Group Preempt'. Below it, the 'Redundant Group Preempt Settings' section contains a 'Group ID (1-32)' text input field and a 'Mode' dropdown menu currently set to 'Disabled'. An 'Apply' button is located to the right. Below the settings is a table with the following data:

Group ID	Mode
1	Disabled

At the bottom right of the table area, there are navigation controls: '1/1', left and right arrows, a '1' in a box, and a 'Go' button.

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 ID	ポトリダントグループ ID を 1～32 の範囲で入力します。
Mode	<p>指定されたポトリダントグループのプリエンプトモードを指定します。</p> <ul style="list-style-type: none"> • Disable - disable モードを使用します。このモードでは、セカンダリーがアクティブになるとプライマリーが復旧しても引き続きアクティブの状態を継続します。 • Delay - delay モードを使用します。このモードでは、セカンダリーがアクティブの状態プライマリーが復旧すると、設定した遅延時間経過後に強制的にアクティブポートをプライマリーに切り替えます。 <ul style="list-style-type: none"> ○ Time : 遅延時間を 0～300 (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。

指定したエントリーを削除するには、**Delete** ボタンをクリックします。

3.4.2 Port Redundant Group

Port Redundant Group 画面では、ポートリダundantグループのポート設定を行います。
本画面を表示するには、**System > Port Redundant > Port Redundant Group** をクリックします。

Port	Status	Group ID	Pri/Sec
Port1/0/3	Down	1	Primary

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。
Group ID	ポートリダundantグループの ID を 1~32 の範囲で入力します。
Type	ポートリダundantグループのタイプを指定します。 <ul style="list-style-type: none"> • Primary : インターフェースをプライマリーインターフェースに指定します。 • Secondary : インターフェースをセカンダリーインターフェースに指定します。

設定を適用するには、**Apply** ボタンをクリックします。

指定したエントリーを削除するには、**Delete** ボタンをクリックします。

3.4.3 Port Redundant Settings

Port Redundant Settings 画面では、ポートリダundantの設定を行います。
本画面を表示するには、**System > Port Redundant > Port Redundant Settings** をクリックします。

Port	Group ID	Mode	Status
Port1/0/3	1	Disabled	Down

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
MAC Address Table Update	MAC アドレステーブル更新フレームの送信を有効または無効にします。有効にした場合、送信する MAC アドレステーブル更新パケットの数を 1~3 から選択します。
FDB Flush Send	FDB フラッシュフレーム（ポートリダンダント）の送信を有効または無効にします。有効にした場合、送信する FDB フラッシュフレームの数を 1~3 から選択します。
FDB Flush Receive	FDB フラッシュフレーム（ポートリダンダント）の受信機能を有効または無効にします。有効にした場合、FDB フラッシュフレーム（ポートリダンダント）を受信したときに、MAC アドレステーブルをクリアします。
VID	FDB フラッシュフレーム（ポートリダンダント）に付与する VLAN タグの VLAN ID を 1~4094 から指定します。デフォルト設定（VLAN ID に 0 を使用）に戻す場合、 Default を選択します。
Destination MAC Address	FDB フラッシュフレーム（ポートリダンダント）の宛先 MAC アドレスを指定します。デフォルト設定を使用するには、 Default オプションを選択します。

設定を適用するには、**Apply** ボタンをクリックします。

3.5 System Log

System Log サブメニューでは、システムログの設定を行います。
以下の項で説明するサブメニューに分かれています。

3.5.1 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。

The screenshot shows the 'System Log Settings' configuration page. It is organized into four main sections, each with an 'Apply' button:

- Log State:** Log State is set to 'Enabled'.
- Source Interface Settings:** Source Interface State is 'Disabled', Type is 'VLAN', and VID is '1-4094'.
- Buffer Log Settings:** Buffer Log State is 'Enabled', Severity is '6 (Informational)', Discriminator Name is '15 chars', and Write Delay is '300' sec.
- Console Log Settings:** Console Log State is 'Disabled', Severity is '4 (Warnings)', and Discriminator Name is '15 chars'.

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（バッファローギング）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	バッファローギングの状態（ Enabled / Disabled / Default ）を選択します。 Default を選択した場合、バッファロー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 Severity に該当するログが記録されます。
Discriminator Name	バッファロー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。Discriminator 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	ローカルバッファのシステムログをフラッシュメモリーに書き込むまでの遅延時間を 0~65535(秒)で指定します。デフォルト設定（300）の場合、ローカルバッファに出力されたログが 300 秒後にフラッシュメモリーに書き込まれます。その間に再起動した場合には、フラッシュメモリーに記録されません。直ちにフラッシュメモリーに記録する場合は 0 に設定します。 Infinite を選択した場合、フラッシュメモリーへの書き込みが行われません。

設定を適用するには、**Apply** ボタンをクリックします。

Console Log Settings では、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。Discriminator 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。

3.5.2 System Log Discriminator Settings

System Log Discriminator Settings 画面では、装置内部のバッファ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分類できます。

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。

System Log Discriminator Settings

Discriminator Log Settings

Discriminator Name: 15 chars

Action: Drops

SYS PORT STP LAC FDB
 LLDP ACL QOS PORTSEC DHCP
 DHCPV6 STORM_CT... SSH CLI SNMP
 ALARM AAA DEVICE RADIUS DOT1X
 BPDU_GUA... MAC CFG FIRMWARE MEAR
 MMRP

Severity: Drops

0 (Emergencies) 1 (Alerts) 2 (Critical) 3 (Errors)
 4 (Warnings) 5 (Notifications) 6 (Informational) 7 (Debugging)

Apply

Name	Action	Facility List	Severity	Severity List	
Name	Drops	PORT,STORM_CTRL	Includes	7	Delete

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 Severity を選択し、指定した Severity 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。

3.5.3 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。

System Log Server Settings

Log Server

Host IPv4 Address Host IPv6 Address

UDP Port (514,1024-65535): 514

Facility: 23

Severity: 4 (Warnings)

Discriminator Name: 15 chars

Apply

Total Entries: 1

Server IP	Severity	Facility	Discriminator Name	UDP Port	
172.31.131.1	Warnings	23		514	Delete

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	Syslog サーバーの IPv4 アドレスを入力します。																																																						
Host IPv6 Address	Syslog サーバーの IPv6 アドレスを入力します。																																																						
UDP Port	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。																																																						
Severity	Syslog サーバーに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。																																																						
Facility	<p>Syslog サーバーに出力するファシリティの番号 (0～23) を選択します。</p> <p>各ファシリティ番号は、特定のファシリティに関連付けられています。以下の表を参照してください。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>番号</th> <th>Name</th> <th>番号</th> <th>Name</th> <th>番号</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><i>user</i></td> <td>9</td> <td><i>clock1</i></td> <td>17</td> <td><i>local1</i></td> </tr> <tr> <td>2</td> <td><i>mail</i></td> <td>10</td> <td><i>auth2</i></td> <td>18</td> <td><i>local2</i></td> </tr> <tr> <td>3</td> <td><i>daemon</i></td> <td>11</td> <td><i>ftp</i></td> <td>19</td> <td><i>local3</i></td> </tr> <tr> <td>4</td> <td><i>auth1</i></td> <td>12</td> <td><i>ntp</i></td> <td>20</td> <td><i>local4</i></td> </tr> <tr> <td>5</td> <td><i>Syslog</i></td> <td>13</td> <td><i>logaudit</i></td> <td>21</td> <td><i>local5</i></td> </tr> <tr> <td>6</td> <td><i>lpr</i></td> <td>14</td> <td><i>logalert</i></td> <td>22</td> <td><i>local6</i></td> </tr> <tr> <td>7</td> <td><i>news</i></td> <td>15</td> <td><i>clock2</i></td> <td>23</td> <td><i>local7</i></td> </tr> <tr> <td>8</td> <td><i>uucp</i></td> <td>16</td> <td><i>local0</i></td> <td></td> <td></td> </tr> </tbody> </table>	番号	Name	番号	Name	番号	Name	1	<i>user</i>	9	<i>clock1</i>	17	<i>local1</i>	2	<i>mail</i>	10	<i>auth2</i>	18	<i>local2</i>	3	<i>daemon</i>	11	<i>ftp</i>	19	<i>local3</i>	4	<i>auth1</i>	12	<i>ntp</i>	20	<i>local4</i>	5	<i>Syslog</i>	13	<i>logaudit</i>	21	<i>local5</i>	6	<i>lpr</i>	14	<i>logalert</i>	22	<i>local6</i>	7	<i>news</i>	15	<i>clock2</i>	23	<i>local7</i>	8	<i>uucp</i>	16	<i>local0</i>		
番号	Name	番号	Name	番号	Name																																																		
1	<i>user</i>	9	<i>clock1</i>	17	<i>local1</i>																																																		
2	<i>mail</i>	10	<i>auth2</i>	18	<i>local2</i>																																																		
3	<i>daemon</i>	11	<i>ftp</i>	19	<i>local3</i>																																																		
4	<i>auth1</i>	12	<i>ntp</i>	20	<i>local4</i>																																																		
5	<i>Syslog</i>	13	<i>logaudit</i>	21	<i>local5</i>																																																		
6	<i>lpr</i>	14	<i>logalert</i>	22	<i>local6</i>																																																		
7	<i>news</i>	15	<i>clock2</i>	23	<i>local7</i>																																																		
8	<i>uucp</i>	16	<i>local0</i>																																																				
Discriminator Name	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。Discriminator 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。																																																						

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。

3.5.4 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。



The screenshot shows the 'System Log' interface. At the top right, there is a 'Clear Log' button. Below it, the text 'Total Entries: 65' is displayed. A table with the following columns is shown: Index, Time, Level, and Log Description. The table contains 10 rows of log entries. At the bottom right, there is a pagination control showing '1/7' and navigation buttons for first, previous, next, last, and a 'Go' button.

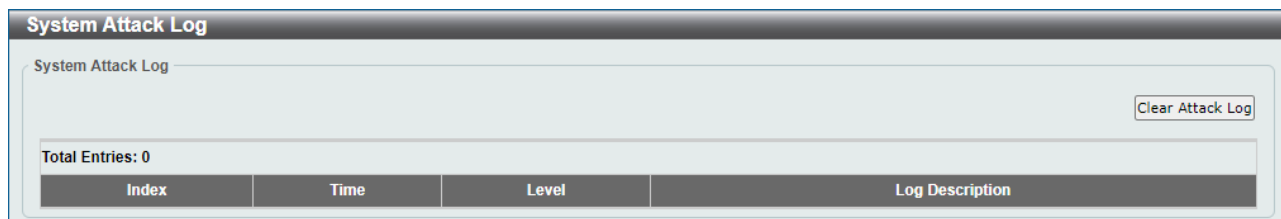
Index	Time	Level	Log Description
65	2024-09-19 12:11:09	INFO(6)	Successful login thr...
64	2024-09-19 11:05:02	INFO(6)	Web session timed ou...
63	2024-09-19 10:44:03	INFO(6)	Successful login thr...
62	2024-09-16 16:09:32	INFO(6)	Web session timed ou...
61	2024-09-16 15:49:49	INFO(6)	Successful login thr...
60	2024-09-16 15:49:10	INFO(6)	Port1/0/1 link up, 1...
59	2024-09-16 09:17:32	INFO(6)	System started up
58	2024-09-16 09:17:32	WARN(4)	System cold start
57	2024-09-11 16:14:45	INFO(6)	Port1/0/1 link up, 1...
56	2024-09-11 16:14:40	INFO(6)	System started up

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。

3.5.5 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。



The screenshot shows the 'System Attack Log' interface. At the top right, there is a 'Clear Attack Log' button. Below it, the text 'Total Entries: 0' is displayed. A table with the following columns is shown: Index, Time, Level, and Log Description. The table is currently empty.

Index	Time	Level	Log Description
-------	------	-------	-----------------

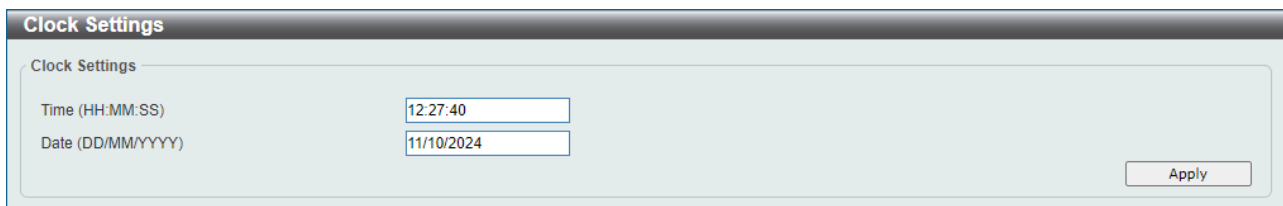
表示されているアタックログをクリアするには、**Clear Attack Log** ボタンをクリックします。

3.6 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います。
以下の項で説明するサブメニューに分かれています。

3.6.1 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。



The screenshot shows a web interface titled "Clock Settings". Inside a light blue bordered box, there are two input fields. The first is labeled "Time (HH:MM:SS)" and contains the text "12:27:40". The second is labeled "Date (DD/MM/YYYY)" and contains the text "11/10/2024". To the right of these fields is a button labeled "Apply".

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	現在の日付を日（DD）、月（MM）、年（YYYY）で入力します。 例：31/12/2024

設定を適用するには、**Apply** ボタンをクリックします。

3.6.2 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 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 **Reccuring** 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。

Time Zone Settings

Summer Time State Disabled ▼

Time Zone + ▼ 9 ▼ 0 ▼

Recurring Settings

From: Week of the Month Last ▼

From: Day of the Week Sunday ▼

From: Month January ▼

From: Time (HH:MM) 00 ▼ 00 ▼

To: Week of the Month Last ▼

To: Day of the Week Sunday ▼

To: Month January ▼

To: Time (HH:MM) 00 ▼ 00 ▼

Offset (30-120) 60

Date Settings

From: Date of the Month 01 ▼

From: Month January ▼

From: Year [Input Field]

From: Time (HH:MM) 00 ▼ 00 ▼

To: Date of the Month 01 ▼

To: Month January ▼

To: Year [Input Field]

To: Time (HH:MM) 00 ▼ 00 ▼

Offset (30-120) 60

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。

3.6.3 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。

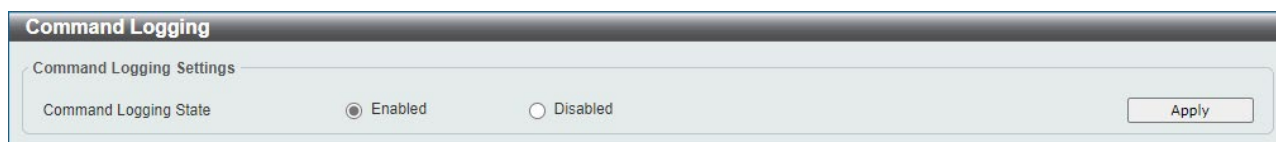
4 Management

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 32 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。

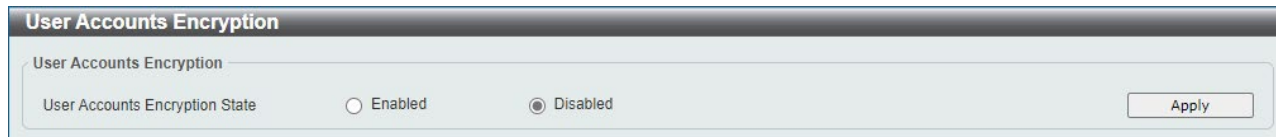
設定を適用するには、**Apply** ボタンをクリックします。

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。 <ul style="list-style-type: none"> • Plain Text：平文パスワードを入力する場合に選択します。 • Encrypted：パスワードを暗号化する場合に選択します。

Password	<p>特権レベル移行のパスワードを入力します。</p> <p>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。</p>
-----------------	--

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	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>ログイン時のパスワードを入力します。</p> <p>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。</p>

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 サブメニューは、設定に応じて以下の項で説明するサブメニューに分かれています。

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 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。

Port	Trap Sending	Trap State
Port1/0/1	Enabled	Enabled
Port1/0/2	Enabled	Enabled
Port1/0/3	Enabled	Enabled
Port1/0/4	Enabled	Enabled
Port1/0/5	Enabled	Enabled
Port1/0/6	Enabled	Enabled
Port1/0/7	Enabled	Enabled
Port1/0/8	Enabled	Enabled
Port1/0/9	Enabled	Enabled
Port1/0/10	Enabled	Enabled

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。

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

The screenshot shows the 'SNMP View Table Settings' interface. It includes a form with the following fields:

- View Name *: 32 chars
- Subtree OID *: N.N.N...N
- View Type: Included (dropdown menu)

Below the form is a table with 8 entries. Each entry has a 'Delete' button.

View Name	Subtree OID	View Type	
restricted	1.3.6.1.2.1.1	Included	Delete
restricted	1.3.6.1.2.1.11	Included	Delete
restricted	1.3.6.1.6.3.10.2.1	Included	Delete
restricted	1.3.6.1.6.3.11.2.1	Included	Delete
restricted	1.3.6.1.6.3.15.1.1	Included	Delete
CommunityView	1	Included	Delete
CommunityView	1.3.6.1.6.3	Excluded	Delete
CommunityView	1.3.6.1.6.3.1	Included	Delete

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。 <ul style="list-style-type: none"> • 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、SNMPv1/2c 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。

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

The screenshot shows the 'SNMP Community Table Settings' interface. It includes a form with the following fields:

- Key Type: Plain Text (dropdown)
- Community Name: 32 chars (text input)
- View Name: 32 chars (text input)
- Access Right: Read Only (dropdown)
- IP Access List Name: 32 chars (text input)

Below the form is a table with 2 entries:

Community Name	View Name	Access Right	IP Access List Name	
public	CommunityView	ro		Delete
private	CommunityView	rw		Delete

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。 <ul style="list-style-type: none"> • 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。

SNMP Group Table Settings

SNMP Group Settings

Group Name * 32 chars

User-based Security Model SNMPv3

Security Level NoAuthNoPriv

IP Access-List Name 32 chars

Read View Name 32 chars

Write View Name 32 chars

Notify View Name 32 chars

Context Name 32 chars

* Mandatory Field

Add

Total Entries: 5

Group Name	Read View Name	Write View Name	Notify View Name	Security Model	Security Level	IP Access-List Name	Context Name	
public	CommunityV...		CommunityV...	v1				Delete
public	CommunityV...		CommunityV...	v2c				Delete
initial	restricted		restricted	v3	NoAuthNoPriv			Delete
private	CommunityV...	CommunityV...	CommunityV...	v1				Delete
private	CommunityV...	CommunityV...	CommunityV...	v2c				Delete

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。 <ul style="list-style-type: none"> • NoAuthNoPriv : 認証と暗号化を行いません。 • AuthNoPriv : 認証は行いますが、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	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • 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。

The screenshot shows the 'SNMP Host Table Settings' interface. It includes a form with the following fields and values:

- Host IPv4 Address: (empty)
- Host IPv6 Address: 2013::1
- User-based Security Model: SNMPv1
- Security Level: NoAuthNoPriv
- UDP Port (1-65535): 162
- Community String / SNMPv3 User Name: 32 chars

Below the form, there is a table with the following data:

Host IP Address	SNMP Version	UDP Port	Community String / SNMPv3 User Name
2013::1	V1	162	private

The table also includes a 'Delete' button for the entry.

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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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 サブメニューは、設定に応じて以下の項で説明するサブメニューに分かれています。

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。

Index	Data Source	Rec. Octets	Rec. PKTs	Broadcast PKTs	Multicast PKTs	Undersize PKTs	Oversize PKTs	Fragments	Jabbers	CRC Error	Collisions	Drop Event	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets
1	Port1/0/1	5398998	42304	205	25285	0	0	0	0	0	0	0	35408	500	690	2922	2784	0

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。

The screenshot shows the 'CPU Protection' configuration interface. It is divided into three main sections:

- CPU Utilization Trace Trigger:** State is set to 'Disable'. Threshold (50-100) is an input field followed by 'percent'. Interval (10-180) is an input field followed by 'sec' and a 'Default' checkbox. An 'Apply' button is on the right.
- System Memory Limit Check:** State is set to 'Disable'. Threshold (80-100) is an input field followed by 'percent' and a 'Default' checkbox. An 'Apply' button is on the right.
- CPU Protection SNMP Trap:** State is set to 'Disable'. An 'Apply' button is on the right.

