

TD61-7604B

ApresiaLightGM200シリーズ

<u>Ver. 2.00</u>

<u>ソフトウェアマニュアル</u>

APRESIA Systems 株式会社

利 正 ・ 仪 訂 米 歴 ネ	制	定	•	改	訂	来	歴	表
-----------------	---	---	---	---	---	---	---	---

容	年月日	No.
	2021年7月15日	-
載を追加	2022年3月16日	А
E意事項を追加		
	2022年6月24日	В
а		

	次
_	

制定・改訂来歴表	1
1 はじめに	5
1.1 本文中の表記について	6
1.2 初期 IP アドレスの設定	7
2 Web UI について	8
2.1 Web UI の接続方法	8
2.2 Web UI の画面説明	9
2.3 デバイス情報	10
2.4 メニューの内容	11
2.5 本書での説明の記載内容について	12
3 System	13
3.1 System Information Settings	13
3.2 Peripheral Settings	14
3.3 Port Configuration	15
3.4 Svstem Log	20
3.5 Time and SNTP	25
4 Management	
4.1 Command Logging	
4 2 User Accounts Settings	29
4.3 User Accounts Encryption	
4 4 Login Method	
4.5 SNMP	34
4.6 RMON	42
4.7 Telnet/Web	
4.8 Session Timeout	،ب ۸۵
4.0 CPU Protection	0 ب
4.9 010 Trotection	50
4.10 Zero Touch Provision	50
4.11 IF Source Internace	55
4.12 File System	
5 LZ Features	
	5/
5.2 VLAN	
5.3 VLAN TUNNET	
5.4 SIP	70
5.5 Loop Detection	76
5.6 Link Aggregation	/8
5.7 L2 Multicast Control	80
5.8 LLDP	95
6 L3 Features	107
6.1 ARP	107
6.2 IPv6 Neighbor	110
6.3 Interface	111

6.4 IPv4 Default Route	
6.5 IPv4 Route Table	
6.6 IPv6 Default Route	
6.7 IPv6 Route Table	
7 QoS	
7.1 Basic Settings	
7.2 Advanced Settings	
8 ACL	
8.1 ACL Configuration Wizard	
8.2 ACL Access List	
8.3 ACL Interface Access Group	
8.4 ACL VLAN Access Map	
8.5 ACL VLAN Filter	
9 Security	
9.1 Port Security	
9.2 802.1X	
9.3 AAA	
9.4 RADIUS	
9.5 TACACS	
9.6 DHCP Snooping	
9.7 MAC Authentication	
9.8 Web Authentication	
9.9 Network Access Authentication	
9.10 Trusted Host	
9.11 Traffic Segmentation Settings	
9.12 Storm Control	
9.13 SSH	
9.14 SSL	
10 DDM	
10.1 DDM Voltage Threshold	
10.2 DDM Bias Current Threshold	
10.3 DDM TX Power Threshold	
10.4 DDM RX Power Threshold	
10.5 DDM Status	
11 Monitoring	
11.1 Utilization	
11.2 Statistics	
11.3 Mirror Settings	
11.4 Device Environment	
12 Green	
12.1 EEE	
13 Alarm	236
13.1 Alarm Settings	
13.2 Alarm Debug	238
14 Save	
······································	

14.1 Write Memory	239
15 Tools	240
15.1 Firmware Upgrade & Backup	240
15.2 Configuration Restore & Backup	245
15.3 Tech-support Backup	250
15.4 Log Backup	251
15.5 Restore & Backup	253
15.6 AAA-local-db Download & Backup	258
15.7 SSL Files Download & Backup	260
15.8 CSR Files Backup	263
15.9 Ping	265
15.10 Trace Route	267
15.11 Reset	269
15.12 Reboot System	270

1 はじめに

本書の目的

本書は、Web ブラウザーを使用して ApresiaLightGM200 シリーズを設定、管理、および監視するユー ザーインターフェース(Web UI)について説明します。

それ以外の説明事項については、以下の各種ドキュメントをご参照ください。

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

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

製品名の表記について

本書では、ApresiaLightGM200シリーズ製品を「装置」「ブリッジ」または「スイッチ」と表記します。

使用条件と免責事項

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

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

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

商標登録

APRESIA は、APRESIA Systems株式会社の登録商標です。

AccessDefender は、APRESIA Systems 株式会社の登録商標です。

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

1.1 本文中の表記について

本文中の表記について、以下に示します。

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

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

1.2 初期 IP アドレスの設定

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

初期 IP アドレスの設定ルール

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



16 進数 10 進数変換

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 | 2.1 Web UI の接続方法

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 50以降
- Google Chrome 50 以降
- Safari 5以降(AppleのmacOSのみ)

2.1 Web UI の接続方法

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

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

注意事項

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

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

Connect to 10.8	5.104.32		
	Labelious	GE	
User Name			
Password			
	Login	Reset	



Web UIの画面は、3つの領域に分かれています。

ΛΡRESΙ Λ	PWR LOOP SD FIT ZTP ON OF NUZER CONSOLE STOP RESET APRESKA 2 4 6	LiphrGM220G7-SS (GIGA LINK # ACT 1) 7 9 11 13 15 7 9 14 13 15 8 10 12 14 16	17 19 17 19 18 20	ACT	領域 2	Refresh Interval
Save - XTools -					🤶 Logged in	as: Administrator, <u>ശ</u> Logout
Fuzzy Search	Device Information		_			
- APLGM220GTSS	Device Information					
🖭 📁 System						
🗈 📁 Management	Device Type	APLGM220GTSS Gigabit Ether	net L2	MAC Address	FC-6D-D1-06-CE-7D	
E E L2 Features	System Name	Switch		IP Address	10.213.119.200	
E L3 Features	System Location			Mask	255.255.255.0	
🗈 📁 QoS	System Contact			Gateway	0.0.0	
III ACL	Boot PROM Version	Build 1.00.00		System Time	30/06/2021 11:34:29	
Security	Firmware Version	Build 2.00.00		Serial Number	306142200001	
	Hardware Version	A				
monitoring Green	1 Million all and					
Green	Utilization					
領域 1	DRAM: FLASH: NVRAM:	Total(KB) 524288 125937 0		領域 3 97745 0	Free(KB) 402968 28192 0	Refresh
		5 Second	1 Minute	5 Minute	Maximum	Clear History Minimum
	CPU Utilization(%):	9	8	7	84	6

Web UI 画面の各領域の説明を、以下に示します。

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

2.3 デバイス情報

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

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

Device Type	APLGM220GTSS Gigab	it Ethernet L2	MAC Address	FC-6D-D1-06-C	E-7D	
System Name	Switch		IP Address	10.213.119.200		
System Location			Mask	255.255.255.0		
System Contact			Gateway	0.0.0.0		
Boot PROM Version	Build 1.00.00		System Time	30/06/2021 11:3	34:29	
Firmware Version	Build 2.00.00		Serial Number	306142200001		
Hardware Version	А					
Utilization						
					Re	resh
	Total(KB)		Used(KB)	Free(KB)		
DRAM:	524288		121320	402968		
FLASH:	125937		97745	28192		
NVRAM:	0		0	0		
					Close	History
	5 Second	1 Minute	5 Minute	Maximum	Minimum	HISCOLY
			o minute	Maximum	TYTE TO THE T	

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

2.4 メニューの内容

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

サイドメニューの各メニューの概要を以下の表に示します。

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

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

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

2.5 本書での説明の記載内容について

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

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

Policy Map				
Create/Delete Policy Map				
Policy Map Name	32 chars			Apply
Traffic Policy				
Policy Map Name	32 chars	Class Map Name	32 chars	Apply
Total Entries: 2				
	Policy	Map Name		
	P	olicy		Delete
	Poli	cy_vlan		Delete
			1/1	< < 1 > > Go
Class Rules				
	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、それを超えたエントリーが存在する場合は複数の ページにまたがります。この場合、テーブル右下にあるページ番号ボタンをクリックするか、または テキストボックスにページ番号を入力して Go ボタンをクリックすると、指定したページに移動します。

3 System

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

System の下にあるサブメニューの一覧を以下の表に示します。

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

3.1 System Information Settings

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

System Information Settings					
System Information Settings					
System Name	Switch				
System Location	255 chars				
System Contact	255 chars	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
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。

3.2 Peripheral Settings

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

Peripher	Peripheral Settings					
Environme	ent Temperature Threshold Settings					
High Thre	shold (-50-85)	70 Default				
Low Thre	shold (-50-85)	0 Default	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
High Threshold	警告温度設定の上限しきい値を-50~85()の範囲で入力します。
	デフォルト値を使用するには、Defaultをチェックします。
Low Threshold	警告温度設定の下限しきい値を-50~85()の範囲で入力します。
	デフォルト値を使用するには、Defaultをチェックします。

3.3 Port Configuration

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

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

3.3.1 Port Settings

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

ort Settings	_	_	_	_	_	_	_	_	_
)efault port-shutdo	own Settings								
State									
Enabled 🗸									
									Apply
Port Settings									
From Port	To Port	State	MDIX		Auto Down	grade Flow Contr	ol		
Port1/0/1 🗸	Port1/0/1	 Enabled 	✓ Auto	~	Disabled	✓ Off	~		
Duplex	Speed	Capability	Advertised		Descriptior	1			
Auto 🗸	Auto	✓ 10M	100M 🗌 1000M		64 chars				Apply
	_			Flow	Control			Auto	
Port	Link Status	State	MDIX	Send	Receive	Duplex	Speed	Downgrade	Description
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	Up	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	
Port1/0/6 Port1/0/7	Down Down	Enabled Enabled	Auto-MDIX Auto-MDIX	Off Off	Off Off	Auto-duplex Auto-duplex	Auto-speed Auto-speed	Disabled Disabled	
Port1/0/6 Port1/0/7 Port1/0/8	Down Down Down	Enabled Enabled Enabled	Auto-MDIX Auto-MDIX Auto-MDIX	Off Off Off	Off Off Off	Auto-duplex Auto-duplex Auto-duplex	Auto-speed Auto-speed Auto-speed	Disabled Disabled Disabled	
Port1/0/6 Port1/0/7 Port1/0/8 Port1/0/9	Down Down Down Down	Enabled Enabled Enabled Enabled	Auto-MDIX Auto-MDIX Auto-MDIX Auto-MDIX	Off Off Off Off	Off Off Off Off	Auto-duplex Auto-duplex Auto-duplex Auto-duplex	Auto-speed Auto-speed Auto-speed Auto-speed	Disabled Disabled Disabled 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。各項目の説明を以下に示します。

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

設定を適用するには、Applyボタンをクリックします。

3.3.2 Port Status

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

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

3.3.3 Port GBIC

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

Port GBIC	A
Port GBIC	
Port1/0/1	
Port1/0/2	
Port1/0/4	
Port1/0/6	
Port1/0/8	
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。

rt Auto Nego ort Auto Nego lote: AN: Aut	egotiation tiation	25: Remote Signaling	: CS: Config Statu	s: CB: Canability B	its:CAB: Canbility	Advertised Bits:		
CRB: C	apbility Receive	ed Bits; RFA: Remote	Fault Advertised;	RFR: Remote Fau	It Received	Auvenised Dits,		
Port	AN	RS	CS	СВ	САВ	CRB	RFA	RFR
Port1/0/1	Enabled	Detected	Complete	10M_Half,	10M_Half,	10M_Half,	Disabled	NoError
Port1/0/2	Enabled	Not Detected	Configuring	10M_Half,	10M_Half,	-	Disabled	NoError
Port1/0/3	Enabled	Detected	Complete	10M_Half,	10M_Half,	10M_Half,	Disabled	NoError
Port1/0/4	Enabled	Not Detected	Configuring	10M_Half,	10M_Half,	-	Disabled	NoError
Port1/0/5	Enabled	Not Detected	Configuring	10M_Half,	10M_Half,	-	Disabled	NoError
Port1/0/6	Enabled	Not Detected	Configuring	10M_Half,	10M_Half,	-	Disabled	NoError
Port1/0/7	Enabled	Not Detected	Configuring	10M_Half,	10M_Half,	-	Disabled	NoError
Port1/0/8	Enabled	Not Detected	Configuring	10M_Half,	10M_Half,	-	Disabled	NoError
Port1/0/9	Enabled	Not Detected	Configuring	10M_Half,	10M_Half,	-	Disabled	NoError
Port1/0/10	Enabled	Not Detected	Configuring	10M_Half,	10M_Half,	-	Disabled	NoError

3.3.5 Error Disable Settings

Error Disable Settings 画面では、装置の機能によりポートが閉塞された場合(Error Disabled 状態)の、自動復旧機能の有効/無効、およびポートが復旧するまでの時間を設定します。

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

State Disabled	Interval (5-86400)	sec Apply	
State Disabled	Interval (5-86400)	sec Apply	
	State	Interval (sec)	
	Disabled	300	
	Disabled	300	
	Disabled	300	
Interface VLAN		Time Left (sec)	
		ErrDisable Cause	

本画面の各項目の説明を以下に示します。

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

設定を適用するには、Applyボタンをクリックします。

3.3.6 Jumbo Frame

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

Jumbo Frame	
Jumbo Frame	
From Port To Port	Maximum Receive Frame Size (64-9216)
Port1/0/1 V Port1/0/1 V	1536 bytes Apply
Port	Maximum Receive Frame Size (bytes)
Port1/0/1	1536
Port1/0/2	1536
Port1/0/3	1536
Port1/0/4	1536
Port1/0/5	1536
Port1/0/6	1536
Port1/0/7	1536
Port1/0/8	1536
Port1/0/9	1536
Port1/0/10	1536

3 System | 3.3 Port Configuration

本画面の各項目の説明を以下に示します。

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

3.4 System Log

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

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

3.4.1 System Log Settings

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

System Log Settings		
Log State		
Log State	Enabled	Apply
Source Interface Settings		
Source Interface State	Disabled	
Туре	VLAN VID (1-4094)	Apply
Buffer Log Settings		
Buffer Log State	Enabled	
Severity	6(Informational)	
Discriminator Name	15 chars	
Write Delay (0-65535)	300 sec Infinite	Apply
Console Log Settings		
Console Log State	Disabled	
Severity	4(Warnings)	
Discriminator Name	15 chars	Apply

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。

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。
Туре	インターフェースのタイプを選択します。VLAN のみ使用可能です。
VID	VLAN ID を 1 ~ 4094 の範囲で入力します。

設定を適用するには、Applyボタンをクリックします。

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

設定を適用するには、Applyボタンをクリックします。

3.4.2 System Log Discriminator Settings

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

	oottingo						
Discriminator Log Settings							
Discriminator Name	15 chars						
Action	Drops 🗸						
[SYS	PORT	STP		LAC		
	FDB		ACL		QOS		
	PORTSEC	DHCP	DHCPV6	3	STORM	/_CT	
	SSH	CLI	SNMP		ALARN	1	
	AAA	DEVICE	RADIUS		DOT1X		
[MAC	CFG	FIRMWA	RE			
Severity	Drops 🗸						
Γ	0(Emergencies)	1(Alerts)	2(Critica	I)	3(Error	s)	
	4(Warnings)	5(Notifications)	6(Inform	ational)	7(Debu	gging)	Apply
Name	Action	Facility List	t	Sever	ity	Severity List	
Name	Drops	CFG		Drop	S	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 Sevirity を選択し、指定した Sevirity に対 する動作オプション (Drops / Includes) を選択します。

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

3.4.3 System Log Server Settings

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

System Log Server Sett	tings	_			_	_
Log Server						
 Host IPv4 Address 		·	O Host IPv6 Address	2013::1		
UDP Port (514,1024-65535)	514		Severity	4(Warnings)		
Facility	23	\checkmark	Discriminator Name	15 chars		
						Apply
Total Entries: 1						
Server IP	Severity	Facility	Discriminat	or Name	UDP Port	
172.31.131.1	Warnings	23	Nam	e	514	Delete

十三三のタゼロのジョン	
本画面の各国日の説明を以	
午回回の日頃日の肌的とい	

ハラメーター	説明								
Host IPv4 Address	Syslog t	ナーバーの IPv	4アド	レスで	を入力します	•			
Host IPv6 Address	Syslog t	ナーバーの IPv	6アド	レスで	を入力します	•			
UDP Port	Syslog t 入力しま	ナーバーの UDF す。	[,] ポート	-番号	を、514 ま;	たは	1024 ~ 6	65535 の範囲で	C
Severity	Syslog t 指定した	ナーバーに出た レベル以上の	力する Sever	ログ(ityに	のレベル(S ニ該当するロ	evir グが	ity)を 出力さ	指定します。 れます。	
Facility	Syslog 1 す。 各ファシ ます。以	ナーバーに出た リティーの番 下の表を参照	りする: 号は、 してく	ファシ 特定 ださ	ィリティーの のファシリ・ い。)番号 ティ・	+ (0~2 - に関連	3)を選択しま 値付けられてい	ŧ
	番号	Name		盱号	Name		番号	Name	
	1	user	9		clock1		17	local1	
	2	mail	1(0	auth2		18	local2	
	3	daemon	1'	1	ftp		19	local3	
	4	auth1	12	2	ntp		20	local4	
	5	Syslog	13	3	logaudit		21	local5	
	6	lpr	14	4	logalert		22	local6	
	7	news	15	5	clock2		23	local7	
	8	uucp	16	6	local0				
						-			
Discriminator Name	Syslog t 字以内で System L ファイル	ナーバーへの出 で入力します .og Discrimin ·です。	出力の挑 ⁻ 。 Dic mator S	辰り分 csrim Setti	けで使用す inator は、 ngs で登録	る Di Sys され7	iscrimi s tem > たフィリ	nator を 15 \$ System Log レタリングプロ	と と コ

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

3.4.4 System Log

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

stem Log			
tal Entrice: 44			Clear Log
Index	Time	Level	Log Description
44	2021-01-26 14:41:28	INFO(6)	Unit 1 Port 20 H-SR
43	2021-01-26 14:40:40	INFO(6)	Successful login thr
42	2021-01-26 14:40:34	WARN(4)	Login failed through
41	2021-01-26 14:40:17	INFO(6)	Unit 1 Port 18 1000B
40	2021-01-26 14:40:16	WARN(4)	Port1/0/1 link up, 1
39	2021-01-26 14:40:16	CRIT(2)	System started up
38	2021-01-26 14:40:16	CRIT(2)	System re-start reas
37	2021-01-26 14:40:16	INFO(6)	Unit 1 Port 17 1000B
36	2021-01-26 14:40:13	INFO(6)	dhcpsnooping : Mode
	2021 01 26 14:40:12	INFO(6)	SSH server is enable

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

3.4.5 System Attack Log

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

System Attack Log				
System Attack Log				
			Clear Attack	_og
Total Entries: 0				
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。

3.5 Time and SNTP

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

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

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

3.5.1 Clock Settings

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

Clock Settings		
Clock Settings		
	44-54-40	
Date (DD / MM / YYYY)	26/1/2021	
		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	現在の年月日を日(DD)、月(MM)、年(YYYY)で入力します。 例:31/12/2021

設定を適用するには、Applyボタンをクリックします。

3.5.2 Time Zone Settings

Time Zone Settings 画面ではタイムゾーンとサマータイムを設定します。

タイムゾーンは、デフォルトで+9:00(日本標準時)が指定されています。

サマータイムの指定は、特定月の指定週の曜日で指定する Recurring モードと、特定月の指定の日付 で指定する Date モードの2種類から選択できます。

通常、日本国内で使用する場合は、タイムゾーンとサマータイムの設定を変更する必要はありません。

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

Time Zone Settings	
V V	
Summer Time State	
Time Zone	
Recurring Setting	
From: Week of the Month	Last
From: Day of the Week	Sun 🗸
From: Month	Jan 🗸
From: Time (HH:MM)	
To: Week of the Month	Last
To: Day of the Week	Sun
To: Month	Jan 🗸
To: Time (HH:MM)	
Offset	60
Date Setting	
From: Date of the Month	01
From: Month	Jan 🗸
From: Year	
From: Time (HH:MM)	
To: Date of the Month	01
To: Month	Jan
To: Year	
To: Time (HH:MM)	
Offset	60
	Apply

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

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

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

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

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

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

設定を適用するには、Applyボタンをクリックします。

3.5.3 SNTP Settings

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

SNTP Settings				
SNTP Global Settings				
Current Time Source	System Clock			
Poll Interval (30-99999)	720	sec		Apply
SNTP Server Setting				
IPv4 Address	• • •) IPv6 Address	2013::1
Total Entries: 1				
SNTP server	Stratum	Version	Last Receive	
172.31.131.1	-	-	-	Delete

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

SNTP サーバーを追加するには、Add ボタンをクリックします。

SNTP サーバーを削除するには、Delete ボタンをクリックします。

4 Management

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

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

4.1 Command Logging

Command Logging 画面では、コマンドロギング機能を設定します。

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

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

Command Logging			
Command Logging Settings			
	0.5-11-1		· · · · · · · · · · · · · · · · · · ·
Command Logging State	 Enabled 	 Disabled 	Арріу

本画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。

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。

User Accounts Settings				
User Management Settings	Session Table			
User Name 32 chars	Privilege (1-15)			
Password Type None 🗸	Password			Apply
Total Entries: 1				
User Name	P	rivilege	Password	
adpro		15	******	Delete
			1/1 < < 1	> > Go

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。

注意事項

デフォルトで登録されているユーザーアカウント「adpro」は、初期アクセス用として特権レベル 15 で予約された特別なアカウントです。セキュリティーの観点から、実際の運用では別のユーザーアカウントを作成し、デフォルトユーザーアカウントを削除することを推奨します。また、このデフォルトユーザーアカウントを使用する場合は、特権レベル 15 のままにしてください。



ユーザー名「ap_recovery」というユーザーアカウントを作成することは可能です が、コンソールポートでの CLI 接続ではログインプロンプトで「ap_recovery」と 入力すると初期化処理が行われるため、ログインアカウントとしては使用できま せん。当該ユーザー名のユーザーアカウントを設定しないでください。 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。

er Accounts S	ettings				
User Management	Settings Set	ession Table			
al Entries: 2					
Туре	User Name	Privilege	Login Time	IP Address	
			10110.00		
console	Anonymous	1	12M26S		

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	
User Privilege	
Action	Enabled Disabled
Privilege	15 💌
Password	35 chars Apply Back

User Privilegeの各項目の説明を以下に示します。

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

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

4.3 User Accounts Encryption

User Accounts Encryption 画面では、ユーザーアカウントの暗号化を設定します。設定情報でユー ザーアカウントのパスワードを暗号化するかどうかを決定します。

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

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

Login Method		
Enable Password		
Level 15 Password T	pe Plain Text Password 32 chars	Apply
Login Method		
Application	Login Method	
Console	No Login	Edit
Telnet	Login	Edit
SSH	Login	Edit
Login Password	ne Diain Taut V Password 23 chara	
Application Console Password 1	Plain Text V Password 32 chars	Арріу
Application	Password	
Telnet	*****	Delete

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

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

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

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

パラメーター	説明
Login Method	指定したライン種別でのログイン方法を、以下のいずれかから選択しま
	 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 カさせる場合に選択します。

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

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

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

設定を適用するには、Applyボタンをクリックします。

登録したパスワードを削除するには、Delete ボタンをクリックします。

4.5 SNMP

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

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

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

SNMPの下にあるサブメニューの一覧を以下の表に示します。

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

4.5.1 SNMP Global Settings

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

SNMP Global Settings	
SNMP Global Settings	
SNMP Global State	
SNMP Response Broadcast Request	
ONING LIDD Dart (4 65525)	
SNMP ODP POIL (1-05535)	161
Trap Source Interface	
Trap Settings	
Trap Global State	 Enabled Disabled
SNMP Authentication Trap	
Port Link Up	
Port Link Down	
Coldstart	
Warmstart	Apply

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	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
Request	(Enabled / Disabled)を選択します。
SNMP UDP Port	SNMP の UDP ポート番号を 1~65535 の範囲で入力します。
Trap Source Interface	SNMP トラップパケットを送信するための送信元アドレスとして、IP ア ドレスが使用されるインターフェースを入力します。

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

パラメーター	説明		
Trap Global State	トラップ通知のグローバル設定(Enabled / Disabled)を選択します。		
SNMP Authentication	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		
Тгар	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。

SNMP Linkchange Trap Settings						
SNMP Linkchange Trap Settings						
From Port	To Port	Trap Sending	Trap State			
Port1/0/1	Port1/0/1	Disabled 🗸	Disabled 🗸	Apply		
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		
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。					

本画面の各項目の説明を以下に示します。

設定を適用するには、Applyボタンをクリックします。

4.5.3 SNMP View Table Settings

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

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

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

NMP View Table	Settings			
SNMP View Settings				
View Name *	32 chars			
Subtree OID *	N.N.NN			
View Type	Included	•		
* Mandatory Field				Add
Total Entrice: 9				
View	Name	Subtree OID	View Type	
rest	ricted	1.3.6.1.2.1.1	Included	Delete
rest	ricted	1.3.6.1.2.1.11	Included	Delete
rest	ricted	1.3.6.1.6.3.10.2.1	Included	Delete
rest	ricted	1.3.6.1.6.3.11.2.1	Included	Delete
rest	ricted	1.3.6.1.6.3.15.1.1	Included	Delete
Commu	inityView	1	Included	Delete
Commu	inityView	1.3.6.1.6.3	Excluded	Delete
Commi	inityView	1361631	Included	Delete

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

本画面の各項目の説明を以下に示します。

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

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

4.5.4 SNMP Community Table Settings

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

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

注意事項

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

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

SNMP Community	Table Setting	js			
SNMP Community Settin	igs				
Кеу Туре	Plain Text	\checkmark			
Community Name	32 chars				
View Name	32 chars				
Access Right	Read Only	\checkmark			
IP Access-List Name	32 chars				
					Add
Total Entries: 2					
Community N	ame	View Name	Access Right	IP Access-List Name	
public		CommunityView	ro		Delete
private		CommunityView	TW		Delete

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

本画面の各項目の説明を以下に示します。

SNMP コミュニティーを追加するには、Add ボタンをクリックします。

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

4.5.5 SNMP Group Table Settings

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

MIB オブジェクトのアクセス範囲を示す SNMP ビューは、SNMP グループに対して操作種別(読み込み、 書き込み、通知)ごとに適用します。SNMP ユーザーはいずれかの SNMP グループに分類され、SNMP グ ループに割り当てた SNMP ビューに応じたアクセス権限を持ちます。

SNMP コミュニティーを登録した場合、対応する SNMP グループが自動的に作成されます。

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

NMP Group	Table Settings						
NMP Group Sett	ings						
Group Name *	32 char	'S	Read V	iew Name 3	2 chars		
User-based Security Model SNMPv1 Vite View Name 32 chars							
Security Level	NoAut	thNoPriv 🔽	Notify V	/iew Name 3	2 chars		
IP Address-List N	lame 32 char	rs					
* Mandatory Field	1						Add
Total Entries: 5							
Group Name	Read View Name	Write View Name	Notify View Name	Security Model	Security Level	IP Address-List Name	
public	CommunityV		CommunityV	v1			Delete
public	CommunityV		CommunityV	v2c			Delete
initial	restricted		restricted	v3	NoAuthNoPriv		Delete
private	CommunityV	CommunityV	CommunityV	v1			Delete
		Oit A/	0				

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	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
Model	る場合は SNMPv3 を指定します。
Write View Name	書き込み操作の SNMP ビュー名を 32 文字以内で入力します。
Security Level	以下のいずれかの SNMPv3 セキュリティーレベルを選択します。
	 NoAuthNoPriv:認証と暗号化を行いません。
	· AuthNoPriv:認証を行いますが、暗号化を行いません。
	· AuthPriv:認証と暗号化を行います。
Notify View Name	トラップ通知の SNMP ビュー名を 32 文字以内で入力します。
IP Access-List Name	ACL を使用して SNMP でアクセスできるユーザーを制限します。