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 Zero Touch Provision

Zero Touch Provision 画面では、Zero Touch Provision（以後、ZTP）を設定します。

装置は起動時に、設定ファイルや ZTP スライドスイッチなどの情報から ZTP が有効かどうかを判定します。ZTP が有効の場合、DHCP クライアントを起動してネットワークアドレスと ZTP 情報を取得します。ZTP 情報は DHCP OFFER メッセージに含まれる、ダウンロードファイル名や取得元の TFTP サーバーの IP アドレスです。ダウンロードファイルは、ブートイメージファイルと設定ファイルのいずれか、もしくは両方です。DHCP のプロセスが正常に完了したら、装置は TFTP サーバーから所定のファイルをダウンロードし、プライマリーブートイメージファイルやプライマリー設定ファイルに上書きします。ダウンロードしたブートイメージファイルが起動時のブートイメージと異なる場合は再起動を行います。

ZTP スライドスイッチ（フロントパネル上）を使用する場合：

- ZTP スライドスイッチが **ON** で、ZTP が **Disabled** の場合、ZTP は無効です。
- ZTP スライドスイッチが **OFF** で、ZTP が **Enabled** の場合、ZTP は無効です。
- ZTP スライドスイッチが **OFF** で、ZTP が **EnableForced** の場合、ZTP は有効です。

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

Zero Touch Provision Settings	
Zero Touch Provision State: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="radio"/> EnableForced Apply	
Zero Touch Provision Information	
ZTP Bootup State:	Enabled Force
ZTP Current State:	Disabled
Current Firmware:	/c:/V3.00.00.0001.had
Current Configure:	/c:/config1.cfg
	Result of last time
ZTP Process Result	-
DHCP Server	-
DHCP Discover Retry	-
TFTP server	-
Gateway IP address	-
Download Firmware	-
Download Configure	-

Zero Touch Provision Settings の各項目の説明を以下に示します。

パラメーター	説明
Zero Touch Provision State	ZTP 機能の状態（ Enabled / Disabled / EnableForced ）を選択します。 EnableForced を選択すると、ZTP 機能が強制的に有効になります。

設定を適用するには、**Apply** ボタンをクリックします。

4.11 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 で設定できるフィールドについて、以下で説明します。

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 で設定できるフィールドについて、以下で説明します。

パラメーター	説明
Source Interface State	FTP 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。

4.12 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。

Drive	Media Type	Size (MB)	File System Type	Label
C:	Flash	215	other	

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	移動先のディレクトリパスを入力します。

入力したディレクトリ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。

ブート情報を削除するには、**Erase BootFile** ボタンをクリックします。

Drive の「C:」ハイパーリンクをクリックすると、C:ドライブに移動して、以下に示す画面に切り替わります。

Index	Info	Attr	Size (byte)	Update Time	Name	Primary Up	Secondary Up	Rename	Delete
1	CFG(*)	-rw	2075	Jan 01 2021 00:00:06	primary.cfg	Primary Up	Secondary Up	Rename	Delete
2	RUN(**)	-rw	45937956	Feb 14 2025 04:23:19	V3.00.00.0001_sec.ha...	Primary Up	Secondary Up	Rename	Delete
3	RUN(*)	-rw	45937956	Feb 14 2025 04:21:01	V3.00.00.0001.had	Primary Up	Secondary Up	Rename	Delete
4		d--	1152	Jan 01 2021 00:01:19	system			Delete	
5	CFG(**)	-rw	2075	Jan 01 2021 00:00:06	secondary.cfg	Primary Up	Secondary Up	Rename	Delete

225832960 bytes total (105107456 bytes free)
 (*) -with primary boot up info
 (**) -with secondary boot up info

前のウィンドウに戻るには、**Previous** ボタンをクリックします。

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。

特定のファイル名を変更するには、**Rename** ボタンをクリックします。

特定のファイルもしくはディレクトリを削除するには、**Delete** ボタンをクリックします。

特定のファイルを起動時ファイルに変更するには、**Primary UP** (プライマリーブートイメージ/設定ファイル)、もしくは **Secondary UP** (セカンダリーブートイメージ/設定ファイル) 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、装置はデフォルト設定に戻ります。
- ❗ プライマリー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自動的にセカンダリーブートイメージファイルを自動的に使用します。

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。

The screenshot shows a 'File System' dialog box. At the top, there is a 'Path' field containing 'c/' and a 'Go' button. Below this is a 'Copy File' section. It contains two rows: 'Source' and 'Destination'. The 'Source' row has a dropdown menu showing 'startup-config' and a text field containing 'C:/config.cfg'. The 'Destination' row has a dropdown menu showing 'running-config' and a text field containing 'C:/config.cfg'. To the right of these fields is a checkbox labeled 'Replace'. At the bottom right of the dialog are 'Apply' and 'Cancel' buttons.

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	<p>コピー元ファイルを以下から選択します。</p> <ul style="list-style-type: none"> • 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 : サーバー証明書ファイルをコピー元とします。 • HTTTPs-private-key : 秘密鍵ファイルをコピー元とします。 • aaa-local-db : ローカルデータベース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	<p>ファイルのコピー先を選択します。</p> <ul style="list-style-type: none"> • 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 : サーバー証明書ファイルをコピー先とします。 • HTTTPs-private-key : 秘密鍵ファイルをコピー先とします。 • aaa-local-db : ローカルデータベースファイルをコピー先とします。 • secondary-config : セカンダリー設定ファイルをコピー先とします。 <p>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。</p>

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。

5 Layer 2 Features

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。以下の項で説明するサブメニューに分かれています。

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 アドレステーブルに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	特定のポートに対する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。

指定した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、**L2 Features > FDB > 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	Aging Destination Hit 機能を有効または無効に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。

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。

Port	Status
Port1/0/1	Enabled
Port1/0/2	Enabled
Port1/0/3	Enabled
Port1/0/4	Enabled
Port1/0/5	Enabled
Port1/0/6	Enabled
Port1/0/7	Enabled
Port1/0/8	Enabled
Port1/0/9	Enabled
Port1/0/10	Enabled

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	指定したポートでの 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。

VID	MAC Address	Type	Port
1	00-00-5E-00-01-E7	Dynamic	Port1/0/1
1	00-03-24-12-01-17	Dynamic	Port1/0/1
1	00-11-22-33-44-55	Static	Port1/0/1
1	00-40-66-91-36-11	Dynamic	Port1/0/1
1	00-40-66-C2-AA-0A	Dynamic	Port1/0/1
1	88-AE-DD-25-DC-CC	Dynamic	Port1/0/1
1	EC-AD-E0-9B-F3-53	Dynamic	Port1/0/1
1	FC-6D-D1-65-F9-F0	Static	CPU
1	01-00-00-00-00-02	Static	Port1/0/5

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。以下の項で説明するサブメニューに分かれています。

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、VLAN 名が VLANXXXX (XXXX は指定した VLAN ID の 4 桁表示) と自動的に設定されます。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 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 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、入力値は以下のいずれかの値になります。 <ul style="list-style-type: none"> • 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、**L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile Interface** をクリックします。

設定できるフィールドを以下に説明します。

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。

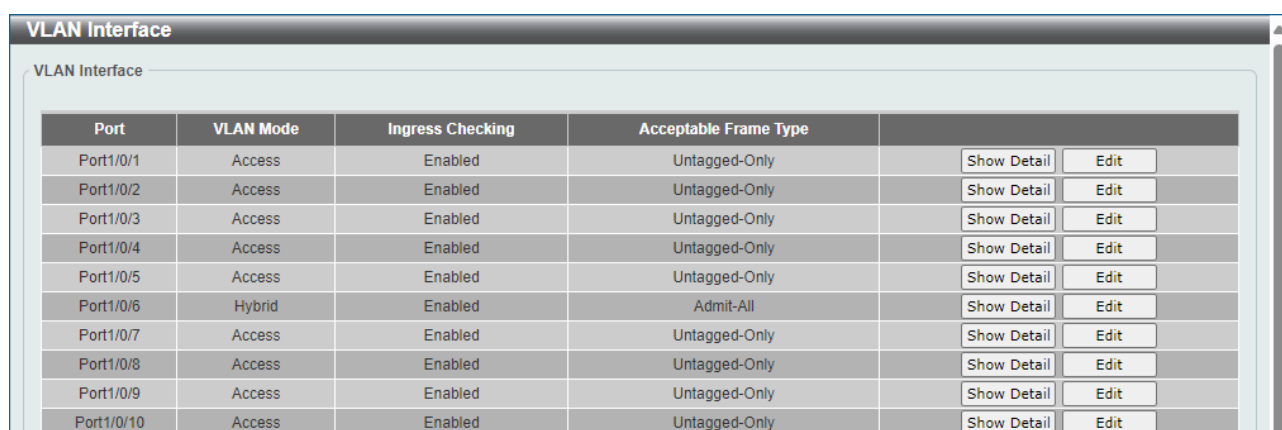
設定を適用するには、**Apply** ボタンをクリックします。

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。

5.2.3 VLAN Interface

VLAN Interface 画面では、VLAN をポートに割り当てます。

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

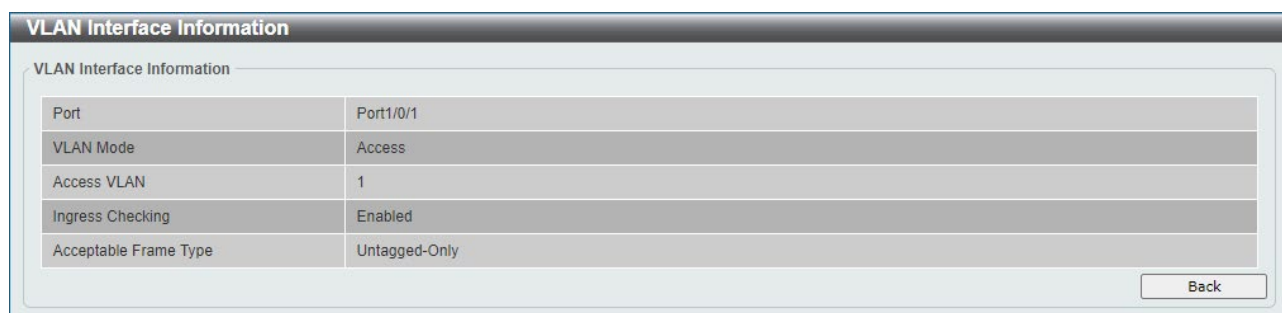


Port	VLAN Mode	Ingress Checking	Acceptable Frame Type	Show Detail	Edit
Port1/0/1	Access	Enabled	Untagged-Only	Show Detail	Edit
Port1/0/2	Access	Enabled	Untagged-Only	Show Detail	Edit
Port1/0/3	Access	Enabled	Untagged-Only	Show Detail	Edit
Port1/0/4	Access	Enabled	Untagged-Only	Show Detail	Edit
Port1/0/5	Access	Enabled	Untagged-Only	Show Detail	Edit
Port1/0/6	Hybrid	Enabled	Admit-All	Show Detail	Edit
Port1/0/7	Access	Enabled	Untagged-Only	Show Detail	Edit
Port1/0/8	Access	Enabled	Untagged-Only	Show Detail	Edit
Port1/0/9	Access	Enabled	Untagged-Only	Show Detail	Edit
Port1/0/10	Access	Enabled	Untagged-Only	Show Detail	Edit

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、以下のページが表示されます。



VLAN Interface Information	
Port	Port1/0/1
VLAN Mode	Access
Access VLAN	1
Ingress Checking	Enabled
Acceptable Frame Type	Untagged-Only

Back

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、**VLAN Mode** によって表示内容（設定項目）が異なります。

The screenshot shows the 'Configure VLAN Interface' configuration window. The 'Port' is 'Port1/0/1'. The 'VLAN Mode' is set to 'Hybrid'. 'Acceptable Frame' is 'Admit All'. 'Ingress Checking' is 'Enabled'. 'Native VLAN' is checked. 'VID (1-4094)' is '1'. 'Action' is 'Add'. 'Add Mode' is 'Untagged'. 'From Port' and 'To Port' are both 'Port1/0/1'. 'Clone' is unchecked. 'Current Hybrid Untagged VLAN Range' and 'Current Hybrid Tagged VLAN Range' are both '1'. 'Back' and 'Apply' buttons are at the bottom right.

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 で Hybrid または Trunk を選択する必要があります。
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 ）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 では VLAN 割り当ての設定の上書きを行います。
Add Mode	VLAN Mode で Hybrid または Dot1q-Tunnel を選択した後、 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2 VLAN 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2 VLAN インターフェース ID を入力します。
Description	レイヤー2 VLAN 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2 VLAN 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。
以下の項で説明するサブメニューに分かれています。

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。

Port	Outer TPID
Port1/0/1	0x8100
Port1/0/2	0x8100
Port1/0/3	0x8100
Port1/0/4	0x8100
Port1/0/5	0x8100
Port1/0/6	0x8100
Port1/0/7	0x8100
Port1/0/8	0x8100
Port1/0/9	0x8100
Port1/0/10	0x8100

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-VLAN タグ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せん。
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 マッピング設定を設定します。

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	元の 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。 <ul style="list-style-type: none"> • 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 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。

すべての VLAN マッピングを表示するには、**View All** 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、スパン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。

以下の項で説明するサブメニューに分かれています。

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。

Port	State	Cost	Guard Root	Link Type	Port Fast	TCN Filter	BPDU Forward	Priority
Port1/0/1	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128
Port1/0/2	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128
Port1/0/3	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128
Port1/0/4	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128
Port1/0/5	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128
Port1/0/6	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128
Port1/0/7	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128
Port1/0/8	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128
Port1/0/9	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128
Port1/0/10	Disabled	0/200000	Disabled	Auto/P2P	Auto/Non-Edge	Disabled	Enabled	128

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。 <ul style="list-style-type: none"> • 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。

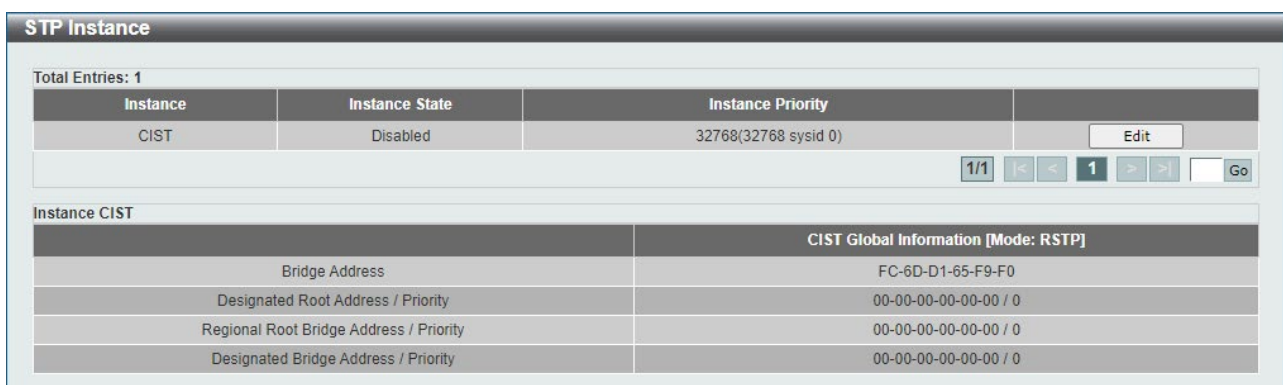
インスタンス ID を再設定するには、**Edit** ボタンをクリックします。

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 ポートを再設定するには、**Edit** ボタンをクリックします。

5.5 MMRP Plus Settings

MMRP Plus Settings サブメニューでは、MMRP-Plus アウェア機能に関する設定を行います。MMRP-Plus の冗長構成には他に MMRP-Plus マスター機能が動作する機器が必要で、本スイッチは MMRP-Plus マスター機能には対応していません。

以下の項で説明するサブメニューに分かれています。

5.5.1 MMRP Plus Global Settings

MMRP Plus Global Settings 画面では、MMRP-Plus アウェア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、**L2 Features > MMRP Plus Settings > MMRP Plus Global Settings** をクリックします。

MMRP Plus Global Settings で設定できる各項目の説明を以下に示します。

パラメーター	説明
State	MMRP-Plus アウェア機能の状態 (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。

MMRP Plus Clear で設定できる各項目の説明を以下に示します。

パラメーター	説明
Ring ID List	MMRP リング ID を指定します。複数指定できます。

Clear Failure ボタンをクリックして、「Failure」状態をキャンセルし、リング復旧プロセスを開始します（「Listening」状態に移行します）。

MMRP Plus の統計情報をクリアするには、**Clear Counter** ボタンをクリックします。

5.5.2 MMRP Plus Configuration

MMRP Plus Configuration 画面では、MMRP Plus の設定を行います。

本画面を表示するには、**L2 Features > MMRP Plus Settings > MMRP Plus Configuration** をクリックします。

MMRP-Plus Configuration

MMRP-Plus Aware

Ring ID (1-1000) Aware Port1 Aware Port2 Default

MMRP Plus Configuration

Ring ID List

Ring Name Default

VID (1-4094) Default

Revertive (0-86400) sec Disable Default

FDB Flush Port From

FDB Flush Port To Default

FDB Flush Timer (0-10) sec Default

Listening Timer (1-86400) sec Default

Hello Timeout (1-86400) sec Default

Ring ID List

Total Entries: 1

ID	Name	Type	Pt1	Pt2	VID	FDB	Pr	Vg	Re	Ht	Lis	
1		RA	1/0/10	1/0/11	1	1	-	-	0	1	10	Show Detail Delete

1/1 < < 1 > > Go

Note: RA : Ring Aware, VID : Hello VID, FDB : FDB Flush Timer, Pr : Port Restart (O: Enable - Disable), Vg : VLAN Group, Re : Revertive Setting, Ht : Hello Timeout Timer, Lis : Listening Timer, P : Port-Channel

MMRP Plus Aware では、リングとアウェア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
Ring ID	MMRP リング ID を 1～1000 の範囲で指定します。
Aware Port1	アウェアポート 1 を指定します。
Aware Port2	アウェアポート 2 を指定します。 デフォルトのアウェアポートを使用するには、 Default オプションを選択します。

設定を適用するには、**Apply** ボタンをクリックします。

MMRP Plus Configuration では、リングの各種設定を行います。各項目の説明を以下に示します。

パラメーター	説明
Ring ID List	MMRP-Plus のリング ID を指定します。
Ring Name	MMRP-Plus のリング名を 32 文字以内で入力します。 デフォルト名を使用するには、 Default オプションを選択します。

VID	MMRP-Plus の制御フレームを処理する VLAN の VLAN ID を 1～4094 の範囲で入力します。デフォルト VID を使用するには、 Default オプションを選択します。
Revertive	MMRP-Plus の切り戻りタイマーを 0～86400（秒）の範囲で入力します。 MMRP-Plus の自動切り戻りを無効にする場合、 Disable オプションを選択します。デフォルト値を使用するには、 Default オプションを選択します。
FDB Flush Port From / FDB Flush Port To	FDB フラッシュフレーム（MMRP-Plus）を受信した場合に MAC アドレステーブルをクリアするポートの範囲を選択します。 デフォルト FDB フラッシュポートを使用するには、 Default オプションを選択します。
FDB Flush Timer	FDB フラッシュフレーム（MMRP-Plus）を受信した場合に、一時的に MAC アドレスの学習を停止するタイマー値を 0～10（秒）の範囲で入力します。 デフォルト値を使用するには、 Default オプションを選択します。
Listening Timer	リスニングタイマー値を 1～86400（秒）の範囲で入力します。デフォルト値を使用するには、 Default オプションを選択します。
Hello Timeout	MMRP-Plus のハローフレームのタイムアウト値を 1～86400（秒）の範囲で入力します。デフォルト値を使用するには、 Default オプションを選択します。

設定を適用するには、**Apply** ボタンをクリックします。

エントリーを削除するには、**Delete** ボタンをクリックします。

Show Detail ボタンをクリックすると、以下の詳細な設定情報を表示するページに移行します。

MMRP Plus Configuration Detail	
MMRP Plus Configuration Detail	
Ring ID	1
Ring Name	
Type	Ring Aware
Aware	Port : 1/0/10
Aware	Port : 1/0/11
VLAN ID	1
Listening Timer	10 s
FDB Flush Timer	1 s
FDB Flush Port	-
Hello Timeout	1 s
Revertive	0 s

前のページに戻るには、**Back** ボタンをクリックします。

5.6 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。

Port	noChkSrc	Action	Loop Detection State	Result	Time Left (sec)
Port1/0/1	Disabled	Shutdown	Disabled	Normal	-
Port1/0/2	Disabled	Shutdown	Disabled	Normal	-
Port1/0/3	Disabled	Shutdown	Disabled	Normal	-
Port1/0/4	Disabled	Shutdown	Disabled	Normal	-
Port1/0/5	Disabled	Shutdown	Disabled	Normal	-
Port1/0/6	Disabled	Shutdown	Disabled	Normal	-
Port1/0/7	Disabled	Shutdown	Disabled	Normal	-
Port1/0/8	Disabled	Shutdown	Disabled	Normal	-

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。
Frame-type Untagged	CTP フレームのタグなしを有効または無効にする場合に選択します。
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。 <ul style="list-style-type: none"> • 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。

5.7 Loop Detection Information

Loop Detection Information 画面では、現在のループ検出をクリアするために使用されます。本画面を表示するには、**L2 Features > Loop Detection Information** をクリックします。

Loop Detection Information で設定できるフィールドを以下に説明します。

パラメーター	説明
From Port / To Port	この構成に関連付けるポートのリストを選択します。

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。

特定のポート情報をクリアするには、**Clear** ボタンをクリックします。

すべてのポート情報をクリアするには、**Clear All** ボタンをクリックします。

すべてのエントリーを表示するには、**View All** ボタンをクリックします。

5.8 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、ポートチャン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。本装置は IEEE802.3ad リンクアグリゲーションに対応し、ポートチャンネル1個で最大 8 ポートの物理ポートを束ねることができます。結合するポートは、すべて同一のリンク速度でリンクアップしている必要があり、異なるリンク速度のメンバーが存在する場合の動作は不定です。

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

Channel Group	Protocol	Max Ports	Member Number	Member Ports	Delete Channel	Show Detail
Port-channel1	Static	8	2	Port1/0/11-1/0/12	Delete Channel	Show Detail
Port-channel2	LACP	8	2	Port1/0/13-1/0/14	Delete Channel	Show Detail

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、ポートチャンネルを登録します。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	ポートチャンネルのグループ番号を 1～8 の範囲で入力します。
Mode	ポートチャンネルの動作モード (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。

チャン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。

チャン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。

チャンネル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。

Port Channel

Port Channel Information

Port Channel 2
Protocol LACP

Port Channel Detail Information

Port	LACP Timeout	Working Mode	LACP State	Port Priority	Port Number	
Port1/0/13	Long	Passive	down	32768	0	Edit
Port1/0/14	Long	Passive	down	32768	0	Edit

Port Channel Neighbor Information

Port	Partner System ID	Partner Port Number	Partner LACP Timeout	Partner Working Mode	Partner Port Priority
Port1/0/13	0,00-00-00-00-00-00	0	Long	Passive	0
Port1/0/14	0,00-00-00-00-00-00	0	Long	Passive	0

Note:

LACP State:
 bndl: Port is attached to an aggregator and bundled with other ports.
 hot-sby: Port is in a hot-standby state.
 down: Port is down.

ポートチャン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 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。

5.9 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。以下の項で説明するサブメニューに分かれています。

5.9.1 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 スヌーピングの各種設定を行います。

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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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 スヌーピングの VLAN 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	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、以下の画面が表示されます。

IGMP Snooping VLAN Parameters

IGMP Snooping VLAN Parameters

VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (host-based)
Report Suppression	Disabled
Suppression Time	10 sec
Querier State	Disabled
Query Version	v3
Query Interval	125 sec
Max Response Time	10 sec
Robustness Value	2
Last Member Query Interval	1 sec
Proxy Reporting	Disabled Source Address (0.0.0.0)
Unknown Data Learning	Enabled
Unknown Data Expiry Time	Infinity
Ignore Topology Change	Disabled

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

IGMP Snooping VLAN Settings

VID (1-4094)	<input type="text" value="1"/>
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Minimum Version	<input type="text" value="1"/> ▼
Fast Leave	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Report Suppression	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Suppression Time (1-300)	<input type="text" value="10"/>
Querier State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Query Version	<input type="text" value="3"/> ▼
Query Interval (1-31744)	<input type="text" value="125"/> sec
Max Response Time (1-25)	<input type="text" value="10"/> sec
Robustness Value (1-7)	<input type="text" value="2"/>
Last Member Query Interval (1-25)	<input type="text" value="1"/> sec
Proxy Reporting	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Source Address <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>
Unknown Data Learning	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Unknown Data Expiry Time (1-65535)	<input type="text" value=""/> sec <input checked="" type="checkbox"/> Infinity
Ignore Topology Change	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

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 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。 レポート抑制が有効の場合、装置はマルチキャストノードから送信される重複レポートを抑制します。同じグループのレポートまたは離脱の抑制は、抑制時間が期限切れになるまで継続されます。同じグループへのレポートまたは離脱メッセージの場合、1 つのレポートまたは離脱メッセージだけが転送されます。残りのレポートおよび離脱メッセージは、抑制されます。
Suppression Time	重複する IGMP 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)。
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 / 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。学習を期限切れにしない場合は、Infinite を選択します。
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、**L2 Features > L2 Multicast Control > 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 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、**L2 Features > L2 Multicast Control > 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。 <ul style="list-style-type: none"> • 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、**L2 Features > L2 Multicast Control > 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	<p>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</p> <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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
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。 <ul style="list-style-type: none"> • VLAN : 対象の IGMP スヌーピング統計情報を表示します。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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。

IPv4 Multicast Unregistered Filter Settings

IPv4 Multicast Unregistered Filter Settings 画面では、未登録 IP マルチキャストグループの転送を制御する未登録 IP マルチキャストフィルタリング機能の設定を行います。本機能が無効の場合、未登録 IP マルチキャストグループのトラフィックは、**L2 Features > L2 Multicast Control > Multicast Filtering** で設定するマルチキャストフィルタリングの設定状況によって転送/廃棄のアクションが決定されます。本機能が有効の場合、未登録 IP マルチキャストグループのトラフィックは、指定された出カインターフェースおよびマルチキャストルーターポートに転送されます。本機能を使用する場合、マルチキャストフィルタリングの設定は **Forward Unregistered** に設定する必要があります。

本画面を表示するには、**L2 Features > L2 Multicast Control > IGMP Snooping > IPv4 Multicast Unregistered Filter Settings** をクリックします。

IPv4 Multicast Unregistered Filter Settings

IPv4 Multicast Unregistered Filter VLAN Settings

VID (1-4094) Enabled Disabled

IPv4 Multicast Unregistered Filter Out-interface Settings

VID (1-4094) From Port To Port

IPv4 Multicast Unregistered Filter Table

VID (1-4094)

Total Entries: 1

VID	Multicast Filter Mode	IPv4 Multicast Unregistered Filter	Ports
1	Forward Unregistered Groups	Disabled	Out-interface: 1/0/10 Mrouter-port: 1/0/10 (Static)

1/1 |< < 1 > >

IPv4 Multicast Unregistered Filter VLAN Settings では、未登録 IP マルチキャストフィルタリングの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
VID	VLAN ID を 1~4094 の範囲で入力し、未登録 IP マルチキャストフィルタリングの状態 (Enabled / 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。

IPv4 Multicast Unregistered Filter Out-interface Settings では、未登録 IP マルチキャストフィルタリングの出カインターフェースを設定します。各項目の説明を以下に示します。

パラメーター	説明
VID	未登録 IP マルチキャストフィルタリングの出カインターフェースを設定する VLAN の VLAN ID を 1~4094 の範囲で入力します。
From Port / To Port	ポートまたはポートの範囲を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

指定したエントリーを削除するには、**Delete** ボタンをクリックします。

IPv4 Multicast Unregistered Filter Table では、未登録 IP マルチキャストフィルタリングの設定を表示します。各項目の説明を以下に示します。

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

入力した情報で特定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。

すべてのエントリーを表示するには、**View All** ボタンをクリックします。

5.9.2 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 スヌーピングの各種設定を行います。

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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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 スヌーピングの VLAN 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	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、以下の画面が表示されます。

MLD Snooping VLAN Parameters

MLD Snooping VLAN Parameters

VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (host-based)
Report Suppression	Disabled
Suppression Time	10 sec
Proxy Reporting	Disabled Source Address (::)
Mrouter Port Learning	Enabled
Querier State	Disabled
Query Version	v2
Query Interval	125 sec
Max Response Time	10 sec
Robustness Value	2
Last Listener Query Interval	1 sec
Unknown Data Learning	Enabled
Unknown Data Expiry Time	Infinity
Ignore Topology Change	Disabled

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。 <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • 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。学習を期限切れにしない場合は、Infinite を選択します。
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、**L2 Features > L2 Multicast Control > 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。

入力した情報に基づいて特定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。

すべてのエントリーを表示するには、**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、**L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings** をクリックします。

MLD Snooping Mrouter Settings

MLD Snooping Mrouter Settings

VID (1-4094) Configuration From Port To Port

MLD Snooping Mrouter Table

VID (1-4094)

Total Entries: 1

VID	Ports
1	1/0/10 (Static)

1/1 < < 1 > > Go

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。 <ul style="list-style-type: none"> • 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、**L2 Features > L2 Multicast Control > 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	<p>システムから 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。</p> <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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	<p>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。</p> <ul style="list-style-type: none"> • VLAN：対象 VLAN の MLD スヌーピング統計情報を表示します。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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。

IPv6 Multicast Unregistered Filter Settings

IPv6 Multicast Unregistered Filter Settings 画面では、未登録 IPv6 マルチキャストグループの転送を制御する未登録 IPv6 マルチキャストフィルタリング機能の設定を行います。本機能は、IPv4 での未登録 IP マルチキャストフィルタリングに相当します。本機能を使用する場合、マルチキャストフィルタリングの設定は **Forward Unregistered** に設定する必要があります。

本画面を表示するには、**L2 Features > L2 Multicast Control > MLD Snooping > IPv6 Multicast Unregistered Filter Settings** をクリックします。

IPv6 Multicast Unregistered Filter VLAN Settings では、未登録 IPv6 マルチキャストフィルタリングの設定を行います。各項目の説明を以下に示します。

パラメーター	説明
VID	VLAN ID を 1～4094 の範囲で入力し、未登録 IPv6 マルチキャストフィルタリングの状態 (Enabled / 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。

IPv6 Multicast Unregistered Filter Out-interface Settings では、未登録 IPv6 マルチキャストフィルタリングの出カインターフェースを設定します。各項目の説明を以下に示します。

パラメーター	説明
VID	未登録 IPv6 マルチキャストフィルタリングの出カインターフェースを設定する VLAN の VLAN ID を 1～4094 の範囲で入力します。
From Port / To Port	ポートまたはポートの範囲を選択します。

設定を適用するには、**Apply** ボタンをクリックします。

指定したエントリーを削除するには、**Delete** ボタンをクリックします。

IPv6 Multicast Unregistered Filter Table では、未登録 IP マルチキャストフィルタリングの設定を表示します。各項目の説明を以下に示します。

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

入力した情報に基づいて特定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。

すべてのエントリーを表示するには、**View All** ボタンをクリックします。

5.9.3 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	<p>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。</p> <ul style="list-style-type: none"> 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。

5.10 LLDP

LLDP サブメニューでは、LLDP に関連する設定を行います。
以下の項で説明するサブメニューに分かれています。

5.10.1 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

LLDP Global Settings

LLDP State Enabled Disabled

LLDP Forward State Enabled Disabled

LLDP Trap State Enabled Disabled

LLDP-MED Trap State Enabled Disabled Apply

LLDP-MED Configuration

Fast Start Repeat Count (1-10) times Apply

LLDP Configurations

Message TX Interval (5-32768) sec

Message TX Hold Multiplier (2-10) sec

Reinit Delay (1-10) sec

TX Delay (1-8192) sec Apply

LLDP System Information

Chassis ID Subtype	MAC Address
Chassis ID	FC-6D-D1-65-F9-F0
System Name	Switch
System Description	Gigabit Ethernet L2 Switch
System Capabilities Supported	Repeater, Bridge
System Capabilities Enabled	Repeater, Bridge

LLDP-MED System Information

Device Class	Network Connectivity Device
Hardware Revision	A1
Firmware Revision	
Software Revision	3.00.00b
Serial Number	314382240009
Manufacturer Name	APRESIA Systems, Ltd.
Model Name	APLGM352XT

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。

5.10.2 LLDP Port Settings

LLDP Port Settings 画面では、LLDP ポート設定を構成するために使用されます。

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

LLDP Port Settings

LLDP Port Settings

From Port: Port1/0/1, To Port: Port1/0/1, Notification: Disabled, Subtype: Local, Admin State: TX and RX, IP Subtype: Default, Action: Enabled, Address:

Note: The address should be the switch's address.

Port	Notification	Subtype	Admin State	IPv4/IPv6 Address
Port1/0/1	Disabled	Local	TX and RX	
Port1/0/2	Disabled	Local	TX and RX	
Port1/0/3	Disabled	Local	TX and RX	
Port1/0/4	Disabled	Local	TX and RX	
Port1/0/5	Disabled	Local	TX and RX	
Port1/0/6	Disabled	Local	TX and RX	
Port1/0/7	Disabled	Local	TX and RX	
Port1/0/8	Disabled	Local	TX and RX	
Port1/0/9	Disabled	Local	TX and RX	
Port1/0/10	Disabled	Local	TX and RX	

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。 <ul style="list-style-type: none"> • 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。 デフォルトでは、 TX and RX オプションが使用されます。
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。

5.10.3 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。

LLDP Management Address List					
All ▾					Find
Subtype	Address	IF Type	OID	Advertising Ports	
IPv4	172.31.131.120 (default)	ifIndex	1.3.6.1.4.1.278.1.48...	-	
IPv4	172.31.131.120	ifIndex	1.3.6.1.4.1.278.1.48...	-	

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	<p>以下のいずれかのサブタイプを選択します。</p> <ul style="list-style-type: none"> • 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。

5.10.4 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。

LLDP Basic TLVs Settings					
From Port	To Port	Port Description	System Name	System Description	System Capabilities
Port1/0/1 ▾	Port1/0/1 ▾	▾	▾	▾	▾
Apply					
Port	Port Description	System Name	System Description	System Capabilities	
Port1/0/1	Disabled	Disabled	Disabled	Disabled	
Port1/0/2	Disabled	Disabled	Disabled	Disabled	
Port1/0/3	Disabled	Disabled	Disabled	Disabled	
Port1/0/4	Disabled	Disabled	Disabled	Disabled	
Port1/0/5	Disabled	Disabled	Disabled	Disabled	
Port1/0/6	Disabled	Disabled	Disabled	Disabled	
Port1/0/7	Disabled	Disabled	Disabled	Disabled	
Port1/0/8	Disabled	Disabled	Disabled	Disabled	
Port1/0/9	Disabled	Disabled	Disabled	Disabled	
Port1/0/10	Disabled	Disabled	Disabled	Disabled	

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。

5.10.5 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。

5.10.6 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。

Port	MAC/PHY Configuration/Status	Link Aggregation	Maximum Frame Size
Port1/0/1	Disabled	Disabled	Disabled
Port1/0/2	Disabled	Disabled	Disabled
Port1/0/3	Disabled	Disabled	Disabled
Port1/0/4	Disabled	Disabled	Disabled
Port1/0/5	Disabled	Disabled	Disabled
Port1/0/6	Disabled	Disabled	Disabled
Port1/0/7	Disabled	Disabled	Disabled
Port1/0/8	Disabled	Disabled	Disabled
Port1/0/9	Disabled	Disabled	Disabled
Port1/0/10	Disabled	Disabled	Disabled

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。

5.10.7 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。

The screenshot shows the 'LLDP-MED Port Settings' configuration window. At the top, there are dropdown menus for 'From Port' (set to Port1/0/1), 'To Port' (set to Port1/0/1), 'Notification', 'Capabilities', and 'Inventory'. An 'Apply' button is located to the right of these dropdowns. Below the dropdowns is a table with the following data:

Port	Notification	Capabilities	Inventory
Port1/0/1	Disabled	Disabled	Disabled
Port1/0/2	Disabled	Disabled	Disabled
Port1/0/3	Disabled	Disabled	Disabled
Port1/0/4	Disabled	Disabled	Disabled
Port1/0/5	Disabled	Disabled	Disabled
Port1/0/6	Disabled	Disabled	Disabled
Port1/0/7	Disabled	Disabled	Disabled
Port1/0/8	Disabled	Disabled	Disabled
Port1/0/9	Disabled	Disabled	Disabled
Port1/0/10	Disabled	Disabled	Disabled

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。

5.10.8 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

LLDP Statistics Information

Last Change Time 0 Clear Counter

Total Inserts 0

Total Deletes 0

Total Drops 0

Total Ageouts 0

LLDP Statistics Ports

Port Port1/0/1 Clear Counter Clear All

Port	Total Transmits	Total Discards	Total Errors	Total Receives	Total TLV Discards	Total TLV Unknowns	Total Ageouts
Port1/0/1	0	0	0	0	0	0	0
Port1/0/2	0	0	0	0	0	0	0
Port1/0/3	0	0	0	0	0	0	0
Port1/0/4	0	0	0	0	0	0	0
Port1/0/5	0	0	0	0	0	0	0
Port1/0/6	0	0	0	0	0	0	0

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。

5.10.9 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。

LLDP Local Port Information

LLDP Local Port Brief Table

Port Port1/0/1 Find Show Detail

Port	Port ID Subtype	Port ID	Port Description
Port1/0/1	Local	Port1/0/1	APRESIA Systems, Ltd. APLGM352...
Port1/0/2	Local	Port1/0/2	APRESIA Systems, Ltd. APLGM352...
Port1/0/3	Local	Port1/0/3	APRESIA Systems, Ltd. APLGM352...
Port1/0/4	Local	Port1/0/4	APRESIA Systems, Ltd. APLGM352...
Port1/0/5	Local	Port1/0/5	APRESIA Systems, Ltd. APLGM352...
Port1/0/6	Local	Port1/0/6	APRESIA Systems, Ltd. APLGM352...
Port1/0/7	Local	Port1/0/7	APRESIA Systems, Ltd. APLGM352...
Port1/0/8	Local	Port1/0/8	APRESIA Systems, Ltd. APLGM352...
Port1/0/9	Local	Port1/0/9	APRESIA Systems, Ltd. APLGM352...
Port1/0/10	Local	Port1/0/10	APRESIA Systems, Ltd. APLGM352...

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、以下のウィンドウが表示されます。

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。

5.10.10 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、以下の画面が表示されます。

LLDP Neighbor Port Information	
LLDP Neighbor Information Table	
Entry ID	1
Chassis ID Subtype	MAC Address
Chassis ID	00-03-24-12-00-00
Port ID Subtype	MAC Address
Port ID	00-03-24-12-01-17
Port Description	
System Name	
System Description	
System Capabilities	
Management Address Entries	Show Detail
Port PVID	0
PPVID Entries	Show Detail
VLAN Name Entries	Show Detail
Protocol Identity Entries	Show Detail
MAC/PHY Configuration/Status	Show Detail
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	0
Unknown TLVs	Show Detail
LLDP-MED Capabilities	Show Detail
Network Policy	Show Detail
Extended Power Via MDI	Show Detail
Inventory Management	Show Detail

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。

6 Layer 3 Features

6.1 ARP

ARP サブメニューでは、ARP テーブルに関する設定を行います。
以下の項で説明するサブメニューに分かれています。

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。

Interface Name	Timeout (min)
vlan1	240

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。

Interface Name	IP Address	Hardware Address	Aging Time	Type
vlan1	172.31.131.1	00-11-22-33-44-AA	Forever	Static
vlan1	172.31.131.120	FC-6D-D1-65-F9-F0	Forever	

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。 <ul style="list-style-type: none"> • 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 インターフェイスで IP アドレスの設定を行います。以下の項で説明するサブメニューに分かれています。

6.3.1 IPv4 Interface

IPv4 Interface 画面では、VLAN インターフェイスの 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。

Interface	State	IP Address	Link Status
vian1	Enabled	172.31.131.120/255.255.255.0 Manual	Up

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 インターフェイスの 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 インターフェイスを検索するには、**Find** ボタンをクリックします。

IPv4 インターフェイスを再設定するには、**Edit** ボタンをクリックします。

IPv4 インターフェイスを削除するには、**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。 <ul style="list-style-type: none"> • Static : IPv4 アドレスを手動で入力します。 • DHCP : DHCP サーバーから IPv4 情報を自動取得します。
IP Address	装置の IPv4 アドレスを入力します。
Mask	装置の IPv4 サブネット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。

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。

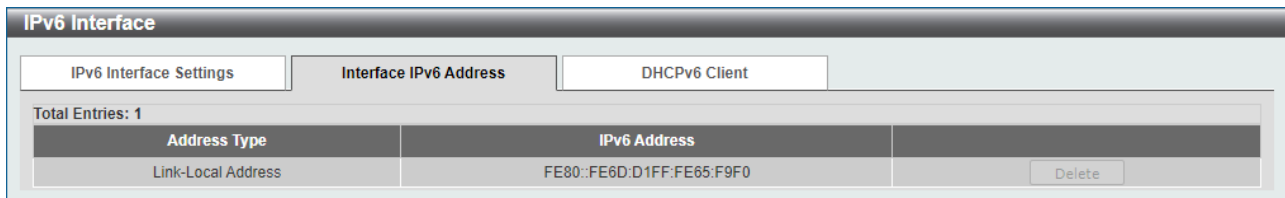
設定を適用するには、**Apply** ボタンをクリックします。

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。

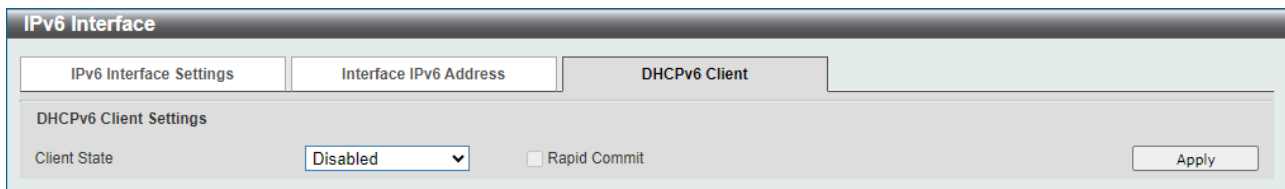
設定を適用するには、**Apply** ボタンをクリックします。

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。 <ul style="list-style-type: none"> • Primary : プライマリールートに登録します。 • Backup : バックアップルートに登録します。

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。

IPv4 Route Table

IPv4 Route Table

IP Address

 Network Address

 Connected Hardware Summary

Find

Total Entries: 1

IP Address	Mask	Gateway	Interface	Distance/Metric	Protocol	Candidate Default
172.31.131.0	255.255.255.0	Directly Connected	vlan1		Connected	-

1/1 << < 1 > >> Go

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。 <ul style="list-style-type: none"> • 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。

IPv6 Address/Prefix Length	Next Hop	Interface	Distance/Metric	Protocol
3FE::/64	Directly Connected	vlan1	0/1	Connected

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

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。
以下の項で説明するサブメニューに分かれています。

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。

Port	Default CoS	Override
Port1/0/1	0	No
Port1/0/2	0	No
Port1/0/3	0	No
Port1/0/4	0	No
Port1/0/5	0	No
Port1/0/6	0	No
Port1/0/7	0	No
Port1/0/8	0	No
Port1/0/9	0	No
Port1/0/10	0	No

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。

Port	Scheduler Method
Port1/0/1	WRR
Port1/0/2	WRR
Port1/0/3	WRR
Port1/0/4	WRR
Port1/0/5	WRR
Port1/0/6	WRR
Port1/0/7	WRR
Port1/0/8	WRR
Port1/0/9	WRR
Port1/0/10	WRR

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	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>デフォルトでは、WRR が使用されます。</p>

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。

Port	Queue ID	WRR Weight	WDRR Quantum
Port1/0/1	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	1	1
Port1/0/2	0	1	1
	1	1	1
	2	1	1
	3	1	1
	4	1	1
	5	1	1
	6	1	1
	7	1	1

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。

CoS	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Apply

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 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。

Queue Rate Limiting

Queue Rate Limiting

From Port: To Port: Queue ID:

Rate Limit: Min Bandwidth (64-10000000) Kbps Min Percent (1-100) % None

Max Bandwidth (64-10000000) Kbps Max Percent (1-100) %

Apply

Port	Queue0		Queue1		Queue2		Queue3		Queue4		Queue5		Queue6		Queue7	
	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate	Min Rate	Max Rate
Port1/0/1	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Port1/0/2	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Port1/0/3	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Port1/0/4	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Port1/0/5	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Port1/0/6	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Port1/0/7	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Port1/0/8	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Port1/0/9	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...
Port1/0/10	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...	No Li...