本画面の各項目の説明を以下に示します。

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。

SNMP Engine ID Local Settings					
SNMP Engine ID Local Settings					
Engine ID 800001160300406655682000 Engine ID length is 24, the accepted character is from 0 to F.	Default 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
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。

SNMP User Table Setti	ngs					
SNMP User Settings						
User Name *	32 chars					
Group Name *	32 chars					
SNMP Version	v1	~				
SNMP V3 Encryption	None					
Auth-Protocol by Password	MD5	Password	1 (8-16 chars)			
Priv-Protocol by Password	None	Password	1 (8-16 chars)			
Auth-Protocol by Key	MD5	 Key (32 c) 	hars)			
Priv-Protocol by Key	None	 Key (32 c) 	hars)			
IP Address-List Name	32 chars					
* Mandatory Field						Add
Total Entries: 1						
User Name Group Nam	e Security Model	Authentication Protocol	Privacy Protocol	Engine ID	IP Address-List Name	
initial initial	V3	None	None	8000011603		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
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	SNMPv3 Encryption で Password を選択した場合に、以下のどちらかの
Password	認証プロトコルを選択し、テキストボックスにパスワードを指定しま
	す。
	MD5:HMAC-MD5-96 認証プロトコルを使用する場合に選択します。
	· SHA:HMAC-SHA 認証プロトコルを使用する場合に指定します。
Priv-Protocol by	SNMPv3 Encryption で Password を選択した場合に、暗号化について以
Password	下のどちらかを選択します。
	· None:暗号化を使用しません。
	 DES56: DES56 ビット暗号化を使用する場合に選択します。テキストボックスにパスワードを入力します。
Auth-Protocol by Key	SNMPv3 Encryption で Key を選択した場合に、以下のどちらかの認証プロトコルを選択し、テキストボックスにキーを指定します。
	· MD5:HMAC-MD5-96認証プロトコルを使用する場合に選択します。
	・ SHA:HMAC-SHA 認証プロトコルを使用する場合に選択します。
Priv-Protocol by Key	SNMPv3 Encryption で Key を選択した場合に、暗号化について以下のどちらかを選択します。
	· None:認証プロトコルを使用しない場合に選択します。
	 DES56: DES56 ビット暗号化を使用する場合に選択します。テキストボックスには、キーを入力します。
IP Access-List Name	ユーザーに関連付ける標準 IP ACL の名称を 32 文字以内で入力します。

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

SNMP ユーザーを削除するには、Delete ボタンをクリックします。

4.5.8 SNMP Host Table Settings

SNMP Host Table Settings 画面では、SNMP トラップの通知ホストを設定します。所定のイベントが発生すると、装置は登録したホスト宛に SNMP トラップを送信します。

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

SNMP Host Table Settings			
SNMP Host Settings			
 Host IPv4 Address 			
O 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		Add
Total Entries: 1			
Host IP Address SNMP	Version UDP Port	Community String / SNMPv3 User Name	
2020::127	V1 162	public	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	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	以下のいずれかのセキュリティーモデルを選択します。
Model	· SNMPv1:SNMPv1を使用します。
	・ SNMPv2c :SNMPv2cを使用します。
	 SNMPv3: SNMPv3を使用します。このセキュリティーモデルの場合、Security Level で SNMPv3 セキュリティーレベルを指定する必要があります。
Security Level	User-based Security Model で SNMPv3 を選択した場合、以下のいずれ かのセキュリティーレベルを選択します。
	 NoAuthNoPriv:認証と暗号化を行いません。
	· AuthNoPriv:認証を行いますが、暗号化を行いません。
	· AuthPriv:認証と暗号化を行います。
UDP Port	UDP ポート番号を 1~65535 の範囲で入力します。
Community String /	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 User Name	SNMPv3 ユーザー名を 32 文字以内で入力します。

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

4.6 RMON

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

RMON の下にあるサブメニューの一覧を以下の表に示します。

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

4.6.1 RMON Global Settings

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

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

RMON Global Settings			
RMON Global Settings			
RMON Rising Alarm Trap	 Enabled 	Disabled	
RMON Falling Alarm Trap	Enabled	 Disabled 	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
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。

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。

MON Statistics Setting	JS			
Port * Port1/0/1	Index (1-65535) *	Owner 127 chars	bbA
index	Port	Owner		
1	Port1/0/1	Owner		Delete Show Detail
				1/1 k < 1 > > G

本画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。

NON	Statistics	Table —																
	Data	Doc	Doc	Doradoaet	Multicast	Undoreizo	Quoreizo	27, 102 202 102 102 202 102 103		CPC		Drop	64	65 407	120 255	256 544	512-	1024
ndex	Data	Rec.	Rec.	BUIAUCASI	Mullicasi	Dirdersize	Oversize	Fragments	Jabbers		Collisions	Drop	04	03-12/	128-233	200-011	1023	1518
	Source	Octets	PKIS	PKIS	PKIS	PKIS	PKIS			Error		Event	Octets	Octets	Octets	Octets	Octets	Octet
1	Port1/0/1	2260813	17379	1301	6670	0	0	30	0	0	152	97	11194	2374	1715	1544	406	146

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。

ort *	Index (1-65535) *	Du				
'ort1/0/1		50	cket Number (1-65535)	Interval (1-36 1800	soo) sec	Owner 127 chars Add
Index Po	rt Bucke	ts Requested	Buckets Granted	Interval	Owner	
1 Port1	/0/1	50	50	1800	Owner	Delete 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
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。

RMON History Ta	able									
RMON History Table										
Index Sample Rec.	Octets Rec. PKTs	Boradcast PKTs	Multicast PKTs U	tilization L	Indersize PKTs	Oversize PKTs	Fragments J	abbers CRC	Error Collision	ns Drop Event
										Back

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。

RMON Alarm Settings				
RMON Alarm Settings				
Index (1-65535) *		Interval (1-21474	3647) *	sec
Variable *	N.N.NN	Туре	Absolute	
Rising Threshold (0-2147483647) *		Falling Threshold	(0-2147483647) *	
Rising Event Number (1-65535)		Falling Event Nun	ber (1-65535)	
Owner	1-127 chars			
				Add
Total Entries: 0				
Index Interval (sec) Variable T	ype Last Value Risi	ng Threshold Falling Threshold	Rising Event No. Falling E	vent No. Startup Alarm Owner

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。
Туре	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。

本画面の各項目の説明を以下に示します。

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。

RN	RMON Event Settings						
RN	NON Even	t Settings					
Ir	ndex (1-65	535) *					
D)escription		1-127 ch	ars			
T	уре		None	~			
С	Community 1-127 chars						
C	Owner		1-127 ch	ars			
							Add
T	otal Entrie	es: 1					
	Index	Description	Community	Event Trigger	Owner	Last Trigger Time	
	1	Event			Owner	0d:0h:0m:0s	Delete View Logs
							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
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。
Туре	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。
Commun i ty	Type で Trap または Log and Trap を選択した場合に、SNMP コミュニ ティーを 127 文字以内で入力します。
Owner	オーナー情報を 127 文字以内で入力します。

入力した情報でイベントエントリーを追加するには、Add ボタンをクリックします。

イベントエントリーを削除するには、Delete ボタンをクリックします。

イベントログを表示するには、View Logs ボタンをクリックします。

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

event Logs Table			
Event Logs Table			
Event Index: 1			
Total Entries: 0			
Log Index	Log Time	Log Description	
			Back

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/Web				
Telnet Settings				
Telnet State Port (1-65535)	Enabled Disabled 23			Apply
Source Interface				
Source Interface State Type	C Enabled O Disabled VLAN	VID (1-4094)		Apply
Web Settings				
Web State Port (1-65535)	Enabled Oisabled			Apply

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	TeInet 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。
Туре	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。

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。

Session Timeout		
Session Timeout		
Web Session Timeout (60-36000) Console Session Timeout (0-1439) Telnet Session Timeout (0-1439) SSH Session Timeout (0-1439)	180 sec Image: Default 3 min Default 3 min Image: Default 3 min Image: Default 3 min Image: Default	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
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。

4.9 CPU Protection

CPU Protection 画面では、CPU 保護機能を設定します。CPU 保護機能には、CPU 使用率チェック機能と、システムメモリー使用率チェック機能があります。

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

CPU Protection		
CPU Utilization Trace Trigger		
State	Disable	
Threshold (50-100)	percent	
Interval (10-180)	sec Default	Apply
System Memory Limit Check		
State	Disable	
Threshold (80-100)	percent Default	Apply
CPU Protection SNMP Trap		
State	Disable	Apply
State	Disable	Apply

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

4.10 Zero Touch Provision

Zero Touch Provision 画面では、Zero Touch Provisioning(以後、ZTP)を設定します。 ZTP は、装置の起動時にイメージファイル、設定ファイルを TFTP サーバーからダウンロードして適用 する機能です。ZTP 機能を使用するには、DHCP サーバーと TFTP サーバーを準備する必要があります。

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					
Zero Touch Provision Settings					
Zero Touch Provision State	 Enabled 	 Disabled 	O EnableForced		Apply
Zero Touch Provision Informatio	n				
ZTP Bootup State:	Enabled Force		Current Firmware:	/c:/V2.00.00b.0013.had	
ZTP Current State:	Disabled		Current Configure:	/c:/primary.cfg	
	Result of last time		Result of this	s 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。

ZTP 機能が動作するかどうかは、Zero Touch Provision State の設定と、装置本体の ZTP スイッチの ポジションの組みあわせによって決まります。

	設定:Disabled	設定:Enabled	設定:EnableForced
ZTP スイッチ ON	(動作しない)	動作する	動作する
ZTP スイッチ OFF	(動作しない)	(動作しない)	動作する

その他の詳細な動作条件や動作内容、注意事項については、以下の説明で記載します。

ZTP の処理フロー

本装置の ZTP の処理のフローは以下の通りです。

1. 装置の起動、ブートイメージおよび設定ファイルの読み込みと適用

装置が起動すると、最初に本体もしくは SD カードに書き込まれたブートローダーを読み込み、所定 のブートイメージと設定ファイルを使用して起動します。ZTP 機能は、読み込んだブートイメージと設 定ファイルを元に動作します。

注意事項



- 起動時のブートイメージもしくは設定ファイルに SD カード上のファイルを使用した場合、設定や ZTP スイッチのポジションによらず、ZTP 機能は動作しません。
- ZTP 機能を使用する際は、L3 Features > Interface > IPv4 Interface の画面で いずれかの VLAN に VLAN インターフェースを割り当てた設定にしてください。初 期設定では VLAN ID:1 に VLAN インターフェースが登録されています。また、VLAN ID:1 以外に VLAN インターフェースを登録した場合、Edit ボタンで詳細設定画面 に移行し、Get IP From パラメーターを DHCP に設定する必要があります。

2. DHCP サーバーからネットワークアドレスや ZTP 処理に関する情報を取得

ZTP の処理を開始し、装置本体の ZTP LED が緑に点灯します。ZTP 機能では、DHCP を使用して TFTP サーバーやイメージファイル、設定ファイルを指定します。TFTP サーバーの情報は必須です。イメージファイル、設定ファイルはいずか一方のみでも動作します。

各パラメーターの指定は DHCP パケット内の以下の情報で行います。

- ・TFTP サーバー:オプション 150(TFTP Server Address)、もしくは siaddr フィールド
- ・イメージファイル:オプション 125(Vendor-Specific Information)
- ・設定ファイル:オプション 67(Bootfile name)、もしくは file フィールド

siaddr フィールドや file フィールドは、DHCP オプションの情報がない場合のみ参照されます。

DHCP オプション 125 を使用してイメージファイル名を通知する場合、4 バイトの enterprise-number に整数型で 278 (Hex 形式で 00 00 01 16)を、1 バイトの subopt-code には 1 を、sub-option-data (可変長)には TFTP サーバー上のファイルパスを Ascii 形式でエンコードした値を、それぞれ指定し てください。

3. TFTP サーバーから所定のファイル (イメージファイル、設定ファイル)を取得

手順2でDHCPサーバーから受信した情報を元に、TFTPサーバーからイメージファイル、設定ファイルをダウンロードします。TFTPサーバーとの通信は、DHCPサーバーから通知されたネットワークアドレス情報(IPアドレス、ゲートウェイアドレス)を使用して行います。TFTPサーバーにアクセスができない場合や、いずれかの指定されたファイルが取得できない場合は、ZTP処理失敗として扱われます。

4. イメージファイル、設定ファイルを適用

ダウンロードしたイメージファイル、設定ファイルを適用します。処理が完了すると、装置前面の ZTP LED が消灯します。

取得した設定ファイルは、装置内部のルートディレクトリー上に書き込まれ、さらにブートロー ダーの内容を書き換えます。取得したイメージファイルはプライマリーブートイメージのファイルに 上書きされます。イメージファイル、設定ファイルの一方が指定されていない場合、そのファイルは 現在適用されているファイルが使用されます。

また、イメージファイルをダウンロードした場合、現在適用しているイメージファイルとの比較が 行われ、バージョンが異なる場合にはダウンロードしたイメージファイルでの再起動を行います。こ の再起動処理ではイメージファイルと設定ファイルの読み込み後に ZTP の処理が行われません。また、 バージョンが同一の場合はここでの再起動の処理が行われません。

DHCP サーバーから通知されたネットワークアドレス情報は、ZTP 機能の処理が完了すると原則として破棄されますが、装置の IP アドレス設定によってはアドレス情報が引き継がれることもあります。

ZTP 失敗時の動作

ZTP の処理に失敗した場合には3分間、装置前面の ZTP LED を赤点灯します。また、装置は現在適用しているブートイメージと設定ファイルを維持します。

ZTP に失敗する主なケースとして以下が挙げられます。DHCP サーバーの設定や TFTP サーバーに保管したファイルなど、ネットワーク環境の見直しを行ってください。

- ・DHCP サーバーから ZTP 処理に関する情報を取得できなかった場合
- ・DHCP パケットで指定された TFTP サーバーとの疎通が取れない場合
- ・DHCP パケットで指定されたファイルを TFTP サーバーから取得できなかった場合

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 Source Interface			
IP TFTP Source Interface			
Source Interface State Interface Type	Disabled VLAN	VID (1-4094)	Apply
IP FTP Source Interface			
Source Interface State Interface Type	Disabled 💙 VLAN 💙	VID (1-4094)	Apply

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

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。

File System					
Path	C:				Go
Сору	Erase Boot				
Drive	Media Type	Size (MB)	File System Type	Label	
<u>C:</u>	Flash	122	FFS		

本画面の各項目の説明を以下に示します。

パラメーター	説明
Path	パスを入力します。

入力したパスに移動するには、Go ボタンをクリックします。

特定のファイルを装置にコピーするには、Copyボタンをクリックします。

ブートファイルを消去するには、Erase Boot ボタンをクリックします。

装置のファイルシステムのルートディレクトリーに移動するには、Drive に表示されている「<u>c:</u>」の八 イパーリンクをクリックします。

「<u>c:</u>」のハイパーリンクをクリックすると、以下に示す画面が表示されます。

Pre	evious	Cre	ate Directory	Сору	Erase Boot			
idex	Info	Attr	Size (byte)	Update Time	Name			
4	DUN(##)		11170044	lop 11 2021 10:40:42	V2.00.00b.0011.bod	Primary Up	Secondary Up	Rename
I RUN("") -IW III7/0844	Jan 11 2021 10:40:42 V2.00.000.0011.	V2.00.00D.0011.lldu		Delete				
2	DUN(*)		44477000	lan 26 2024 40:46:20	V2.00.00b.0012 bad	Primary Up	Secondary Up	Rename
2	RUN(*)	-1W	111//332	Jan 26 2021 10.46.39 V2.00.00D.0013.nad	v2.00.000.0013.11au		Delete	
2	050(#*)		1206	lan 26 2024 40:40:25	20.000110.0005	Primary Up	Secondary Up	Rename
з	CFG()	-1 W	1290	Jan 20 2021 10.48.20	secondary.cig		Delete	
	050/#		4757	1 00 0004 44-00-00		Primary Up	Secondary Up	Rename
4	CFG(^)	-rw	1/5/	Jan 26 2021 14:39:00	primary.crg		Delete	
5		d	0	Jan 26 2021 05:39:49	<u>system</u>		Delete	

入力したパスに移動するには、Goボタンをクリックします。

前の画面に戻るには、Previousボタンをクリックします。

装置のファイルシステム内に新しいディレクトリを作成するには、Create Directory をクリックします。

ファイルを装置にコピーするには、Copy ボタンをクリックします。

ブートファイルを消去するには、Erase Boot ボタンをクリックします。

Copy ボタンをクリックすると、以下に示す画面が表示されます。

File System			
Path	c:/		Go
Copy File			
Source	startup-config 🗸	C:/config.cfg	
Destination	running-config 🔽	C:/config.cfg	Replace
			Apply Cancel

Copy Fileの各項目の説明を以下に示します。

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

コピーを開始するには、Applyボタンをクリックします。

プロセスを破棄するには、Cancel ボタンをクリックします。

各ファイルの操作について

ファイルをプライマリーブートイメージ、またはプライマリー設定ファイルに指定するには、Primary Up ボタンをクリックします。

ファイルをセカンダリーブートイメージ、またはセカンダリー設定ファイルに指定するには、 Secondary Up ボタンをクリックします。

ファイル名を変更するには、Rename ボタンをクリックします。

ファイルを削除するには、Deleteボタンをクリックします。

注意事項



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



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

5 L2 Features

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

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

5.1 FDB

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

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

5.1.1 Static FDB

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

Unicast Static FDB

Unicast Static FDB 画面では、MAC アドレステーブル登録するユニキャスト MAC アドレスのスタ ティックエントリーを設定します。

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

Unicast Static FDB				
Unicast Static FDB				
Port Port1/0/1	VID (1-4094)	MAC Address 00-84-57-00-00-00	Apply	
Total Entries: 1			Delete All	
VID	MAC Address	Port		
1	00-11-22-33-44-55	Port1/0/10	Delete	
		1/1 < <	1 > > Go	

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

本画面の各項目の説明を以下に示します。

設定を適用するには、Applyボタンをクリックします。

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

エントリーを削除するには、Deleteボタンをクリックします。

Multicast Static FDB

Multicast Static FDB 画面では、マルチキャスト MAC アドレステーブル登録するスタティックエント リーを設定します。

本画面を表示するには、Static FDB > Multicast Static FDB をクリックします。

Multicast Static FDB			
From Port To Port1/0/1 V	o Port VID (1-4094) Port1/0/1	MAC Address 01-00-00-00-02	Add Delete
Total Entries: 1			Delete All
VID	MAC Address	Egress Ports	
1	01-00-00-00-02	Port1/0/10	Delete
		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	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 AII 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。

MAC Address Table Settings			
Global Settings	MAC Address Port Learning Settings		
Aging Time (0, 10-1000000) Aging Destination Hit	300 sec OEnabled ODisabled Apply		

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

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

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

設定を適用するには、Applyボタンをクリックします。

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

MAC Address Table Settings		
Global Settings MAC Address Port Learning Settings		
From Port To Port State Port1/0/1 Port1/0/1 Enabled	Apply	
Port	State	
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	選択したポートでの MAC アドレス学習の状態 (Enabled / Disabled)を 選択します。

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。

IAC Address Tal	ble			
AC Address Table –				
Port	Port1/0/1		Clear Dynamic by Port	Find
VID (1-4094)			Clear Dynamic by VLAN	Find
MAC Address	00-84-57-00-00-00	Clear Dynamic by MAC Find		
Total Entries: 9			Clear All	View All
VID	MAC Address	Туре	Port	
1	00-00-5E-00-01-E7	Dynamic	Port1/0/1	
1	00-03-24-12-01-15	Dynamic	Port1/0/1	
1	00-11-22-33-44-55	Static	Port1/0/10	
1	00-40-66-55-68-20	Static	CPU	
1	00-40-66-91-36-11	Dynamic	Port1/0/1	
1	00-40-66-C2-AA-0A	Dynamic	Port1/0/1	
1	10-BF-48-D6-E2-E2	Dynamic	Port1/0/1	
1	10-BF-48-D6-E3-3B	Dynamic	Port1/0/1	
1	01-00-00-00-02	Static	Port1/0/10	
			1/1 < < 1 >	> Go

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

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

選択したポートにエントリーされているダイナミック MAC アドレスをクリアするには、Clear Dynamic by Port ボタンをクリックします。

選択した VLAN ID にエントリーされているダイナミック MAC アドレスをクリアするには、Clear Dynamic by VLAN ボタンをクリックします。

入力したダイナミック MAC アドレスをクリアするには、Clear Dynamic by MAC ボタンをクリックします。

入力した情報でエントリーを検索するには、Find ボタンをクリックします。

すべてのダイナミック MAC アドレスをクリアするには、Clear All ボタンをクリックします。

MAC アドレステーブルにエントリーされているすべての MAC アドレスを表示するには、View All ボタ ンをクリックします。

5.2 VLAN

VLAN サブメニューでは、VLAN の登録やポートへの割り当てなどの設定を行います。

VLAN の下にあるサブメニューの一覧を以下の表に示します。

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

5.2.1 802.1Q VLAN

802.1Q VLAN 画面では、VLAN を設定します。

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

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

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

3 or 2-5				Apply	Delete
				Find	View All
		Untergood Member Donte			
VLAN Name	Tagged Member Ports	Unlagged Member Ports	VLANType		
	3 or 2-5	3 or 2-5	3 or 2-5	3 or 2-5	3 or 2-5 Apply

802.1Q VLAN の各項目の説明を以下に示します。

パラメーター	説明
VID List	作成または削除する VLAN ID のリストを入力します。
	、Apply ボタンをクリックします。
802.1Q VLAN を削除するには	、Delete ボタンをクリックします。

Find VLAN の各項目の説明を以下に示します。

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

入力した情報で VLAN を検索するには、Find ボタンをクリックします。

すべての VLAN を表示するには、View All ボタンをクリックします。

VLAN を再設定するには、Edit ボタンをクリックします。

VLAN を削除するには、Delete ボタンをクリックします。

5.2.2 802.1v Protocol VLAN

802.1v Protocol VLAN サブメニューでは、プロトコル VLAN の設定を行います。

プロトコル VLAN は、Ethernet ヘッダーなどのデータリンク層のフレーム情報から上位層のプロトコル (たとえば IP や IPv6、ARP など)を識別し、所定の VLAN にマッピングする機能です。

Protocol VLAN Profile

Protocol VLAN Profile 画面では、プロトコル VLAN のプロファイルを設定します。

本画面を表示するには、L2 Features > VLAN > 802.1v Protocol VLAN > Protocol VLAN Profile を クリックします。

Add Protocol VLAN Profile Profile ID (1-16) Frame Type Ether Type (0x0-0xFFFF) 0x Total Entries: 1 Ether Type Profile ID Frame Type Ether Type Ether Type							
Profile ID (1-16) Frame Type Ethernet2 Ether Type (0x0-0xFFFF) 0x Total Entries: 1 Profile ID Frame Type Ether Type							
Total Entries: 1 Profile ID Frame Type Ether Type	Profile ID (1-16) Frame Type Ethernet2 V Ether Type (0x0-0xFFFF) 0x Apply						
Profile ID Frame Type Ether Type	Total Entries: 1						
1 Ethernet2 0xFFFF(User define)	Ether Type						

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

本画面の各項目の説明を以下に示します。

設定を適用するには、Applyボタンをクリックします。

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

Protocol VLAN Profile Interface

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



本画面の各項目の説明を以下に示します。

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

設定を適用するには、Applyボタンをクリックします。

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

5.2.3 VLAN Interface

VLAN Interface 画面では、VLAN をポートに割り当てます。

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

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

アクセスモードは、ポートに 1 個のタグなし VLAN のみを割り当てるモードで、ポートベース VLAN と も呼ばれます。対象ポートでは、原則として(ダイナミック VLAN などの機能が適用されない限り)割 り当てた VLAN に対するタグなしフレームの送受信処理を行います。

本装置は、デフォルトですべてのポートがアクセスモードで、VLAN ID:1 のタグなし VLAN が割り当て られています。

トランクモードは、1 つのポートに複数のタグ VLAN を割り当てることができます。タグ VLAN に割り当 てた VLAN でのフレーム転送処理が発生する場合、対象ポートからタグ付きフレームで送信します。ト ランクモードでは、ネイティブ VLAN と呼ばれる 1 個のタグなし VLAN を割り当てることができます。 ネイティブ VLAN でのフレーム転送処理が発生する場合、対象ポートからタグなしフレームで転送しま す。また、対象ポートで受信したタグなしフレームは、ネイティブ VLAN での入力として処理されます。 ハイブリッドモードでは、トランクモードでのタグ VLAN とネイティブ VLAN の割り当てに加えて、複数のタグなし VLAN を割り当てることができます。タグ VLAN に割り当てた VLAN でのフレーム転送の処理はトランクモードと同じです。タグなし VLAN に割り当てた VLAN での転送処理が発生した場合は、対象ポートからタグなしフレームで転送します。対象ポートで受信したタグなしフレームは、プロトコル VLAN などの機能が適用されない限り、ネイティブ VLAN での入力として処理されます。ハイブリッドモードでのネイティブ VLAN の VLAN ID は PVID とも呼ばれます。

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

Port	VLAN Mode	Ingress Checking	Acceptable Frame Type	
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	Access	Enabled	Untagged-Only	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

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

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

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

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

インターフェース上の VLAN の詳細情報が表示されます。 前の画面に戻るには、Back ボタンをクリックします。 Edit ボタンをクリックすると、以下に示す画面が表示されます。以下の画面は、選択している VLAN モードによって表示内容(設定項目)が異なります。

Configure VLAN Interface			
Configure VLAN Interface			
Port	Port1/0/1	Clone	
VLAN Mode	Hybrid 🗸	From Port	To Port
Acceptable Frame	Untagged Only	Port1/0/1 🔽	Port1/0/1 🗸
Ingress Checking	Enabled Disabled		
Native VLAN	✓ Native VLAN		
VID (1-4094)	1		
Action	Add		
Add Mode	Untagged Tagged		
Allowed VLAN Range			
Current Hybrid untagged VLAN Range			
Current Hybrid tagged VLAN Range			
			Back Apply

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

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

設定を適用するには、Applyボタンをクリックします。

前の画面に戻るには、Backボタンをクリックします。

5.2.4 L2VLAN Interface Description

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

L2VLAN Interface Description	_					
Create L2VLAN Interface Description						
L2VLAN Interface Description D	otion rs			Apply		
Find L2VLAN Interface Description						
L2VLAN Interface Find View All						
Total Entries: 2						
Interface	Status	Administrative	Description			
L2VLAN 1	up	enabled		Delete Description		
L2VLAN 2	down	enabled		Delete Description		
			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
L2VLAN Interface	レイヤー2VLAN インターフェース ID を入力します。
Description	レイヤー2VLAN インターフェースの説明を 64 文字以内で入力します。

設定を適用するには、Applyボタンをクリックします。

入力した情報でレイヤー2VLAN インターフェースを検索するには、Find ボタンをクリックします。 すべてのレイヤー2VLAN を表示するには、View All ボタンをクリックします。

レイヤー2VLAN から説明を削除するには、Delete Description ボタンをクリックします。

5.3 VLAN Tunnel

VLAN Tunnel サブメニューでは、VLAN トンネル機能の設定を行います。

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

VLAN Tunnel の下にあるサブメニューの一覧を以下の表に示します。

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

5.3.1 Dot1q Tunnel Settings

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

Dot1q Tunnel Setting	js			
TPID Settings	Dot1q Tunn	el Port Settings		
Inner TPID (0x1-0xffff)	0x 8100			Apply
From Port	To Port	Outer TPID (0x1-0xffff)		
Port1/0/1 🗸	Port1/0/1 🗸	0x 8100		Apply
	Port		Outer TPID	
	Port1/0/1		0×8100	
	Port1/0/2		0x8100	
	Port1/0/3		0×8100	
	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-tag が付けられているかどうかを判断するために使用されま		
	す。内部 TPID は、システムごとに設定できます。		
From Port / To Port	使用するポート範囲を選択します。		
Outer TPID	外部 TPID 値を 0x1~0xFFFF の範囲で入力します(デフォルト:		
	0x8100)。		

設定を適用するには、Applyボタンをクリックします。

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

Dot1q Tunnel Settings				
TPID Settings	Dot1q Tunnel Port Settings			
From Port To Port Port1/0/1 V Port	Trust Inner Priority	Miss Drop Disabled 💌	Insert Dot1q Tag (1-4094)	Apply
Port	Trust Inner Priority		Miss Drop	Insert Dot1q Tag
Port1/0/1	Disabled		Disabled	
Port1/0/2	Disabled		Disabled	
Port1/0/3	Disabled		Disabled	
Port1/0/4	Disabled		Disabled	
Port1/0/5	Disabled		Disabled	
Port1/0/6	Disabled		Disabled	
Port1/0/7	Disabled		Disabled	
Port1/0/8	Disabled		Disabled	
Port1/0/9	Disabled		Disabled	
Port1/0/10	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	使用するポート範囲を選択します。
Trust Inner Priority	この設定が Enabled の場合、受信したタグ付きフレームの VLAN タグの 優先度情報がサービス VLAN タグに反映されます。
Miss Drop	この設定が Enabled の場合、受信したタグ付きフレームの VLAN 情報が VLAN マッピングエントリーまたはルールと一致しない場合、受信フ レームは破棄されます。
Insert Dot1q Tag	トンネルポートで受信したタグなしフレームに挿入する 802.1Q VLAN ID を 1~4094 の範囲で入力します。

5.3.2 VLAN Mapping Settings

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

VLAN Mapping Setting	js		_	_	_	_
VLAN Mapping Settings						
From Port Port1/0/1	To Port Port1/0/1	Original VID List 3 or 2-5 (1-4094)	Original In	ner VID (1-4094)		
Action	VID	Inner VID	Priority			
Translate 🗸	(1-4094)	(1-4094)	0	\checkmark		Apply
Port Port1/0/1 Total Entries: 2						Find
Port	Original VLAN	Translated VLAN		Priority	Status	
Port1/0/10	1/1	translate 2/2		0	Inactive	Delete
Port1/0/11	1/1	translate 2/2		0	Inactive	Delete
				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	使用するポート範囲を選択します。
Original VID List	VLAN ID リストを 1~4094 の範囲で入力します。
Original Inner VID	カスタマーVLAN ID を 1~4094 の範囲で入力します。Action が Dot1q- tunnel の場合は使用しません。
Action	以下のどちらかのアクションを選択します。
	 Translate:トランクポートで VLAN 変換を実行する場合に選択します。受信フレームの VLAN 情報が Original VLAN に一致すると、指定した VLAN によって置き換えられます。
	 Dot1q-tunnel:トンネルポートで受信したフレームの VLAN 情報が 指定された Original VLAN と一致すると、VID で指定された S-VLAN タグが追加されます。
VID	VLAN IDを1~4094の範囲で入力します。
Inner VID	変換するカスタマーVLAN IDを 1~4094 の範囲で入力します。Action が
	Dot1q-tunnel の場合は使用しません。
Priority	802.1p 優先度の値として 0~7 のいずれかを選択します。
Port	検索に使用するポートを選択します。

設定を適用するには、Applyボタンをクリックします。

入力した情報で VLAN マッピングを検索するには、Find ボタンをクリックします。

VLAN マッピングを削除するには、Delete ボタンをクリックします。

5.4 STP

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

STP の下にあるサブメニューの一覧を以下の表に示します。

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

5.4.1 STP Global Settings

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

STP Global Settings		
STP State		
STP State	Disabled Denabled	Apply
STP Traps		
STP New Root Trap	Disabled Denabled	
STP Topology Change Trap	Disabled Disabled	Apply
STP Mode		
STP Mode	RSTP	Apply
STP Priority		
Priority (0-61440)	32768	Apply
TP Configuration		
Bridge Max Age (6-40)	20 sec Bridge Hello Time (1-2) 2 sec	
Bridge Forward Time (4-30)	15 sec TX Hold Count (1-10) 6 times	S
Max Hops (6-40)	20 times NNI BPDU Address Dot1d	Apply

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。

5 L2 Features | 5.4 STP

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	の値を選択します。
設定を適用するには	on ly ボタンをクリック	

設定を適用するには、Applyボタンをクリックします。

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

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

STP Port Setti	ngs							
STP Port Settings								
From Port		Port1/0/1	✓ To Port	Port1/0/1				
Cost (1-200000000, 0=Auto)			State	Enabled 🗸	Guard Root	Disabled 🗸		
Link Type		Auto	✓ Port Fast	Network 🗸	TCN Filter	Disabled 🗸		
BPDU Forward		Disabled	✓ Priority	128 🗸	Hello Time (1-2)		sec	Apply
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。
	 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。

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 Identif	cation	
MST Configuration Identification		
Configuration Name Revision Level (0-65535) Digest	00:40:66:55:68:20 0 AC36177E50283CD4B83821D8AB26DE62	Apply
Instance ID Settings		
Instance ID (1-16)		
Action VID List	Add VID 🔽 1 or 3-5	Apply
Total Entries: 1		
Instance ID	VID List	
CIST	1-4094	Edit Delete
		1/1 < 1 > > Go

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。

Entries: 1			
Instance	Instance State	Instance Priority	
CIST	Disabled	32768(32768 sysid 0)	Edit
			1/1 < < 1 > >
0107			
nce CIST			
nce CIST		CIST Global	Info[Mode RSTP]
	Bridge Address	CIST Global 00-40-	Info[Mode RSTP] 66-55-68-20
Ince CISI	Bridge Address esignated Root Address / Priority	CIST Global 00-40- 00-00-00	Info[Mode RSTP] 66-55-68-20 0-00-00-00 / 0
E CISI E Rej	Bridge Address resignated Root Address / Priority pional Root Bridge Address / Priority	CIST Global 00-40- 00-00-00 00-00-00 00-00-00	Info[Mode RSTP] 66-55-68-20 0-00-00 / 0 0-00-00 / 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
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。

MSTP Port Information	on				
MSTP Port Information —					
Port Port1/0/1					Clear Detected Protocol Find
Instance ID	Cost	Priority	Status	Role	
CIST	200000	128	Forwarding	NonStp	Edit
					1/1 < < 1 > > Go

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。

本画面の各項目の説明を以下に示します。

選択したポートで検出されたプロトコル設定をクリアするには、Clear Detected Protocol ボタンをク リックします。

入力した情報で MSTP ポート情報を検索するには、Find ボタンをクリックします。

MSTP ポート情報を再設定するには、Edit ボタンをクリックします。

5.5 Loop Detection

Loop Detection 画面では、ループ検知機能を設定します。

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

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

oop Detection						
oop Detection Global S	iettings					
.oop Detection State Disabled Enabled VLAN ID List 1-4094		Mode Port-bas Interval (1-32767) 10		ed V sec Appl		
oop Detection Port Set	tings					
From Port Port1/0/1	To Port Port1/0/	1 💌	noChkSrc Disabled	Action Shutdown	~	State Disabled Apply
Port	noChkSrc	Action	Loop Detection Sta	ate	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	a na mina na n
Port1/0/9	Disabled	Shutdown	Disabled		Normal	-
Port1/0/10	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。
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。

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

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。

5.6 Link Aggregation

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

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

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

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

ink Aggregation	_	_			
System Priority (1-655 Load Balance Algorith System ID	35) 32 m So 32	768 purce Destination 768,00-40-66-55-68	MAC 🗸 3-20		Apply Apply
Channel Group Inform	ation				
From Port	To Port	Gro	up ID (1-8)	Mode	
Port1/0/1 🗸	Port1/0/1	▼		On 🔽	Add Delete Member Port
Note: Each Channel Group supports up to 8 member ports.					
Total Entries: 2					
Channel Group	Protocol	Max Ports	Member Number	Member Ports	
Port-channel1	Static	8	2	1/0/12-1/0/13	Delete Channel Channel Detail
Port-channel2	LACP	8	2	1/0/14-1/0/15	Delete Channel Channel Detail

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

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

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

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

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

チャネルグループを追加するには、Add ボタンをクリックします。

グループからメンバーポートを削除するには、Delete Member Port ボタンをクリックします。

チャネルグループを削除するには、Delete Channel ボタンをクリックします。

チャネルの詳細情報を表示するには、Channel Detail ボタンをクリックします。

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

ort Channel Info	rmation					
Port Channel	2					
Protocol	LACP					
ort Channel Deta	il Information					
Port	LACP Timeout	Working Mode	e LACP State	Port Priority	Port Number	
Port1/0/14	Long	Active	down	32768	0	Edit
Port1/0/15	Long	Active	down	32768	0	Edit
Port	Partner System ID	Partner PortNo	Partner LACP Timeout	Partner Working	Mode Partne	r Port Priority
Port1/0/14	0,00-00-00-00-00	0	Long	Passive		0
Port1/0/15	0,00-00-00-00-00-00	0	Long	Passive		0
Note: LACP State:	hed to an aggregator and bund	led with other ports. d but able to switch data tra	iffic).			Back

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

Edit ボタンをクリックした後の各項目の説明を以下に示します。

パラメーター	説明
LACP Timeout	LACP タイムアウトのモード (Short / Long)を選択します。Short の場合は 3 秒間に LACP フレームを受信しないときにダウンとみなします。 Long の場合は 90 秒間に LACP フレームを受信しないときにダウンとみなします。 このパラメーターを LACP フレームで通知することで、Short の場合は 1 秒間隔 Lang の場合は 20 秒間隔石 対向デザイスが LACP スレームを
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。

5.7 L2 Multicast Control

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

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

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

5.7.1 IGMP Snooping

IGMP Snooping サブメニューでは、IGMP スヌーピング機能の設定を行います。

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

IGMP Snooping Settings

IGMP Snooping Settings 画面では、IGMP スヌーピングのグローバル設定を行います。

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

IGMP Snooping Settings			
Global Settings			
Global State	Enabled Obisabled		
Dynamic Mrouter Aging Time (10-65535)	300 sec		
Unknown Data Limit (1-64)	64 ✔No Lin	nit	Apply
IGMP Snooping Unknown Data All	VID(1-4094)	IP Address	Clear
VLAN Status Settings			
VID (1-4094)	OEnabled OEnabled		Apply
IGMP Snooping Table			
VID (1-4094)			Find View All
Total Entries: 1			
VID	VLAN Name	Status	
1	default	Enabled	Show Detail Edit
			1/1 < < 1 > > Go

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	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~
Time	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	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
Data	ます。クリアする対象を以下のいずれかから選択します。
	· AII:すべてのエントリーをクリアします。
	・ VLAN:指定した VLAN のエントリーをクリアします。
	○ VID :VLAN IDを1~4094の範囲で入力します。
	· Group:指定したグループのエントリーをクリアします。
	○ IP Address:グループアドレスを入力します。

設定を適用するには、Applyボタンをクリックします。

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

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

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

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

IGMP Snooping VLAN Parameters	
IGMD Spooning VI AN Darameters	
Tomir shooping verw rarameters	
VID	1
Status	Enabled
Minimum Version	v1
Fast Leave	Disabled (host-based)
Report Suppression	Disabled
Suppression Time	10 seconds
Querier State	Disabled
Query Version	v3
Query Interval	125 seconds
Max Response Time	10 seconds
Robustness Value	2
Last Member Query Interval	1 seconds
Proxy Reporting	Disabled Source Address (0.0.0)
Unknown Data Learning	Enabled
Unknown Data Expiry Time	Infinity
Ignore Topology Change	Disabled
	Modify

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)	1
Status	Enabled Disabled
Minimum Version	
Fast Leave	OEnabled OEnabled
Report Suppression	OEnabled
Suppression Time (1-300)	10
Querier State	OEnabled OEnabled
Query Version	3
Query Interval (1-31744)	125 sec
Max Response Time (1-25)	10 sec
Robustness Value (1-7)	2
Last Member Query Interval (1-25)	1 sec
Proxy Reporting	OEnabled ODisabled
Unknown Data Learning	Enabled Disabled
Unknown Data Expiry Time (1-65535)	sec √ Infinity
Ignore Topology Change	OEnabled OEnabled
	Apply

IGMP	Snoop i ng	VLAN	Settings	では、	IGMP	スヌー	ピング	ブの詳細設	定を行い	います。	各項目	の説明を	·以下
に示	します。												

パラメーター	説明				
Minimum Version	IGMP バージョン(1 / 2 / 3)を選択します。				
Fast Leave	IGMP スヌーピング即時離脱機能の状態 (Enabled / Disabled)を選択				
	します。Enabled の場合、メンバーから IGMP グループ離脱メッセージ				
	を受信すると、メンバーを即座に削除します。				
Report Suppression	レポート抑制の状態(Enabled / Disabled)を選択します。				
	レポート抑制機能は、IGMPv1 および IGMPv2 メッセージに対してのみ動 作します				
	レポート抑制が無効の場合、装置はマルチキャストノードからの IGMP				
	メッセージをすべてマルチキャストルーターに転送します。レポート抑				
	制が有効の場合、Suppression Time で指定した期間内にマルチキャス				
	トノードからの同じタイプ(メンバーシップレポート/グループ離脱)の				
	メッセージを複数受信すると、1 個のメッセージに集約してマルチキャ				
·					
Suppression lime	レホート抑制機能の抑制時間(秒)を 1~300 の軛囲で入力します(テ フォルト:10 秒)。				
Querier State	クエリア機能の状態(Enabled / Disabled)を選択します。クエリア機				
	能は、通常はマルチキャストルーターが送信する IGMP クエリーを代行				
	して送信する機能です。マルチキャストルーターが存在しない環境で、				
	マルチキャストノードの情報を適切に更新するために必要になります。				
Query Version	クエリアが送信するジェネラルクエリーのバージョン(1 / 2 / 3)を 選択します。				
Query Interval	クエリアが送信するジェネラルクエリーの送信間隔を 1~31744(秒)				
	の範囲で入力します。				
Max Response Time	ジェネラルクエリーの応答待ち時間を 1~25(秒)の範囲で入力しま す。				
Robustness Value	ロバストネス変数を1~7の範囲で入力します(デフォルト:2)。				
Last Member Query	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				
Interval	る間隔を1~25(秒)の範囲で入力します。				
Proxy Reporting	プロキシレポート機能の状態(Enabled / Disabled)を指定します。				
	· Source Address:プロキシレポートの送信元アドレスを入力しま す。				
Unknown Data Learning	マルチキャストトラフィックを受信した際に、メンバー不在のエント				
C C	リーを作成する場合は Enabled を選択します。				
	 Unknown Data Expiry Time:メンバー不在のエントリーの有効期限 を1~65535(秒)の範囲で入力します。 				
Ignore Topology Change	トポロジー変更の無視機能の状態(Enabled / Disabled)を選択しま				
	70				

IGMP Snooping Groups Settings

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

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

IGMP Snooping Groups Settings									
IGMP Snooping Static Groups Settings									
VID (1-4094)	Group Address	From Port Port1/0/1	To Port Port1/0/1	~	Apply	Delete			
VID (1-4094)	Group Address				Find	View All			
Total Entries: 1									
VID		Group Addres	5	_	Ports				
1		224.0.1.0			1/0/10				
					1/1 < 1 >	> > Go			
IGMP Snooping Groups Tabl	e ————								
VID (1-4094)	Group Address								
•	0				Find	View All			
Total Entries: 0									
VID	Group Address	Sou	Irce Address	FM	Exp(sec)	Ports			

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

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

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

パラメーター	説明					
VID	ラジオボタンをクリックし、マルチキャストグループの VLAN ID を 1~ 4094 の範囲で入力します。					
Group Address	ラジオボタンをクリックし、グループアドレスを入力します。					
入力した情報で IGMP スヌーピンググループを検索するには、Find ボタンをクリックします。						

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

IGMP Snooping Mrouter Settings

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

IGMP Snooping Mrouter Settings											
GMP Snooping Mrouter Setting	IGMP Snooping Mrouter Settings										
VID (1-4094)	Configuration Port	From Port Port1/0/1	To Port Port1/0/1	Apply Delete							
GMP Snooping Mrouter Table	IGMP Snooping Mrouter Table VID (1-4094) Find View All										
Total Entries: 1	Total Entries: 1										
VID Ports											
1			1/0/10 (Static)								
				1/1 < < 1 > > Go							

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

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

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

IGMP Snooping Statistics Settings

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

IGMP Snooping Statistics Settings														
IGMP Snooping Statistics Settings														
Statistics VID (1-4094)						From PortTo PortPort1/0/1Port1/0/1				V Clear				
IGMP Snooping	Statistics Ta	able												
Find Type		VID (1-4	094)		From Port		I	o Port						
VLAN	~	1			Port1/0/1			Port1/0/1	\checkmark			Find	Vie	ew All
Total Entries: 1														
		IGM	Pv1				IGN	IPv2				IGN	IPv3	
Port RX TX RX TX RX							T	¢						
	Report	Query	Report	Query	Report	Query	Leave	Report	Query	Leave	Report	Query	Report	Query
Port1/0/9	0	0	0	0	0	0	0	0	0	0	0	0	0	0
											1/1	< 1	> >	Go

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

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

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

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

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

5.7.2 MLD Snooping

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

MLD Snooping Settings

MLD Snooping Settings 画面では、MLD スヌーピングのグローバル設定を行います。

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

MLD Snooping Settings			
Global Settings			
Global State			
Unknown Data Limit (1.64)		14	- Appelu
Unknown Data Limit (1-04)	04 Veldu	L	Арріу
MLD Snooping Unknown Data All	VID (1-4094)	Group Address FFE0::1	Clear
VLAN Status Settings			
VID (1-4094)	Enabled		Apply
MLD Snooping Table			
VID (1-4094)			Find View All
Total Entries: 1			
VID	VLAN Name	Status	
1	default	Enabled	Show Detail Edit
			1/1 < < 1 > > Go

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。 AII:すべてのエントリーをクリアします。 VLAN:指定した VLAN のエントリーをクリアします。 VID:VLAN IDを1~4094の範囲で入力します。 Group:指定したグループのエントリーをクリアします。 Group Address: グループアドレスを入力します。

設定を適用するには、Applyボタンをクリックします。

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

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

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

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

MLD Snooping VLAN Parameters MLD Snooping VLAN Parameters VID 1 Status Enabled Minimum Version ٧1 Disabled (host-based) Fast Leave Disabled Report Suppression Suppression Time 10 seconds Disabled Source Address (::) Proxy Reporting Mrouter Port Learning Enabled Disabled Querier State Query Version v2 Query Interval 125 seconds Max Response Time 10 seconds Robustness Value 2 1 seconds Last Listener Query Interval Unknown Data Learning Enabled Unknown Data Expiry Time Infinity Ignore Topology Change Disabled Modify

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	
MLD Snooping VLAN Settings	
VID (1-4094)	1
Status	Enabled Disabled
Minimum Version	
Fast Leave	CEnabled OEnabled
Report Suppression	CEnabled Obisabled
Suppression Time (1-300)	10
Proxy Reporting	Cenabled Disabled Source Address [e80::1
Mrouter Port Learning	Enabled Disabled
Querier State	CEnabled OEnabled
Query Version	2
Query Interval (1-31744)	125 sec
Max Response Time (1-25)	10 sec
Robustness Value (1-7)	2
Last Listener Query Interval (1-25)	1 sec
Unknown Data Learning	Enabled Obisabled
Unknown Data Expiry Time(1-65535)	sec 🗹 Infinity
Ignore Topology Change	CEnabled OEnabled
	Apply

MLD	Snooping	VLAN	Settings	では、	MLD	スヌ-	-ピン	グの詳細設	定を行い	います。	各項目の	D説明をり	大下に
示し	,ます。												

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

MLD Snooping Groups Settings

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

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

MLD Snooping Group	os Settings	_	_	_	_	_	_
MLD Snooping Static Group	os Settings						
VID (1-4094)	Group Address FF11::11	From Port Port1/0/1	To Po	rt 1/0/1 💌		Apply	Delete
VID (1-4094)	Group Address					Find	View All
Total Entries: 1							
VID		Group Add	dress			Ports	
1		ff11::1	1			1/0/10	
						1/1 < < 1 >	> Go
MLD Snooping Groups Tab	le						
VID (1-4094)	Group Address					Find	View All
Total Entries: 0							
VID	Group Address		Source Address		FM	Exp(sec)	Ports

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

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

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

パラメーター	説明		
VID	ラジオボタンをクリックし、マルチキャストグループの VLAN ID を 1~		
	4094 の範囲で入力します。		
Group Address	ラジオボタンをクリックし、グループアドレスを入力します。		
 入力した情報で MLD スヌーピンググループを検索するには、Find ボタンをクリックします。			

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

MLD Snooping Mrouter Settings

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

MLD Snooping Mrouter Set	ttings			
MLD Snooping Mrouter Settings				
VID (1-4094) Con	onfiguration ort	From Port Port1/0/1	To Port Port1/0/1	Apply Delete
MLD Snooping Mrouter Table				Find View All
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。
	· Port:対象ポートをスタティックのルーターポートにします。
	· Forbidden Port:対象ポートを非ルーターポートにします。
	・ Learn PIMv6:対象ポートで IPv6 PIM でのルーターポートの学習を
	行います。
From Port / To Port	ポートまたはポートの範囲を選択します。

設定を適用するには、Applyボタンをクリックします。

登録したルーターポートを削除するには、Deleteボタンをクリックします。

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

パラメーター	説明		
VID	VLAN IDを1~4094の範囲で入力します。		
、 入力した情報でルーターポートを検索するには、Find ボタンをクリックします。			

すべてのルーターポートを表示するには、View All ボタンをクリックします。

MLD Snooping Statistics Settings

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

MLD Snooping Statistics Settings								
MLD Snooping Statistics Settings								
Statistics	VID (1-4094)		From Port Port1/0/	1 🔽	To Port Port1/0	/1		Clear
MLD Snooping Statistics Tab	le							
Find Type VLAN	VID (1-4094)	F	From Port Port1/0/10	To Po	nt 1/0/10 ♥	[Find	View All
Total Entries: 1	Total Entries: 1 MI Dv1 MI Dv2							
Port	RX		ТХ		RX	ТХ	RX	TX
	Report	Done	Report	Done	Report	Report	Query	Query
Port1/0/10	0	0	0	0	0	0	0	0
						1/1	< < 1 ;	> > Go

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

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

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

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

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

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

5.7.3 Multicast Filtering

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

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

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

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

Multicast Filtering				
Multicast Filtering				
VID List	3 or 1-5	Multicast Filter Mode	Forward Unregistered	Apply
Total Entries: 2				
	VLAN		Multicast Filter Mode	
	default		Forward Unregistered Groups	
	VLAN0002		Forward Unregistered Groups	
			1/1 < <	1 > > Go

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

本画面の各項目の説明を以下に示します。

5.8 LLDP

LLDP サブメニューでは、LLDP に関連する設定を行います。

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

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

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

LLDPの下にあるサブメニューの一覧を以下の表に示します。

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

5.8.1 LLDP Global Settings

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

LLDP Global Settings		~
LLDP Global Settings		
LLDP State	⊖Enabled ()Disabled	
LLDP Forward State	OEnabled ODisabled	
LLDP Trap State	OEnabled ODisabled	
LLDP-MED Trap State	OEnabled OEnabled	Apply
LLDP-MED Configuration		
Fast Start Repeat Count (1-10)	4 times	Apply
LLDP Configurations		
Message TX Interval (5-32768)	30 sec	
Message TX Hold Multiplier (2-10)	4 sec	
ReInit Delay (1-10)	2 sec	
TX Delay (1-8192)	2 sec	Apply
LLDP System Information		
Chassis ID Subtype	MAC Address	
Chassis ID	00-40-66-55-68-20	
System Name	Switch	
System Description	APLGM220GTSS 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		
Firmware Revision	1.00.00	
Software Revision	2.00.00b	~

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。

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。
Relnit Delay	LLDP 再初期化の実行保留時間を1~10(秒)の範囲で入力します。
TX Delay	LLDP フレームの連続送信時の最小送信間隔(保留時間)を 1~8192 (秒)の範囲で入力します。Message TX Interval の 1/4 以下の値を設 定してください。

設定を適用するには、Applyボタンをクリックします。

5.8.2 LLDP Port Settings

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

LLDP Port Settings					
LLDD Dort Sottings					
LLDF Fort Setungs					
From Port To Port	Notification Sub	otype Admir	n State IP Subtype	Action Address	
Port1/0/1 🗸 Port1/0	D/1 🗸 Disabled 🗸 Lo	cal 🗸 TX a	and RX 🗸 Default 🗸	Disabled 🗸	
Note: The address should be	the switch's address.				Apply
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		

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

本画面の各項目の説明を以下に示します。

設定を適用するには、Applyボタンをクリックします。

5.8.3 LLDP Management Address List

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

LDP Management Address List					
				Find	
Subtype	Address	IF Type	OID	Advertising Ports	
IPv4	10.85.104.32(default)	IfIndex	1.3.6.1.4.1.278.1.45	-	
IDv/	10 85 104 32	lfindex	136141278145	-	

本画面の各項目の説明を以下に示します。

パラメーター	説明
Subtype	以下のいずれかのサブタイプを選択します。
	 AII: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
	白側のボックスに、検察する IPV4 アトレスを入力します。
	IPv6:IPv6 アドレスで検索します。IPv6 を選択すると表示される
	右側のボックスに、検索する IPv6 アドレスを入力します。

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

5.8.4 LLDP Basic TLVs Settings

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

LLDP Basic TL	LDP Basic TLVs Settings						
LLDP Basic TLVs \$	LLDP Basic TLVs Settings						
From Port Port1/0/1	To Port Port Description Port1/0/1 Disabled	System Name Disabled	System Description System Capat Disabled	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。

5.8.5 LLDP Dot1 TLVs Settings

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

LLDP Dot1 TLV	's Settings						
LLDP Dot1 TLVs Se	LLDP Dot1 TLVs Settings						
From Port Port1/0/1	To Port Port1/0/1	Port VLAN Disabled	Protocol VLAN Disabled	VLAN Name Disabled	Protocol Identity Disabled None Apply		
Port	Port VLAN ID	Enabled	I Port and Protocol VID	Enabled VLAN Name	Enabled Protocol Identity		
Port1/0/1	Disabled						
Port1/0/2	Disabled	i in the second s					
Port1/0/3	Disabled						
Port1/0/4	Disabled			neue geen beren berein berbeiten berein berein berein berein berein b			
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。
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 / AII)を選択します。通知しない場合は Disabled を選択します。

5.8.6 LLDP Dot3 TLVs Settings

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

LLDP Dot3 TLVs S	Settings			
LLDP Dot3 TLVs Settin	gs			
From Port Port1/0/1	To Port Port1/0/1	MAC/PHY Configuration/Status Disabled	Link Aggregation	Maximum Frame Size Disabled Apply
Port	MAC/PHY Con	ïguration/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	Dis	abled	Disabled	Disabled
Port1/0/6	Dis	abled	Disabled	Disabled
Port1/0/7	Disabled		Disabled	Disabled
Port1/0/8	Disabled		Disabled	Disabled
Port1/0/9	Dis	abled	Disabled	Disabled
Port1/0/10	Dis	abled	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	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
Configuration/Status	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。