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。 <ul style="list-style-type: none">• Min Bandwidth : キューの保証帯域を 64~1000000 (Kbps) の範囲で指定します。<ul style="list-style-type: none">○ 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。<ul style="list-style-type: none">○ 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。
以下の項で説明するサブメニューに分かれています。

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 値のリマージ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。

Port	Trust State	DSCP Mutation Map
Port1/0/1	Trust CoS	
Port1/0/2	Trust CoS	
Port1/0/3	Trust CoS	
Port1/0/4	Trust CoS	
Port1/0/5	Trust CoS	
Port1/0/6	Trust CoS	
Port1/0/7	Trust CoS	
Port1/0/8	Trust CoS	
Port1/0/9	Trust CoS	
Port1/0/10	Trust CoS	

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。

Port	CoS	DSCP List
Port1/0/1	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63
Port1/0/2	0	0-7
	1	8-15
	2	16-23
	3	24-31
	4	32-39
	5	40-47
	6	48-55
	7	56-63

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。

Port	Color	CoS List
Port1/0/1	Green	0-7
	Yellow	
	Red	
Port1/0/2	Green	0-7
	Yellow	
	Red	
Port1/0/3	Green	0-7
	Yellow	
	Red	
Port1/0/4	Green	0-7
	Yellow	
	Red	

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。

Port	Color	DSCP List
Port1/0/1	Green	0-63
	Yellow	
	Red	
Port1/0/2	Green	0-63
	Yellow	
	Red	
Port1/0/3	Green	0-63
	Yellow	
	Red	
Port1/0/4	Green	0-63
	Yellow	
	Red	

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 **Matchc 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。

Match ボタンをクリックすると、ルールを追加・削除する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	<p>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。</p> <p>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</p>
DSCP List	<p>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。</p> <p>IPv4 パケットのみを照合する場合、 IPv4 only をチェックします。</p>
Precedence List	<p>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。</p> <p>IPv4 パケットのみと照合するには、 IPv4 only をチェックします。</p>
Protocol Name	<p>フレームをプロトコルを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。</p>
VID List	<p>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。</p>

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。

Aggregate Policer

Single Rate Settings

Aggregate Policer Name *

Normal Burst Size (0-16384) Kbyte

Conform Action Transmit DSCP IP

Violate Action None DSCP IP

* Mandatory Field

Two Rate Settings

Average Rate * (0-10000000) Kbps

Maximum Burst Size (0-16384) Kbyte

Exceed Action Transmit DSCP IP

Color Aware Disabled

Total Entries: 1

Name	Average Rate	Normal Burst Size	Max. Burst Size	Conform Action	Exceed Action	Violate Action	Color Aware	
Name	50000	500		Transmit	Transmit		Disabled	Delete

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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。

The screenshot shows the 'Aggregate Policer' configuration interface. The 'Two Rate Settings' tab is active. Fields include:

- Aggregate Policer Name: []
- CIR (0-10000000): [] Kbps
- PIR (0-10000000): [] Kbps
- Confirm Burst (0-16384): [] Kbyte
- Peak Burst (0-16384): [] Kbyte
- Conform Action: [Transmit] [DSCP] [1P]
- Exceed Action: [Drop] [DSCP] [1P]
- Violate Action: [Drop] [DSCP] [1P]
- Color Aware: [Disabled]

 A table below shows the configuration for 1 entry:

Name	CIR	Confirm Burst	PIR	Peak Burst	Conform Action	Exceed Action	Violate Action	Color Aware
Name	5000	500	8000	800	Transmit	Drop	Drop	Disabled

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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。

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。

Set Action ボタンをクリックすると、以下の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、リマーケティングは行いません。

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。
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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。

設定できるフィールドを以下に説明します。

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

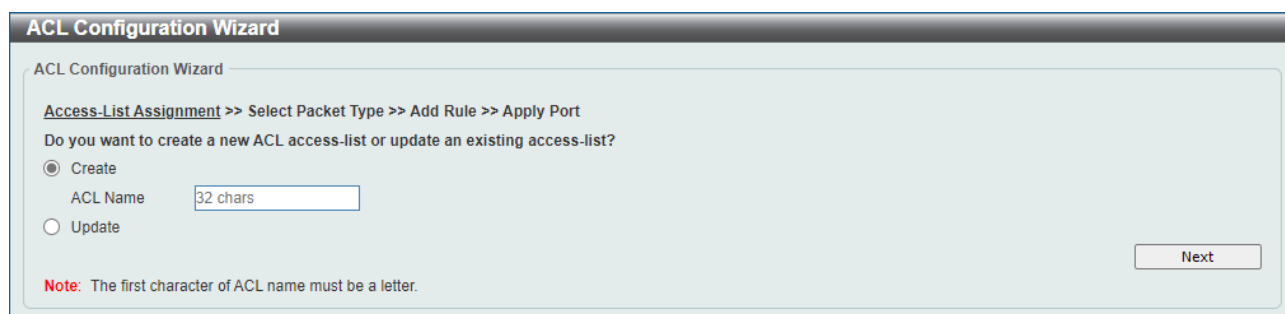
8.1 ACL Configuration Wizard

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ます、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。

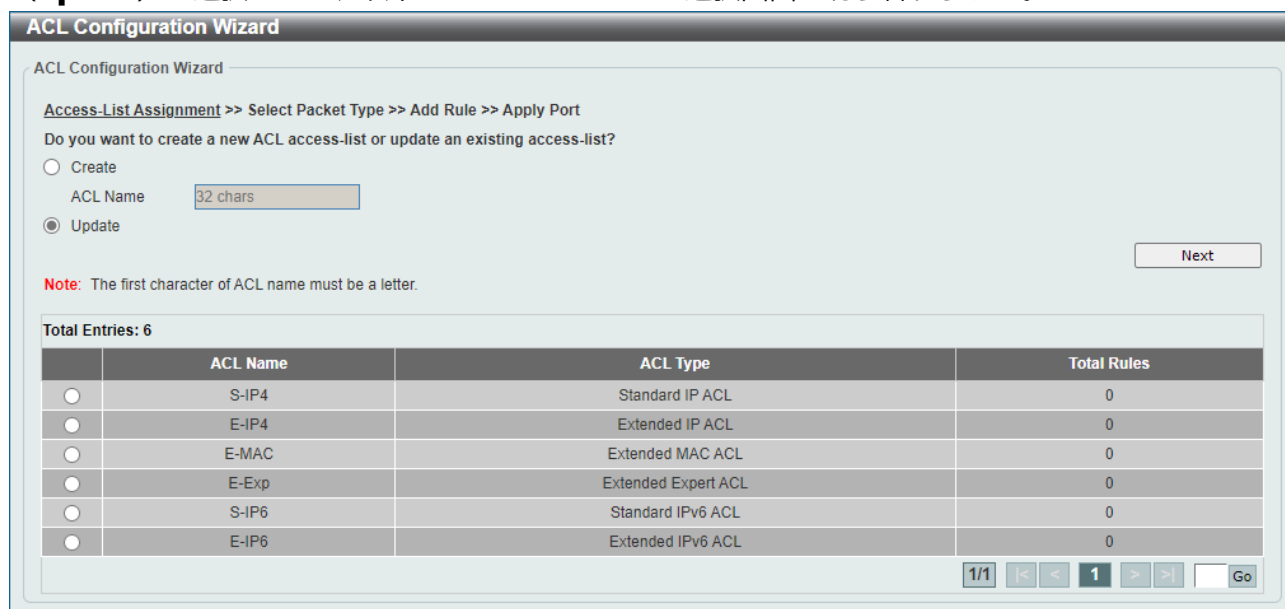
ACL 構成ウィザードは、ステップ 1~4 の 4 段階の操作で実行されます。

8.1.1 ステップ 1：作成/更新

ACL 構成ウィザードを使用するには、**ACL > ACL Configuration Wizard** をクリックします。



ACL 構成ウィザードの最初の画面（ステップ 1）では、ACL の新規作成もしくは更新を選択します。新規作成（**Create**）の場合、ACL プロファイル名を入力して Next ボタンをクリックします。更新（**Update**）を選択すると、以下の ACL プロファイル選択画面に切り替わります。



	ACL Name	ACL Type	Total Rules
<input type="radio"/>	S-IP4	Standard IP ACL	0
<input type="radio"/>	E-IP4	Extended IP ACL	0
<input type="radio"/>	E-MAC	Extended MAC ACL	0
<input type="radio"/>	E-Exp	Extended Expert ACL	0
<input type="radio"/>	S-IP6	Standard IPv6 ACL	0
<input type="radio"/>	E-IP6	Extended IPv6 ACL	0

表示されたテーブルから、編集する ACL プロファイルを選択して、**Next** ボタンをクリックします。

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
Create	ACL を新規作成する場合に選択します。
ACL Name	ACL プロファイル名を 32 文字以内で入力します。
Update	既存の ACL プロファイルを更新する場合に選択します。また、更新する ACL を一覧で選択します。

次の手順に進むには、**Next** ボタンをクリックします。

8.1.2 ステップ 2：パケットタイプの選択

ステップ 2 では、ACL プロファイルを作成します。ステップ 1 で更新を選択した場合、ステップ 2 はスキップします。

以下に示す画面から、作成する ACL プロファイルの ACL 種別を指定します。

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
Extended MAC ACL	拡張 MAC ACL を作成/更新する場合に選択します。
IPv4 ACL	標準 IPv4 ACL を作成/更新する場合に選択します。
Extended IPv4 ACL	拡張 IPv4 ACL を作成/更新する場合に選択します。
IPv6 ACL	標準 IPv6 ACL を作成/更新する場合に選択します。
Extended IPv6 ACL	拡張 IPv6 ACL を作成/更新する場合に選択します。
Expert ACL	エキスパート ACL を作成/更新する場合に選択します。

前の手順に戻るには、**Back** ボタンをクリックします。

次の手順に進むには、**Next** ボタンをクリックします。

8.1.3 ステップ 3：ルールの追加

拡張 MAC ACL

ステップ 1 で **Create** または **Update** を選択し、ステップ 2 で **Extended MAC ACL** を選択して **Next** 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。

ACL Configuration Wizard 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 ルール番号を 1～65535 の範囲で入力します。 ACL ルール番号を自動で生成するには、 Auto Assign を選択します。

Assign Rule criteria の各項目の説明を以下に示します。

パラメーター	説明
Source	送信元 MAC アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は送信元 MAC アドレスを入力します。 <ul style="list-style-type: none"> • Any：すべての送信元ホストを判定条件とする場合に選択します。 • Host：送信元ホストの MAC アドレスを指定する場合に選択します。右のボックスに送信元ホストの MAC アドレスを入力します。 • MAC：送信元 MAC アドレスとワイルドカード値を指定する場合に選択します。右のボックスに送信元 MAC アドレスを入力し、Wildcard ボックスにワイルドカード値を入力します。

Destination	宛先 MAC アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は宛先 MAC アドレスを入力します。 <ul style="list-style-type: none"> • Any：すべての宛先ホストを判定条件とする場合に選択します。 • Host：宛先ホストの MAC アドレスを指定する場合に選択します。右のボックスに宛先ホストの MAC アドレスを入力します。 • MAC：宛先 MAC アドレスとワイルドカード値を指定する場合に選択します。右のボックスに宛先 MAC アドレスを入力し、Wildcard ボックスにワイルドカード値を入力します。
Specify Ethernet Type	イーサネットタイプ (aarp / appletalk / decent-iv / etype-6000 / etype-804 / lat / lavc-sca / mop-console / mop-dump / vines-echo / vines-ip / xns-idp / arp) を選択します。
Ethernet Type	イーサネットタイプの 16 進数の値を 0x0~0xFFFF の範囲で入力します。適切な 16 進数の値を自動で入力するには、 Specify Ethernet Type でイーサネットタイプのプロファイルを選択します。
Ethernet Type Mask	イーサネットタイプマスクの 16 進数の値を 0x0~0xFFFF の範囲で入力します。適切な 16 進数の値を自動で入力するには Specify Ethernet Type でイーサネットタイプのプロファイルを選択します。
CoS	使用する CoS 値として、 0~7 のいずれかを選択します。
VID	ACL ルールに関連付ける VLAN ID を 1~4094 の範囲で入力します。
Action	ルールが実行するアクション (Permit / Permit Authentication-Bypass / Deny) を選択します。

前の手順に戻るには、**Back** ボタンをクリックします。

次の手順に進むには、**Next** ボタンをクリックします。

標準 IPv4 ACL

ステップ 1 で **Create** または **Update** を選択し、ステップ 2 で **IPv4 ACL** を選択して **Next** 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。

ACL Configuration Wizard 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 ルール番号を 1～65535 の範囲で入力します。 ACL ルール番号を自動で生成するには、 Auto Assign を選択します。

Assign Rule Criteria の各項目の説明を以下に示します。

パラメーター	説明
Source	送信元 IPv4 アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は IPv4 アドレスを入力します。 <ul style="list-style-type: none"> • Any：すべての送信元ホストを判定条件とする場合に選択します。 • Host：送信元ホストの IPv4 アドレスを指定する場合に選択します。右のボックスに送信元ホストの IPv4 アドレスを入力します。 • IP：送信元 IPv4 アドレスを指定する場合に選択します。右のボックスに送信元 IPv4 アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard：ワイルドカードビットマップを使用し、送信元 IP アドレスのグループを入力します。ビット値 1 に対応するビットはチェック対象外になります。ビット値 0 に対応するビットはチェック対象になります。
Destination	宛先 IPv4 アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は IPv4 アドレスを入力します。 <ul style="list-style-type: none"> • Any：すべての宛先ホストを判定条件とする場合に選択します。 • Host：ここに宛先ホストの IPv4 アドレスを指定する場合に選択します。右のボックスに宛先ホストの IPv4 アドレスを入力します。 • IP：宛先 IPv4 アドレスを指定する場合に選択します。右のボックスに宛先 IPv4 アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard：ワイルドカードビットマップを使用し、宛先 IPv4 アドレスのグループを入力します。ビット値 1 に対応するビットはチェック対象外になります。ビット値 0 に対応するビットはチェック対象になります。
Action	ルールが実行するアクション (Permit / Permit Authentication-Bypass / Deny) を選択します。

前の手順に戻るには、**Back** ボタンをクリックします。

次の手順に進むには、**Next** ボタンをクリックします。

拡張 IPv4 ACL

ステップ 1 で **Create** または **Update** を選択し、ステップ 2 で **Extended IPv4 ACL** を選択して **Next** 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。

ACL Configuration Wizard 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 ルール番号を 1～65535 の範囲で入力します。 ACL ルール番号を自動で生成するには、 Auto Assign を選択します。
Protocol Type	プロトコルタイプオプション (TCP / UDP / ICMP / EIGRP (88) / ESP (50) / GRE (47) / IGMP (2) / OSPF (89) / PIM (103) / VRRP (112) / IP-in-IP (94) / PCP (108) / Protocol ID / None) を選択します。 <ul style="list-style-type: none"> • Value : プロトコル ID を手動で入力する場合、0～255 の範囲で入力します。 • Fragments : パケットフラグメントフィルタリングを含める場合にチェックします。

Assign Rule Criteria の各項目の説明を以下に示します。

パラメーター	説明
Source	<p>送信元 IPv4 アドレス設定を以下のいずれかから選択します。また、設定に必要な場合は送信元 IPv4 アドレスを入力します。</p> <ul style="list-style-type: none"> • Any：すべての送信元ホストを判定条件とする場合に選択します。 • Host：送信元ホストの IPv4 アドレスを指定する場合に選択します。右のボックスに送信元ホストの IPv4 アドレスを入力します。 • IP：送信元の IPv4 アドレスを指定する場合に選択します。右のボックスに送信元 IPv4 アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard：ワイルドカードビットマップを使用し、送信元 IPv4 アドレスのグループを入力します。ビット値 1 に対応するビットはチェック対象外になります。ビット値 0 に対応するビットはチェック対象になります。
Destination	<p>宛先 IPv4 アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は宛先 IPv4 アドレスを入力します。</p> <ul style="list-style-type: none"> • Any：すべての宛先ホストを判定条件とする場合に選択します。 • Host：宛先ホストの IPv4 アドレスを指定する場合に選択します。右のボックスに宛先ホストの IPv4 アドレスを入力します。 • IP：宛先 IPv4 アドレスを指定する場合に選択します。右のボックスに宛先 IPv4 アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard：ワイルドカードビットマップを使用し、宛先 IPv4 アドレスのグループを入力します。ビット値 1 に対応するビットはチェック対象外になります。ビット値 0 に対応するビットはチェック対象になります。
Source Port	<p>送信元ポートを選択します。また、以下のいずれかの条件を選択してポート番号を指定します。プロトコルタイプ TCP および UDP でのみ使用できます。</p> <ul style="list-style-type: none"> • =：選択したポートを指定する場合に選択します。 • >：選択したポートよりポート番号が大きいすべてのポートを指定する場合に選択します。 • <：選択したポートよりポート番号が小さいすべてのポートを指定する場合に選択します。 • ≠：選択したポートを除くすべてのポートを指定する場合に選択します。 • Range：ポートを開始ポート番号と終了ポート番号の範囲で指定する場合に選択します。ドロップダウンリストにポート番号が表示されない場合は、ボックスにポート番号を手動で入力することもできます。

Destination Port	宛先ポートを選択します。また、以下のいずれかの条件を選択してポート番号を指定します。プロトコルタイプ TCP および UDP でのみ使用できます。 <ul style="list-style-type: none"> • = : 選択したポートを指定する場合に選択します。 • > : 選択したポートよりポート番号が大きいすべてのポートを指定する場合に選択します。 • < : 選択したポートよりポート番号が小さいすべてのポートを指定する場合に選択します。 • ≠ : 選択したポートを除くすべてのポートを指定する場合に選択します。 • Range : ポートを開始ポート番号と終了ポート番号の範囲で指定する場合に選択します。ドロップダウンリストにポート番号が表示されない場合は、ボックスにポート番号を手動で入力することもできます。
Specify ICMP Message Type	ICMP メッセージタイプを選択します。 プロトコルタイプ ICMP でのみ使用できます。
ICMP Message Type	ICMP Message Type が選択されていない場合に、ICMP メッセージタイプの数値を 0~255 の範囲で入力します。 ICMP Message Type を選択すると、数値が自動で入力されます。 プロトコルタイプが ICMP でのみ使用できます。
Message Code	ICMP Message Type が選択されていない場合に、メッセージコードの数値を 0~255 の範囲で入力します。 ICMP Message Type を選択すると、数値が自動で入力されます。 プロトコルタイプ ICMP でのみ使用できます。
IP Precedence	IP Precedence 値 (routine (0) / priority (1) / immediate (2) / flash (3) / flash-override (4) / critical (5) / internet (6) / network (7)) を選択します。
ToS	ToS 値 (normal (0) / min monetary cost (1) / max reliability (2) / max throughput (4) / min delay (8)) を選択します。
DSCP	DSCP 値 (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) / および ef (46)) を選択します。 <ul style="list-style-type: none"> • Value : 手動で DSCP 値を入力する場合、0~63 の範囲で入力します。
TCP Flag	TCP フラグ (ack / fin / psh / rst / syn / urg) を選択し、ルールにフラグを含めます。プロトコルタイプ TCP でのみ使用できます。
Action	ルールが実行するアクション (Permit / Permit Authentication-Bypass / Deny) を選択します。

前の手順に戻るには、**Back** ボタンをクリックします。

次の手順に進むには、**Next** ボタンをクリックします。

標準 IPv6 ACL

ステップ 1 で **Create** または **Update** を選択し、ステップ 2 で **IPv6 ACL** を選択して **Next** 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。

ACL Configuration Wizard 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 ルール番号を 1～65535 の範囲で入力します。 ACL ルール番号を自動で生成するには、 Auto Assign を選択します。

Assign Rule Criteria の各項目の説明を以下に示します。

パラメーター	説明
Source	送信元 IPv6 アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は送信元 IPv6 アドレスを入力します。 <ul style="list-style-type: none"> • Any：すべての送信元ホストを判定条件とする場合に選択します。 • Host：送信元ホストの IPv6 アドレスを指定する場合に選択します。右のボックスに送信元ホストの IPv6 アドレスを入力します。 • IPv6：送信元 IPv6 アドレスを指定する場合に選択します。右のボックスに送信元 IPv6 アドレスを入力します。 ○ Prefix Length：送信元の IPv6 アドレスのプレフィックス長を入力します。