5.8.7 LLDP-MED Port Settings

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

LLDP-MED Port Settings						
LLDP-MED Port Settings						
From Port To Port Port1/0/1 Port1/0/1	Notification Capabilities Inventory Disabled Disabled Disabled Application					
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。

5.8.8 LLDP Statistics Information

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

LDP Statist	tics Information						
LLDP Statistics	Information						
Last Change Ti	ime	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	U	0	0	0	0
Port1/0/2	0	0	0	0	0	0	0
Port1/0/2 Port1/0/3	0	0	0	0	0 0 0 0	0 0 0	0 0 0
Port1/0/2 Port1/0/3 Port1/0/4	0 0 0	0 0 0 0	0	0 0 0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
Port1/0/2 Port1/0/3 Port1/0/4 Port1/0/5	0 0 0 0	0	0 0 0 0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0
Port1/0/2 Port1/0/3 Port1/0/4 Port1/0/5 Port1/0/6	0 0 0 0 0	0 0 0 0 0	0 0 0 0 0	000000000000000000000000000000000000000	0 0 0 0 0 0	0 0 0 0 0 0	0 0 0 0 0 0
Port1/0/2 Port1/0/3 Port1/0/4 Port1/0/5 Port1/0/6 Port1/0/7	0 0 0 0 0 0	0 0 0 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Port1/0/2 Port1/0/3 Port1/0/4 Port1/0/5 Port1/0/6 Port1/0/7 Port1/0/8	0 0 0 0 0 0 0		0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0
Port1/0/2 Port1/0/3 Port1/0/4 Port1/0/5 Port1/0/6 Port1/0/7 Port1/0/8 Port1/0/9	0 0 0 0 0 0 0 0 0		0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 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。

5.8.9 LLDP Local Port Information

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

LLDP Local Port Info	LDP Local Port Information				
LLDP Local Port Brief Tab	LDP Local Port Brief Table				
Port Port1/0/1	V		Find Show Detail		
Port	Port ID Subtype	Port ID	Port Description		
Port1/0/1	Local	Port1/0/1	APRESIA Systems, Ltd APLGM220G		
Port1/0/2	Local	Port1/0/2	APRESIA Systems, Ltd APLGM220G		
Port1/0/3	Local	Port1/0/3	APRESIA Systems, Ltd APLGM220G		
Port1/0/4	Local	Port1/0/4	APRESIA Systems, Ltd APLGM220G		
Port1/0/5	Local	Port1/0/5	APRESIA Systems, Ltd APLGM220G		
Port1/0/6	Local	Port1/0/6	APRESIA Systems, Ltd APLGM220G		
Port1/0/7	Local	Port1/0/7	APRESIA Systems, Ltd APLGM220G		
Port1/0/8	Local	Port1/0/8	APRESIA Systems, Ltd APLGM220G		
Port1/0/9	Local	Port1/0/9	APRESIA Systems, Ltd APLGM220G		
Port1/0/10	Local	Port1/0/10	APRESIA Systems, Ltd APLGM220G		

本画面の各項目の説明を以下に示します。

パラメーター	説明
Port	情報を表示するポート番号を選択します。

入力した情報で LLDP ローカルポート情報を検索するには、Find ボタンをクリックします。

LLDP ローカルポート情報の詳細を表示するには、Show Detail ボタンをクリックします。

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

LLDP Local Port Information		
LLDP Local Information Table		
Port	Port1/0/1	
Port ID Subtype	Local	
Port ID	Port1/0/1	
Port Description	APRESIA Systems, Ltd APLGM220GTSS HW firmware 2.00.00b Port 1 on Unit 1	
Port PVID	1	
Management Address Count	<u>0</u>	
PPVID Entries	<u>0</u>	
VLAN Name Entries Count	1	
Protocol Identity Entries Count	<u>0</u>	
MAC/PHY Configuration/Status	Show Detail	
Link Aggregation	Show Detail	
Maximum Frame Size	1536	
LLDP-MED Capabilities	Show Detail	
		Back

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

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

LLDP Local Port Information	
LLDP Local Information Table	
Port	Port1/0/1
Port ID Subtype	Local
Port ID	Port1/0/1
Port Description	APRESIA Systems, Ltd APLGM220GTSS HW firmware 2.00.00b Port 1 on Unit 1
Port PVID	1
Management Address Count	Q
PPVID Entries	<u>0</u>
VLAN Name Entries Count	1
Protocol Identity Entries Count	<u>0</u>
MAC/PHY Configuration/Status	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536
LLDP-MED Capabilities	Show Detail
	Back
MAC/PHY Configuration/Status	
Auto-Negotiation Support	Supported
Auto-Negotiation Enabled	Enabled
Auto-Negotiation Advertised Capability	6c01(hex)
Auto-Negotiation Operational MAU Type	001e(hex)

前の画面に戻るには、Backボタンをクリックします。

5.8.10 LLDP Neighbor Port Information

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

DP Neighl	or Port Brief Table					
ort	Port1/0/1				Find	Clear
						Clear All
otal Entrie	s: 1					Clear All
otal Entrie Entity	s: 1 Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	Clear All

本画面の各項目の説明を以下に示します。

パラメーター	説明
Port	情報を表示するポート番号を選択します。
•	

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

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

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	00-03-24-12-01-13
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 Back

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

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

LLDP Neighbor Port Information		
LLDP Neighbor Information Table		
Entry ID	1	
Chassis ID Subtyne	, MAC Address	
Chassis ID	00-03-24-12-00-00	
Port ID Subtyne	MAC Address	
Port ID	00-03-24-12-01-13	
Port Description		
System Name		
System Description		
System Canabilities		
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	Back
MAC/PHY Configuration/Status		
None		

前の画面に戻るには、Backボタンをクリックします。

6 L3 Features

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

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

6.1 ARP

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

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

6.1.1 ARP Aging Time

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

ARP Aging Time		
ARP Aging Time		
Total Entries: 1		
Interface Name	Timeout (min)	
vlan1	240	Edit
		1/1 K K 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
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。

tatic ARP						
tatic ARP						
IP Address	· · Hardw	are Address 00-11-22-33-4	4-AA			Apply
Interface Name	IP Address	Hardware Address	Aging Time	Туре		
vlan1	10.85.104.32	00-40-66-55-68-20	Forever		Edit	Delete
	172.31.131.1	00-11-22-33-44-55	Forever	Static	Edit	Delete
					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	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。

RP Table				
ARP Search				
 Interface VLAN (1-4094)) IP Address	Mask	
O Hardware Address	00-11-22-33-44-55) Type All 💙		Find
Total Entries: 2				Clear All
Interface Name	IP Address	Hardware Address	Aging Time (min)	Туре
vlan1	10.85.104.32	00-40-66-55-68-20	Forever	Delete
vlan1	10.90.90.10	10-BF-48-D6-E2-E2	240	Delete
			1/1 < <	1 > > Go

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。
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レ 検索する
	MAC アドレスを入力します。
Туре	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 (AII / Dynamic)を選択します。

本画面の各項目の説明を以下に示します。

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。

Pv6 Neighbor						
IPv6 Neighbor Settings						
Interface VLAN (1-4094)	IPv6 Address	2013::1	MAC Address	11-22-33-44-AA-	FF	Apply
Interface VLAN (1-4094)	IPv6 Address	2013::1			Find	Clear
Total Entries: 1						Clear All
IPv6 Address	Link-La	ayer Addr	Interface	Туре	State	
2021::1	00-11-22	2-33-44-66	vlan1	Static		Delete
				1/1	<u> </u> < < '	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
Interface VLAN	VLAN インターフェースの VLAN ID を 1~4094 の範囲で入力します。
IPv6 Address	IPv6 アドレスを入力します。
MAC Address	MAC アドレスを入力します。

設定を適用するには、Applyボタンをクリックします。

入力した情報で IPv6 ネイバーを検索するには、Find ボタンをクリックします。

インターフェースのすべてのダイナミック IPv6 ネイバー情報をクリアするには、Clear ボタンをク リックします。

すべてのダイナミック IPv6 ネイバー情報をクリアするには、Clear All ボタンをクリックします。 IPv6 ネイバーを削除するには、Delete ボタンをクリックします。

6.3 Interface

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

Interfaceの下にあるサブメニューの一覧を以下の表に示します。

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

6.3.1 IPv4 Interface

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

IPv4 Interface				
IPv4 Interface				
Interface VLAN (1-4094)				Apply Find
Total Entries: 1				
Interface	State	IP Address	Link Status	
vlan1	Enabled	10.85.104.32/255.0.0.0 Manual	Up	Edit 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
Interface VLAN	VLAN インターフェースの VLAN ID を 1~4094 の範囲で入力します。

設定を適用するには、Applyボタンをクリックします。

入力した情報で IPv4 インターフェースを検索するには、Find ボタンをクリックします。

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

IPv4 インターフェースを削除するには、Delete ボタンをクリックします。

Edit ボタンをクリックすると、以下に示す画面が表示されます。

IPv4 Interface Configure			
IPv4 Interface Settings			
Interface	vlan1		Back
Settings			
State	Enabled V	1	
Description	64 chars]	Apply
IP Settings			
Get IP From	Static		
IP Address	· · ·		
Mask	· · ·		Apply Delete

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、Backz	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	t、 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	ξす。
----------------	----------	-------------	---------------	-----

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

設定を適用するには、Applyボタンをクリックします。

設定を削除するには、Deleteボタンをクリックします。

6.3.2 IPv6 Interface

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

IPv6 Interface			
IPv6 Interface			
Interface VLAN (1-4094)			Apply Find
Total Entries: 1			
Interface	IPv6 State	Link Status	
vlan1	Disabled	Up	Detail
			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
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。

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			
IPv6 Interface Settings	Interface IPv6 Address	DHCPv6 Client	
Interface IPv6 State	vlan1 Disabled		Back Apply
Static IPv6 Address Settings IPv6 Address	E	UI-64 🗌 Link Local	Apply
NS Interval Settings NS Interval (0-3600000)	0 ms		Apply

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。

ace IPv6 Address	DHCPv6 Client	
	IPv6 Address	
fi	e80::240:66ff:fe55:6820	Delete
172	2:31:131::123/64 (Manual)	Delete
	ace IPv6 Address	ace IPv6 Address DHCPv6 Client IPv6 Address fe80::240:66ff:fe55:6820 172:31:131::123/64 (Manual)

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。

IPv6 Interface			
IPv6 Interface Settings	Interface IPv6 Address	DHCPv6 Client	
DHCPv6 Client Settings			
Client State	Disabled 🗸 R	apid Commit	Apply

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

パラメーター 訊	明
Client State DHC	CPv6 クライアント機能の状態(Enabled / Disabled)を選択しま
す。	,
Rap	oid Commit をチェックすると、DHCPv6 の高速コミットの要求を行い
まつ	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。

IPv4 Default Route				
IPv4 Default Route				
Gateway Backup State	Default Route			Apply
Total Entries: 1				
IP Address	Mask	Gateway	Interface Name	
0.0.0.0	0.0.0.0	172.31.131.254		Delete
			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
Gateway	ルートのゲートウェイの IPv4 アドレスを入力します。
Backup State	以下のどちらかのバックアップ状態を選択します。
	· Primary:プライマリールートを登録します。
	· Backup:バックアップルートを登録します。

設定を適用するには、Applyボタンをクリックします。

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

6.5 IPv4 Route Table

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

IPv4 Route Table						
IPv4 Route Table						
IP Address IP Address Network Address Connected O Hardware O Summary Find						
IP Address	Mask	Gateway	Interface	Distance/Metric	Protocol	Candidate Default
10.0.0.0	255.0.0.0	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。

IPv6 Default Route							
IPv6 Default Route							
	Default Route						
Interface VLAN (1-4094)							
Next Hop IPv6 Address 3F	E1::1						
Backup State PI	ease Select			[Apply		
Total Entries: 1	Total Entries: 1						
IPv6 Address/Prefix Length	Next Hop	Interface Name	Protocol	Active			
::/0	172:31:131::254	vlan1	Static	No	Delete		
			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
Interface VLAN	VLAN インターフェースの VLAN ID を 1~4094 の範囲で入力します。
Next Hop IPv6 Address	ルートのネクストホップの IPv6 アドレスを入力します。
Backup State	以下のどちらかのバックアップ状態を選択します。
	· Primary:ルートを、宛先へのプライマリールートとして指定する 場合に選択します。
	 Backup:ルートを、宛先へのバックアップルートとして指定する場合に選択します。

設定を適用するには、Applyボタンをクリックします。

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

6.7 IPv6 Route Table

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

Pv6 Route Table				
Pv6 Route Table				
Connected Summary				Find
Total Entries: 1 entries, 1 routes				
Total Entries: 1 entries, 1 routes IPv6 Address/Prefix Length	Next Hop	Interface	Distance/Metric	Protocol
Total Entries: 1 entries, 1 routes IPv6 Address/Prefix Length 2020::/64	Next Hop Directly Connected	Interface vlan1	Distance/Metric 0/1	Protocol 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

QoS メニューでは、優先制御に関する設定を行うことができます。

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

QoSの下にあるサブメニューの一覧を以下の表に示します。

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

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

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

7.1 Basic Settings

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

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

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

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					
Port Default CoS					
From Port Port1/0/1	To Port Port1/0/1	Default CoS Override 	○ None	Apply	
	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 Me	thod		
Port Scheduler Method			
From Port Port1/0/1	To Port Port1/0/1	Scheduler Method WRR Apply	
	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	

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

設定を適用するには、Applyボタンをクリックします。

7.1.3 Queue Settings

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

Queue Settings							
Queue Settings							
From Port To Port Port1/0/1 Port1/0/1	Queue ID WRR We	ight (0-127) WDRR Quan	tum (0-127)				
Port	Queue ID	WRR Weight	WDRR Quantum				
	0	1	1				
	1	1	1				
	2	1	1				
Port1/0/1	3	1	1				
i orthori	4	1	1				
	5	1	1				
	6	1	1				
	7	1	1				
	0	1	1				
	1	1	1				
	2	1	1				
Port1/0/2	3	1	1				
	4	1	1				
	5	1	1				
	6	1	1				
	7	1	1				

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。

本画面の各項目の説明を以下に示します。

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 to Queue Mapping	
CoS	Queue ID
0	2 🗸
1	0 🗸
2	1 🗸
3	3 💌
4	4
5	5 💌
6	6
7	7 💌
	Арріу

本画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。

7.1.5 Port Rate Limiting

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

Port Rate Limit	ting			
Port Rate Limiting				
From Port Port1/0/1	To Port Direction Port1/0/1 Input	Rate Limit Bandwidth (64-1000000) Percent (1-100) None	Kbps Burst Size (0-163) % Burst Size (0-163)	80) Kbyte 80) Apply
Dort		Input	Outpu	t
T OIL	Rate	Burst	Rate	Burst
Port1/0/1	No Limit	No Limit	No Limit	No Limit
Port1/0/2	No Limit	No Limit	No Limit	No Limit
Port1/0/3	No Limit	No Limit	No Limit	No Limit
Port1/0/4	No Limit	No Limit	No Limit	No Limit
Port1/0/5	No Limit	No Limit	No Limit	No Limit
Port1/0/6	No Limit	No Limit	No Limit	No Limit
Port1/0/7	No Limit	No Limit	No Limit	No Limit
Port1/0/8	No Limit	No Limit	No Limit	No Limit
Port1/0/9	No Limit	No Limit	No Limit	No Limit
Port1/0/10	No Limit	No Limit	No Limit	No Limit

本画面の各項目の説明を以下に示します。

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

7.1.6 Queue Rate Limiting

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

ueue Rate Limiting																
From Port To Port Queue ID Rate Limit Port1/0/1 Image: Constraint of the state of the st																
Queue0 Queue1 Queue2 Queue3 Queue4 Queue5 Queue6 Que								ue7								
Port	Min	Max														
	Rate															
Port1/0/1	No Li															
Port1/0/2	No Li															
Port1/0/3	No Li															
Port1/0/4	No Li															
Port1/0/5	No Li															
Port1/0/6	No Li															
Port1/0/7	No Li															
Port1/0/8	No Li															
Port1/0/9	No Li															
Port1/0/10	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。
	・ Min Bandwidth :キューの保証帯域を 64~1000000(Kbps)の範囲 で指定します。
	 Max Bandwidth:キューの制限帯域を 64 ~ 1000000 (Kbps)の 範囲で指定します。
	 Min Percent:キューの保証帯域をポートの帯域に対する百分率で 指定します。入力範囲は1~100(%)です。
	 Max Percent:キューの制限帯域をポートの帯域に対する百分 率で指定します。入力範囲は1~100(%)です。
	 None:選択したポートのキューの帯域制限を解除する場合に選択します。デフォルトでは、すべてのポートのすべてのキューでこの設定が選択されています。

7.2 Advanced Settings

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

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

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

DSCP 値によるクラシフィケーション

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

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

ポリシングの基本動作

本装置のポリシングでは、所定のトラフィックの帯域をモニタリングし、帯域の利用状況に応じて指 定したアクション実行します。アクションには、フレームの破棄、透過、および優先制御値の書き換 えがあります。

観測されたトラフィックは、帯域の利用状況に応じて 3 段階に分類されます。ポリシングの方式に よって分類方法は異なりますが、基本的には以下のトラフィックカラーに分類されます。

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

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

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

ポリシングの設定

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

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

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

7.2.1 DSCP Mutation Map

DSCP Mutation Map 画面では、DSCP の変換マップを設定します。これは、CoS の指標が DSCP 値の場合 に、DSCP 値のリマーキングを行う際に使用するプロファイルです。

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

P Mutation Map												
utation Name	nput DSCP List (0-63)	Output DSCP	(0-63)									
chars											Apply	
tal Entries: 1												
							Digiti	in ones				
Mutation Name	Digit in tens	0	1	2	3	4	5	6	7	8	9	
	00	0	1	2	3	4	5	6	7	8	9	
	10	11	11	12	13	14	15	16	17	18	19	
	20	20	21	22	23	24	25	26	27	28	29	
Name	30	30	31	32	33	34	35	36	37	38	39	Delete
	40	40	41	42	43	44	45	46	47	48	49	
	50	50	51	52	53	54	55	56	57	58	59	
		0.0	64	60	60							

本画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 an	nd Mutation Binding		
Port Trust State and Mu	tation Binding		
From Port Port1/0/1	To Port Port1/0/1	Trust State	DSCP Mutation Map 32 chars None Apply
Por	t	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	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。

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。

DSCP CoS Mapping				
DSCP CoS Mapping				
From Port Port1/0/1	To Port CoS Port1/0/1 V 0 V	DSCP List (0-63)		
Port	CoS	DSCP List		
	0	0-7		
	1	8-15		
	2	16-23		
Port1/0/1	3	24-31		
FOILINNT	4	32-39		
	5	40-47		
	6	48-55		
	7	56-63		
	0	0-7		
	1	8-15		
	2	16-23		
Port1/0/2	3	24-31		
1011102	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。

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。

CoS Color Mapping			~
CoS Color Mapping			
From Port To F Port1/0/1 V	Port CoS List (0-7)	Color Green 💌	Apply
Port	Color	CoS List	
	Green	0-7	
Port1/0/1	Yellow		
	Red		
	Green	0-7	
Port1/0/2	Yellow		
	Red		
	Green	0-7	
Port1/0/3	Yellow		
	Red		
	Green	0-7	
Port1/0/4	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。

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。

DSCP Color Mappin	Ig		~
DSCP Color Mapping			
From Port To F Port1/0/1 V Por	Port DSCP List (0-63)	Color Green	Apply
Port	Color	DSCP List	
	Green	0-63	
Port1/0/1	Yellow		
	Red		
	Green	0-63	
Port1/0/2	Yellow		
	Red	an na kana na k	noni nara noni nara noni n
	Green	0-63	
Port1/0/3	Yellow		
	Red		
in An an a nadionean maileana maileana an ai	Green	0-63	
Port1/0/4	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。

7.2.6 Class Map

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

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

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

Class Map			
Class Map Name	32 chars	Multiple Match Criteria Match A	Apply Apply
Total Entries: 2			
Class	Map Name	Multiple Match Criteria	
cla	ss-map	Match Any	Match Delete
clas	s-default	Match Any	Match Delete
			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
Class Map Name	クラスマップ名を 32 文字以内で入力します。
Multiple Match Criteria	ルールの照合基準(Match All / Match Any)を選択します。
• • • •	

クラスマップを登録するには、Apply ボタンをクリックします。

クラスマップにルールを追加・削除するには、Match ボタンをクリックします。

クラスマップ自体を削除するには、Deleteボタンをクリックします。

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

ass Map				_	_
Class Map Name	32 chars	Multiple Match Criteria	Match Any 🗸		Apply
Total Entries: 2					
Class Map Na	ame	Multiple Match Criteria			
class-map)	Match Any		Match	Delete
class-defau	lt	Match Any		Match	
			1/1	< < 1	> > G
Class Map Information					
Class Map Name	class-map				
Multiple Match Criteria	Match Any				
Match 802.1P	0				
Match Inner 802 1P	0				

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

Match Rule	
Class Map Name	class-map
Match:	
None	
 Specify 	
ACL Name	32 chars
O CoS List (0-7)	0,5-7
O DSCP List (0-63)	1,2,61-63
O Precedence List (0-7)	0,5-7
O Protocol Name	None
O VID List (1-4094)	1,3-5
	Back Apply

Match Rule画面の各項目の説明を以下に示します。

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

設定を適用するには、Applyボタンをクリックします。

前の画面に戻るには、Backボタンをクリックします。

7.2.7 Aggregate Policer

Aggregate Policer 画面では、集約ポリサーを設定します。集約ポリサーは、ポリシーマップに割り当てる共通プロファイルです。

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

Aggregate Policer					_		
Single Rate Settings	Two R	ate Settings					
Aggregate Policer Name			Avera (0-100	ge Rate * 00000)		Kbps	
Normal Burst Size (0-16384)		Kbyte	Maxin (0-163	um Burst Size 84)		Kbyte	
Conform Action	Transmit	✓ DSCP 1P	Excee	d Action	Transmit	✓ DSCP 1P	
Violate Action	None	✓ DSCP 1P	Color	Aware	Disabled	~	
* Mandatory Field						[Apply
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
					1/1	< < 1 >	> Go

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

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

設定を適用するには、Applyボタンをクリックします。

集約ポリサーを削除するには、Deleteボタンをクリックします。

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

Aggregate Policer				_	_	
Single Rate Settings	Two Rate Setting	IS				
Aggregate Policer Name *						
CIR * (0-1000000)	Kt	ops	Confirm Burst (0-16384))	Kbyte	
PIR * (0-10000000)	Kt	ops	Peak Burst (0-16384)		Kbyte	
Conform Action	Transmit 🔽 D	SCP 1P	Exceed Action	Drop	✓ DSCP	1P
Violate Action	Drop 🗸 D:	SCP 1P	Color Aware	Disabled	~	
* Mandatory Field						Apply
Total Entries: 1						
Name CIR Confirm Burs	st PIR Peak Burst	Conform Action	Exceed Action	Violate Action	Color Aware	
Name 5000 500	8000 800	Transmit	Drop	Drop	Disabled	Delete
					1/1 < < 1	> > Go

Two Rate Settings タブの各項目の説明を以下に示します。

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

設定を適用するには、Applyボタンをクリックします。

集約ポリサーを削除するには、Deleteボタンをクリックします。

7.2.8 Policy Map

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

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

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

Policy Map				
Create/Delete Policy Map				
Policy Map Name	32 chars			Apply
Traffic Policy				
Policy Map Name	32 chars	Class Map Name	32 chars	Apply
Total Entries: 1				
	Polic	cy Map Name		
		policy		Delete
			1/1 < <	1 > > Go
policy Rules				
	Class Map Name			
	class-map		Set Action Policer	Delete
			1/1 < <	1 > > Go

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

パラメーター	説明		
Policy Map Name	作成または削除するポリシーマップ名を 32 文字以内で入力します。		
 設定を適用するには、Apply ボタンをクリックします。			

Traffic Policyの各項目の説明を以下に示します。

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

設定を適用するには、Applyボタンをクリックします。

ポリシーマップを削除するには、Delete ボタンをクリックします。

ポリシーマップのテーブル上でいずれかのポリシーマップの行をクリックすると、ポリシーマップ上 で登録したすべてのクラスマップが表示されます。

トラフィックに対する追加のアクションを設定するには、Set Action ボタンをクリックします。 ポリシングの設定を登録するには、Policer ボタンをクリックします。

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

Policy Map				
Create/Delete Policy Map				
Policy Map Name	32 chars			Apply
, only map reame	52 61015			
Traffic Policy				
Policy Map Name	32 chars	Class Map Name	32 chars	Apply
Total Entries: 1				
	Dolicy	Man Name		_
	T OILCY T	olicy		Delete
	ч	oncy	1/1	
				GO
policy Rules				
	Class Map Name			
	class-map		Set Action Policer	Delete
			1/1 < <	1 > > Go
Policy Map Information				
Policy Map Name	policy			
Class Map Name	class-map			
set 802.1P	0			
police cir	200000			
police bc	1000			
police pir	100000			
police be	16000			
conform-action	Transmit			
exceed-action	Drop			
violate-action	Dron			

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

Set Action		
Policy Map Name Class Map Name	policy class-map	
Set Action		
⊖None		
 Specify 		
New Precedence (0-7)	None IPv4 only	
ONew DSCP (0-63)	None IPv4 only	
ONew CoS (0-7)	None	
ONew CoS Queue (0-7)	None	
		Back Apply

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

Set Action 画面の各項目の説明を以下に示します。

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。

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		
Policy Map Name	policy	
Class Map Name	class-map	
Police Action		
○ None		
 Specify 	Police 🗸	
Average Rate * (0-10000000)		Kbps
Normal Burst Size (0-16384)		Kbyte
Maximum Burst Size (0-16384)		Kbyte
Conform Action	Transmit 🗸	DSCP 1P
Exceed Action	Transmit 🗸	DSCP 1P
Violate Action	None	DSCP 1P
Color Aware	Disabled 🗸	
* Mandatory Field		
		Back Apply

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

Police Action 画面の各項目の説明を以下に示します。

前の画面に戻るには、Backボタンをクリックします。

7.2.9 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。

Policy Binding					
Policy Binding Settin	ng				
From Port Port1/0/1	To Port Port1/0/1	Direction	Policy Map Name 32 chars 	○ None	Apply
	Port		Direction	Policy Map Name	
	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				
F	Port1/0/10				

本画面の各項目の説明を以下に示します。

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

8 ACL

ACL メニューでは、アクセスコントロールリスト(ACL)の登録を行います。

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

ACLの下にあるサブメニューの一覧を以下の表に示します。

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

ACL プロファイル

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

本装置で指定できる ACL の種別は以下の通りです。

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

ACL 種別ごとの検査範囲と適用可能なモジュール

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

「IP ACL」、「IPv6 ACL」、「MAC ACL」は、フレームの検査対象を示します。「IP ACL」では IPv4 パケットを、「IPv6 ACL」では IPv6 パケットを、「MAC ACL」では原則として非 IP パケットを検査対 象とします。

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

ACLルール

ACL ルールは、フレームの合致する条件と、合致した場合のアクションを定めたものです。合致条件は、 ACL 種別に基づいて定めることができます。たとえば、標準 IP ACL の場合、特定の送信元や宛先 IP ア ドレスを合致条件に指定できますが、特定の MAC アドレスは合致条件に指定できません。 8 ACL | 8.1 ACL Configuration Wizard

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

物理ポートに適用する ACL プロファイルでは、許可(permit)と拒否(deny)のルールの組み合わせ でポリシーを構成し、物理ポートでの合致条件とアクションは ACL ルールに従います。

ACL による VLAN フィルター

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

適用 ACL プロファイル数

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

8.1 ACL Configuration Wizard

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

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-ACLの作成 / 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 Configuration Wizard	
ACL Configuration Wizard	
Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port	
Do you want to create a new ACL access-list or update an existing access-list?	
Create	
ACL Name 32 chars	
O Update	
	Next
Note: The first character of ACL name must be a letter.	

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 Configuration Wizard				
ACL Configuration Wizard				
Access-List A	Accase List Assignment 55 Solart Darkat Type 55 Add Rule 55 Annly Dort			
Do you want	to create a new ACL access-list or	update an existing access-list?		
 Create 				
ACL Name	e 32 chars			
 Update 				
			Next	
Note: The firs	st character of ACL name must be a le	etter.		
Total Entries:	Total Entries: 6			
	ACL Name	ACL Type	Total Rules	
0	S-IP4	Standard IP ACL	1	
•	E-IP4	Extended IP ACL	0	
0	E-MAC	Extended MAC ACL	0	
•	E-MAC Expert	Extended MAC ACL Extended Expert ACL	0 0	
•	E-MAC Expert S-IP6	Extended MAC ACL Extended Expert ACL Standard IPv6 ACL	0 0 0	
• • •	E-MAC Expert S-IP6 E-IP6	Extended MAC ACL Extended Expert ACL Standard IPv6 ACL Extended IPv6 ACL	0 0 0 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。

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 プロファイルを使用してルールを登録する場合に選択しま す。また、更新する ACL を一覧から選択します。

本画面の各項目の説明を以下に示します。

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。

ACL Configuration Wizard	
ACL Configuration Wizard	
Access-List Assignment >> <u>Select Packet Type</u> >> Add Rule >> Apply Port	
Which type of packet do you want to monitor?	
Extended MAC ACL	
⊖IPv4 ACL	
OExtended IPv4 ACL	
OIPv6 ACL	
OExtended IPv6 ACL	
OExpert ACL	
Back	Next

本画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。

uence No. (1-65535)		OAuto A	ssign		
MAC Address	Ethernet Type	802.1Q VLAN]		
MAC Address Any Host MAC Wildcar Ethernet Type Specify Ethernet Type Ethernet Type Mask (0 802.1Q VLAN	11-DF-36-4B-A7-CC 11-DF-36-4B-A7-CC 1 11-DF-36-4B-A7-CC Please Sele FFFF) x0-0xFFFF)	Any Any Output Destination MAC Wildca	11-DF-36-4B-A7-CC 11-DF-36-4B-A7-CC ard 11-DF-36-4B-A7-CC		
CoS Please Select /ID(1-4094) ction	ermit O Permit Authentica	ation-Bypass 🔿 Deny		Back	Next

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。

最初にステップ3に移行した段階では、Assign Rule Criteriaの領域にはAction以外の設定項目は表示されていません。最初に、フレームの検査対象を指定するために、MAC Address、Ethernet Type、 802.1Q VLAN のいずれかのボタンをクリックします。例えば、送信元 MAC アドレスを検査してアクションを指定する場合には、MAC Address のボタンをクリックします。検査対象が複数に渡る場合は、複数のボタンをクリックします。

該当するボタンをクリックすると、それぞれに対応した設定項目の欄が出現しますので、判定条件に 合致した設定を行います。

ASSION KUIE UTITETIA の合項日の説明を以下に示します	Assian	Rule	Criteria	の各項目	の説明をい	以下に示し	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。
	· 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。
	· 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。石のホックスに宛先 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-8042 / 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
	うなす。 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。

	Assignment >> Select Packet Type >>	Add Rule >> Apply Pe	ort	
ease assi	gn a sequence number to create a new	rule.		
Sequence	No. (1-65535)	OA	uto Assign	
Assign Ru	Ile Criteria			
IPv	4 Address			
IPv4 Add	iress			
	Any	Any		
	OHost · · ·		đ	
		Destination		
Source	OIP · · ·	OIP .		
Source	OIP · · · ·	UIP Wile	lcard	

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。

最初にステップ3に移行した段階では、Assign Rule Criteriaの領域にはAction以外の設定項目は表示されていません。フレームの IP アドレスを検査対象とする場合、IPv4 Address ボタンをクリックします。対応した設定項目の欄が出現しますので、判定条件に合致した設定を行います。

Assign	Rule	Criteria	の各項目の説明を以下に示します	f 。
--------	------	----------	-----------------	------------

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。
	· 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。
	 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。
	· 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。
	○ Wildcard: ワイルドカードビットマップを使用し、宛先 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。
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。
- - - - - - - - - - - - - -	ビクンキクリックレキオ

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。

Configuration Wizard						
ess-List Assignment >> S	elect Packet Type >> <u>A</u>	dd Rule >> Apply Port				
ase assign a sequence nu	mber to create a new ru	lle.				
equence No. (1-65535)		OAuto As	sign			
tocol Type	TCP	✓	(0-255) F	ragments		
ssign Rule Criteria						
IPv4 Address	Port	IPv4 DSCP	TCP Flag			
IPv4 Address						
Any		Any				
OHost	· · · · ·	O Host	and the second second			
	· · · · · · ·	OIP	· · · · · · ·			
Wildcard		Wildcare				
Port						
Source Port Please	Select 🔽					
Please	Select 🔽	(0-65535) Please	Select 🖌	(0-65535)		
Destination Port Please	Select 🔽					
Please	Select 🗸	(0-65535) Please	Select 🗸	(0-65535)		
IPv4 DSCP						
IP Precedence Please	e Select 🗸 ToS Ple	ease Select 🗸				
ODSCP (0-63) Please	e Select 🗸					
TCP Flag						
TCP Flag ack fin	pshrstsynurg					
Action	mit 🔘 Permit Authen	ication-Bypass O Deny				
					Back	Next

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。
	 Value: プロトコル ID を手動で入力する場合、0~255 の範囲で入 力です。
	 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。

最初にステップ3に移行した段階では、Assign Rule Criteriaの領域にはAction以外の設定項目は表示されていません。最初に、フレームの検査対象を指定するために、IPv4 Address、Port、IPv4 DSCP、 TCP Flag のいずれかのボタンをクリックします。該当するボタンをクリックすると、それぞれに対応した設定項目の欄が出現しますので、判定条件に合致した設定を行います。

Assign Rule Criteria の谷頃目の詋明を以卜に示しま

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送信元 IPv4 アドレスを入力します。
	· 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。 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。
	 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	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。
	· 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。
	○ 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	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。
	· =: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。 =: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たい提合は、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	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。
	フロトコルタイフ ICMP でのみ使用できます。
Message Code	ICMP Message Type か選択されていない場合に、メッセーショードの数 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 優先順位(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))を迭折します。
DOUP	(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。
	 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 Conf	iguration Wiz	ard	_	_		_	_	
ACL Configu	ration Wizard							
Access-Lis	Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Port							
Please ass	ign a sequence n	umber to create a new rul	e.					
 Sequence 	e No. (1-65535)		(Auto Assign				
- Assian R	ule Criteria			-				
Assign K	ule Criteria							
IP	/6 Address							
IDv6 Ad	draee							
IF VU AU	Any			 Any 				
	OHost	2012::1		OHost	2012::1			
Source	O IPv6	2012::1	Destination	OIPv6	2012::1			
	Prefix Lengt	h		Prefix Len	gth			
Action	 Permi 	it 🔿 Permit Authenticatio	on-Bypass 🔘	Deny				
							Back	Next

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。

最初にステップ3に移行した段階では、Assign Rule Criteriaの領域にはAction以外の設定項目は表示されていません。フレームの IPv6 アドレスを検査対象とする場合、IPv6 Address ボタンをクリックします。対応した設定項目の欄が出現しますので、判定条件に合致した設定を行います。

Assign Rule Criteriaの各項目の説明をし	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。
	· 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 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。
	· 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。
	 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。
☆の壬岐にウスには Bask =	

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	
ACL Configuration Wizard	
Access-List Assignment >> Select Packet Type >> <u>Add Rule</u> >> Apply Port	
Please assign a sequence number to create a new rule.	
Sequence No. (1-65535) OAuto Assign	
Protocol Type TCP (0-255) Fragments	
Assign Rule Criteria	
IPv6 Address Port IPv6 DSCP TCP Flag Flow Label	
IPv6 Address	
Any	
O Host 2012:::1 O Host 2012:::1	
OIPv6 2012::1 OIPv6 2012::1	
Prefix Length Prefix Length	
Port	
Source Port Please Select	
Please Select V (0-65535) Please Select V (0-65535)	
Destination Port Please Select V	
Please Select V (0-65535) Please Select V (0-65535)	
IPv6 DSCP	
DSCP (0-63) Please Select	
TCP Flag	
ICP Flag_jacktinpshrstsynurg	
Flow Label	
Action • Permit Autoentication-Bypass • Deny	ack Next

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 ルール番号を目動で生成するには、Auto Assign を選択します。
Protocol Type	プロトコルタイプ(TCP / UDP / ICMP / Protocol ID / ESP (50) / PCP (108) / SCTP (132) / None)を選択します。 · Value:手動でプロトコル ID を入力する場合、0~255の範囲で入 カレます
	・ 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。

最初にステップ3に移行した段階では、Assign Rule Criteriaの領域にはAction以外の設定項目は表示されていません。最初に、フレームの検査対象を指定するために、IPv6 Address、Port、IPv6 DSCP、 TCP Flag、Flow Label のいずれかのボタンをクリックします。該当するボタンをクリックすると、それぞれに対応した設定項目の欄が出現しますので、判定条件に合致した設定を行います。

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。
	· 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 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。
	· 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。
	 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	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。
	· =: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。
	· =: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	ICMP メッセージタイプを選択します。
Туре	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。
	フロトコルタイフ 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。
IPv6 DSCP	DSCP 值 (default (0) / af11 (10) / af12 (12) / af13 (14) / af21
	(18) / af22 (20) / af23 (22) / af31 (26) / af32 (28) / af33 (30)
	$/$ at 41 (34) / at 42 (36) / at 43 (38) / cs1 (8) / cs2 (16) / cs3 (24) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef (46)) \overline{z}
	· 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。
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。

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 W	izard					
ACL Configuration Wizard						
Access-List Assignment >>	Select Packet Type >> A	dd Rule >> Apply Port				
Please assign a sequence n	umber to create a new ru	ıle.				
Sequence No. (1-65535)	TOD	OAuto As	sign			
Protocol Type	TCP	~	(0-255)	Fragments		
Assign Rule Chiena						
IPv4 Address	MAC Address	Port	IPv4 DSCP	TCP Flag	802.1Q VLAN	
IDv/ Address						
 Any 		Any				
OHost		OHost				
Source		Destination OIP				
Wildcard		Wildcar	d			
MAC Address						
 Any 		 Any 		_		
OHost	11-DF-36-4B-A7-CC	OHost	11-DF-36-4B-A7-CC			
OMAC	11-DF-36-4B-A7-CC	OMAC	11-DF-36-4B-A7-CC]		
Wildcard	11-DF-36-4B-A7-CC	Wildca	rd 11-DF-36-4B-A7-CC]		
Port						
Source Port Please	e Select 🗸					
Please	e Select 🗸	(0-65535) Please	Select 🗸	(0-65535)		
Destination Port Please	e Select 🗸					
Please	e Select 🔽	(0-65535) Please	Select V	(0-65535)		
ID: 4 DSCD						
IPV4 DSCP	sa Salact V Tas Pla	asa Salact				
TCP Flag	Deb First Flown Flura					
	panaynurg					· · · · · ·
902 10 VI AN						
Or O Diseas Calast						
Cos Please Select						
VID(1-4094)						
Action P	ermit O Permit Authent	tication-Bypass 🔿 Deny				
					Back Nex	t.
						v

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(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。
	 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:ハクットノラクメノトノイルダリンクを含める場合に チェックします。

最初にステップ3に移行した段階では、Assign Rule Criteriaの領域にはAction以外の設定項目は表示されていません。最初に、フレームの検査対象を指定するために、IPv4 Address、MAC Address、 Port、IPv4 DSCP、TCP Flag、802.1Q VLAN のいずれかのボタンをクリックします。該当するボタンを クリックすると、それぞれに対応した設定項目の欄が出現しますので、判定条件に合致した設定を行 います。

Assian	Rule	Criteria	の各項目の説明を以下に示します。
лээтуп	Nule	Uniteria	

パラメーター	説明
Source IPv4 Address	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。
	· 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。
	○ 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	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
Address	正に必要な場合は宛先 IPV4 アドレスを入力します。
	・ Host : 宛元 ホストの IPv4 アト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。
	 ○ 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	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。
	· 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 アドレスとワイルドカード値を入力しま す。

Destination MAC Address	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。
	· 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	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
	てきより。
	 ・>: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。
	 く: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。
	・ =: 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。
	 く: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	ICMP メッセージタイプを選択します。
Туре	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 ICMP でのみ使用できます
Massage Code	ノローコルフィノ IUMF Cのの使用できます。 ICMP Massang Tung が選択されていたい提合に、マッセージョードの物
พธรรสมุข บบนช	
	ICMP Message Type を選択すると、数値が目動で入力されます。 プロトコルタイプ ICMP でのみ使用できます。

IP Precedence	IP 優先順位(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。
	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。

ACL Configuration Wizard	
ACL Configuration Wizard	
Access-List Assignment >> Select Packet Type >> Add Rule >> <u>Apply Port</u> Which port(s) do you want to apply the Access-List?	
From Port To Port Direction Port1/0/1 Port1/0/1 In	Back 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
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。

i i jpe					AGE Name 52 chai	3		Tinu
tal Entrie	s: 6						[Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	S-IPv4	Standard IP ACL	10	10	Disabled		Edit	Delete
2000	E-IPv4	Extended IP ACL	10	10	Disabled		Edit	Delete
6000	MAC	Extended MAC ACL	10	10	Disabled		Edit	Delete
8000	Expert	Extended Expert ACL	10	10	Disabled		Edit	Delete
11000	S-IP6	Standard IPv6 ACL	10	10	Disabled		Edit	Delete
13000	E-IP6	Extended IPv6 ACL	10	10	Disabled		Edit	Delete
						1/1	< < 1 >	>
					Clea	r All Counter	Clear Counter	Add Rule
Sequen	ce No.	Action	Rule			Counter		

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

以下は、ACL プロファイルのテーブル上で一番上の行をクリックした例です。

CL Access	List							
ACL Type	All	• ID (1-14999)		O A	CL Name 32 chars			Find
otal Entrie	s: 6						[Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	S-IP4	Standard IP ACL	10	10	Disabled		Edit	Delete
2000	E-IP4	Extended IP ACL	10	10	Disabled		Edit	Delete
6000	MAC	Extended MAC ACL	10	10	Disabled		Edit	Delete
8000	Expert	Extended Expert ACL	10	10	Disabled		Edit	Delete
11000	S-IP6	Standard IPv6 ACL	10	10	Disabled		Edit	Delete
13000	E-IP6	Extended IPv6 ACL	10	10	Disabled		Edit	Delete
						1/1 <	< 1 >	Go
6-IP4 (ID: 1)	Rule				Clear	All Counter C	lear Counter	Add Rule
Sequen	ce No.	Action	Rule		C	Counter		
10)	Permit	any any	any any				Delete
1/1 K < 1 > > Go								
ac Access-	List Enable IP-Pa	ckets						
Mae Assess List Feeble IB Baskete Okto								

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(AII / 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。

ACL Access List の各項目の説明を以下に示します。

入力した情報で ACL プロファイルを検索するには、Find ボタンをクリックします。

ACL プロファイルを作成するには、Add ACL ボタンをクリックします。

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

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

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

設定を適用するには、Applyボタンをクリックします。

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

CL Ac	cess List			_		_	_	
CL Acc	ess List							
ACL Typ	e All		(1-14999)		O ACL Name 32	chars	[Find
fotal En	ntries: 6						[Add ACL
ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
1	S-IP4	Standard IP ACL	10	10	Disabled 🗸		Apply	Delete
2000	E-IP4	Extended IP ACL	10	10	Disabled		Edit	Delete
6000	MAC	Extended MAC ACL	10	10	Disabled		Edit	Delete
8000	Expert	Extended Expert ACL	10	10	Disabled		Edit	Delete
11000	S-IP6	Standard IPv6 ACL	10	10	Disabled		Edit	Delete
13000	E-IP6	Extended IPv6 ACL	10	10	Disabled		Edit	Delete
						1/1	< < 1 >	>

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。

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。

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。

Apply

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			
	· Standard IP ACLの場合、1~1999の範囲で入力します。		
	· Extended IP ACLの場合、2000~3999の範囲で入力します。		
	· Standard IPv6 ACLの場合、11000~12999の範囲で入力します。		
	· Extended IPv6 ACLの場合、13000~14999の範囲で入力します。		
	· Extended MAC ACLの場合、6000~7999の範囲で入力します。		
	・ Extended Expert ACLの場合、8000~9999の範囲で入力します。		
ACL Name	ACL 名を 32 文字以内で入力します。		

設定を適用するには、Applyボタンをクリックします。

8.2.1 IP ACL

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

Add ACL Rule	
Add ACL Rule	
ID ACL Name ACL Type Sequence No. (1-65535) Action	1 S-IP4 Standard IP ACL (If it isn't specified, the system automatically assigns.) Permit O Permit Authentication-Bypass O Deny
Match IP Address	
Any	Any
OHost .	· · · · · ·
Source OIP ·	
Wildcard .	· · · · · · · · · · · · · · · · · · ·
	Back Apply

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

Add ACL Rule			
Add ACL Rule			
ID ACL Name ACL Type	2000 E-IP4 Extended IP ACL		
Action	Permit O Permit Authentication-Rypass O Deny		
Protocol Type	TCP (0-255) Fragments		
Match IP Address			
• Any • Any • Host • Chost • Chost			
Match Port Source Port Please Select			
Please Select	✓ (0-65535) Please Select ✓ (0-65535)		
Destination Port Please Select			
Please Select	✓ (0-65535) Please Select ✓ (0-65535)		
TCP Flag	ackfinpshrstsynurg		
IP Precedence Please Select ODSCP (0-63) Please Select	ToS Please Select V		
	Back Apply		

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

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

パラメーター	説明
Sequence No.	ACL ルールのシーケンス番号を 1~65535 の範囲で入力します。指定し
	ない場合、自動採番のルールに従って自動的に生成します。
Action	すべての条件に合致した IPv4 パケットに対するアクション(Permit /
	Permit Authentication-Bypass / Deny)を選択します。
Protocol Type	拡張 IP ACL の場合に表示されます。
	条件とするプロトコルをドロップダウンリストから選択します。手動で
	フロトコル番号を指定する場合、Protocol IDを選択します。Noneを選
	· Fragments: フラクスノドされたバグッドを指定します。
Source	送信元 IPv4 アドレスの条件を設定します。また、条件を指定するため の IPv4 アドレスやワイルドカードマスクを入力します。
	· Any:すべての送信元ホストを合致条件とします。
	・ Host:指定した送信元 IPv4 アドレスを条件とします。
	· IP:指定した送信元 IPv4 アドレスグループを条件とします。IPv4
	アドレスとワイルドカードマスクの組み合わせで指定します。
	○ Wildcard:ワイルドカードマスクを指定します。
Destination	宛先 IPv4 アドレスの条件を設定します。また、条件を指定するための
	IPv4 アドレスやワイルドカードマスクを入力します。
	· Any:すべての宛先ホストを合致条件とします。
	・ Host:指定した宛先 IPv4 アドレスを条件とします。
	· IP:指定した宛先 IPv4 アドレスグループを条件とします。 IPv4 ア
	ドレスとワイルドカードマスクの組み合わせで指定します。
	○ Wildcard : ワイルドカードマスクを指定します。
IP Precedence	拡張 IP ACL の場合に表示されます。
	IP Precedence 値の条件を(routine (0) / priority (1) / immediate
	(2) / TIASN (3) / TIASN-OVERFICE (4) / CRITICAL (5) / INTERNET
	(0) / hethork (7) / Chile Ce より。 医穴のない場合、 11 / recedence
ToS	拡張 IP ACL の場合に表示されます。
	ToS 値の条件を(normal (0) / min-monetary-cost (1) / max-
	reliability (2) / max-throughput (4) / min-delay (8)) で指定でき
	ます。選択しない場合、ToS 値を判定条件としません。
DSCP	拡張 IP ACL の場合に表示されます。
	DSCP 値の条件を (default (0) / af11 (10) / af12 (12) / af13 (14)
	/ at21 (18) / at22 (20) / at23 (22) / at31 (26) / at32 (28) / at33 (30) / at41 (34) / at42 (36) / at43 (38) / cc1 (8) / cc2
	(16) / cs3 (24) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef
	(46))で指定できます。選択しない場合、手動で DSCP 値の条件を指定
	できます。DSCP 値が指定されていない場合、DSCP 値を判定条件としま
	せん。

設定を適用するには、Applyボタンをクリックします。

前の画面に戻るには、Backボタンをクリックします。

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

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

パラメーター	前明
Source Port	プロトコル条件が TCP または UDP の場合のみ表示されます。 送信元 TCP/UDP ポート番号の条件を設定します。また、条件を指定する ためのポート番号を入力します。ドロップダウンリストで上位プロトコ ルを選択すると、ウェルノウンポートが自動的に入力されます。条件を 指定しない場合、送信先 TCP/UDP ポート番号を判定条件としません。 ・ =:指定したポート番号と一致する場合を条件とします。 ・ >:指定したポート番号より大きい場合を条件とします。 ・ :指定したポート番号より小さい場合を条件とします。 ・ :指定したポート番号と一致しない場合を条件とします。 ・ :指定したポート番号と一致しない場合を条件とします。
Destination Port	プロトコル条件が TCP または UDP の場合のみ表示されます。
	宛先 TCP/UDP ポート番号の条件を設定します。また、条件を指定するためのポート番号を入力します。ドロップダウンリストズト位プロトフリ
	めのホート留号を八刀します。トロックタワクリストでエ位ノロトコル を選択すると、ウェルノウンポートが自動的に入力されます。条件を指
	定しない場合、宛先 TCP/UDP ポート番号を判定条件としません。
	ポート番号の条件の指定方法(= / > / < / / Range)は、Source
Specify ICMP Message	POTTと同してす。 プロトコル冬件がICMPの提合のみ表示されます
Type	ICMP メッセージの条件をメッセージの種類で指定します。メッセージ
	タイプやメッセージコードは自動的に入力されます。指定しない場合、
	メッセージタイプとメッセージコードを手動で入力できます。
ICMP Message Type	プロトコル条件が ICMP の場合のみ表示されます。
	ICMP メッセージタイプの条件を設定します。指定されていない場合、
Nacasa Cada	TOMP スツセージの種類を判定宗件としません。 プロトコリ条件が IOMP の担合のユミニされます
message code	ノロトコル宗性がTOMPの場合のの表示されます。 ICMP メッセージコードの条件を設定します。指定されていたい場合
	ICMP メッセージコードを判定条件としません。
TCP Flag	プロトコル条件が TCP の場合のみ表示されます。
-	TCP フラグ(ack / fin / psh / rst / syn / urg)を判定条件としま
	す。チェックされていない TCP フラグは判定条件としません。

設定を適用するには、Applyボタンをクリックします。

前の画面に戻るには、Backボタンをクリックします。

8.2.2 IPv6 ACL

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

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	ermit O Permit	rmit Authentica	ation-Bypass	 Deny 		
Match IPv6 Address						
Any			 Any 			
OHost	2012::1		OHost	2012::1		
Source OIPv6	2012::1	Destination	◯ IPv6	2012::1		
Prefix Le	ngth		Prefix Leng	gth		
					Back	Apply

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

Add ACL Rule	
Add ACL Rule	
ID ACL Name ACL Type Sequence No. (1-65535) Action Protocol Type	13000 E-IP6 Extended IPv6 ACL (If it isn't specified, the system automatically assigns.) Permit O Permit Authentication-Bypass O Deny TCP V (0-255) Fragments
Match IPv6 Address Any OHost 2012::1 Source IPv6 2012::1 Prefix Length	Any OHost 2012::1 IPv6 2012::1 Prefix Length
Match Port Source Port Please Select V Please Select V Destination Port Please Select V	(0-65535) Please Select 💙 (0-65535)
Please Select TCP Flag DSCP (0-63) Flow Label (0-1048575)	Image: Constraint of the second se
	Back Apply