Destination	宛先 IPv6 アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は宛先 IPv6 アドレスを入力します。 <ul style="list-style-type: none">• Any : すべての宛先ホストを判定条件とする場合に選択します。• Host : 宛先ホストの IPv6 アドレスを指定する場合に選択します。右のボックスに宛先ホストの IPv6 アドレスを入力します。• IPv6 : 宛先 IPv6 アドレスを指定する場合に選択します。右のボックスに宛先 IPv6 アドレスを入力します。<ul style="list-style-type: none">○ Prefix Length : 宛先 IPv6 アドレスのプレフィックス長を入力します。
Action	ルールが実行するアクション (Permit / Permit Authentication-Bypass / Deny) を選択します。

前の手順に戻るには、**Back** ボタンをクリックします。

次の手順に進むには、**Next** ボタンをクリックします。

拡張 IPv6 ACL

ステップ 1 で **Create** または **Update** を選択し、ステップ 2 で **Extended IPv6 ACL** を選択して **Next** 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。

ACL Configuration Wizard 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 ルール番号を 1～65535 の範囲で入力します。ACL ルール番号を自動で生成するには、 Auto Assign を選択します。
Protocol Type	<p>プロトコルタイプ (TCP / UDP / ICMP / Protocol ID / ESP(50) / PCP(108) / SCTP(132) / None) を選択します。</p> <ul style="list-style-type: none"> • Value : 手動でプロトコル ID を入力する場合、0～255 の範囲で入力します。 • Fragments : パケットフラグメントフィルタリングを含める場合にチェックします。

Assign Rule Criteria の各項目の説明を以下に示します。

パラメーター	説明
Source	<p>送信元 IPv6 アドレスを以下のいずれかから選択します。また、設定に必要な場合は送信元 IPv6 アドレスを入力します。</p> <ul style="list-style-type: none"> • Any : すべての送信元ホストを判定条件とする場合に選択します。 • Host : 送信元ホストの IPv6 アドレスを指定する場合に選択します。右のボックスに送信元ホストの IPv6 アドレスを入力します。 • IPv6 : 送信元 IPv6 アドレスを指定する場合に選択します。右のボックスに送信元 IPv6 アドレスを入力します。 <ul style="list-style-type: none"> ○ Prefix Length : 送信元 IPv6 アドレスのプレフィックス長を入力します。
Destination	<p>宛先 IPv6 アドレスの設定を以下のいずれかから選択して入力します。また、設定に必要な場合は宛先 IPv6 アドレスを入力します。</p> <ul style="list-style-type: none"> • Any : すべての宛先ホストを判定条件とする場合に選択します。 • Host : 宛先ホストの IPv6 アドレスを指定する場合に選択します。右のボックスに宛先ホストの IPv6 アドレスを入力します。 • IPv6 : 宛先 IPv6 アドレスを指定する場合に選択します。右のボックスに宛先 IPv6 アドレスを入力します。 <ul style="list-style-type: none"> ○ Prefix Length : 宛先 IPv6 アドレスのプレフィックス長を入力します。
Source Port	<p>送信元ポートを選択します。また、以下のいずれかの条件を選択してポート番号を指定します。プロトコルタイプ TCP および UDP でのみ使用できます。</p> <ul style="list-style-type: none"> • = : 選択したポートを指定する場合に選択します。 • > : 選択したポートよりポート番号が大きいすべてのポートを指定する場合に選択します。 • < : 選択したポートよりポート番号が小さいすべてのポートを指定する場合に選択します。 • ≠ : 選択したポートを除くすべてのポートを指定する場合に選択します。 • Range : ポートを開始ポート番号と終了ポート番号の範囲で指定する場合に選択します。ドロップダウンリストにポート番号が表示されない場合は、ボックスにポート番号を手動で入力することもできます。

Destination Port	宛先ポートを選択します。また、以下のいずれかの条件を選択してポート番号を指定します。プロトコルタイプ TCP および UDP でのみ使用できます。 <ul style="list-style-type: none"> • = : 選択したポートを指定する場合に選択します。 • > : 選択したポートよりポート番号が大きいすべてのポートを指定する場合に選択します。 • < : 選択したポートよりポート番号が小さいすべてのポートを指定する場合に選択します。 • ≠ : 選択したポートを除くすべてのポートを指定する場合に選択します。 • Range : ポートを開始ポート番号と終了ポート番号の範囲で指定する場合に選択します。ドロップダウンリストにポート番号が表示されない場合は、ボックスにポート番号を手動で入力することもできます。
Specify ICMP Message Type	ICMP メッセージタイプを選択します。 プロトコルタイプ ICMP でのみ使用できます。
ICMP Message Type	ICMP Message Type が選択されていない場合に、ICMP メッセージタイプの数値を入力します。 ICMP Message Type を選択すると、数値が自動で入力されます。 プロトコルタイプ ICMP でのみ使用できます。
Message Code	ICMP Message Type が選択されていない場合に、メッセージコードの数値を入力します。 ICMP Message Type を選択すると、数値が自動で入力されます。 プロトコルタイプ ICMP でのみ使用できます。
DSCP	DSCP 値 (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)) を選択します。 <ul style="list-style-type: none"> • Value : 手動で DSCP 値を入力する場合、0~63 の範囲で入力します。
Traffic Class	トラフィッククラスの値を 0~255 の範囲で入力します。
TCP Flag	TCP フラグ (ack / fin / psh / rst / syn / urg) を選択し、ルールにフラグを含めます。 プロトコルタイプ TCP でのみ使用できます。
Flow Label	フローラベルの値を 0~1048575 の範囲で入力します。
Action	ルールがアクション (Permit / Permit Authentication-Bypass / Deny) を選択します。

前の手順に戻るには、**Back** ボタンをクリックします。

次の手順に進むには、**Next** ボタンをクリックします。

拡張エキスパート ACL

ステップ1で **Create** または **Update** を選択し、ステップ2で **Expert ACL** を選択して **Next** 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。

ACL Configuration Wizard 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 ルール番号を 1～65535 の範囲で入力します。 ACL ルール番号を自動で生成するには、 Auto Assign を選択します。

Protocol Type	<p>プロトコルタイプ (TCP / UDP / ICMP / EIGRP(88) / ESP(50) / GRE(47) / IGMP(2) / OSPF(89) / PIM(103) / VRRP(112) / IP-in-IP(94) / PCP(108) / Protocol ID / None) を選択します。</p> <ul style="list-style-type: none"> • Value : 手動でプロトコル ID を入力する場合、0~255 の範囲で入力します。 • Fragments : パケットフラグメントフィルタリングを含める場合にチェックします。
----------------------	--

Assign Rule Criteria の各項目の説明を以下に示します。

パラメーター	説明
Source (IPv4 Address)	<p>送信元 IPv4 アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は送信元 IPv4 アドレスを入力します。</p> <ul style="list-style-type: none"> • Any : すべての送信元ホストを判定条件とする場合に選択します。 • Host : 送信元ホストの IPv4 アドレスを指定する場合に選択します。右のボックスに送信元ホストの IPv4 アドレスを入力します。 • IP : 送信元 IPv4 アドレスを指定する場合に選択します。右のボックスに送信元 IPv4 アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard : ワイルドカードビットマップを使用し、送信元 IPv4 アドレスのグループを入力します。ビット値 1 に対応するビットは、チェック対象外になります。ビット値 0 に対応するビットはチェック対象になります。
Destination (IPv4 Address)	<p>宛先 IPv4 アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は宛先 IPv4 アドレスを入力します。</p> <ul style="list-style-type: none"> • Any : すべての宛先ホストを判定条件とする場合に選択します。 • Host : 宛先ホストの IPv4 アドレスを指定する場合に選択します。右のボックスに宛先ホストの IPv4 アドレスを入力します。 • IP : 宛先 IPv4 アドレスを指定する場合に選択します。右のボックスに宛先 IPv4 アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard : ワイルドカードビットマップを使用し、宛先 IPv4 アドレスのグループを入力します。ビット値 1 に対応するビットは、チェック対象外になります。ビット値 0 に対応するビットは、チェック対象になります。

Source (MAC Address)	<p>送信元 MAC アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は送信元 MAC アドレスを入力します。</p> <ul style="list-style-type: none"> • Any : すべての送信元ホストを判定条件とする場合に選択します。 • Host : 送信元ホストの MAC アドレスを指定する場合に選択します。右のボックスに送信元ホストの MAC アドレスを入力します。 • MAC : 送信元 MAC アドレスを指定する場合に選択します。右のボックスに送信元 MAC アドレスを入力します。 ○ Wildcard : 送信元 MAC アドレスと Wildcard 値を入力します。
Destination (MAC Address)	<p>宛先 MAC アドレスの設定を以下のいずれかから選択します。また、設定に必要な場合は宛先 MAC アドレスを入力します。</p> <ul style="list-style-type: none"> • Any : すべての宛先ホストを判定条件とする場合に選択します。 • Host : 宛先ホストの MAC アドレスを指定する場合に選択します。右のボックスに宛先ホストの MAC アドレスを入力します。 • MAC : 宛先 MAC アドレスを指定する場合に選択します。右のボックスに宛先 MAC アドレスを入力します。 ○ Wildcard : 宛先 MAC アドレスとワイルドカード値を入力します。
Source Port	<p>送信元ポートを選択します。また、以下のいずれかの条件を選択してポート番号を指定します。プロトコルタイプ TCP および UDP でのみ使用できます。</p> <ul style="list-style-type: none"> • = : 選択したポートを指定する場合に選択します。 • > : 選択したポートよりポート番号が大きいすべてのポートを指定する場合に選択します。 • < : 選択したポートよりポート番号が小さいすべてのポートを指定する場合に選択します。 • ≠ : 選択したポートを除くすべてのポートを指定する場合に選択します。 • Range : ポートを開始ポート番号と終了ポート番号の範囲で指定する場合に選択します。ドロップダウンリストにポート番号が表示されない場合は、ボックスにポート番号を手動で入力することもできます。

Destination Port	宛先ポートを選択します。また、以下のいずれかの条件を選択してポート番号を指定します。プロトコルタイプ TCP および UDP でのみ使用できます。 <ul style="list-style-type: none"> • = : 選択したポートを指定する場合に選択します。 • > : 選択したポートよりポート番号が大きいすべてのポートを指定する場合に選択します。 • < : 選択したポートよりポート番号が小さいすべてのポートを指定する場合に選択します。 • ≠ : 選択したポートを除くすべてのポートを指定する場合に選択します。 • Range : ポートを開始ポート番号と終了ポート番号の範囲で指定する場合に選択します。ドロップダウンリストにポート番号が表示されない場合は、ボックスにポート番号を手動で入力することもできます。
Specify ICMP Message Type	ICMP メッセージタイプを選択します。 プロトコルタイプが ICMP でのみ使用できます。
ICMP Message Type	ICMP Message Type が選択されていない場合に、ICMP メッセージタイプの数値を 0~255 の範囲で入力します。 ICMP Message Type を選択すると、数値が自動で入力されます。 プロトコルタイプ ICMP でのみ使用できます。
Message Code	ICMP Message Type が選択されていない場合に、メッセージコードの数値を 0~255 の範囲で入力します。 ICMP Message Type を選択すると、数値が自動で入力されます。 プロトコルタイプ ICMP でのみ使用できます。
IP Precedence	IP Precedence 値 (routine (0) / priority (1) / immediate (2) / flash (3) / flash-override (4) / critical (5) / internet (6) / network (7)) を選択します。
ToS	ToS 値 (normal (0) / min monetary cost (1) / max reliability (2) / max throughput (4) / min delay (8)) を選択します。
DSCP	DSCP 値 (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)) を選択します。 <ul style="list-style-type: none"> • Value : 手動で DSCP 値を入力する場合、0~63 の範囲で入力します。
TCP Flag	TCP フラグ (ack / fin / psh / rst / syn / urg) を選択し、ルールにフラグを含めます。 プロトコルタイプ TCP でのみ使用できます。
CoS	CoS 値として、 0~7 のいずれかから選択します。
VID	ACL ルールに関連付ける VLAN ID を 1~4094 の範囲で入力します。

Action	ルールが実行するアクション（ Permit / Permit Authentication-Bypass / Deny ）を選択します。
---------------	---

前の手順に戻るには、**Back** ボタンをクリックします。

次の手順に進むには、**Next** ボタンをクリックします。

8.1.4 ステップ 4：ポートの適用

Next 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。

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。
Direction	方向を選択します。 In のみ選択できます。

前の手順に戻るには、**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。ステップ 1 の画面（**ACL Configuration Wizard** 画面）に戻ります。

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。

ACL Access List

ACL Access List

ACL Type: ID (1-14999) ACL Name

Total Entries: 6

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	S-IP4	Standard IP ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
2000	E-IP4	Extended IP ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
6000	E-MAC	Extended MAC ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
8000	E-Expert	Extended Expert ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
11000	S-IP6	Standard IPv6 ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
13000	E-IP6	Extended IPv6 ACL	10	10	Disabled		<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

1/1 < < 1 > > Go

S-IP4 (ID: 1) Rule

Sequence No.	Action	Rule	Counter	
10	Permit	any any		<input type="button" value="Delete"/>

1/1 < < 1 > > Go

MAC Access-List Enable IP-Packets

MAC Access-List Enable IP-Packets State Enabled Disabled

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	<p>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。</p> <p>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。</p>

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。

The screenshot displays the 'ACL Access List' configuration page. At the top, there are search filters for ACL Type (set to 'All'), ID (1-14999), and ACL Name (32 chars). Below this, a table lists 6 ACL entries. The first entry (ID: 1) is selected, and its details are expanded in a sub-table. The sub-table shows the rule configuration for 'S-IP4 (ID: 1) Rule', including the sequence number (1), action (Permit), rule (any any), and counter. At the bottom, the 'MAC Access-List Enable IP-Packets' section is visible, with the 'Disabled' radio button selected and an 'Apply' button.

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。 <ul style="list-style-type: none"> • 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 標準 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。

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 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。
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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ Wildcard：ワイルドカードマスクを指定します。

設定を適用するには、**Apply** ボタンをクリックします。

前の画面に戻るには、**Back** ボタンをクリックします。

8.2.2 拡張 IP ACL

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。

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 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	<p>プロトコルタイプのオプション（TCP / UDP / ICMP / EIGRP(88) / ESP(50) / GRE(47) / IGMP(2) / OSPF(89) / PIM(103) / VRRP(112) / IP-in-IP(94) / PCP(108) / Protocol ID / None）を選択します。</p> <ul style="list-style-type: none"> • Value：プロトコル ID を手動で入力する場合、0～255 の範囲で入力します。 • Fragments：パケットフラグメントフィルタリングを含める場合にチェックします。
Source	<p>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。</p> <ul style="list-style-type: none"> • Any：すべての送信元ホストを合致条件とします。 • Host：送信元 IPv4 アドレスを条件とします。 • IP：送信元の IPv4 アドレスを入力します。 ○ Wildcard：ワイルドカードマスクを指定します。

Destination	<p>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。</p> <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ Wildcard：ワイルドカードマスクを指定します。
Source Port	<p>送信元ポートを選択します。</p> <ul style="list-style-type: none"> • =：選択したポートを指定する場合に選択します。 • >：選択したポートよりポート番号が大きいすべてのポートを指定する場合に選択します。 • <：選択したポートよりポート番号が小さいすべてのポートを指定する場合に選択します。 • ≠：選択したポートを除くすべてのポートを指定する場合に選択します。 • Range：ポートを開始ポート番号と終了ポート番号の範囲で指定する場合に選択します。ドロップダウンリストにポート番号が表示されない場合は、ボックスにポート番号を手動で入力することもできます。 <p>このパラメータを指定できるのは、プロトコルタイプが TCP と UDP の場合のみです。</p>
Destination Port	<p>宛先ポートを選択します。</p> <ul style="list-style-type: none"> • =：選択したポートを指定する場合に選択します。 • >：選択したポートよりポート番号が大きいすべてのポートを指定する場合に選択します。 • <：選択したポートよりポート番号が小さいすべてのポートを指定する場合に選択します。 • ≠：選択したポートを除くすべてのポートを指定する場合に選択します。 • Range：ポートを開始ポート番号と終了ポート番号の範囲で指定する場合に選択します。ドロップダウンリストにポート番号が表示されない場合は、ボックスにポート番号を手動で入力することもできます。
Specify ICMP Message Type	<p>ICMP メッセージタイプを選択します。 プロトコルタイプ ICMP でのみ使用できます。</p>

ICMP Message Type	<p>ICMP Message Type が選択されていない場合に、ICMP メッセージタイプの数値を 0~255 の範囲で入力します。</p> <p>ICMP Message Type を選択すると、数値が自動で入力されます。プロトコルタイプ ICMP でのみ使用できます。</p>
Message Code	<p>ICMP Message Type が選択されていない場合に、メッセージコードの数値を 0~255 の範囲で入力します。</p> <p>ICMP Message Type を選択すると、数値が自動で入力されます。プロトコルタイプ ICMP でのみ使用できます。</p>
TCP Flag	TCP フラグ (ack / fin / psh / rst / syn / urg) を選択し、ルールにフラグを含めます。プロトコルタイプ TCP でのみ使用できます。
IP Precedence	IP Precedence 値 (routine (0) / priority (1) / immediate (2) / flash (3) / flash-override (4) / critical (5) / internet (6) / network (7)) を選択します。
ToS	ToS 値 (normal (0) / min monetary cost (1) / max reliability (2) / max throughput (4) / min delay (8)) を選択します。
DSCP	<p>DSCP 値 (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)) を選択します。</p> <ul style="list-style-type: none"> • Value : 手動で DSCP 値を入力する場合、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。

前の画面に戻るには、**Back** ボタンをクリックします。

8.2.3 標準 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。

Add ACL Rule

Add ACL Rule

ID 11000

ACL Name S-IP6

ACL Type Standard IPv6 ACL

Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.)

Action Permit Deny

Match IPv6 Address

Source Any Host IPv6 Prefix Length

Destination Any Host IPv6 Prefix Length

Time Range

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 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。
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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ Prefix Length : プレフィックス長を入力します。

設定を適用するには、**Apply** ボタンをクリックします。

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 IPv6 ACL

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。

Add ACL Rule

Add ACL Rule

ID: 13000
 ACL Name: E-IPv6
 ACL Type: Extended IPv6 ACL
 Sequence No. (1-65535): (If it isn't specified, the system automatically assigns.)
 Action: Permit Deny
 Protocol Type: (0-255) Fragments

Match IPv6 Address

Source: Any Host IPv6 Prefix Length:

Destination: Any Host IPv6 Prefix Length:

Match Port

Source Port: (0-65535) (0-65535)

Destination Port: (0-65535) (0-65535)

TCP Flag: ack fin psh rst syn urg

DSCP (0-63) Value (0-63)

Traffic Class (0-255)

Flow Label (0-1048575)

Time Range

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 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	<p>プロトコルタイプのオプションを（TCP / UDP / ICMP / Protocol ID / ESP(50) / PCP(108) / SCTP(132) / None）を選択します。</p> <ul style="list-style-type: none"> • Value：プロトコル ID を手動で入力する場合、0～255 の範囲で入力します。 • Fragments：パケットフラグメントフィルタリングを含める場合にチェックします。
Source	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • 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。
Source Port	<p>送信元ポートの値を選択します。</p> <ul style="list-style-type: none"> • = : 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。 <p>このパラメータを指定できるのは、プロトコルタイプが TCP と UDP の場合のみです。</p>
Destination Port	<p>宛先ポートの値を選択します。</p> <ul style="list-style-type: none"> • = : 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。 <p>このパラメータを指定できるのは、プロトコルタイプが TCP と UDP の場合のみです。</p>
TCP Flag	<p>プロトコル条件が TCP の場合のみ表示されます。</p> <p>プロトコル条件が TCP の場合のみ表示されます。 (ack / fin / psh / rst / syn / urg) を判定条件とします。</p> <p>チェックされていない TCP フラグは判定条件としません。</p>
Specify ICMP Message Type	<p>プロトコルタイプが 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。</p>
ICMP Message Type	<p>ICMP Message Type を選択しない場合は、使用する ICMP メッセージタイプの数値をここに入力します。</p> <p>ICMP Message Type を選択した場合は、この数値が自動的に入力されます。</p> <p>このパラメータを指定できるのは、プロトコルタイプが ICMP の場合のみです。</p>

Message Code	<p>ICMP Message Type を選択しない場合は、使用するメッセージコードの数値をここに入力します。</p> <p>ICMP Message Type を選択した場合は、この数値が自動的に入力されます。</p> <p>このパラメータを指定できるのは、プロトコルタイプが ICMP の場合のみです。</p>
DSCP	<p>使用する 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。</p> <ul style="list-style-type: none"> Value : DSCP 値は、手動でここに入力することもできます。範囲は 0~63 です。
Traffic Class	トラフィッククラスの値を 0~255 の範囲で入力します。
Flow Label	フローラベルの値を 0~1048575 の範囲内で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

前の画面に戻るには、**Back** ボタンをクリックします。

8.2.5 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。

Add ACL Rule

Add ACL Rule

ID: 6000
ACL Name: E-MAC
ACL Type: Extended MAC ACL
Sequence No. (1-65535): (If it isn't specified, the system automatically assigns.)
Action: Permit Deny

Match MAC Address

Source: Any Host MAC Wildcard:

Destination: Any Host MAC Wildcard:

Match Ethernet Type

Specify Ethernet Type:
Ethernet Type (0x0-0xFFFF):
Ethernet Type Mask (0x0-0xFFFF):

CoS:
VID(1-4094):
Time Range:

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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ○ 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。
Time Range	ACL ルールの時間範囲プロファイル名を、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。