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

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

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1場合、自動採番のルールに従って自動的に生成します。Actionずべての条件に合致した IPv6 パケットに対するアクション(Permit / Permit Authentication-Bypass / Deny)を選択します。Protocol Type拡張 IPv6 ACL の場合に表示されます。 条件とするプロトコルをドロップダウンリストから選択します。手動で プロトコル番号を指定する場合、Protocol IDを選択します。 キャンクロシンストから選択します。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。 ・ Any: すべての送信元ホストを合数条件とします。 ・ Host: 指定した送信元 IPv6 アドレスグループを条件とします。 ・ Host: 指定した送信元 IPv6 アドレスグループを条件とします。 ・ Prof: 指定した送信元 IPv6 アドレスグループを条件とします。 ・ Nore デレスングレフィックス長を入力します。 ・ Nore デビスやプレフィックス長を入力します。 ・ Prof: 指定した逆に見て、IPv6 アドレスを条件とします。 ・ IPv6 アドレスクジレーブを条件とします。 ・ Prof: 活定した宛先 IPv6 アドレスグループを条件とします。 ・ Host: 活定した宛先 IPv6 アドレスグループを条件とします。 ・ Nore: 古宅したジロフィックス長を入力します。 ・ Any: すべての宛先ホストを合致条件とします。 ・ Nose: 活定した宛先 IPv6 アドレスグループを条件とします。 ・ Prof: 活定した宛先 IPv6 アドレスグループを条件とします。 ・ Nose: 活定したごりフィックス長を入力します。 ・ Prof: 活定した宛先 IPv6 アドレスグループを条件とします。 ・ Nose: 活定した宛先 IPv6 アドレスグループを条件とします。 ・ Profix Length: ブレフィックス長を入力します。 ・ Profix Length: ブレフィックス長を小力します。 (Add)) af11 (10) / af12 (12) / af13 (14) / af21 (18) / af22 (20) / af33 (30) / af31 (26) / af32 (28) / af33 (30) / af31 (31) / cs1 (6) / cs3 (24) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef (46)) で指定できます。 ボボロい場合、SDCP 値が指定されていない場合、SDCP 値が指定されていない場合、SDCP 値が指定されていない場合、SDCP 値を指定できま。 ・ DSCP 値の条件を (detault (0) / af12 (12) / af13 (14) / af21 (18) / af22 (20) / af33 (30) / cs1 (6) / cs3 (24) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef (46)) で指定できま。 オーのメル値を判定条件としません。Flow Label拡張 IPv6 ACL の場合に表示されます。 アローラベル値を判定条件としません。	パラメーター	説明
Actionすべての条件に合致した IPv6 パケットに対するアクション (Permit / Permit Authentication-Bypass / Deny)を選択します。Protocol Type拡張 IPv6 ACL の場合に表示されます。 条件とするプロトコルをドロップダウンリストから選択します。smで プロトコル番号を指定する場合、Protocol ID を選択します。None を選 択した場合、プロトコルを判定条件としません。 ・ Fragments: フラグメントされたパケットを指定します。Source送信元 IPv6 アドレスの条件を設定します。また、条件を指定するため の IPv6 アドレスやプレフィックス長を入力します。 ・ Host : 指定した送信元 IPv6 アドレスを条件とします。 ・ Host : 指定した送信元 IPv6 アドレスクシーンスを条件とします。 ・ Host : 指定した送信元 IPv6 アドレスクシーンスを条件とします。 ・ Host : 指定した送信元 IPv6 アドレスクシーンスを条件とします。 ・ IPv6 アドレスとプレフィックス長を入力します。 ・ Not : 指定した効先 IPv6 アドレスクループを条件とします。 ・ IPv6 アドレスやプレフィックス長を入力します。Destination宛先 IPv6 アドレスの条件を設定します。また、条件を指定するための IPv6 アドレスやプレフィックス長を入力します。 ・ Any: すべての宛先亦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。 ・ SCPDSCP拡張 IPv6 ACL の場合に表示されます。 DSCP 値の条件を (default (0) / af11 (10) / af12 (12) / af13 (14) / af21 (18) / af22 (20) / af33 (30) / cs1 (8) / cs2 (16) / cs3 (24) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef (46)) C指定できます。 アローラベル値を判定条件としますん。Flow Label拡張 IPv6 ACL の場合に表示されます。 の気件を公式のよう の条件をします。 アローラベル値 (0 ~ 1048575) の条件を入力します。指定しない場合は フローラベル値を判定条件としますん。	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。
Protocol Type 拡張 IPv6 ACL の場合に表示されます。 条件とするブロトコルをドロップダウンリストから選択します。手動で ブロトコル番号を指定する場合、Protocol ID を選択します。None を選 択した場合、ブロトコルを料定条件としません。 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 アドレスの条件を設定します。また、条件を指定するため。 Any:すべての送信元ホストを合数条件とします。 Host:指定した送信元 IPv6 アドレスの条件を設定します。 Nost:指定した送信元 IPv6 アドレスを条件とします。 Profix Length:ブレフィックス長の組み合わせて指定します。 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:指定した送信元 IPv6 アドレスグループを条件とします。 Nost:指定した送信元 IPv6 アドレスグループを条件とします。 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:指定した送信元 IPv6 アドレスグループを条件とします。 IPv6:指定した送信元 IPv6 アドレスグループを条件とします。 Nost:指定した送信元 IPv6 アドレスグループを条件とします。 Pv6 アドレスやブレフィックス長を入力します。 Nost:指定した完先 IPv6 アドレスグループを条件とします。 IPv6:指定した完先 IPv6 アドレスグループを条件とします。 OSCP 拡張 IPv6 ACL の場合に表示されます。 DSCP 値の条件を (default (0) / af11 (10) / af12 (12) / af13 (14) / af33 (30) / af41 (34) / af42 (36) / af43 (38) / cs1 (8) / cs2 (16) / cs3 (24) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef (46)) Cf指定できます。選択しない場合、DSCP 値を指定できます。 Flow Label 拡張 IPv6 ACLの場合に表示されます。 They Act の場合に表示されます。 フローラベル値 (0 ~ 1048575) の条件を入力します。指定しない場合は フローラベル値を測定条件としません。	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。 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 アドレスを条件とします。 IPv6 アドレスとブレフィックス長の組み合わせで指定します。 o Prefix Length:プレフィックス長を入力します。 Pv6 アドレスとブレフィックス長の組み合わせで指定します。 o Prefix Length:プレフィックス長を入力します。 Pv6 アドレスやプレフィックス長を入力します。 Any:すべての宛先ホストを合致条件とします。 IPv6 アドレスやプレフィックス長を入力します。 Pv6 アドレスやプレフィックス長を入力します。 IPv6: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。 Nost:指定した宛先 IPv6 アドレスグループを条件とします。 Pv6:指定した宛先 IPv6 アドレスグループを条件とします。 OBSCP 拡張 IPv6 ACL の場合に表示されます。 DSCP 値の条件を (default (0) / af11 (10) / af12 (12) / af13 (14) / af22 (20) / af33 (30) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef (46)) で指定できます。選択しない場合、JSCP 値を指定できます。 Flow Label 拡張 IPv6 ACL の場合に表示されます。 They Acl の場合に表示されます。 Tu-ラベル値 (0~1048575) の条件を入力します。指定しない場合は Tu-ラベル値を判定条件としません。	Protocol Type	拡張 IPv6 ACL の場合に表示されます。 条件とするプロトコルをドロップダウンリストから選択します。手動で プロトコル番号を指定する場合、Protocol ID を選択します。None を選 択した場合、プロトコルを判定条件としません。 Fragments:フラグメントされたパケットを指定します。
Destination 宛先 IPv6 アドレスの条件を設定します。また、条件を指定するための IPv6 アドレスやプレフィックス長を入力します。 Any:すべての宛先ホストを合致条件とします。 Host:指定した宛先 IPv6 アドレスを条件とします。 IPv6:指定した宛先 IPv6 アドレスグループを条件とします。 OPv6:指定した宛先 IPv6 アドレスグループを条件とします。 Pv6:指定した宛先 IPv6 アドレスグループを条件とします。 OPv6:指定した宛先 IPv6 アドレスグループを条件とします。 Pv6:指定した宛先 IPv6 アドレスグループを条件とします。 OPv6:指定した宛先 IPv6 アドレスグループを条件とします。 Pv6:指定した宛先 IPv6 アドレスグループを条件とします。 OPv6:指定した宛先 IPv6 アドレスグループを条件とします。 OPv6:指定した宛先 IPv6 アドレスグループを条件とします。 OPv6:指定した宛先 IPv6 アドレスグループを条件とします。 DSCP 拡張 IPv6 ACL の場合に表示されます。 DSCP 値の条件を (default (0) / af11 (10) / af12 (12) / af13 (14) / af21 (18) / af22 (20) / af23 (22) / af31 (26) / af32 (28) / af33 (30) / af41 (34) / af42 (36) / af43 (38) / cs1 (8) / cs2 (16) / cs3 (24) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef (46)) で指定できます。選択しない場合、手動で DSCP 値を指定できます。 DSCP 値が指定されていない場合、DSCP 値を判定条件としません。 Flow Label 拡張 IPv6 ACL の場合に表示されます。 フローラベル値 (0 ~ 1048575) の条件を入力します。指定しない場合は フローラベル値を判定条件としません。	Source	 送信元 IPv6 アドレスの条件を設定します。また、条件を指定するための IPv6 アドレスやプレフィックス長を入力します。 Any:すべての送信元ホストを合致条件とします。 Host:指定した送信元 IPv6 アドレスを条件とします。 IPv6:指定した送信元 IPv6 アドレスグループを条件とします。 IPv6 アドレスとプレフィックス長の組み合わせで指定します。 Prefix Length:プレフィックス長を入力します。
DSCP 拡張 IPv6 ACL の場合に表示されます。 DSCP 値の条件を(default (0) / af11 (10) / af12 (12) / af13 (14) / af21 (18) / af22 (20) / af23 (22) / af31 (26) / af32 (28) / af33 (30) / af41 (34) / af42 (36) / af43 (38) / cs1 (8) / cs2 (16) / cs3 (24) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef (46)) で指定できます。選択しない場合、手動で DSCP 値を指定できます。DSCP 値が指定されていない場合、DSCP 値を判定条件としません。 Flow Label 拡張 IPv6 ACL の場合に表示されます。 フローラベル値 (0~1048575) の条件を入力します。指定しない場合は フローラベル値を判定条件としません。	Destination	 宛先 IPv6 アドレスの条件を設定します。また、条件を指定するための IPv6 アドレスやプレフィックス長を入力します。 Any: すべての宛先ホストを合致条件とします。 Host:指定した宛先 IPv6 アドレスを条件とします。 IPv6:指定した宛先 IPv6 アドレスグループを条件とします。IPv6 アドレスとプレフィックス長の組み合わせで指定します。 o Prefix Length:プレフィックス長を入力します。
Flow Label 拡張 IPv6 ACL の場合に表示されます。 フローラベル値(0~1048575)の条件を入力します。指定しない場合は フローラベル値を判定条件としません。	DSCP	拡張 IPv6 ACL の場合に表示されます。 DSCP 値の条件を (default (0) / af11 (10) / af12 (12) / af13 (14) / af21 (18) / af22 (20) / af23 (22) / af31 (26) / af32 (28) / af33 (30) / af41 (34) / af42 (36) / af43 (38) / cs1 (8) / cs2 (16) / cs3 (24) / cs4 (32) / cs5 (40) / cs6 (48) / cs7 (56) / ef (46)) で指定できます。選択しない場合、手動で DSCP 値を指定できま す。DSCP 値が指定されていない場合、DSCP 値を判定条件としません。
	Flow Label	拡張 IPv6 ACL の場合に表示されます。 フローラベル値 (0~1048575)の条件を入力します。指定しない場合は フローラベル値を判定条件としません。

設定を適用するには、Applyボタンをクリックします。

前の画面に戻るには、Backボタンをクリックします。

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

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

設定を適用するには、Applyボタンをクリックします。

前の画面に戻るには、Backボタンをクリックします。

8.2.3 拡張 MAC ACL

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

Add ACL Rule	
Add ACL Rule	
ID 6000 ACL Name MAC ACL Type Exten Sequence No. (1-65535) Action • P	Inded MAC ACL (If it isn't specified, the system automatically assigns.) (ermit Permit Authentication-Bypass Deny
OHost 11-DF-30 Source OMAC 11-DF-30 Wildcard 11-DF-30	6-4B-A7-CC OHost 11-DF-36-4B-A7-CC 0-Hast 11-DF-36-4B-A7-CC 0-Hast 11-DF-36-4B-A7-CC 0-Hast 11-DF-36-4B-A7-CC 0-Hast 11-DF-36-4B-A7-CC
Match Ethernet Type Specify Ethernet Type Ethernet Type (0x0-0xFFFF) Ethernet Type Mask (0x0-0xFFFF CoS Please Select VID(1-4094)	Please Select

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

本画面の各項目の説明を以下に示します。

_____ 設定を適用するには、Apply ボタンをクリックします。

前の画面に戻るには、Back ボタンをクリックします。

8.2.4 拡張エキスパート ACL

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

Add ACL Rule
Add ACL Rule B000 ID 8000 ACL Name Expert ACL Type Extended Expert ACL Sequence No. (1-65535) (If it isn't specified, the system automatically assigns.) Action Permit O Permit Authentication-Bypass O Deny Protocol Type TCP (0-255) Fragments
Imatch if Address Imatch if Address Imatch if Address Imatch if Addres Imatch if Address <
Match MAC Address • Any
Match Port Source Port Please Select O(-65535) Pleas
 ● IP Precedence Please Select ▼ ToS Please Select ▼ ● DSCP (0-63) Please Select ▼
TCP Flagackfinpshrstsynurg VID(1-4094) CoS Please Select V

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

8.3 ACL Interface Access Group

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

ACL Interface A	Access Group)						
ACL Interface Acce	ess Group							
From Port Port1/0/1	To Port Port1/0/1	Direction	Action Add	Type IP ACL 🔽	ACL Name	Please Select	Appl	ly
Port					In			
POIL		IP ACL	IF	Pv6 ACL	MAC	ACL	Expert ACL	
Port1/0/1								
Port1/0/2	ilike da telateta telateta tela tela. 		a 168 da ista ista ista ista ista ista S.		29-lahdahdahdahdahdahdahda		ta international e la tratación de la terraria de l	
Port1/0/3								
Port1/0/4								
Port1/0/5								
Port1/0/6	2009) je so na far far far far far far far far far				64 gelerlerlerlerbeiteterlerler		yan barbarbarbarbarbarbarbarbarbarbarbarbarb	
Port1/0/7								
Port1/0/8							n gan ban ban ban ban ban ban ban ban ban b	
Port1/0/9								
Port1/0/10								

本画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。
Туре	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。

	ID	ACL Name	ACL Type
0	1	S-IP4	Standard IP ACL
•	2000	E-IP4	Extended IP ACL
			1/1 < < 1 > >

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。

ACL VLAN Access N	lap							
ACL VLAN Access Map								
Access Map Name Sub Map Number (1-65538 Action	32 chars 5) Forward							Apply
Access Map Name	32 chars		Counter State	Disabled	~			Apply
Access Map Name	32 chars					Clear All Counter	Clear Counter	Find
Total Entries: 1								
Access Map Name	Sub Map Number	Action	Ma	tch Access-List		Counter State		
Мар	1	Forward				Disabled	Binding	Delete
						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
Access Map Name	VLAN アクセスマップ名を 32 文字以内で入力します。
Sub Map Number	サブマップ番号を1~65535 の範囲で入力します。
Action	実行するアクション(Forward / Drop / Redirect)を選択します。
	Redirect を選択した場合は、リダイレクト先のインターフェースをド
	ロップダウンリストで選択します。
Counter State	カウンター機能の状態(Enabled / Disabled)を選択します。

設定を適用するには、Applyボタンをクリックします。

すべての VLAN アクセスマップのカウンター情報をクリアするには、Clear All Counter ボタンをク リックします。

表示されている VLAN アクセスマップのカウンター情報をクリアするには、Clear Counter ボタンをク リックします。

入力した情報で VLAN アクセスマップを検索するには、Find ボタンをクリックします。

ACL プロファイルと VLAN アクセスマップを関連付けるには、Binding ボタンをクリックします。

VLAN アクセスマップを削除するには、Delete ボタンをクリックします。

Binding ボタンをクリックすると、以下に示す画面が表示されます。

Match Access-List				
Match Access-List				
Access Map Name	Мар			
Sub Map Number	1			
Match IP Access-List				
	Please Select		Apply	Delete
O Match IPv6 Access-List				
	Please Select		Apply	Delete
O Match MAC Access-Lis	t			
	Please Select		Apply	Delete

Match Access-List の各項目の説明を以下に示します。

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

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

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

	ID	ACL Name	ACL Type
0	1	S-IP4	Standard IP ACL
•	2000	E-IP4	Extended IP ACL
			1/1 < < 1 > >

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

8.5 ACL VLAN Filter

ACL VLAN Filter 画面では、VLAN フィルターを設定します。登録した VLAN アクセスマップを VLAN に 割り当てることができます。

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

ACL VLAN Filter				
ACL VLAN Filter				
Access Map Name	32 chars			
Action	Add 🗸]		
VID List	1,3-5	All VLANs		Apply
Total Entries: 1				
Access Map Nam	e		VID List	
Мар			1-4094	Delete
				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
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、AII VLANs を チェックします。

設定を適用するには、Applyボタンをクリックします。

VLAN フィルターを削除するには、Delete ボタンをクリックします。

9 Security

Security メニューでは、ポートアクセス認証やネットワーク認証など、セキュリティーに関連する設定を行います。

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

Securityの下にあるサブメニューの一覧を以下の表に示します。

ポートアクセス認証

ポートに接続するクライアントを識別し、ネットワークへのアクセスを許可するか、拒否するかを決 定する機能です。アクセス未許可のクライアントからのトラフィックはブロックされます。ポートア クセス認証を使用するポートでは、受信したフレームの送信元 MAC アドレスからクライアント情報を 確認し、認証が許可されていなければ認証の処理を行います。クライアントの認証では通常、認証 サーバー(RADIUS サーバーもしくは TACACS+サーバー)に身元を照会する方式で運用されますが、装 置自身に登録したローカルデータベースを参照する方式も使用可能です。ローカルデータベースによ る認証は IEEE802.1X 認証では使用できません。

ポートアクセス認証の種類は以下の通りです。

- IEEE802.1X 認証
- MAC アドレス認証
- Web 認証

なお、DHCP スヌーピングはクライアントの認証は行いませんが、本装置ではポートアクセス認証の一つとして分類されます。

1 ポートに複数のポートアクセス認証を有効にした場合、いずれかの方式で許可されればネットワーク へのアクセスが許可されます。ポートアクセス認証は、認証の種類によらずすべての許可クライアン トの合算で最大 128 台まで行うことができます。

9.1 Port Security

Port Security サブメニューでは、ポートセキュリティー機能の設定を行います。

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

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

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

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

9.1.1 Port Security Global Settings

Port Security Global Settings 画面では、ポートセキュリティー機能のシステム全体での最大登録 MAC アドレス数を設定します。

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

Dort Security System Settings	
For sound system sounds	
System Maximum Address (1-12288)	V No Limit

本画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 Security Port Settings									
Port Security	Port Settings								
From Port	To Port	State	Maxim	um (0-12288) Violatio	on Action Sect	urity Mode	Aging Time (0-	1440) Aging Ty	be
Port1/0/1	 Port1/0/1 	✓ Disable	d 🗸 32	Prote	ect 🗸 Del	ete-on-Timeo(🗸		Absolut	e 🗸
									Apply
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	前明
From Port / To Port	ポートまたはポートの範囲を選択します。
State	ポートセキュリティー機能の状態(Enabled / Disabled)を選択しま す。
Maximum	選択したポートへの接続を許可する MAC アドレスの最大数を 0~12288 の範囲で入力します(デフォルト:32)。
Violation Action	違反状態でのアクションを以下のいずれかから選択します。
	 Protect:信頼できない通信をすべて破棄します。カウンターには 記録しません。
	· Restrict:信頼できない通信をすべて破棄します。カウンターに計 上し、システムログの記録を行います。
	· Shutdown:違反状態になるとポートをシャットダウンします。シス テムログの記録を行います。
Security Mode	セキュリティーモードを以下のどちらかから選択します。
	 Permanent:学習したエントリーは永続エントリーとなり、ユー ザーが手動で削除しない限り削除されません。このエントリーは設 定ファイルに記録されます。
	 Delete-on-Timeout:学習したエントリーは期限付きエントリーとなります。期限付きエントリーは失効すると自動的に削除されます。
Aging Time	エントリーのエージング時間を 0~1440(分)の範囲で入力します。0 の場合は期限付きであっても失効しません。
Aging Type	エントリーの失効モードを以下から選択します。
	· Absolute:指定した時間で自動失効してエントリーを削除します。
	 Inactivity:指定した期間内に該当するクライアントからフレーム を受信しない場合にエントリーを削除します。

設定を適用するには、Applyボタンをクリックします。

9.1.3 Port Security Address Entries

Port Security Address Entries 画面では、ポートセキュリティーの管理テーブルの表示や、エント リーの手動登録および削除を行います。

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

Port Security Addr	ess Entries			
Port Security Address E	Intries			
Port Port1/0/1 Total Entries: 1	MAC Address 00-84-57-00-0	0-00 Permanent	VID (1-4094) Add	Delete Clear by Port Clear by MAC Clear All
Port	VID	MAC Address	Address Type	Remaining Time (mins)
Port1/0/10	1	00-11-22-33-44-88	Permanent	-
				1/1 K K 1 > X 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	VLAN ID を入力します。範囲は 1 ~ 4094 です。

入力した情報でポートセキュリティーエントリーを追加するには、Add ボタンをクリックします。

入力した情報でポートセキュリティーエントリーを削除するには、Delete ボタンをクリックします。

選択したポートのポートセキュリティーエントリーのカウンターをクリアするには、Clear by Port ボ タンをクリックします。

入力した MAC アドレスのポートセキュリティーエントリーのカウンターをクリアするには、Clear by MAC ボタンをクリックします。

すべてのポートセキュリティーエントリーのカウンターをクリアするには、Clear All ボタンをクリックします。
9.2 802.1X

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

802.1Xの下にあるサブメニューの一覧を以下の表に示します。

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

9.2.1 802.1X Global Settings

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

802.1X Global Settings			
802.1X Global Settings			
802.1X State Mode MAC-Authentication-Fail	Disabled V C Enabled	Disabled	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
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。

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 Sett	lings						
From Port		To Port	PAE	Authenticator			
Port1/0/1	✓	Port1/0/1	Disa	abled 🗸			
Quiet-Period (5-	-65535)	No Quiet-Period	TX-P	eriod (5-65535)		No TX-Period	
60	sec		30	se	c		
Re-Authperiod	(5-2147483647)	Supp-Timeout (5-6553	5) Ignor	e-eapol-start	1	Reauthentication	
3600	sec	30	sec Disa	abled 🗸		Disabled 🗸	Apply
Port	PAE Authentica	tor Quiet-Period	Re-Authperiod	SuppTimeout	TX Period	Ignore-eapol-start	Reauthentication
Port1/0/1	None	60	3600	30	30	Disabled	Disabled
Port1/0/2	None	60	3600	30	30	Disabled	Disabled
Port1/0/3	None	60	3600	30	30	Disabled	Disabled
Port1/0/4	None	60	3600	30	30	Disabled	Disabled
Port1/0/5	None	60	3600	30	30	Disabled	Disabled
Port1/0/6	None	60	3600	30	30	Disabled	Disabled
Port1/0/7	None	60	3600	30	30	Disabled	Disabled
Port1/0/8	None	60	3600	30	30	Disabled	Disabled
Port1/0/9	None	60	3600	30	30	Disabled	Disabled
Port1/0/10	None	60	3600	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。
Quiet-Period	認証失敗時のブロック時間を 5~65535(秒)の範囲で入力します。
No Quiet-Period	認証失敗時にブロック時間を設けない場合にチェックします。
TX-Period	EAP-Request/Identity を送信する間隔を 5~65535(秒)の範囲で入力 します。
No TX-Period	定期的な EAP-Request/Identity を送信しない場合にチェックします。
Re-Authperiod	再認証期間を 5~2147483647(秒)の範囲で入力します。
Supp-Timeout	EAP-Request/Identity の応答待ち時間を 5~65535(秒)の範囲で入力 します。
lgnore-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。

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。

Authentication Se	ssions Information			
- Authentication Session	s Information			
From Port	To Port			
Port1/0/1 🔽	Port1/0/1		Init	ReAuth
				J

本画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。

Authenticato	or Statistics											
Port	Port1/0											Find
	T OIT IN											Thid
Total Entrie	es: 0											
Port	Frames	Frames	Start	Reqid	LogOff	Req	Respid	Resp	Invalid	Error	Last Version	Last Source
	RX	тх	RX	тх	RX	ТХ	RX	RX	RX	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
Port	ポート番号を選択します。

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

9.3 AAA

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

AAA の下にあるサブメニューの一覧を以下の表に示します。

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

本装置で AAA モジュールによる認証と認可に対応する機能は、ポートアクセス認証と CLI のログイン 認証です。AAA モジュールが有効になると、装置の CLI のログイン時の認証処理は AAA モジュールに よって実行されます。

また、AAA モジュールでは、ネットワーク利用状況(Network アカウンティング)、システムイベント (System アカウンティング)、CLI のコマンド発行(Command アカウンティング)、および CLI のログ イン / ログアウト(Exec アカウンティング)のアカウンティング要求に対応します。

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

9.3.1 AAA Global Settings

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

AAA Global Setting	IS				
AAA State Settings					
		Enabled			Annle
AAA Sidle	Obisabled	Enabled			Арріу

本画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。

9.3.2 Application Authentication Settings

Application Authentication Settings 画面では、CLI のログイン認証の認証方式を設定します。認証 方式は各ライン種別で指定可能です。

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

Application Authentication Settings		
Application Authentication Settings		
Application	Login Method List	
Console	default	Edit
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 Secutiry > AAA > Authentication Settings の AAA Authentication Exec タブで登録したプロファイルです。

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

9.3.3 Application Accounting Settings

Application Accounting Settings 画面では、CLI の Exec アカウンティングと Command アカウンティングの方式を設定します。

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

Application Accounting Settings			
Application Accounting Exec Method List			
Application		Exec Method List	
Console			Edit
Telnet			Edit
SSH			Edit
Application Accounting Commands Method List – Application Console V Level	1 💟	Commands Method List 32 chars	Apply
Total Entries: 1			
Application	Level	Commands Method List	
SSH	15	1	Delete
			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。

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。

編集画面での各項目の説明を以下に示します。

設定を適用するには、Applyボタンをクリックします。

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

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

設定を適用するには、Applyボタンをクリックします。

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

9.3.4 Authentication Settings

Authentication Settings 画面では、ポートアクセス認証の認証方式を設定します。また、CLI でのロ グイン認証のメソッドリストのプロファイルを登録します。

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

Authenti	cation Settings	_				
AAA Au	thentication Network	AAA A	Ithentication Exec	AAA Authentication Control Sufficien	t	
AAA Auth	entication 802.1X					
Status	Enabled	~				
Method 1	local	~	Method 2 Pl	ease Select 🗸		No Force VLAN
Method 3	Please Select	\checkmark	Method 4 Pl	ease Select 🗸	[Apply
AAA Auth	entication MAC-Auth					
Status	Enabled	~				
Method 1	local	~	Method 2	ease Select 🗸		No Force VLAN
Method 3	Please Select	\checkmark	Method 4 Pl	ease Select 🗸	[Apply
AAA Auth	entication WEB-Auth					
Status	Enabled	\checkmark				
Method 1	local	~	Method 2	ease Select 🗸		No Force VLAN
Method 3	Please Select	\checkmark	Method 4 Pl	ease Select 🗸		Apply

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(IEEE	E802.1X	認証、M	IAC 認言	Ε、 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	き。				

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

設定を適用するには、Applyボタンをクリックします。

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

Authentica	tion Settings					_
AAA Authe	entication Networ	k AAA Authenticati	AAA Authenti	cation Control Sufficient		
AAA Authen	tication Enable					
Status	Disabled	~				
Method 1	Please Selec	t 🗸	Method 2	Please Select 🗸		
Method 3	Please Selec	t 💙	Method 4	Please Select 🗸		Apply
AAA Authen	tication Login					
List Name	32 chars					
Method 1	none	~	Method 2	Please Select 🗸		
Method 3	Please Selec	t 🗸	Method 4	Please Select 🗸		Apply
Total Entries	:1					
N	lame	Method 1	Method 2	Method 3	Method 4	
N	lame	radius	tacacs+	local		Delete

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

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

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。

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

設定を適用するには、Applyボタンをクリックします。

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

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

Authenti	cation Settings			
AAA Au	thentication Network	AAA Authentication Exec	AAA Authentication Control Sufficient	
Web	Disabled	V	Apply	
MAC	Disabled	Y	Apply	
Login	Disabled	V	Apply	

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。

9.3.5 Accounting Settings

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

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

Accounting	Settings					
AAA Acco	unting Network	AAA Accounting System	AAA	Accounting Exec	AAA Accounting Commands	
Default	Disabled	\checkmark				
Accounting mode	Please Select	\checkmark				
Method 1	Please Select	\checkmark	Method 2	Please Select		
Method 3	Please Select	\checkmark	Method 4	Please Select		Apply

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

AAA	Accounting Network	タブでは、	Network	アカウンテ	ィングのモー	・ドやメソッ	ッドリスト	►を設定しま
す。	各項目の説明を以下は	こ示します。						

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

設定を適用するには、Applyボタンをクリックします。

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

Accounting	Settings					
AAA Acco	unting Network	AAA Accounting System	AAA	Accounting Exec	AAA Accounting Commands	
Default	Disabled	\checkmark				
Accounting mode	Please Select	\checkmark				
Method 1	Please Select	\checkmark	Method 2	Please Select		
Method 3	Please Select	\checkmark	Method 4	Please Select		Apply

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

本画面の各項目の説明を以下に示します。

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。

Accounting Settings							
AAA Accounti	ng Network A/	AA Accounting System	AAA Accounting E	xec	AAA Accou	inting Commands	
List Name 32	chars						
Accounting no	one 🗸						
Method 1 Pl	ease Select 🗸 🗸		Method 2 Please Se	lect 💉	-		
Method 3 Pl	ease Select 🗸		Method 4 Please Se	lect 💽	2		Apply
Total Entries: 1							
Name	Accounting mode	Method 1	Method 2	Meth	od 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。
	· none :Exec アカウンティングの処理を行いません。
	・ start-stop: Exec アカウンティングを有効にします。
Method 1 ~ Method 4	各メソッドの照会方法(group / radius / tacacs+)を選択します。

設定を適用するには、Applyボタンをクリックします。

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

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

Accounti	ng Settings							
AAA Ao	counting Network	AAA Acc	counting System	AAA A	ccounting Exec	AAA	A Accounting Commands]
Level	1	~						
List Name	32 chars							
Accounting mode	none	~						
Method 1	Please Select	\checkmark	N	lethod 2	Please Select	~		
Method 3	Please Select	\checkmark	N	Aethod 4	Please Select	~		Apply
Total Entrie	es: 1							
Level	Name Account	ting mode	Method 1	Met	nod 2	Method 3	Method 4	
1	List n	one						Delete
	[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
Level	特権レベルを 1~15 から選択します。指定した特権レベルで使用可能な コマンドが対象になります。
List Name	Command アカウンティングのメソッドリストのプロファイル名を入力します。
Accounting mode	Command アカウンティングのモードを以下のどちらかから選択します。
	 none: Command アカウンティングの処理を行いません。
	 start-stop: Command アカウンティングを有効にします。
Method 1 ~ Method 4	各メソッドの照会方法(group / radius / tacacs+)を選択します。

設定を適用するには、Applyボタンをクリックします。

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

9.4 RADIUS

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

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

9.4.1 RADIUS Global Settings

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

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

9.4.2 RADIUS Server Settings

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

RADIUS Server Settings						
RADIUS Server Settings						
 IP Address 		01	v6 Address	2013::1		
Authentication Port (0-65535)	1812	Acc	ounting Port (0-65535)	1813		
Retransmit (0-20)	2	times Time	eout (1-255)	5	sec	
Кеу Туре	Plain Text 💙	Key		32 chars		Apply
Total Entries: 1			:			
IPv4/IPv6 Address	Authentication Port	Accounting P	ort Timeout	Retransmit	Key	
172.31.131.1	1812	1813	5	2	*****	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	アカウンティングの UDP ポート番号を 0~65535 の範囲で入力します。
	アカウンティングを使用しない場合は、0 を入力します。
Retransmit	再送処理の回数を 0~20 の範囲で入力します(デフォルト:2)。
	再送を行わない場合は、0を入力します。
Timeout	RADIUS サーバーの応答待ち時間を1~255(秒)の範囲で入力します。
Кеу Туре	共有鍵の入力タイプ(Plain Text / Encrypted)を選択します。
Кеу	RADIUS サーバーとの通信に使用する共有鍵を登録します。Key Type で
	選択した入力タイプに応じて入力します。

設定を適用するには、Applyボタンをクリックします。

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

9.4.3 RADIUS Group Server Settings

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

RADIUS Group Server	Settings								
RADIUS Group Server Settin	gs								
Group Server Name IP Address IPv6 Address Total Entries: 2	32 chars								Add
Group Server Name			IDv//IDvf	Addrose					
Group Server Maine	170.01.101		H- ¥4/IF ¥0	Address					
Group	1/2.31.131	-	-	-	-	-	-	Detail	Delete
radius		-	-	-	-	-	-		

本画面の各項目の説明を以下に示します。

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

入力した情報で RADIUS サーバーグループや RADIUS サーバーを追加するには、Add ボタンをクリックします。

RADIUS サーバーグループの詳細を表示するには、Detail ボタンをクリックします。

RADIUS サーバーグループを削除するには、Delete ボタンをクリックします。

Detailボタンをクリックすると、次のページが表示されます。

RADIUS Group Server Settings	
Group Server Name: Group	
IPv4/IPv6 Address	
172.31.131.251	Delete
	Back

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

9.4.4 RADIUS Statistic

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

RADIUS Statistic			
RADIUS Statistic			
Group Server Name Please Select			Clear Clear All
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			Clear
Parameter	Authentication Por	rt	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ティングの統計情報を 表示するテーブルの2種類が表示されます。RADIUS サーバー一覧のテーブル上で RADIUS サーバーの行 をクリックすると、統計情報表示テーブルで該当するサーバーの統計情報が表示されます。

本画面の各項目の説明を以下に示します。

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

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

すべての RADIUS サーバーの統計情報をクリアするには、Clear All ボタンをクリックします。

特定の RADIUS サーバーの統計情報をクリアするには、統計情報テーブルの Clear ボタンをクリックします。

9.5 TACACS

TACACS サブメニューでは、TACACS+サーバーの設定を行います。

TACACSの下にあるサブメニューの一覧を以下の表に示します。

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

9.5.1 TACACS Server Settings

TACACS Server Settings 画面では、TACACS+サーバーを登録します。

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

TACACS Server Set	tings	_			
TACACS Server Settings					
●IP Address	· · ·				
Port (1-65535)	49	Timeout	(1-255) 5	sec	
Кеу Туре	Plain Text 💌	Key	254 chars		Apply
Total Entries: 1					
IPv4 Address	Port	Timeout	Key		
172.31.131.0	49	5	*****		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	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。
Кеу Туре	共有鍵の入力タイプ(Plain Text / Encrypted)を選択します。
Кеу	TACACS+サーバーとの通信に使用する共有鍵キーを登録します。Key Type で選択した入力タイプに応じて入力します。

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

9.5.2 TACACS Group Server Settings

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

ACACS Group Serve	er Settings								
ACACS Group Server Set	tings								
Group Server Name IP Address Total Entries: 2			32 ch	ars 	•				Add
Group Server Name				IPv4 A	Address				
group	172.31.1	-	-	-	-	-	-	-	Detail Delete
	470.04.4				_		-	_	

本画面の各項目の説明を以下に示します。

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

入力した情報で TACACS+サーバーグループや TACACS+サーバーを追加するには、Add ボタンをクリック します。

TACACS+サーバーグループ詳細を表示するには、Detail ボタンをクリックします。

TACACS+サーバーグループを削除するには、Delete ボタンをクリックします。

Detail ボタンをクリックすると、以下に示す画面が表示されます。

TACACS Group Server Settings	
Group Server Name: group	
IP Address	
172.31.131.254	Delete
	Back

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

9.5.3 TACACS Statistic

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

CACS Statistic							
ACACS Statistic							
Froup Server Name	Pleas	e Select 🔽				Clear by Group	Clear All
TACACS Server Address	State	Socket Opens	Socket Closes	Total Packets Sent	Total Packets Recv	Reference Count	

本画面の各項目の説明を以下に示します。

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

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

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

9.6 DHCP Snooping

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

本装置では、DHCP スヌーピングはポートアクセス認証の一つとして分類され、クライアント情報は他のポートアクセス認証と同じ管理テーブルで処理されます。

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

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

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

9.6.1 DHCP Snooping Global Settings

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

DHCP Snoopi	ng Global Setting	S		
DHCP Snooping O	ilobal Settings			
DHCP Snooping		Enabled	ODisabled	
DHCP Snooping	lode Deny	OEnabled	Obsabled	
DHCP Snooping	Node MAC-Authenticatio	n OEnabled	ODisabled	Apply
DHCP Snooping M	lode Timer			
DHCP Snooping	Mode Timer (0, 30-60480	1800]	Apply
Ma	de	Timer	Remaining time	
De	ny		-jj	

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

設定を適用するには、Applyボタンをクリックします。

9.6.2 DHCP Snooping Binding Entry

DHCP Snooping Binding Entry 画面では、バインディングデータベースを表示します。

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

DHCP Snooping Binding Entry				
DHCP Snooping Binding Entry				
Total Entries: 0				
MAC Address	IP Address	Port	Expiry	Туре

9.6.3 DHCP Snooping Interface

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

DHCP Snooping Interface			
DHCP Snooping Interface			
From Port Port1/0/1	To Port Port1/0/1	State Disabled	Apply
	Port	Sti	nte
	Port1/0/1	Disa	bled
	Port1/0/2	Disa	bled
	Port1/0/3	Disa	bled
Port1/0/4		Disa	bled
Port1/0/5		Disa	bled
Port1/0/6		Disa	bled
Port1/0/7		Disa	bled
Port1/0/8		Disa	bled
	Port1/0/9	Disa	bled
	Port1/0/10	Disa	bled

本画面の各項目の説明を以下に示します。

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

設定を適用するには、Applyボタンをクリックします。

9.6.4 DHCP Snooping Static Entry

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

DHCP Snooping Static En	ntry		
DHCP Snooping Static Entry			
From Port	Port1/0/1		
To Port	Port1/0/1		
State	Disabled		
OIP	· · ·		
⊖ IPv6	2021::1	Apply	
Total Entries: 1	Total Entries: 1		
	Port	IP/IPv6	
	Port1/0/10	172.31.131.222	
		1/1 < < 1 > > Go	

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

本画面の各項目の説明を以下に示します。

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

9.7 MAC Authentication

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

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

MAC Authentication				
MAC Authentication Global Settings				
MAC Authentication State	Enabled Disabled			
Ignore DHCP	 Enabled Disabled 			Apply
Discard-Time	300 sec Default			Apply
MAC Authentication Password Settings				
Password	63 chars Encrypt 🖌 Def	fault		Apply
MAC Authentication User Nmae MAC For	rmat Settings			
Case	Lowercase 🗸			
Delimiter	None 🗸			
Delimiter Number	2			Apply
MAC Authentication Port Settings				
From Port	To Port	State		
Port1/0/1	Port1/0/1	Disabled V		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	~
	P0R1/0/8		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。
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。

MAC Authentication Passwo	d Settings	の各項目の説明を	以下に示します。
---------------------------	------------	----------	----------

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

設定を適用するには、Applyボタンをクリックします。

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

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

設定を適用するには、Applyボタンをクリックします。

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

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

9.8 Web Authentication

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

Web 認証機能を使用すると、装置が未認証端末からの外部 Web サイトへのアクセスを検知した場合に、 そのトラフィックを終端します。Web 認証リダイレクトオプションを使用すると、未認証端末との間に 一種のなりすましによる偽装セッションを確立し、HTTP リダイレクトで Web 認証を行うための認証サ イトに誘導します。

未認証端末は、Web ブラウザーの直接アクセス、または Web 認証リダイレクトオプションを用いた HTTP リダイレクトによる誘導によって認証サイトにアクセスし、認証に成功するまではポートへのア クセスが制限されます。

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

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

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

9.8.1 Web Authentication Global Settings

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

Web Authentication	Global Settings			
Web Authentication Glob	al Settings			
Web Authentication State	Enabled Disabled			Apply
Web Authentication Setti	ings			
Virtual IP	IPv4	IPv4 Address		
https-port	443 Default			
Redirect State	Enable 🗸	Snooping proxy-port	Default	
Redirect proxy-port	Default			
Logging web-access	Off 🗸	HTTP Session Timeout	30 Default	
Overwrite	Disable 🔽	Jump-URL Original	Disable	Apply

Web	Authentication	Global	Settings の各項	目の説明を以て	「に示します。
-----	----------------	--------	--------------	---------	---------

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

設定を適用するには、Applyボタンをクリックします。

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

パラメーター	説明
Virtual IP	仮想 IP アドレスとタイプを以下のいずれかから選択します。
	· IPv4: IPv4 アドレスを使用する場合に選択します。
	○ IPv4 Address :仮想 IPv4 アドレスを入力します。
	· IPv6: IPv6 アドレスを使用する場合に選択します。
	○ IPv6 Address :仮想 IPv6 アドレスを入力します。
	 URL: 仮想 URL を使用する場合に選択します。
	○ Virtual URL:仮想 URL を入力します。
https-port	HTTPS の TCP ポート番号を入力します。デフォルト(443)に戻す場合
	は、Default をチェックします。
Redirect State	Web 認証リダイレクトの状態を以下のいずれかから選択します。
	· Disabled :Web 認証リダイレクトを無効にします。
	· Disabled HTTP:HTTPのWeb認証リダイレクトを無効にします。
	 Disabled HTTPS: HTTPSのWeb認証リダイレクトを無効にします。
	・ Enabled:HTTP/HTTPSのWeb認証リダイレクトを有効にします。
Snooping proxy-port	HTTP プロキシのプロキシポート番号を入力します。このパラメーター
	を設定すると、HTTP 通信の検知や装置内部の Web 認証ポータルの待ち
	受けを、指定したボート番号でも行います。デフォルト(0:指定しな
Dedirect prove port	い)に戻り場合は、Defaultをナエックしより。
Redirect proxy-port	HILP フロキシのフロキシホート番号を八刀します。このハフメーター 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
UTTD Second Timeout	
	Web 認証ホータルの TITP ビッションタイムアクド時間を 5~00 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	このバラメーターが Enabled の場合、認証前にアクセスした URL にジャ
	ンノしまり。DISADIED の場合はシャンフしません。

注意事項



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

9.8.2 Web Authentication Port Settings

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

Web Authentication Port Set	ttings			
Web Authentication Port Settings				
From Port To Port1/0/1 Port	o Port Port1/0/1	State Disabled	TTL (1-255)	ault Apply
Port Channel Sta Port-Channel1 V	tate Disabled	TTL (1-255)		Apply
Port		State		ΠL
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		
interface port 1/0/9		Disabled		
interface port 1/0/10		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	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。
ΤΤL	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。

9.9 Network Access Authentication

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

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

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

9.9.1 Network Access Authentication Global Settings

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

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

Network Access Authentication (Global Settings			
General Settings				
Authentication Port Vlan Mode	 Enabled Disabled 			Apply
AAA local database				
User Name	63 chars	VID (1-4094)		
Password Type	Plain Text	Password	63 chars	Apply
Total Entries: 1				
User Name	Password	Password Type	VID	
username	*****	Plaintext	1	Delete
			1/1 < <	1 > > Go

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

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。

AAA local database の各項目の説明を以下に示します。

設定を適用するには、Applyボタンをクリックします。

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

9.9.2 Network Access Authentication Sessions Information

Network Access Authentication Sessions Information 画面では、ポートアクセス認証のセッション 情報を表示します。また、認証済みホストの認証を解除します。

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

Network Access Authentication Sea	ssions Information	~
Network Access Authentication Session	is Information	
Port Type	Port1/0/1 V dhcp-snooping V	Find Find View All
Network Access Authentication Clear S	essions	
MAC Address 00-84-57- IPv4 Address 2013::1 User 2013::1	00-00-00	Clear by MAC Clear by IPv4 Clear by IPv6 Clear by User
Authentication Sessions Total		1
Total Discarded Hosts		0
Authentication Sessions Information		
Total Entries: 1		
DHCP-Snooping	Success	
Authentication State	Success	
MAC Address	170.04 101.000	
Client IP Address	1/2.31.131.222	
liser	0	
Time	2.04:18	
Aging Time	0:00:00	~

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

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

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

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

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

入力した MAC アドレスでポートアクセス認証のセッション情報をクリアするには、Clear by MAC ボタ ンをクリックします。

入力した IPv4 アドレスでポートアクセス認証のセッション情報をクリアするには、Clear by IPv4 ボ タンをクリックします。

入力した IPv6 アドレスでポートアクセス認証のセッション情報をクリアするには、Clear by IPv6 ボ タンをクリックします。

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

9.10 Trusted Host

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

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

Trusted Host			
Trusted Host			
ACL Name Note: The first characte	32 chars er of ACL name must be a lette	Type Telnet V er.	Apply
Total Entries: 1			
	Туре	ACL Name	
	Telnet	ACL	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
ACL Name	適用する標準 IP ACL 名を 32 文字以内で入力します。
Туре	適用するアプリケーションの種類(Telnet / SSH / Ping)を選択しま す。

設定を適用するには、Applyボタンをクリックします。

トラストホストを削除するには、Delete ボタンをクリックします。

9.11 Traffic Segmentation Settings

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

Traffic Segmentatio	on Settings			
Traffic Segmentation Set	tings			
From Port Port1/0/1	To Port Port1/0/1	From Forward Port	To Forward Port Port1/0/1	Add Delete
Port			Forwarding Domain	
Port1/0/14			Port1/0/16-1/0/17	
Port1/0/	15		Port1/0/16-1/0/17	

本画面の各項目の説明を以下に示します。

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

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

9.12 Storm Control

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

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

torm Control		_		_	
torm Control Polling Set	tings				
Polling Interval (5-600)	5 sec	Shutdown Retries (0-360)	3 times [) Infinite	Apply
torm Control Port Settin	gs				
From Port To	Port Type Port1/0/1 Broadcast	Action	Level Type (C	PS Rise),2-2147483647)	PPS Low (0-2147483647)
					Apply
Total Entries: 36					
Port	Storm	Action	Threshold	Current	State
	Broadcast		-	-	Inactive
Port1/0/1	Multicast	Drop	-	-	Inactive
	Unicast		-	-	Inactive
	Broadcast		-	-	Inactive
Port1/0/2	Multicast	Drop	-	-	Inactive
	Unicast		-	-	Inactive
	Broadcast		-	-	Inactive
Port1/0/3	Multicast	Drop	-	-	Inactive
	Unicast		-	-	Inactive
	Broadcast		-	-	Inactive
	Droddodot				
Port1/0/4	Multicast	Drop			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。

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

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Туре	ストームコントロールのタイプ(Broadcast / Multicast / Unicast)
	を選択します。
	アクションがシャットダウンモードに設定されている場合、ユニキャス
	トは既知と未知の両方のユニキャストパケットを参照します。これによ
	し、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、ホートかシャットダワンされます。アクションかシャットダワン
	モート以外に設定されている場合、ユーキャストは木丸のユーキャスト パケットを参照します。
Action	実行するアクションを以下のいずれかから選択します。
	· None:アクションを実施しません。
	· Shutdown:ポートをシャットダウンします。
	· Drop:上限値を超えるパケットをドロップする場合に選択します。
Level Type	ストームコントロールの上限値と下限値の基準(PPS / Kbps / Level)
	を選択します。
PPS Rise	Level Type が PPS の場合に表示されます。
	ストームコントロールの上限値を pps(パケット/秒)で指定します。0
	もしくは 2~2147483647 の範囲で入力します。0 を指定すると、設定が
	装直に反映されに後の取初のハクットを除く該ヨトフノイックか利限さ
	イルスタ。
PPS LOW	LEVEI Type か PPS の場合に表示されより。
	ストームコノトロールの下喉旭を pps で指定しま 9。0~214/48364/の 筋囲で入力します。このパラメーターを指定したい提合。 ppg pige の
	戦回でハガしより。このハフスーラーを指定しない場合、PPS RISE の 80%の値が使用されます。

設定を適用するには、Applyボタンをクリックします。

PPS Rise および PPS Low で 0 を指定できるのは Ver.2.00.01 以降です。

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	To Port	Туре	Action	Level Type	KBPS Rise (2-2147483647)	KBPS Low (2-2147483647)		
Port1/0/1 💌	Port1/0/1 🔽	Broadcast 🗸	None 💌	Kbps 💙	Kbps	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。

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

Storm Control Port Settings									
From Port	To Port	Туре	Action	Level Type	Level Rise (1-100)	Level Low (1-100)			
Port1/0/1	Port1/0/1 🔽	Broadcast 🗸	None 🗸	Level 🗸	%	%			
						Apply			

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。

9.13 SSH

SSH サブメニューでは、CLI の SSH サーバー機能や SSH ユーザーに関する設定を行います。

SSHの下にあるサブメニューの一覧を以下の表に示します。

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

9.13.1 SSH Global Settings

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

SSH Global Settings		
SSH Global Settings		
IP SSH Server State	Disabled	
IP SSH Service Port (1-65535)	22	
SSH Server Mode	V2	
Authentication Timeout (30-600)	120 sec	
Authentication Retries (1-32)	3 times	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
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。
9.13.2 Host Key

Host Key 画面では、SSH ホスト鍵を表示および生成します。 本画面を表示するには、Security > SSH > Host Key をクリックします。

Host Key		
Host Key Management		
Crypto Key Type Key Modulus	RSA V 768 V bit	Generate Delete
Host Key		
Crypto Key Type	RSA 🗸	
Key pair was generated at	14:28:02, 2020-12-28	
Key Size	1024	
Key Data	AAAAB3NzaC1yc2EAAAADAQABAAAAgQC7vWBzkKqM	

Host Key Management の各項目の説明を以下に示します。

パラメーター	前明
Crypto Key Type	生成するホスト鍵の暗号タイプ(RSA / DSA)を選択します。
Key Modulus	ホスト鍵の鍵長を以下のいずれかから選択します。
	・ 360 ビット
	・ 512 ビット
	・ 768 ビット
	・ 1024 ビット
	- 2048 ビット

選択した内容でホストキーを生成するには、Generate ボタンをクリックします。 選択した内容でホストキーを削除するには、Delete ボタンをクリックします。

Host Keyの各項目の説明を以下に示します。

パラメーター	説明
Crypto Key Type	表示する SSH ホスト鍵の暗号タイプ(RSA / DSA)を選択します。

9.13.3 SSH Server Connection

SSH Server Connection 画面では、SSH サーバー接続テーブルを表示します。 本画面を表示するには、Security > SSH > SSH Server Connection をクリックします。

SSH Server Co	nnection			
SSH Table				
Total Entries: 1				
SID	Version	Cipher	User ID	Client IP Address
0	V2	aes256-cbc/hmac-sha1	15	10.90.90.10

9.13.4 SSH User Settings

SSH User Settings 画面では、SSH ユーザーを設定および表示します。 本画面を表示するには、Security > SSH > SSH User Settings をクリックします。

SSH User Settings					
SSH User Settings					
User Name	32 chars	Authentication Method	Password V		
Key File	779 chars	Host Name	255 chars		
IPv4 Address	· · · ·	O IPv6 Address	2013::1	Apply	
Total Entries: 1					
User Name	Authentication Method	Key File	Host Name	Host IP	
15	Password				
	1/1 K < 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	認証方法を以下のいずれかから選択します。		
	· Password:パスワード認証方式を使用します。ローカルユーザーア カウントのパスワードを使用します。		
	· Public Key:公開鍵認証方式を使用します。		
	 ○ Key File: 公開鍵ファイル名と場所を 779 文字以内で入力します。 		
	· Host-based:ホストベース認証方式を使用します。		
	○ Host Name:ホスト名を 255 文字以内で入力します。		
	 IPv4 Address: IPv4 アドレスを指定する場合、ラジオボタン をクリックし、右のボックスに SSH クライアントの IPv4 アド レスを入力します。 		
	 IPv6 Address: IPv6 アドレスを指定する場合、ラジオボタン をクリックし、右のボックスに SSH クライアントの IPv6 アド レスを入力します。 		

設定を適用するには、Applyボタンをクリックします。

9.14 SSL

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

項番	メニュー名	概要
9.14.1	SSL Global Settings	SSL 機能のグローバル設定
9.14.2	SSL Information	SSL の証明書や CSR 情報の表示

9.14.1 SSL Global Settings

SSL Global Settings 画面では、SSL 機能の設定を行います。 本画面を表示するには、Security > SSL > SSL Global Settings をクリックします。

SSL Global Settings					
SSL Global Settings					
SSL Status Erase SSL-files	O Enabled			Apply Erase	
Import File					
File Select Destination File Name	Certificate OPrivate Key	Browse (The file name range is 1-32 cl	hars.)	Apply	
Note: You can access the File Svs	Note: You can access the File System name to manage these imported files				
Generate CSR And RSA Key					
Country Name (2 letter code)		JP			
State or Province Name (full name)	Tokyo			
Locality Name (eg, city)		Shibuya-ku			
Organization Name (eg, company)	1	Apresia			
Organizational Unit Name (eg, sec	tion)	Accounting			
Common Name (YOUR domain na	ame)	www.example.com			
Email Address		mail@example.com			
Key Length (512-2048)		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。

パラメーター	説明
File Select	読み込むファイルの種類(Certificate / Private Key)を選択します。
	ファイルの種類を選択した後、Browse ボタンをクリックしてローカル PC 上のファイルを選択します。
Destination File Name	宛先ファイル名を 32 文字以内で入力します。

<u>Import Fileの各項目の説明を以下に示します。</u>

設定を適用するには、Applyボタンをクリックします。

Genera<u>te CSR And RSA Keyの</u>各項目の説明を以下に示します。_____

パラメーター	説明
Country Name	国コードを 2 文字で入力します。日本の国コードは JP です。
State or Province Name	都道府県名を入力します。
Locality Name	地域(市)名を入力します。
Organization Name	組織名(会社名)を入力します。
Organization Unit Name	組織単位(部門)名を入力します。
Common Name	ドメイン名を入力します。
Email Address	連絡先のメールアドレスを入力します。
Key Length	CSR/RSA キーの長さを 512~2048 の範囲で入力します。

設定を適用するには、Applyボタンをクリックします。

9.14.2 SSL Information

SSL Information 画面では、SSL の証明書および CSR 情報を表示します。 本画面を表示するには、Security > SSL > SSL Information をクリックします。

SSL Information	
SSL Https-certificate	
Certificate Information:	
Certificate Version :3	
Serial Number :00:80:2D: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 :2017-02-16 06:54:58	
Not After :2037-02-11 06:54:58	
Public Key Alg:rsaEncryption	
Signed Using :RSA+SHA256	
RSA Key Size :2048 bits	
SSL Https-private-key	
Private key is embedded in firmware.	
SSL CSR	
Certificate Request:	
Data:	
Version: 1 (0x1)	
Subject: C=JP, ST=Province, L=City, O=Company, OU=Department, CN=www.domain.com/emailAddress=mail@domain.com	
Subject Public Key Info:	
Public Key Algorithm: rsaEncryption	
Public-Key: (2048 bit)	
Modulus:	
00:ac:b7:7d:1f:7a:9d:6b:1d:ad:af:03:b4:7e:84:	
2f:d3:80:c0:b0:e1:a3:b7:31:8f:21:b5:5a:94:d6:	
5d:62:0d:f4:bb:00:c0:b3:3b:e1:36:7d:c7:c0:1e:	
1c a3 ce 23 2c 7t 1a 2b ef 51 f3 6c 2f 5b b3	
88:051c:65:45)9a:44:8c:0Td7:91:07:5e:44:16:	
5a/6e/fb/0b/86/3e/bd/ec/222/c5/cb/9e/aa/85/24/	~
15:6d:a2:d0:c3:c5:4b:d1:65:e8:6f:19:2f:8d:70:	

10 DDM

DDM メニューでは、SFP ポートでのデジタル診断監視(以後、DDM)の情報を確認できます。 **DDM** の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
10.1	DDM Voltage Threshold	DDM 電圧しきい値の表示
10.2	DDM Bias Current Threshold	DDM バイアス電流しきい値の表示
10.3	DDM TX Power Threshold	DDM 送信電力しきい値の表示
10.4	DDM RX Power Threshold	DDM 受信電力しきい値の表示
10.5	DDM Status	DDM の状態表示

10.1 DDM Voltage Threshold

DDM Voltage Threshold 画面では、DDM 電圧しきい値の情報を表示します。 本画面を表示するには、DDM > DDM Voltage Threshold をクリックします。

High Alarm (V)	High Warning (V)	Low Warning (V)	Low Alarm (V)
3.700	3.600	3.000	2.900
	High Alarm (V) 3.700	High Alarm (V) High Warning (V) 3.700 3.600	High Alarm (V) High Warning (V) Low Warning (V) 3.700 3.600 3.000

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。

Port	Current	High Alarm (mA)	High Warning (mA)	Low Warning (mA)	Low Alarm (mA)
Port1/0/19	8.053	11.800	10.800	5.000	4.000

10.3 DDM TX Power Threshold

DDM TX Power Threshold 画面では、DDM TX 電力しきい値の情報を表示します。 本画面を表示するには、DDM > DDM TX Power Threshold をクリックします。

	Current		High Alarm		Hiah V	High Warning		Low Warning		Low Alarm	
Port	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm	
Port1/0/19	0.574	-2.411	0.832	-0.800	0.661	-1.800	0.316	-5.000	0.251	-6.000	

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。

	Curre	High	High Alarm		High Warning		Low Warning		Low Alarm	
Port —	mW	dBm	mW	dBm	mW	dBm	mW	dBm	mW	dBm
Port1/0/19	0.000	_	1.000	0.000	0 794	-1 000	0.016	-18 013	0.010	-20.000