前の画面に戻るには、**Back** ボタンをクリックします。

8.2.6 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。

設定できるフィールドを以下に説明します。

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。指定されていない場合、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。
Protocol Type	<p>プロトコルタイプのオプション（TCP / UDP / ICMP / EIGRP(88) / ESP(50) / GRE(47) / IGMP(2) / OSPF(89) / PIM(103) / VRRP(112) / IP-in-IP(94) / PCP(108) / Protocol ID / None）を選択します。</p> <ul style="list-style-type: none"> • Value : プロトコル ID を 0～255 の範囲で入力します。手動で入力することもできます。 • Fragments : パケットフラグメントフィルタリングを含める場合はこのオプションを選択します。

Source (Match IP Address)	<p>送信元 IPv4 アドレスを選択して入力します。選択できるオプションは次のとおりです。</p> <ul style="list-style-type: none"> • Any：このルールの条件に従ってすべての送信元トラフィックが評価されます。 • Host：送信元ホストの IPv4 アドレスを入力します。 • IP：送信元の IPv4 アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard：ワイルドカードビットマップを使用して送信元 IPv4 アドレスのグループを入力します。ビット値 1 に対応するビットはチェック対象外になります。ビット値 0 に対応するビットはチェック対象になります。
Destination (Match IP Address)	<p>宛先 IPv4 アドレスを選択して入力します。選択できるオプションは次のとおりです。</p> <ul style="list-style-type: none"> • Any：このルールの条件に従ってすべての宛先トラフィックが評価されます。 • Host：宛先ホストの IPv4 アドレスを入力します。 • IP：宛先 IPv4 アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard：ワイルドカードビットマップを使用して宛先 IPv4 アドレスのグループを入力します。ビット値 1 に対応するビットはチェック対象外になります。ビット値 0 に対応するビットはチェック対象になります。
Source (Match MAC Address)	<p>送信元 MAC アドレスを選択して入力します。選択できるオプションは次のとおりです。</p> <ul style="list-style-type: none"> • Any：このルールの条件に従ってすべての送信元トラフィックが評価されます。 • Host：送信元ホストの MAC アドレスを入力します。 • MAC：送信元 MAC アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard：表示されたスペースに、送信元 MAC アドレスとワイルドカードの値を入力します。
Destination (Match MAC Address)	<p>宛先 MAC アドレスを選択して入力します。選択できるオプションは次のとおりです。</p> <ul style="list-style-type: none"> • Any：このルールの条件に従ってすべての宛先トラフィックが評価されます。 • Host：宛先ホストの MAC アドレスを入力します。 • MAC：宛先 MAC アドレスを入力します。 <ul style="list-style-type: none"> ○ Wildcard：表示されたスペースに、宛先 MAC アドレスとワイルドカードの値を入力します。

Source Port	<p>送信元ポートの値を選択して入力します。選択できるオプションは次のとおりです。</p> <ul style="list-style-type: none"> • = : 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 : 選択した開始ポート番号から終了ポート番号までの範囲が使用されます。または、ドロップダウンリストでポート番号を選択できなければ、表示されたスペースに手動でポート番号を入力できます。 <p>このパラメータを指定できるのは、プロトコルタイプが TCP と UDP の場合のみです。</p>
Destination Port	<p>ここで宛先ポートの値を選択して入力します。選択できるオプションは次のとおりです。</p> <ul style="list-style-type: none"> • = : 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 : 選択した開始ポート番号から終了ポート番号までの範囲が使用されます。または、ドロップダウンリストでポート番号を選択できなければ、表示されたスペースに手動でポート番号を入力できます。 <p>このパラメータを指定できるのは、プロトコルタイプが TCP と UDP の場合のみです。</p>
Specify ICMP Message Type	<p>使用する ICMP メッセージタイプをここで選択します。</p> <p>このパラメータを指定できるのは、プロトコルタイプが ICMP の場合のみです。</p>
ICMP Message Type	<p>ICMP Message Type を選択しない場合は、使用する ICMP メッセージタイプの数値をここに入力します。範囲は 0~255 です。</p> <p>ICMP Message Type を選択した場合は、この数値が自動的に入力されます。</p> <p>このパラメータを指定できるのは、プロトコルタイプが ICMP の場合のみです。</p>

Message Code	<p>ICMP Message Type を選択しない場合は、使用するメッセージコードの数値をここに入力します。範囲は 0~255 です。</p> <p>ICMP Message Type を選択した場合は、この数値が自動的に入力されます。</p> <p>このパラメータを指定できるのは、プロトコルタイプが ICMP の場合のみです。</p>
IP Precedence	使用する IP Precedence 値を (routine (0) / priority (1) / immediate (2) / flash (3) / flash-override (4) / critical (5) / internet (6) / network (7)) から選択します。
ToS	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。
DSCP	<p>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) / および ef(46)) で指定できます。</p> <ul style="list-style-type: none"> • Value : DSCP 値は、手動でここに入力することもできます。範囲は 0~63 です。
TCP Flag	<p>プロトコルタイプが TCP の場合のみ表示されます。</p> <p>TCP フラグ (ack / fin / psh / rst / syn / urg) を判定条件とします。</p>
VID	VLAN ID を 1~4094 の範囲で入力します。
CoS	CoS 値を 0~7 の範囲内で選択します。

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。

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。



The screenshot shows the 'Match Access-List' configuration window. At the top, it displays 'Access Map Name: Map' and 'Sub Map Number: 1'. There are three radio button options: 'Match IP Access-List' (selected), 'Match IPv6 Access-List', and 'Match MAC Access-List'. Each option has a 'Please Select' button and 'Apply' and 'Delete' buttons.

Match Access-List の各項目の説明を以下に示します。

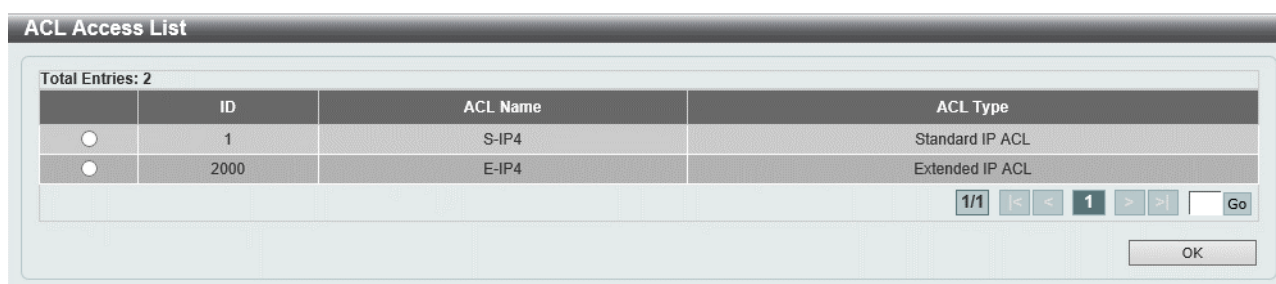
パラメーター	説明
Match IP Access-List	適用する IP ACL が表示されます。
Match IPv6 Access-List	適用する IPv6 ACL が表示されます。
Match MAC Access-List	適用する MAC ACL が表示されます。

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。



The screenshot shows the 'ACL Access List' selection window. It displays 'Total Entries: 2'. Below is a table with columns 'ID', 'ACL Name', and 'ACL Type'. There are two entries: ID 1 (S-IP4, Standard IP ACL) and ID 2000 (E-IP4, Extended IP ACL). At the bottom, there are navigation buttons (1/1, left arrow, 1, right arrow, Go) and an 'OK' button.

ID	ACL Name	ACL Type
1	S-IP4	Standard IP ACL
2000	E-IP4	Extended IP ACL

VLAN アクセスマップに関連付ける ACL を選択するには、ラジオボタンを選択します。

選択した ACL を適用するには、**OK** ボタンをクリックします。

8.5 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。

8.6 ACL Resource Reserved Group

ACL Resource Reserved Group 画面では、ACL リソースを使用する機能でのリソースの使用状況をグループ順に表示します。

本画面を表示するには、**ACL > ACL Resource Reserved Group** をクリックします。



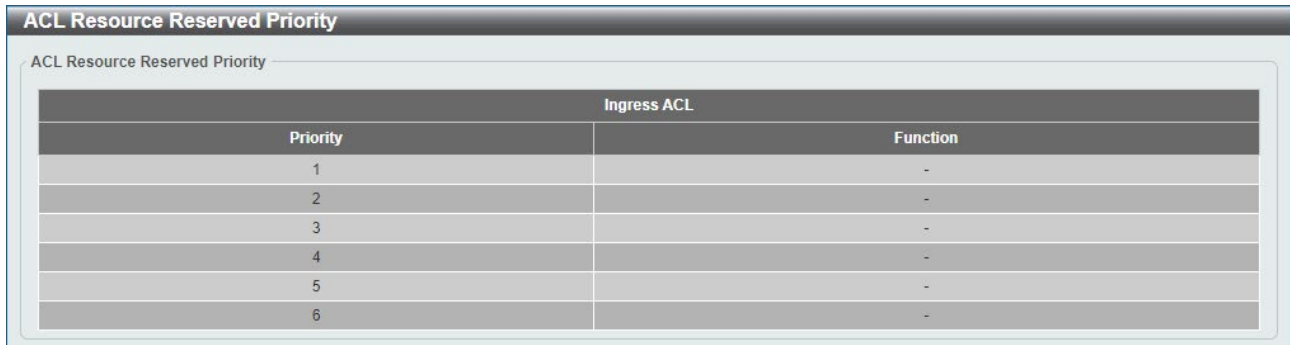
The screenshot displays the 'ACL Resource Reserved Group' interface. It features a table with the following structure:

ACL Resource Reserved Group	
Ingress ACL	
Group	Function
1/2	-
1/3	-
1/4	-
1/5	-
1/6	-
1/7	-

8.7 ACL Resource Reserved Priority

ACL Resource Reserved Priority 画面では、ACL リソースの使用状況を優先度順に表示します。

本画面を表示するには、**ACL > ACL Resource Reserved Priority** をクリックします。



ACL Resource Reserved Priority	
Ingress ACL	
Priority	Function
1	-
2	-
3	-
4	-
5	-
6	-

9 Security

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。
以下の項で説明するサブメニューに分かれています。

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。

Port	Maximum	Current No.	Violation Action	Violation Count	Security Mode	Admin State	Current State	Aging Time	Aging Type
Port1/0/1	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Port1/0/2	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Port1/0/3	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Port1/0/4	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Port1/0/5	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Port1/0/6	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Port1/0/7	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Port1/0/8	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Port1/0/9	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute
Port1/0/10	32	0	Protect	-	Delete-on-Timeout	Disabled	-	0	Absolute

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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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	エントリーのエイジング時間を 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。 <ul style="list-style-type: none"> • 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。

Port Security Address Entries

Port Security Address Entries

Port: Port1/0/1 MAC Address: 00-84-57-00-00-00 Permanent VID (1-4094):

Add Delete Clear by Port Clear by MAC

Total Entries: 1 Clear All

Port	VID	MAC Address	Address Type	Remaining Time (mins)
Port1/0/10	1	00-11-22-33-44-88	Permanent	-

1/1 < < 1 > > Go

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	ここに 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 認証の設定を行います。以下の項で説明するサブメニューに分かれています。

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。

802.1X Port Settings

802.1X Port Settings

From Port: Port1/0/1, To Port: Port1/0/1, PAE Authenticator: None, Server Timeout (5-65535): 30 sec

Quiet-Period (5-65535): 60 sec, No Quiet-Period: , TX-Period (5-65535): 30 sec, No TX-Period:

Re-Authperiod (5-2147483647): 3600 sec, Supp-Timeout (5-65535)(5-65535): 30 sec, Ignore-eapol-start: None, Reauthentication: Disabled

Apply

Port	PAE Authenticator	Quiet-Period	Re-Authperiod	SuppTimeout	Server Timeout	TX Period	Ignore-eapol-start	Reauthentication
Port1/0/1	None	60	3600	30	30	30	Disabled	Disabled
Port1/0/2	None	60	3600	30	30	30	Disabled	Disabled
Port1/0/3	None	60	3600	30	30	30	Disabled	Disabled
Port1/0/4	None	60	3600	30	30	30	Disabled	Disabled
Port1/0/5	None	60	3600	30	30	30	Disabled	Disabled
Port1/0/6	None	60	3600	30	30	30	Disabled	Disabled
Port1/0/7	None	60	3600	30	30	30	Disabled	Disabled
Port1/0/8	None	60	3600	30	30	30	Disabled	Disabled
Port1/0/9	None	60	3600	30	30	30	Disabled	Disabled
Port1/0/10	None	60	3600	30	30	30	Disabled	Disabled

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。
Server Timeout	認証サーバーの応答待ち時間時間を 5～65535 (秒) の範囲で入力します (デフォルト: 30 秒)。
Quiet-Period	認証失敗時のブロック期間を 5～65535 (秒) の範囲で入力します (デフォルト: 60 秒)。 ブロック期間を使用しない場合は、 No Quiet Period オプションを選択します。
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。 定期的な EAP-Request/Identity の送信を無効にする場合は、 No TX Period オプションを選択します。
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 Access Defender

Access Defender サブメニューでは、Access Defender と呼ばれる認証基盤に関する共通設定を行います。ポートアクセス認証は Access Defender により制御が行われます。

以下の項で説明するサブメニューに分かれています。

9.3.1 Access Defender Global Settings

Access Defender Global Settings 画面では、AccessDefender のログアウト設定を行います。

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

Time	Type
20:0	dot1x

Logout Clock タブでは、ポートアクセス認証を解除するタイマ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
Time	ポートアクセス認証の強制ログアウト時間を 24 時間形式 (HH:MM) で入力します。 例：22:40
Type	ログアウトを行う認証クライアントのタイプを指定します <ul style="list-style-type: none"> • MAC：MAC 認証クライアントをログアウトします。 • Dot1x：IEEE 802.1X 認証クライアントをログアウトします。 • Web：Web 認証クライアントをログアウトします。

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。

指定したエントリーを削除するには、**Delete** ボタンをクリックします。

Logout Timeout タブを選択すると、以下の画面が表示されます。

Logout Timeout では、ポートアクセス認証の有効期間を設定します。各項目の説明を以下に示します。

パラメーター	説明
Second	有効期間を 10～86400（秒）の範囲で入力します。 Default を選択すると 0 として計算され、 Minute 、 Hour 、 Day のいずれの設定もない場合は有効期間がない設定となります。
Minute	有効期間（分）を 0～59 の範囲で入力します。この時間は、 Second の値に秒換算で加算されます。
Hour	有効期間（時）を 0～23 の範囲で入力します。この時間は、 Second の値に秒換算で加算されます。
Day	有効期間（日）を 0～31 の範囲で入力します。この時間は、 Second の値に秒換算で加算されます。
Type	有効期間を設定する認証クライアントのタイプを以下から選択します。 <ul style="list-style-type: none"> • MAC： MAC 認証クライアントの有効期限を指定します。 • Dot1x： IEEE 802.1X 認証クライアントの有効期限を指定します。 • Web： Web 認証クライアントの有効期限を指定します。

設定を適用するには、**Apply** ボタンをクリックします。

すべてのエントリを削除するには、**Delete All** ボタンをクリックします。

指定したエントリを削除するには、**Delete** ボタンをクリックします。

Logout Aging Time タブを選択すると、以下の画面が表示されます。

Logout Aging Time タブでは、ポートアクセス認証の無通信タイムアウト時間を設定します。各項目の説明を以下に示します。

パラメーター	説明
Second	無通信タイムアウト時間を 10～86400（秒）の範囲で入力します。 Default を選択すると 0 として計算され、 Minute 、 Hour 、 Day のいずれの設定もない場合は無通信タイムアウトがない設定となります。
Minute	無通信タイムアウト時間（分）を 0～59 の範囲で入力します。この時間は、 Second の値に秒換算で加算されます。
Hour	無通信タイムアウト時間（時）を 0～23 の範囲で入力します。この時間は、 Second の値に秒換算で加算されます。
Day	無通信タイムアウト時間（日）を 0～31 の範囲内で入力します。この時間は、 Second の値に秒換算で加算されます。
Type	ログアウトする認証済みクライアントのタイプを指定します。選択できるオプションは次のとおりです。 <ul style="list-style-type: none"> • MAC： MAC 認証クライアントのタイムアウト時間を設定します。 • Dot1x： IEEE 802.1X 認証クライアントのタイムアウト時間を設定します。 • Web： Web 認証クライアントのタイムアウト時間を設定します。

設定を適用するには、**Apply** ボタンをクリックします。

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。

指定したエントリーを削除するには、**Delete** ボタンをクリックします。

Logout Link Down タブを選択すると、以下の画面が表示されます。

Logout Link Down タブでは、リンクダウン発生時にポートアクセス認証の解除を行わないポートを設定します。各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	リンクダウン発生時にポートアクセス認証の解除を行わない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、**Disable** ボタンをクリックします。

指定したエントリーを削除するには、**Delete** ボタンをクリックします。

Logout Link Down Time タブを選択すると以下の画面が表示されます。

Logout Link Down Time タブでは、リンクダウン発生時にポートアクセス認証の解除を保留するポートと猶予期間を設定します。各項目の説明を以下に示します。

パラメーター	説明
Time	リンクダウン発生時のポートアクセス認証を解除するまでの猶予期間を1～300（秒）の範囲で入力します。猶予期間内にリンクが回復した場合、認証は解除されません。
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。

指定したポートでこの機能を有効にするには、**Enable** ボタンをクリックします。

指定したエントリーを削除するには、**Delete** ボタンをクリックします。

9.3.2 Access Defender Port Settings

Access Defender Port Settings 画面では、AccessDefender のポートを設定します。

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

Port	Roaming	Max Client
Port1/0/1	Disabled	
Port1/0/2	Disabled	
Port1/0/3	Disabled	
Port1/0/4	Disabled	
Port1/0/5	Disabled	
Port1/0/6	Disabled	
Port1/0/7	Disabled	
Port1/0/8	Disabled	
Port1/0/9	Disabled	
Port1/0/10	Disabled	

Access Defender Port Settings で設定できるフィールドについて、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。
Roaming	認証ローミング機能の状態 (Enabled / Disabled) を選択します。
Max Client	ポートの最大認証端末数を 1~128 の範囲内で入力します。

設定を適用するには、**Apply** ボタンをクリックします。

9.3.3 Access Defender Port Information

Access Defender Port Information 画面では、AccessDefender のポート情報を表示します。

本画面を表示するには、**Security > Access Defender > Access Defender Port Information** をクリックします。

Port	MAC	802.1X	Web	DHCPSPNP	Roaming	Static	TTL
Port1/0/1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Port1/0/2	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Port1/0/3	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Port1/0/4	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Port1/0/5	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Port1/0/6	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Port1/0/7	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Port1/0/8	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Port1/0/9	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Port1/0/10	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

9.3.4 Access Defender Static MAC

Access Defender Static MAC 画面では、AccessDefender のスタティック MAC 設定を行います。

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

MAC Address	Port	VLAN ID
01-00-00-00-00-02	interface port 1/0/10	1

Access Defender Static MAC で設定できるフィールドについて、各項目の説明を以下に示します。

パラメーター	説明
Port	使用するポートを指定します。
MAC Address	スタティック認証済み端末の MAC アドレスを入力します。
VLAN ID	スタティック認証済み端末に関連付けられている VLAN ID を 1～4094 の範囲内で指定します。

設定を適用するには、**Apply** ボタンをクリックします。

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。

指定したエントリーを削除するには、**Delete** ボタンをクリックします。

9.4 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。
以下の項で説明するサブメニューに分かれています。

9.4.1 AAA Global Settings

AAA Global Settings 画面では、アカウントिंग（以降、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。

9.4.2 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。

Application	Login Method List	
Console	default	Edit
Telnet	default	Edit
SSH	default	Edit

Edit ボタンをクリックすると、該当するライン種別の認証方式を編集する画面に移行します。

Application	Login Method List	
Console	default	Apply
Telnet	default	Edit
SSH	default	Edit

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 Security > AAA > Authentication Settings の AAA Authentication 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。

9.4.3 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。

The screenshot shows the 'Application Accounting Settings' page. The 'Application Accounting Exec Method List' section contains a table with the following data:

Application	Exec Method List	
Console		Edit
Telnet		Edit
SSH		Edit

The 'Application Accounting Commands Method List' section shows the following configuration:

Application: Console, Level: 1, Commands Method List: 32 chars, Apply

Total Entries: 1

Application	Level	Commands Method List	
SSH	15	1	Delete

Navigation: 1/1, 1, Go

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。

The screenshot shows the 'Application Accounting Settings' page. The 'Application Accounting Exec Method List' section contains a table with the following data:

Application	Exec Method List	
Console	<input type="text"/>	Apply
Telnet		Edit
SSH		Edit

The 'Application Accounting Commands Method List' section shows the following configuration:

Application: Console, Level: 1, Commands Method List: 32 chars, Apply

Total Entries: 1

Application	Level	Commands Method List	
SSH	15	1	Delete

Navigation: 1/1, 1, Go

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。

9.4.4 Authentication Settings

Authentication Settings 画面では、ポートアクセス認証やログイン認証などの方式（メソッドリスト）を設定します。。

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。 <ul style="list-style-type: none"> • 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。 • local : 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	<p>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。</p> <ul style="list-style-type: none"> • 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。 • enable : 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。
- **local** : ローカルデータベースで認証します。
- **group** : 指定したサーバグループに照会を行います。右のボックスにサーバグループ名を 32 文字以内で入力します。
- **radius** : サーバグループ「radius」に照会します。
- **tacacs+** : サーバグループ「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。

9.4.5 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。

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。 <ul style="list-style-type: none"> 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 (none / 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。

AAA Accounting System で設定できるフィールドについて、以下で説明します。

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。 <ul style="list-style-type: none"> • 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 (none / 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。

The screenshot shows the 'AAA Accounting Exec' configuration page. It includes a 'List Name' field (32 chars), an 'Accounting mode' dropdown set to 'none', and four 'Method' dropdowns (Method 1: None, Method 2: Please Select, Method 3: Please Select, Method 4: Please Select). An 'Apply' button is present. Below the form is a table with 1 entry:

Name	Accounting mode	Method 1	Method 2	Method 3	Method 4	
List	none					Delete

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。 <ul style="list-style-type: none"> • 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 (none / 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 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。 <ul style="list-style-type: none"> • 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 (none / 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。

9.5 RADIUS

RADIUS サブメニューでは、RADIUS サーバーの設定を行います。
以下の項で説明するサブメニューに分かれています。

9.5.1 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。

RADIUS Global Settings では、RADIUS サーバー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
Dead Time	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。

RADIUS Server Attribute MAC Format Settings では、RADIUS 要求パケットの属性値で使用する MAC アドレスのフォーマットを設定します。各項目の説明を以下に示します。

パラメーター	説明
Case	MAC アドレスで使用する英文字の大文字と小文字の区別の形式（ Lowercase / Uppercase ）を選択します。

Delimiter	MAC アドレスで使用する区切り文字 (Hyphen / Colon / Dot / None) を選択します。
Delimiter Number	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。

9.5.2 RADIUS Server Settings

RADIUS Server Settings 画面では、RADIUS サーバーの設定を構成するために使用されます。本画面を表示するには、**Security > RADIUS > RADIUS Server Settings** をクリックします。

RADIUS Server Settings

RADIUS Server Settings

IP Address

IPv6 Address

Authentication Port (0-65535)

Accounting Port (0-65535)

Retransmit (0-20) times

Timeout (1-255) sec

Key Type

Key

Total Entries: 1

IPv4/IPv6 Address	Authentication Port	Accounting Port	Timeout	Retransmit	Key	
172.31.131.1	1812	1813	5	2	*****	<input type="button" value="Delete"/>

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	アカウントティングの UDP ポート番号を 0~65535 の範囲で入力します。アカウント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。

9.5.3 RADIUS Group Server Settings

RADIUS Group Server Settings 画面では、RADIUS サーバークラスタを設定します。
本画面を表示するには、**Security > RADIUS > RADIUS Group Server Settings** をクリックします。

RADIUS Group Server Settings

RADIUS Group Server Settings

Group Server Name: 32 chars

IPv4 Address

IPv6 Address: 2013::1

Add

Total Entries: 2

Group Server Name	IPv4/IPv6 Address									
Group	2013::1	-	-	-	-	-	-	-	-	Show Detail
radius	172.31.131...	-	-	-	-	-	-	-	-	Delete

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 サーバークラスタ名を 32 文字以内で入力します。
IPv4 Address	追加する RADIUS サーバークラスタの IPv4 アドレスを入力します。
IPv6 Address	追加する RADIUS サーバークラスタの IPv6 アドレスを入力します。

入力した情報で RADIUS サーバークラスタや RADIUS サーバークラスタを追加するには、**Add** ボタンをクリックします。

RADIUS サーバークラスタの詳細を表示するには、**Show Detail** ボタンをクリックします。

RADIUS サーバークラスタを削除するには、**Delete** ボタンをクリックします。

Show 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 Group Server Settings

Group Server Name: Group

IPv4/IPv6 Address	
2013::1	Delete

Back

RADIUS サーバークラスタから RADIUS サーバークラスタを削除するには、**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。

9.5.4 RADIUS Statistics

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 Statistics** をクリックします。

RADIUS Statistic

RADIUS Statistic

Group Server Name:

Total Entries: 1

RADIUS Server Address	Authentication Port	Accounting Port	State
172.31.131.1	1812	1813	Up

1/1 |< < 1 > >| Go

RADIUS Server Address: 172.31.131.1

Parameter	Authentication Port	Accounting Port
Round Trip Time	0	0
Access Requests	0	NA
Access Accepts	0	NA
Access Rejects	0	NA
Access Challenges	0	NA
Acct Request	NA	0
Acct Response	NA	0
Retransmissions	0	0
Malformed Responses	0	0
Bad Authenticators	0	0
Pending Requests	0	0
Timeouts	0	0
Unknown Types	0	0
Packets Dropped	0	0

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トिंग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 サーバーグループ名を選択します。

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。

9.6 TACACS

TACACS サブメニューでは、TACACS+サーバーの設定を行います。
以下の項で説明するサブメニューに分かれています。

9.6.1 TACACS Server Settings

TACACS Server Settings 画面では、TACACS+サーバーの設定を構成するために使用されます。
本画面を表示するには、**Security > TACACS > TACACS Server Settings** をクリックします。

TACACS Server Settings

TACACS Server Settings

IP Address:

Port (1-65535):

Key Type:

Timeout (1-255): sec

Key:

Total Entries: 1

IPv4 Address	Port	Timeout	Key
172.31.131.0	49	5	*****

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。

9.6.2 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。

9.7 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。以下の項で説明するサブメニューに分かれています。

9.7.1 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。

9.7.2 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。

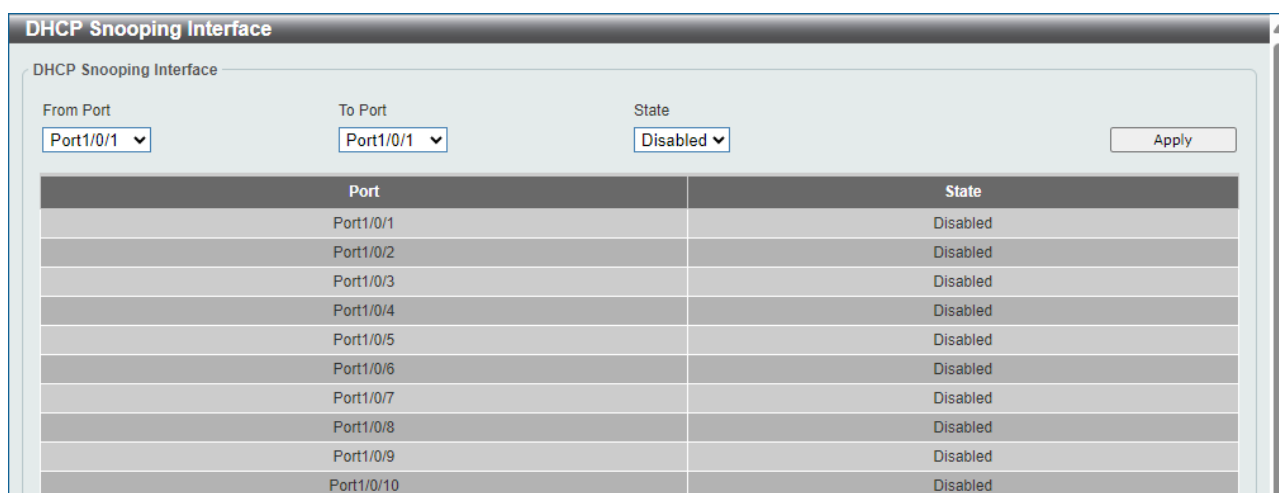
本画面を表示するには、**Security > DHCP Snooping > DHCP Snooping Binding Entry** をクリックします。



9.7.3 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。

9.7.4 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。

DHCP Snooping Static Entry

DHCP Snooping Static Entry

From Port: Port1/0/1

To Port: Port1/0/1

State: Disabled

IP

IPv6: 2021::1

Apply

Total Entries: 1

Port	IP/IPv6
Port1/0/10	172.31.131.222

1/1 < < 1 > > Go

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の IPv4 アドレスを入力します。
IPv6	スタティックエントリの IPv6 アドレスを入力します。

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

9.8 BPDU Guard

BPDU Guard 画面では、BPDU ガードを設定します。

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

Port	State	Mode	Status
Port1/0/1	Disabled	Shutdown	Normal
Port1/0/2	Disabled	Shutdown	Normal
Port1/0/3	Disabled	Shutdown	Normal
Port1/0/4	Disabled	Shutdown	Normal
Port1/0/5	Disabled	Shutdown	Normal
Port1/0/6	Disabled	Shutdown	Normal
Port1/0/7	Disabled	Shutdown	Normal
Port1/0/8	Disabled	Shutdown	Normal

BPDU Guard Settings の各項目の説明を以下に示します。

パラメーター	説明
BPDU Guard State	BPDU ガードのグローバル状態 (Enabled / Disabled) を選択します。
BPDU Guard Trap State	BPDU ガードのトラップ通知機能の状態 (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。

BPDU Guard 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	BPDU ガードの状態 (Enabled / Disabled) を選択します。を選択します。
Mode	BPDU ガードモードを (Drop / Block / Shutdown) から選択します。 <ul style="list-style-type: none"> • Drop : ポートが Attacked 状態になったとき、受信したすべての BPDU パケットを破棄します。 • Block : ポートが Attacked の状態になったとき、すべてのパケット (BPDU パケットを含む) を破棄します。 • Shutdown : ポートが Attacked の状態になったとき、ポートを Error Disabled 状態にして閉塞します。

設定を適用するには、**Apply** ボタンをクリックします。

9.9 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

MAC Authentication Global Settings

MAC Authentication State Enabled Disabled

Ignore DHCP Enabled Disabled

Max Discard (100-200) Default

Discard-Time sec Default

MAC Authentication Password Settings

Password Encrypt Default

MAC Authentication User Name MAC Format Settings

Case

Delimiter

Delimiter Number

MAC Authentication Port Settings

From Port To Port State

Port	State
Port1/0/1	Disabled
Port1/0/2	Disabled
Port1/0/3	Disabled
Port1/0/4	Disabled
Port1/0/5	Disabled
Port1/0/6	Disabled
Port1/0/7	Disabled
Port1/0/8	Disabled
Port1/0/9	Disabled

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。
Max Discard	MAC 認証に失敗して Discard 状態に登録されるクライアントの上限数を 100～200 の範囲で入力します。 デフォルト値を使用するには、 Default オプションを選択します。

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。

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。

9.10 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。

以下の項で説明するサブメニューに分かれています。

9.10.1 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。 <ul style="list-style-type: none"> • IPv4 : IPv4 アドレスを使用する場合に選択します。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> • 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 Enable の場合、認証前にアクセスした URL にジャンプします。 Disable 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。

9.10.2 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。

Port	State	TTL
interface port 1/0/1	Disabled	
interface port 1/0/2	Disabled	
interface port 1/0/3	Disabled	
interface port 1/0/4	Disabled	
interface port 1/0/5	Disabled	
interface port 1/0/6	Disabled	
interface port 1/0/7	Disabled	
interface port 1/0/8	Disabled	

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。

9.11 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。

以下の項で説明するサブメニューに分かれています。

9.11.1 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、認証属性によって動的に割り当てられた 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。

削除するには、**Delete** ボタンをクリックします。

9.11.2 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 Session 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。

9.12 Trusted Host

Trusted Host 画面では、アプリケーション（Telnet、SSH、Ping、および Web（HTTP））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。

The screenshot shows the 'Trusted Host' configuration page. At the top, there is a title bar 'Trusted Host'. Below it, the 'Trusted Host' section contains an 'ACL Name' input field with a '32 chars' limit and a 'Type' dropdown menu set to 'Telnet'. An 'Apply' button is on the right. A red note states: 'Note: The first character of ACL name must be a letter.' Below this is a table with 'Total Entries: 1'. The table has three columns: 'Type', 'ACL Name', and an action column. The first row shows 'Telnet' in the 'Type' column, 'ACL' in the 'ACL Name' column, and a 'Delete' button in the action column.

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 / Web ）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。

9.13 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。

Port	Forwarding Domain
Port1/0/10	Port1/0/11

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	受信ポートの範囲選択します。
From Forward Port / To Forward Port	転送ポートの範囲選択します。

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。

9.14 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值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值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

Storm Control Polling Settings

Polling Interval (5-600) sec Shutdown Retries (0-360) times Infinite

Storm Control Port Settings

From Port To Port Type Action Level Type PPS Rise (0,2-2147483647) pps PPS Low (0-2147483647) pps

Total Entries: 156

Port	Storm	Action	Threshold	Current	State
Port1/0/1	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
Port1/0/2	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
Port1/0/3	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive
Port1/0/4	Broadcast	Drop	-	-	Inactive
	Multicast		-	-	Inactive
	Unicast		-	-	Inactive

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 で設定できるフィールドについて、以下で説明します。

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	<p>ストームコントロールのタイプ (Broadcast / Multicast / Unicast) を選択します。</p> <p>アクションが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。</p>
Action	<p>実行するアクションを以下のいずれかから選択します。</p> <ul style="list-style-type: none"> • 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	<p>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。</p>
PPS Rise	<p>Level Type が PPS の場合に表示されます。</p> <p>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。0~2147483647 の範囲で入力します。</p>
PPS Low	<p>Level Type が PPS の場合に表示されます。</p> <p>ストームコントロールの下限値を pps で指定します。0~2147483647 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。</p>

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。

Storm Control Port Settings

From Port: Port1/0/1 | To Port: Port1/0/1 | Type: Broadcast | Action: Drop | Level Type: Kbps | KBPS Rise (2-2147483647): [] Kbps | KBPS Low (2-2147483647): [] Kbps | Apply

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 として **Level** オプションを選択した場合、**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。

9.15 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。以下の項で説明するサブメニューに分かれています。

9.15.1 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。

9.15.2 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。 <ul style="list-style-type: none"> • 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。

9.15.3 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。

SSH Server Connection				
SSH Table				
Total Entries: 0				
SID	Version	Cipher	User ID	Client IP Address

9.15.4 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。

SSH User Settings				
SSH User Settings				
User Name	32 chars	Authentication Method	Password	
Key File	779 chars	Host Name	255 chars	
<input checked="" type="radio"/> IPv4 Address		<input type="radio"/> IPv6 Address	2013::1	Apply
Total Entries: 1				
User Name	Authentication Method	Key File	Host Name	Host IP
15	Password			
1/1 < < 1 > > Go				

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	認証方式を以下のいずれかから選択します。 <ul style="list-style-type: none">• 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。<ul style="list-style-type: none">○ 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。<ul style="list-style-type: none">○ 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。

9.16 SSL

SSL サブメニューでは、SSL 機能に関する設定を行います。
以下の項で説明するサブメニューに分かれています。

9.16.1 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

SSL Global Settings

SSL Status Enabled Disabled Apply

Erase SSL-files Erase

Import File

Certificate Private Key

File Select Choose File No file chosen (The file name range is 1-32 chars.)

Destination File Name Apply

Note: You can access the File System page to manage these imported files.

Generate CSR And RSA Key

Country Name (2 letter code)

State or Province Name (full name)

Locality Name (eg, city)

Organization Name (eg, company)

Organizational Unit Name (eg, section)

Common Name (YOUR domain name)

Email Address

Key Length (512-2048) Apply

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、 Choose File 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。

9.16.2 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。

SSL Information
SSL Https-certificate Certificate Information: Certificate Version :3 Serial Number :80:2D:5E:A8:BD:8D:53:C3 Issuer Name :C=JP, ST=Tokyo, L=Chiyoda-ku, O=Example Domain., OU=Example Group., CN=Apresia/emailAddress=example@example.com Subject Name :C=JP, ST=Tokyo, L=Chiyoda-ku, O=Example Domain., OU=Example Group., CN=Apresia/emailAddress=example@example.com Not Before :Feb 16 06:54:58 2017 GMT Not After :Feb 11 06:54:58 2037 GMT Public Key Alg:rsaEncryption Signed Using :sha256WithRSAEncryption RSA Key Size :2048 bits
SSL Https-private-key Private key is embedded in firmware.
SSL CSR ERROR: No valid certificate request.

10 DDM

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。

DDM Voltage Threshold					
DDM Voltage Threshold					
Port	Current	High Alarm (V)	High Warning (V)	Low Warning (V)	Low Alarm (V)
Port1/0/51	3.274	3.700	3.600	3.000	2.900

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

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。

DDM Bias Current Threshold					
DDM Bias Current Threshold					
Port	Current	High Alarm (mA)	High Warning (mA)	Low Warning (mA)	Low Alarm (mA)
Port1/0/51	7.895	11.800	10.800	5.000	4.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

10.3 DDM TX Power Threshold

DDM TX Power Threshold 画面は、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。

DDM TX Power Threshold										
Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
Port1/0/51	0.574	-2.411	0.832	-0.800	0.661	-1.800	0.316	-5.000	0.251	-6.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

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。

DDM RX Power Threshold										
DDM RX Power Threshold										
Port	Current		High Alarm		High Warning		Low Warning		Low Alarm	
	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
Port1/0/51	0.228	-6.416	1.000	0.000	0.794	-1.000	0.016	-18.013	0.010	-20.000

Note: ++ : high alarm, + : high warning, - : low warning, -- : low alarm
A: The threshold is administratively configured.

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。

DDM Status						
DDM Status						
Total Entries: 1						
Port	Voltage (V)	Bias Current (mA)	TX Power		RX Power	
			mW	dBm	mW	dBm
Port1/0/51	3.274	7.894	0.572	-2.430	0.228	-6.418

Note: ++: high alarm, +: high warning, -: low warning, --: low alarm

11 Monitoring

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。

Port	TX (packets/sec)	RX (packets/sec)	TX (bits/sec)	RX (bits/sec)	Utilization
Port1/0/1	0	0	0	0	0
Port1/0/2	0	0	0	0	0
Port1/0/3	0	0	0	0	0
Port1/0/4	0	0	0	0	0
Port1/0/5	0	0	0	0	0
Port1/0/6	0	0	0	0	0
Port1/0/7	0	0	0	0	0
Port1/0/8	0	0	0	0	0
Port1/0/9	0	0	0	0	0
Port1/0/10	0	0	0	0	0

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。以下の項で説明するサブメニューに分かれています。

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。

Port	RX				TX				Show Detail
	Rate		Total		Rate		Total		
	bytes/sec	packets/sec	bytes	packets	bytes/sec	packets/sec	bytes	packets	
Port1/0/1	0	0	547881	3712	0	0	1091982	1518	Show Detail
Port1/0/2	0	0	0	0	0	0	0	0	Show Detail
Port1/0/3	0	0	0	0	0	0	0	0	Show Detail
Port1/0/4	0	0	0	0	0	0	0	0	Show Detail
Port1/0/5	0	0	0	0	0	0	0	0	Show Detail
Port1/0/6	0	0	0	0	0	0	0	0	Show Detail
Port1/0/7	0	0	0	0	0	0	0	0	Show Detail
Port1/0/8	0	0	0	0	0	0	0	0	Show Detail
Port1/0/9	0	0	0	0	0	0	0	0	Show Detail
Port1/0/10	0	0	0	0	0	0	0	0	Show Detail

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。

すべてのポートから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。

Port1/0/1	
RX rate	0 bytes/sec
TX rate	0 bytes/sec
RX bytes	547881
TX bytes	1091982
RX rate	0 packets/sec
TX rate	0 packets/sec
RX packets	3712
TX packets	1518
RX multicast	1006

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。

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	
Port1/0/1	547881	2687	1006	19	1091982	1518	0	0	Show Errors
Port1/0/2	0	0	0	0	0	0	0	0	Show Errors
Port1/0/3	0	0	0	0	0	0	0	0	Show Errors
Port1/0/4	0	0	0	0	0	0	0	0	Show Errors
Port1/0/5	0	0	0	0	0	0	0	0	Show Errors
Port1/0/6	0	0	0	0	0	0	0	0	Show Errors
Port1/0/7	0	0	0	0	0	0	0	0	Show Errors
Port1/0/8	0	0	0	0	0	0	0	0	Show Errors
Port1/0/9	0	0	0	0	0	0	0	0	Show Errors

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。

指定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、次のウィンドウが表示されます。

Port1/0/1 Counters Errors	
Align-Err	0
Fcs-Err	0
Rcv-Err	0
Undersize	0
Xmit-Err	0
OutDiscard	0
Single-Col	0
Multi-Col	0
Late-Col	0

前の画面に戻るには、**Back** ボタンをクリックします。

一覧に表示された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、カウンター情報を表示するために使用されます。

本画面を表示するには、**Monitoring > Statistics > Counters** をクリックします。

Port	linkChange	
Port1/0/1	4	Show Detail
Port1/0/2	0	Show Detail
Port1/0/3	0	Show Detail
Port1/0/4	0	Show Detail
Port1/0/5	0	Show Detail
Port1/0/6	0	Show Detail
Port1/0/7	0	Show Detail
Port1/0/8	0	Show Detail
Port1/0/9	0	Show Detail

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 packets 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 packets 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 packets 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 packets 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。

packets 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。



Port1/0/1 Counters	
rxHCTotalPkts	3712
txHCTotalPkts	1518
rxHCUnicastPkts	2687
txHCUnicastPkts	1518
rxHCMulticastPkts	1006
txHCMulticastPkts	0
rxHCBroadcastPkts	19
txHCBroadcastPkts	0
rxHCOctets	547881
txHCOctets	1091982
rxHCPlsOctets	2628

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

Mirror Settings

Session Number: 1

Destination: Port

Port: Port1/0/1

Source: Port

From Port: Port1/0/1

To Port: Port1/0/1

Frame Type: Both

CPU RX

Add Delete

Mirror Session Table

All Session: 1 Find

Session Number	Session Type	Show Detail
1	Local Session	Show Detail

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。 <ul style="list-style-type: none"> ● 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。 <ul style="list-style-type: none"> ● Port : 送信元ポートを設定する場合に選択します。 <ul style="list-style-type: none"> ○ From Port / To Port : 送信元ポートの範囲を選択します。 ○ 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。 <ul style="list-style-type: none"> ➢ 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。 ○ 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。 <ul style="list-style-type: none"> ○ 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 で設定できるフィールドについて、以下で説明します。

パラメーター	説明
Mirror Session Type	<p>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。</p> <ul style="list-style-type: none"> • 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、次の画面が表示されます。



The screenshot shows a window titled "Mirror Session Detail" with a table of configuration parameters. A "Back" button is visible in the bottom right corner.

Mirror Session Detail	
Session Number	1
Session Type	Local Session
Both Port	Port1/0/13
RX Port	
TX Port	
CPU RX	
Flow Based Source	
Destination Port	Port1/0/9

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。

Device Environment		
Detail Temperature Status		
Unit	Status	Current Temperature
1	Normal	27C
Detail Fan Status		
Items	Status	
Right Fan 1	(OK)	
Right Fan 2	(OK)	
Health Status		
Unit	Status	Failure Code
1	Normal	0x00000
Switch Power Consumption		
Unit	Value(W)	
1	25	

12 Green

12.1 EEE

EEE 画面では、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。

From Port	To Port	State	Apply
Port1/0/1	Port1/0/1	Disabled	Apply
Port	State		
Port1/0/1	Disabled		
Port1/0/2	Disabled		
Port1/0/3	Disabled		
Port1/0/4	Disabled		
Port1/0/5	Disabled		
Port1/0/6	Disabled		
Port1/0/7	Disabled		
Port1/0/8	Disabled		
Port1/0/9	Disabled		
Port1/0/10	Disabled		

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

13.1 Alarm Settings

Alarm Settings 画面では、ブザーおよび警告 LED のアラームの設定を行います。

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。
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。 <ul style="list-style-type: none"> • 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。
-----------------	--

設定を適用するには、**Apply** ボタンをクリックします。

Warning-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、または 1～60 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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と、ブザーの鳴動のオンとオフを切り替えます。

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。 Apply ボタンをクリックすると、警告 LED のオンとオフが切り替わります。

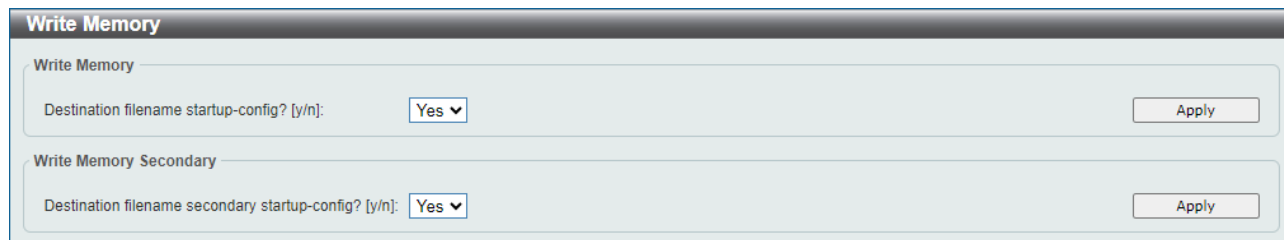
14 Save

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** ボタンをクリックすると、設定保存に関するサブメニューが出現します。

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。



The screenshot shows the 'Write Memory' configuration interface. It consists of two main sections, each with a title bar and a form area. The first section is titled 'Write Memory' and contains a label 'Destination filename startup-config? [y/n]:' followed by a dropdown menu currently set to 'Yes' and an 'Apply' button. The second section is titled 'Write Memory Secondary' and contains a similar label 'Destination filename secondary startup-config? [y/n]:' with a dropdown menu set to 'Yes' and an 'Apply' button.

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

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 **Tool** ボタンをクリックすると、ファイルのアップロード/ダウンロードに関するサブメニューが出現します。

15.1 Firmware Upgrade & Backup

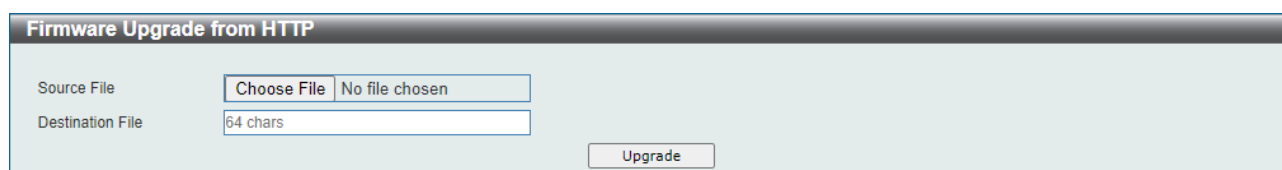
Firmware Upgrade & Backup サブメニューからは、イメージファイルのアップロードとダウンロードを実行します。

以下の項で説明するサブメニューに分かれています。

15.1.1 Firmware Upgrade from HTTP

Firmware Upgrade from HTTP 画面では、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。



The screenshot shows a web interface titled "Firmware Upgrade from HTTP". It contains two input fields: "Source File" with a "Choose File" button and "No file chosen" text, and "Destination File" with "64 chars" text. An "Upgrade" button is located at the bottom right.

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	ソースファームウェアファイルの選択後、このフィールドにファイル名とパスが表示されます。テキストボックス内をダブルクリックするか、ボタンをクリックしてローカル PC にあるファームウェアファイルの場所に移動します。
Destination File	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。

The screenshot shows the 'Firmware Upgrade from TFTP' interface. It features a header bar with the title. Below it, there are several input fields: 'TFTP Server IP' with a radio button for IPv4 (selected) and IPv6; 'Source File' with a '64 chars' label; and 'Destination File' with a '64 chars' label. An 'Upgrade' button is located at the bottom right.

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 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。
Destination File	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。

The screenshot shows the 'Firmware Upgrade from FTP' interface. It features a header bar with the title. Below it, there are several input fields: 'FTP Server IP' with a radio button for IPv4 (selected) and IPv6; 'TCP Port (1-65535)'; 'User Name' with a '32 chars' label; 'Password' with a '15 chars' label; 'Source File' with a '64 chars' label; and 'Destination File' with a '64 chars' label. An 'Upgrade' button is located at the bottom right.

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 File	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 File	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、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。

The screenshot shows the 'Firmware Backup to HTTP' interface. It features a 'Source File' input field with a '64 chars' character limit indicator. To the right of the input field is a 'Backup' button.

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	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。

The screenshot shows the 'Firmware Backup to TFTP' interface. It includes a 'TFTP Server IP' field with radio buttons for 'IPv4' (selected) and 'IPv6'. Below it are 'Source File' and 'Destination File' input fields, both with '64 chars' character limit indicators. A 'Backup' button is located at the bottom right.

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	ここで 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	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 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。

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 の範囲内で入力します。
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 File	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 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。

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 サブメニューからは、設定ファイルのバックアップ、リストアを実行できます。

以下の項で説明するサブメニューに分かれています。

15.2.1 Configuration Restore from HTTP

Configuration Restore from HTTP 画面では、ローカル PC 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 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	リストア元の構成ファイルの選択後、このフィールドにファイル名とパスが表示されます。テキストボックス内をダブルクリックするか、ボタンをクリックしてローカル PC にある設定ファイルの場所に移動します。
Destination File	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。 <ul style="list-style-type: none"> • 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 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。
Destination File	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。 <ul style="list-style-type: none"> • 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 File	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 File	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。 <ul style="list-style-type: none"> • 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、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 File	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。 <ul style="list-style-type: none"> • 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	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	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。 <ul style="list-style-type: none"> • 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 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。

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 File	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。 <ul style="list-style-type: none"> • 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 File	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

Tech-support サブメニューからは、技術サポート情報のバックアップを実行できます。以下の項で説明するサブメニューに分かれています。

15.3.1 Tech-support Store to SD Card Settings

Tech-support Store to SD Card Settings 画面では、装置本体前面にある BUZZER STOP ボタンの操作による、SD カードに技術サポート情報を書き込む機能を有効または無効にします。

本画面を表示するには、**Tools > Tech-support > Tech-support Store to SD Card Settings** 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。

15.3.2 Tech-support Backup to HTTP

Tech-support Backup to HTTP 画面では、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 > Tech-support Backup to HTTP** をクリックします。

技術サポート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。

15.3.3 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 > 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	ここで 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。

技術サポート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 サブメニューからは、システムログのバックアップを実行できます。以下の項で説明するサブメニューに分かれています。

15.4.1 Log Backup to HTTP

Log Backup to HTTP 画面では、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。 <ul style="list-style-type: none"> • System Log オプションを選択すると、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 File	TFTP サーバーでの保存ファイル名とパスを 64 文字で入力します。

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。 <ul style="list-style-type: none">• 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 サブメニューからは、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。

以下の項で説明するサブメニューに分かれています。

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。

The screenshot shows the 'Restore from TFTP' configuration window. It contains the following elements:

- TFTP Server IP:** A text input field followed by radio buttons for 'IPv4' (selected) and 'IPv6'.
- Prefix:** A text input field with a '12 chars' label.
- Source Path:** A text input field with a '64 chars' label.
- Option:** Two checkboxes labeled 'no-access-defender' and 'no-software'.
- Reboot:** A checkbox.
- Restore:** A button located at the bottom right of the form.

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	ここで 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	AccessDefender 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 接続用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	AccessDefender 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	AccessDefender 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。

The screenshot shows the 'Backup to TFTP' configuration interface. It includes the following elements:

- TFTP Server IP:** A text input field followed by radio buttons for 'IPv4' (selected) and 'IPv6'.
- Prefix:** A text input field with a '12 chars' label.
- Destination Path:** A text input field with a '64 chars' label.
- Option:** Two checkboxes labeled 'no-access-defender' and 'no-software'.
- Backup:** A button located at the bottom right of the form.

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 サーバー上の保存先ファイルパスをここに入力します。
no-access-defender	AccessDefender 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 接続のユーザー名を 32 文字以内で入力します。
Password	FTP 接続用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ここに入力します。
no-access-defender	AccessDefender 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 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。

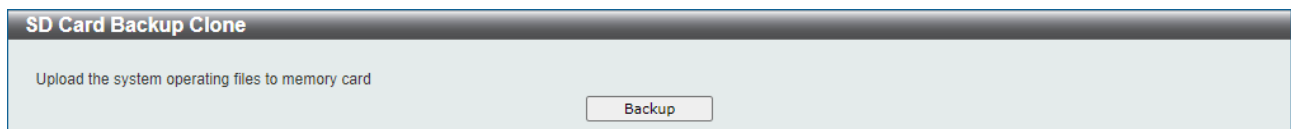
パラメーター	説明
Prefix	各ファイルに付加するプレフィックスを 12 文字以内で入力します。
Destination Path	SD カードの保存先ファイルパスを入力します。
no-access-defender	AccessDefender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。

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 サブメニューからは、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。

以下の項で説明するサブメニューに分かれています。

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 サブメニューからは、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。

以下の項で説明するサブメニューに分かれています。

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 サブメニューからは、CSR ファイルのバックアップを実行できます。以下の項で説明するサブメニューに分かれています。

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 サーバー上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。

The screenshot shows the 'Ping' tool interface with two sections: 'IPv4 Ping' and 'IPv6 Ping'. Each section has a 'Start' button at the bottom right.

IPv4 Ping settings:

- Target IPv4 Address: []
- Ping Times (1-255): [] Infinite
- Timeout (1-99): [1] sec
- Interval (1-3600): [1] sec
- Size (32-1500): [32] bytes
- Source IPv4 Address: []

IPv6 Ping settings:

- Target IPv6 Address: [2233::1]
- Ping Times (1-255): [] Infinite
- Timeout (1-99): [1] sec
- Interval (1-3600): [1] sec
- Size (32-1500): [100] bytes
- Source IPv6 Address: []

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 を選択します。
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。

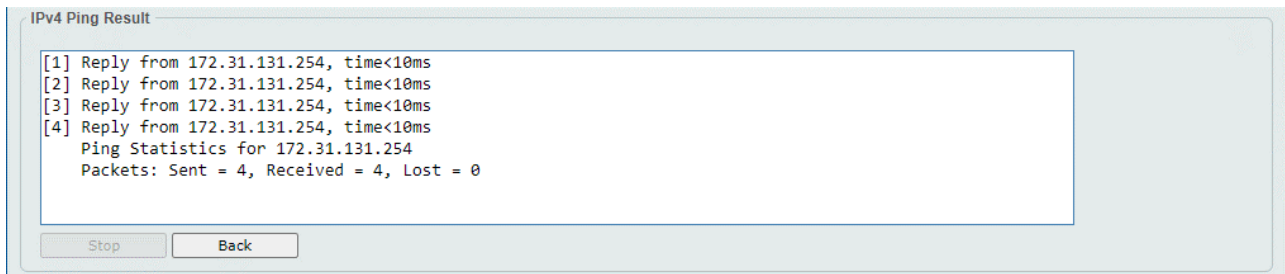
IPv6 Ping の各項目の説明を以下に示します。

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。

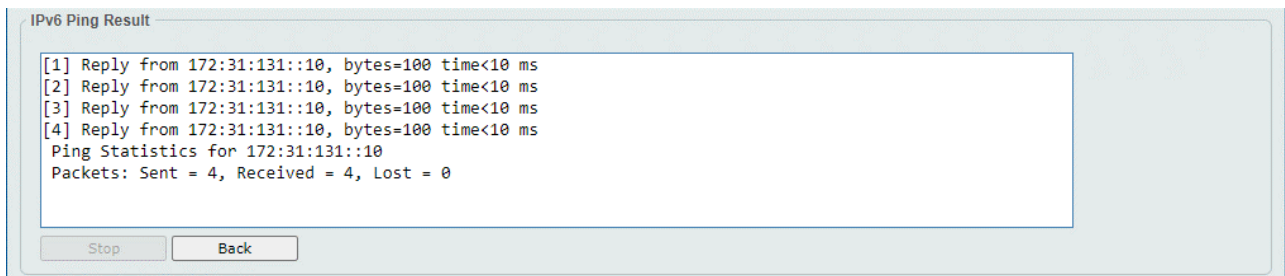


```

IPv4 Ping Result
[1] Reply from 172.31.131.254, time<10ms
[2] Reply from 172.31.131.254, time<10ms
[3] Reply from 172.31.131.254, time<10ms
[4] Reply from 172.31.131.254, time<10ms
Ping Statistics for 172.31.131.254
Packets: Sent = 4, Received = 4, Lost = 0
  
```

Stop Back

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。



```

IPv6 Ping Result
[1] Reply from 172:31:131::10, bytes=100 time<10 ms
[2] Reply from 172:31:131::10, bytes=100 time<10 ms
[3] Reply from 172:31:131::10, bytes=100 time<10 ms
[4] Reply from 172:31:131::10, bytes=100 time<10 ms
Ping Statistics for 172:31:131::10
Packets: Sent = 4, Received = 4, Lost = 0
  
```

Stop Back

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。

Trace Route

IPv4 Trace Route

IPv4 Address

Max TTL (1-255)

Port (1-65535)

Timeout (1-65535) sec

Probe Number (1-1000)

IPv6 Trace Route

IPv6 Address

Max TTL (1-255)

Port (1-65535)

Timeout (1-65535) sec

Probe Number (1-1000)

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。

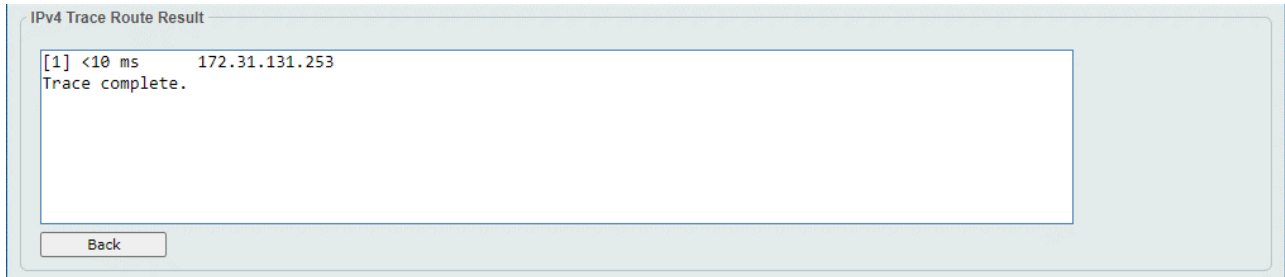
Traceroute を実行するには、**Start** ボタンをクリックします。

IPv6 Trace Route の各項目の説明を以下に示します。

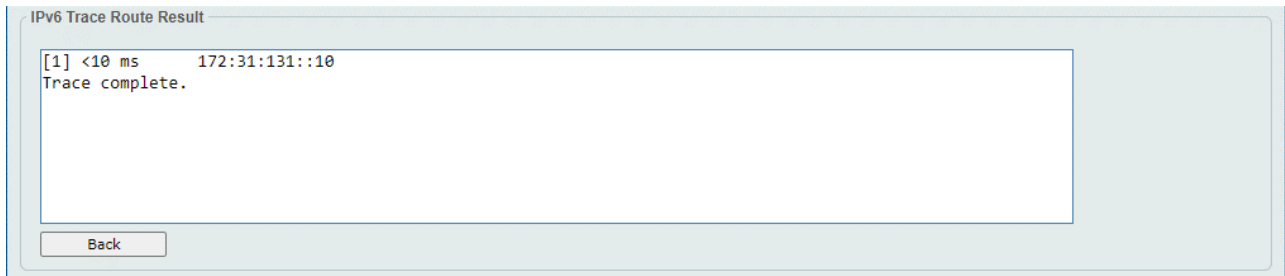
パラメーター	説明
IPv6 Address	宛先の IPv6 アドレスを入力します。
Max TTL	Traceroute の最大 TTL を 1～255 の範囲で入力します。
Port	Traceroute の TCP/UDP ポート番号を 1～65535 の範囲で入力します。
Timeout	Traceroute の各ホップのタイムアウトを 1～65535 (秒) の範囲で入力します。
Probe Times	Traceroute のプローブ回数を 1～1000 の範囲で入力します (デフォルト: 3)。

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。

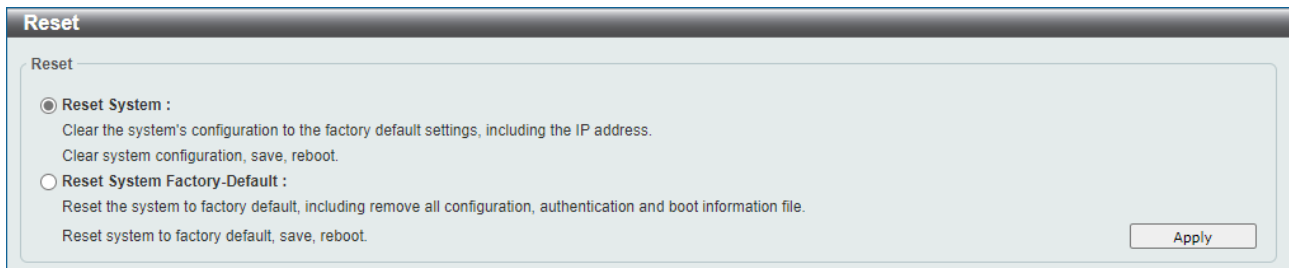


Trace Route を停止して、**Trace Route** 画面に戻るには、**Back** ボタンをクリックします。

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。



Reset

Reset

- Reset System :**
Clear the system's configuration to the factory default settings, including the IP address.
Clear system configuration, save, reboot.
- Reset System Factory-Default :**
Reset the system to factory default, including remove all configuration, authentication and boot information file.
Reset system to factory default, save, reboot.

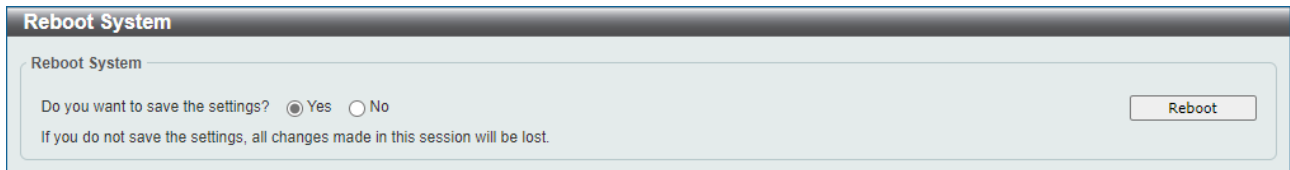
Apply

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。



The screenshot shows a dialog box titled "Reboot System". Inside the dialog, there is a question: "Do you want to save the settings?" with two radio buttons: "Yes" (selected) and "No". Below this, a warning message reads: "If you do not save the settings, all changes made in this session will be lost." A "Reboot" button is located in the bottom right corner of the dialog.

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。



The screenshot shows a progress bar within a "Reboot System" window. The text above the bar reads "Saving and rebooting system, please wait...". The progress bar is partially filled with blue, and the number "25%" is displayed next to it.

ApresiaLightGM300 シリーズ Ver.3.00 SW マニュアル

Copyright(c) 2025 APRESIA Systems, Ltd.

2025 年 2 月 初版

APRESIA Systems 株式会社

東京都中央区築地二丁目 3 番 4 号

メトロシティ築地新富町 8 階

<https://www.apresiasystems.co.jp/>