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。

il Entries: 1			ТХГ	Power	RX Po	wer
Port	Voltage (V)	Bias Current (mA)	mW	dBm	mW	dBm
Port1/0/20	3.391	8.137	0.569	-2.447	0.000	-

11 Monitoring

Monitoring メニューでは、装置のハードウェア状態の監視に関する設定を行います。また、ポートミ ラーリングの設定を行います。

	•	
項番	メニュー名	概要
11.1	Utilization	ハードウェアの使用率情報の表示
11.2	Statistics	統計情報の表示
11.3	Mirror Settings	ポートミラーリングの設定
11.4	Device Environment	デバイス環境情報の表示

Monitoringの下にあるサブメニューの一覧を以下の表に示します。

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 Utilization					
Port Utilization					
From Port Port1/0/1	1 🔽 To Port Po	rt1/0/1 🔽		Find	Refresh
Port	TX (packets/sec)	RX (packets/sec)	TX (bits/sec)	RX (bits/sec)	Utilization
Port1/0/1	0	1	0	496	1
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。 Statistics の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
11.2.1	Port	ポートの帯域利用状況や統計情報の表示
11.2.2	Port Counters	パケット統計カウンターの概要情報の表示
11.2.3	Counters	パケット統計カウンターの詳細情報の表示

11.2.1 Port

Port 画面では、物理ポートの帯域利用状況や統計情報の概要情報を表示します。 本画面を表示するには、Monitoring > Statistics > Port をクリックします。

ort									
Port									
From Port P	ort1/0/1 🔽	To Port	Port1/0/1	•				Find	Refresh
								Clear	Clear All
		RX				ТХ			
Port		Rate	To	tal		Rate	To	tal	
	bytes/sec	packets/sec	bytes	packets	bytes/sec	packets/sec	bytes	packets	
Port1/0/1	496	1	7966900	50282	0	0	9090416	20133	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 表示されているポートの統計 選択したポートの統計情報を すべてのポートの統計情報を ポート統計情報の詳細を表示	検索するには、Find ボタンをクリックします。 情報を更新するには、Refresh ボタンをクリックします。 クリアするには、Clear ボタンをクリックします。 クリアするには、Clear All 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 Detail	
Port Detail	
	Back Refresh
Port1/0/1	
RX rate	496 bytes/sec
TX rate	0 bytes/sec
RX bytes	7990761
TX bytes	9115296
RX rate	1 packets/sec
TX rate	0 packets/sec
RX packets	50407
TX packets	20189
RX multicast	21832
RX broadcast	639
RX CRC error	0
RX undersize	0
RX oversize	0
RX fragment	0
RX jabber	0
RX dropped Pkts	21908
RX MTU exceeded	0
TX CRC error	0
TX excessive deferral	0
TX single collision	0
TX excessive collision	0
TX late collision	0
TX collision	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 Counters	ort Counters								
Port Counters									
From Port P	From Port Port1/0/1 🗸 To Port Port1/0/1 🗸 Find Refresh								
								Clea	r Clear All
Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts	
Port1/0/1	8005436	27993	21864	639	9136151	19786	446	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
Port1/0/10	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。				
選択したポートのパケット統計カウンター情報をクリアするには、Clear ボタンをクリックします。				

すべてのポートのパケット統計カウンター情報をクリアするには、Clear All ボタンをクリックします。 ポートで検出されたエラーの数を表示するには、Show Errors ボタンをクリックします。

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

Counters Errors	
Counters Errors	
	Back Refresh
	Duck Kertein
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
Excess-Col	0
Carri-Sen	0
Runts	0
Giants	0
Symbol-Err	0
SQETest-Err	0
DeferredTx	0
IntMacTx	0
IntMacRx	0

前の画面に戻るには、Backボタンをクリックします。

一覧に表示されている情報を更新するには、Refreshボタンをクリックします。

11.2.3 Counters

Counters 画面では、物理ポートのパケット統計カウンターの詳細情報を表示します。 本画面を表示するには、Monitoring > Statistics > Counters をクリックします。

Counters				
Counters				
From Port Port1/0/1	To Port	Port1/0/1 🔽	Find	Refresh
			Clear	Clear All
Port		linkChange		
Port1/0/1		1		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
Port1/0/10		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。

選択したポートのパケット統計カウンター情報を検索するには、Findボタンをクリックします。 表示されているパケット統計カウンター情報を更新するには、Refreshボタンをクリックします。 選択したポートのパケット統計カウンター情報をクリアするには、Clearボタンをクリックします。 すべてのポートのパケット統計カウンター情報をクリアするには、Clear Allボタンをクリックします。 パケット統計カウンター情報を表示するには、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 Counters Detail			
ort Counters Detail			
		Back	Refresh
D-dd/0/d Countered			
Port1/0/1 Counters	50927		_
	20202		
	20395		
	40040		
	19943		
	21984		
TXHCMUITICASTPKTS	450		
rxHCBroadcastPkts	640		
txHCBroadcastPkts	0		
rxHCOctets	8059888		
txHCOctets	9210301		
rxHCPkt64Octets	38344		
rxHCPkt65to127Octets	723		
rxHCPkt128to255Octets	865		
rxHCPkt256to511Octets	7838		
rxHCPkt512to1023Octets	3065		
rxHCPkt1024to1518Octets	2		
rxHCPkt1519to1522Octets	0		
rxHCPkt1519to2047Octets	0		
rxHCPkt2048to4095Octets	0		
rxHCPkt4096to9216Octets	0		
txHCPkt64Octets	1220		
txHCPkt65to127Octets	1138		
txHCPkt128to255Octets	1733		

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 💌	
		Port
Destination	Port 🗸	Port1/0/1
		From Port To Port Frame Type
Source	Port 🗸	Port1/0/1 V Both V
		CPU RX
		Add Delete
Mirror Session Table –		
All Session 🗸	1 🗸	Find
	Session Number	Session Type
	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。			
	· Port:宛先ポートを選択します。			
Source	送信元ポート番号または ACL を指定する場合にチェックします。			
	· Port:送信元ポートを設定する場合に選択します。			
	○ 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。			
	Ø Both:受信と送信の両方のトラフィックに適用します。			
	Ø RX:受信トラフィックのみに適用します。			
	Ø 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。 			
	 ○ ACL Name: ミラーリングするパケットの条件として使用する ACL 名を 32 文字以内で入力します。 			

ポートミラーリングの設定を追加するには、Add ボタンをクリックします。

ポートミラーリングの設定を削除するには、Deleteボタンをクリックします。

Mirror Session Tableの各項目の説明を以下に示します。

パラメーター	説明
Mirror Session Type	表示するミラーリング設定情報を以下のいずれかから選択します。
	· All Session:すべての設定を表示する場合に選択します。
	· Session Number:選択したセッション番号の設定のみ表示する場合
	に選択します。右のドロップダウンリストで、表示するセッション
	番号として1~4のいずれかを選択します。

入力した情報でポートミラーリングを検索するには、Find ボタンをクリックします。 ミラーリング設定の詳細情報を表示するには、Show Detail ボタンをクリックします。

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

r Session Detail	
Session Number	1
Session Type	Local Session
Both Port	Port1/0/18-Port1/0/20
RX Port	
TX Port	
CPU RX	
Flow Based Source	
Destination Port	Port1/0/17

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	40.5C		
Health Status				
Unit	Status	Failure Code		
1	Normal	0×00000		
Slide Switch Status				
Unit		Status		
1		Off		

12 Green | 12.1 EEE

12 Green

Green メニューでは、装置のポート省電力機能に関する設定を行います。

12.1 EEE

EEE 画面は、IEEE 802.3az で規定される EEE の設定を行います。 本画面を表示するには、Green > EEE をクリックします。

EEE			
EEE Settings			
From Port	To Port	State	
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	
	Port1/0/11	Disabled	
	Port1/0/12	Disabled	
	Port1/0/13	Disabled	
in Director will not a provident control base a provident control base a provident control base and the second s	Port1/0/14	Disabled	
	Port1/0/15	Disabled	
s El moderne muchane prodenne muchane prodenne muchane	Port1/0/16	Disabled	
	Port1/0/17	-	
1. Definition of the first of t	Port1/0/18	Ter sense and the sense in the sense of the sense	
	Port1/0/19	-	
	Port1/0/20		

本画面の各項目の説明を以下に示します。

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

設定を適用するには、Applyボタンをクリックします。

13 Alarm

Alarm メニューでは、ブザーや警告 LED による警告通知に関する設定を行います。 Alarm の下にあるサブメニューの一覧を以下の表に示します。

項番	メニュー名	概要
13.1	Alarm Settings	ブザー、警告 LED の動作の設定
13.2	Alarm Debug	ブザー、警告 LED のテストの実施

13.1 Alarm Settings

Alarm Settings 画面では、ブザーおよび警告 LED のアラーム設定を行います。 本画面を表示するには、Alarm > Alarm Settings をクリックします。

Alarm Settings						
Buzzer Global Settings						
Buzzer State Buzzer Beep Type Warning Time Left:	Disabled Default 60 sec		Current Status: Duration (1-60; 0: Infinite)		Inactive 60	sec Apply
Warn-LED Global Settings -						
Warn-LED State	Disabled		Duration (1-60; 0: Infinite)		60	sec Apply
Alarm Port Settings						
From Port Port1/0/1 Alarm Mode All	V	To Port Cuase	Port1/0/1 V All V	State	Disabled	Apply
Port	State			Cause Enable	ed	
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			-		

パラメーター	説明
Buzzer State	ブザー警告機能のグローバル設定(Enabled / Disabled)を選択しま
	す。
Current Status	ブザー警告機能のグローバル設定状態が表示されます。
Buzzer Beep Type	ブザー警告音のパターンを以下のいずれかから選択します。
	 Default:ビープ音を2秒間鳴らして2秒間無音というパターンを 繰り返す場合に選択します。
	 Type 1: 2秒間ビープ音を鳴らして8秒間無音というパターンを 繰り返す場合に選択します。
	 Type 2: ビープ音を5秒間鳴らして5秒間無音というパターンを繰り返す場合に選択します。
	 Type 3: ビープ音を8秒間鳴らして2秒間無音というパターンを繰り返す場合に選択します。
Duration	ブザーの動作時間(秒)を 0~60 の範囲で入力します。0 を指定する と、警告イベント発生時にブザー音の警告が行われません。
Warning Time Left	警告イベント発生時のブザー停止までの残時間が表示されます。

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

設定を適用するには、Applyボタンをクリックします。

Warn-LED Global Settingsの各項目の説明を以下に示します。

パラメーター	説明
Warn-LED State	警告 LED の状態(Enabled / Disabled)を選択します。
Duration	警告 LED の動作時間(秒)を0~60 の範囲で入力します。0 を指定する と、警告イベント発生時に警告 LED による警告が行われません。

設定を適用するには、Applyボタンをクリックします。

Alarm Port Settingsの各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	ポートまたはポートの範囲を選択します。
Alarm Mode	警告イベント発生時のアラームモードを以下から選択します。
	· AII: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。
	· AII: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。

Alarm Debug			
Buzzer Beep Debug			
Buzzer Beep Debug (Apply again to cancel)			Apply
Warn-LED Blink Debug			
Warn-LED Blink Debug (Apply again to cancel)			
From Port Port1/0/1	To Port	Port1/0/1	
			Apply

Buzzer Beep Debug の各項目の説明を以下に示します。

パラメーター	説明
Buzzer Beep Debug	ブザーのテストを行います。Apply ボタンをクリックするたびに、鳴動 と停止が切り替わります。

Warning LED Blink Debugの各項目の説明を以下に示します。

パラメーター	説明
From Port / To Port	警告 LED のテストを行います。テストする警告 LED のポートの範囲を選択し、Apply ボタンをクリックするたびに、オンとオフが切り替わります。

14 Save

画面上部のフロントパネルビューに表示されているツールバーに表示されている Save ボタンをクリックし、表示されるサブメニューの Write Memory をクリックすると、現在の設定を保存する画面に移行します。

14.1 Write Memory

 Write Memory 画面では、現在の設定情報を起動時設定に書き込みます。

 本画面を表示するには、Save > Write Memory をクリックします。

Write Memory	
Write Memory	
Destination filename startup-config? [y/n]:	Apply
Write Memory Secondary	
Destination filename secondary startup-config? [y/n]: Yes	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
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
Write Memory Secondary	Yesを選択して Apply ボタンをクリックすると、現在の設定情報をセカ
······································	ンダリーの起動時設定ファイルに書き込みます。

15 Tools

Tool ボタンから、イメージファイルや設定ファイルの操作を行うことができます。 Tool ボタンをクリックすると以下のサブメニューが出現します。

項番	メニュー名	概要
15.1	Firmware Upgrade & Backup	イメージファイルの操作
15.2	Configuration Restore & Backup	設定ファイルの操作
15.3	Tech-support Backup	技術サポート情報のバックアップ
15.4	Log Backup	システムログのバックアップ
15.5	Restore & Backup	一括リストアと一括バックアップ
15.6	AAA-local-db Download & Backup	AAA ローカルデータベースファイルの操作
15.7	SSL Files Download & Backup	SSL 関連ファイルの操作
15.8	CSR Files Backup	CSR 関連ファイルの操作
15.9	Ping	Ping の実行
15.10	Trace Route	Traceroute の実行
15.11	Reset	システムリセットの実行
15.12	Reboot System	システム再起動の実行

15.1 Firmware Upgrade & Backup

Firmware Upgrade & Backup メニューからは、イメージファイルのアップロードとダウンロードを実行 します。起動するファームウェアを、装置にアップロードしたイメージファイルに更新する場合、装 置の再起動が必要になります。また、アップロードしたイメージファイルが起動イメージに指定され ていない場合は、Management > File Systemの画面で起動イメージを変更する必要があります。

Firmware Upgrade & Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.1.1	Firmware Upgrade from HTTP	HTTP でローカル PC からイメージファイルを取得
15.1.2	Firmware Upgrade from TFTP	TFTP サーバーからイメージファイルを取得
15.1.3	Firmware Upgrade from FTP	FTP サーバーからイメージファイルを取得
15.1.4	Firmware Backup to HTTP	HTTP でローカル PC にイメージファイルを保管
15.1.5	Firmware Backup to TFTP	TFTP サーバーにイメージファイルを保管
15.1.6	Firmware Backup to FTP	FTP サーバーにイメージファイルを保管

15.1.1 Firmware Upgrade from HTTP

Firmware Upgrade from HTTP 画面では、HTTP でローカル PC から装置にイメージファイルをアップ ロードします。

本画面を表示するには、Tools > Firmware Upgrade & Backup > Firmware Upgrade from HTTP をクリックします。

Firmware Upgrade from HTTP		
Source File	Browse	
Destination	File or Path (64 chars)	
		Upgrade

本画面の各項目の説明を以下に示します。

パラメーター	説明	
Source File	Browse ボタンをクリックし、ローカル PC 上のイメージファイルを選択 します。Browse ボタンの左のボックスにファイル名とパスが表示され ます。	
Destination	装置に保存するファイル名とパスを 64 文字以内で入力します。	
· イメージファイルのフップロードを明始するには、Upgrade ボタンをクリックレキオ		

イメーシファイルのアッフロードを開始するには、Upgrade ホ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。

Firmware Upgrade from TFTP		
TFTP Server IP	• • IPv4	
	◯ IPv6	
Source	File or Path (64 chars)	
Destination	File or Path (64 chars)	
	Upgrade	

本画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(I Pv4 / I Pv6)を指定します。
Source	TFTP サーバー上のファイル名とパスを 64 文字以内で入力します。
Destination	装置に保存するファイル名とパスを 64 文字以内で入力します。

イメージファイルのアップロードを開始するには、Upgrade ボタンをクリックします。

15.1.3 Firmware Upgrade from FTP

Firmware Upgrade from FTP画面では、FTPサーバーからイメージファイルをアップロードします。 本画面を表示するには、Tools > Firmware Upgrade & Backup > Firmware Upgrade from FTP をク リックします。

Firmware Upgrade	e from FTP
ETD Conver ID	
FIF Serverie	
TCP Port (1-65535)	
User Name	32 chars
Password	15 chars
Source	File or Path (64 chars)
Destination	File or Path (64 chars)
	Upgrade

本画面の各項目の説明を以下に示します。

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジ
	オボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1~65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Source	FTP サーバー上のファイル名とパスを 64 文字以内で入力します。
Destination	装置に保存するファイル名とパスを 64 文字以内で入力します。

イメージファイルのアップロードを開始するには、Upgrade ボタンをクリックします。

15.1.4 Firmware Backup to HTTP

Firmware Backup to HTTP 画面では、HTTP でローカル PC にイメージファイルをバックアップします。 本画面を表示するには、Tools > Firmware Upgrade & Backup > Firmware Backup to HTTP をクリッ クします。

Firmware Ba	kup to HTTP	
Source	File or Path (64 chars)	
	Backup	

本画面の各項目の説明を以下に示します。

パラメーター	説明
Source	装置のファームウェアファイル名とパスを 64 文字以内で入力します。

イメージファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.1.5 Firmware Backup to TFTP

Firmware Backup to TFTP 画面では、TFTP サーバーにイメージファイルをバックアップします。 本画面を表示するには、Tools > Firmware Upgrade & Backup > Firmware Backup to TFTP をクリッ クします。

Firmware Backup to TFTP		
TFTP Server IP	· · · · • • IPv4	
	◯ IPv6	
Source	File or Path (64 chars)	
Destination	File or Path (64 chars)	
	Backup	

本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラ
	ジオボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
Source	装置のイメージファイル名とパスを 64 文字以内で入力します。
Destination	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

イメージファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.1.6 Firmware Backup to FTP

Firmware Backup to FTP 画面では、FTP サーバーにイメージファイルをバックアップします。 本画面を表示するには、Tools > Firmware Upgrade & Backup > Firmware Backup to FTP をクリック します。

Firmware Backup to FTP		
FTP Server IP	· · · • • • • • • • • • • • • • • • • •	
	◯ IPv6	
TCP Port (1-65535)		
User Name	32 chars	
Password	15 chars	
Source	File or Path (64 chars)	
Destination	File or Path (64 chars)	
	Backup	

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジ オボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1~65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Source	装置のイメージファイル名とパスを 64 文字以内で入力します。
Destination	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

イメージファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.2 Configuration Restore & Backup

Configuration Restore & Backup メニューからは、設定ファイルのバックアップ、リストアを実行できます。

Configuration Restore & Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.2.1	Configuration Restore from HTTP	HTTP でローカル PC から設定ファイルを取得
15.2.2	Configuration Restore from TFTP	TFTP サーバーから設定ファイルを取得
15.2.3	Configuration Restore from FTP	FTP サーバーから設定ファイルを取得
15.2.4	Configuration Backup to HTTP	HTTP でローカル PC に設定ファイルを保管
15.2.5	Configuration Backup to TFTP	TFTP サーバーに設定ファイルを保管
15.2.6	Configuration Backup to FTP	FTP サーバーに設定ファイルを保管

15.2.1 Configuration Restore from HTTP

Configuration Restore from HTTP 画面では、HTTP でローカル PC から設定ファイルを復元できます。 本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Restore from HTTP をクリックします。

Configuration Restore from HTTP		
Source File	Bro	wse
Destination	File or Path (64 chars)	running-config startup-config
Replace		
		Restore

本画面の各項目の説明を以下に示します。

パラメーター	説明
Source File	テキストボックスをダブルクリックするか、Browse ボタンをクリック し、ローカル PC 上の設定ファイルを選択します。Browse ボタンの左の ボックスにファイル名とパスが表示されます。
Destination	装置に保存する設定ファイル名とパスを 64 文字以内で入力します。 running-configをチェックすると、現在の設定に反映します。 startup-configをチェックすると、起動時設定に反映します。
Replace	装置の設定ファイルを置き換える場合にチェックします。

設定ファイルの復元を開始するには、Restore ボタンをクリックします。

15.2.2 Configuration Restore from TFTP

Configuration Restore from TFTP 画面では、TFTP サーバーから設定ファイルを復元します。 本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Restore from TFTP をクリックします。

Configuration Restore from TFTP	
TFTP Server IP	· · · • • • • • • • • • • • • • • • • •
	○ IPv6
Source	File or Path (64 chars)
Destination	File or Path (64 chars)
Replace	
	Restore

本画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
	ジオホタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
Source	TFTP サーバー上のファイル名とパスを 64 文字以内で入力します。
Destination	装置に保存する設定ファイル名とパスを 64 文字以内で入力します。
	 running-configをチェックすると、現在の設定に反映します。
	· startup-configをチェックすると、起動時設定に反映します。
Replace	装置の設定ファイルを置き換える場合にチェックします。

設定ファイルの復元を開始するには、Restore ボタンをクリックします。

15.2.3 Configuration Restore from FTP

Configuration Restore from FTP 画面では、FTP サーバーから設定ファイルを復元します。 本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Restore from FTP をクリックします。

Configuration Restore from FTP	
FTP Server IP	· · · • • IPV4
	O IPv6
TCP Port (1-65535)	
User Name	32 chars
Password	15 chars
Source	File or Path (64 chars)
Destination	File or Path (64 chars) Image: running-config Image: startup-config
Replace	
	Restore

15 Tools | 15.2 Configuration Restore & Backup

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジ
	オボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1~65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Source	FTP サーバー上のファイル名とパスを 64 文字以内で入力します。
Destination	装置に保存する設定ファイル名とパスを 64 文字以内で入力します。
	・ running-configをチェックすると、現在の設定に反映します。
	 startup-configをチェックすると、起動時設定に反映します。
Replace	装置の設定ファイルを置き換える場合にチェックします。

本画面の各項目の説明を以下に示します。

設定ファイルの復元を開始するには、Restore ボタンをクリックします。

15.2.4 Configuration Backup to HTTP

Configuration Backup to HTTP 画面では、HTTP でローカル PC に設定ファイルをバックアップします。 本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Backup to HTTP をクリックします。

Configuration Backup to HTTP		
Source	File or Path (64 chars)	running-config startup-config Backup

本画面の各項目の説明を以下に示します。

パラメーター	説明
Source	装置上の設定ファイル名とパスを 64 文字以内で入力します。
	・ running-configをチェックすると、現在の設定を取得します。
	· startup-configをチェックすると、起動時設定を取得します。

設定ファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.2.5 Configuration Backup to TFTP

Configuration Backup to TFTP 画面では、TFTP サーバーに設定ファイルをバックアップします。 本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Backup to TFTP をクリックします。

Configuration Backup to TFTP		
TFTP Server IP	• IPv4	
	O IPv6	
Source	File or Path (64 chars)	running-config startup-config
Destination	File or Path (64 chars)	
		Backup

本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジ
	オボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
Source	装置上の設定ファイル名とパスを 64 文字以内で入力します。
	・ running-configをチェックすると、現在の設定を取得します。
	· startup-configをチェックすると、起動時設定を取得します。
Destination	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

設定ファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.2.6 Configuration Backup to FTP

Configuration Backup to FTP 画面では、FTP サーバーに設定ファイルをバックアップします。 本画面を表示するには、Tools > Configuration Restore & Backup > Configuration Backup to FTP をクリックします。

Configuration Bac	kup to FTP	
FTP Server IP	• IPV4	
	◯ IPv6	
TCP Port (1-65535)]
User Name	32 chars]
Password	15 chars]
Source	File or Path (64 chars)	running-config startup-config
Destination	File or Path (64 chars)]
		Backup

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
	オホタンでIPアドレスの形式(IPv4 / IPv6)を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1~65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Source	装置上の設定ファイル名とパスを 64 文字以内で入力します。
	・ running-configをチェックすると、現在の設定を取得します。
	· startup-configをチェックすると、起動時設定を取得します。
Destination	FTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

本画面の各項目の説明を以下に示します。

設定ファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.3 Tech-support Backup

Tech-support Backup メニューからは、技術サポート情報のバックアップを実行できます。 Tech-support Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.3.1	Tech-support Backup to HTTP	HTTP でローカル PC に技術サポート情報を保存
15.3.2	Tech-support Backup to TFTP	TFTP サーバーに技術サポート情報を保存

15.3.1 Tech-support Backup to HTTP

Tech-support Backup to HTTP 画面では、HTTP でローカル PC に技術サポート情報ファイルをバック アップします。

本画面を表示するには、Tools > Tech-support Backup > Tech-support Backup to HTTP をクリック します。

Tech-support Backup to HTTP		
Tech-support backup to HTTP		
	Backup	

技術サポート情報ファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.3.2 Tech-support Backup to TFTP

Tech-support Backup to TFTP 画面では、TFTP サーバーに技術サポート情報ファイルをバックアップ します。

本画面を表示するには、Tools > Tech-support Backup > Tech-support Backup to TFTP をクリック します。

Tech-support Ba	Tech-support Backup to TFTP		
TFTP Server IP	• • • • • • • • • • • • • • • • • • •		
	O IPv6		
Destination	File or Path (64 chars)		
	Backup		

本画面の各項目の説明を以下に示します。

パラメーター	前明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラ
	ジオボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
Destination	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

技術サポート情報ファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.4 Log Backup

Log Backup メニューからは、システムログのバックアップを実行できます。 Log Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.4.1	Log Backup to HTTP	HTTP でローカル PC にシステムログを保存
15.4.2	Log Backup to TFTP	TFTP サーバーにシステムログを保存

15.4.1 Log Backup to HTTP

Log Backup to HTTP 画面では、HTTP でローカル PC にシステムログをバックアップします。 本画面を表示するには、Tools > Log Backup > Log Backup to HTTP をクリックします。

Log Backup to HT	TP
Log Type	System Log Attack Log Backup

本画面の各項目の説明を以下に示します。

パラメーター	説明	
Log Type	バックアップするログの種類を以下のどちらかから選択します。	
	· System Log を選択すると、システムログをバックアップします。	
	・ Attack Logを選択すると、アタックログをバックアップします。	

システムログのバックアップを開始するには、Backup ボタンをクリックします。

15.4.2 Log Backup to TFTP

Log Backup to TFTP 画面では、TFTP サーバーにシステムログをバックアップします。 本画面を表示するには、Tools > Log Backup > Log Backup to TFTP をクリックします。

Log Backup to TFTP		
TFTP Server IP	· · · · • • • • • • • • • • • • • • • •	
	O IPv6	
Destination	File or Path (64 chars)	
Log Type	System Log ○ Attack Log	
	Backup	
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	
	シオホダンでIPアドレスの形式(IPV4 / IPV6)を指定します。	
Destination	FTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。	
Log Type	バックアップするログの種類を以下のどちらかから選択します。	
	・ System Log を選択すると、システムログをバックアップします。	
	· Attack Logを選択すると、アタックログをバックアップします。	

本画面の各項目の説明を以下に示します。

ー システムログのバックアップを開始するには、Backup ボタンをクリックします。

15.5 Restore & Backup

Restore & Backup メニューからは、イメージファイルや構成ファイルなどのファイル一式の一括レス トアおよびバックアップを実行できます。

Restore & Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.5.1	Restore from TFTP	TFTP サーバーから一括レストアを実施
15.5.2	Restore from FTP	FTP サーバーから一括レストアを実施
15.5.3	Restore from SD Card	SD カードから一括レストアを実施
15.5.4	Backup to TFTP	TFTP サーバーに一括バックアップを実施
15.5.5	Backup to FTP	FTP サーバーに一括バックアップを実施
15.5.6	Backup to SD Card	SD カードに一括バックアップを実施
15.5.7	SD Card Backup Clone	SD カードにクローンファイルをバックアップ

15.5.1 Restore from TFTP

Restore from TFTP 画面では、TFTP サーバーから一括レストアを行います。 本画面を表示するには、Tools > Restore & Backup > Restore from TFTP をクリックします。

Restore from TF TP	
TETP Server IP	
IFIF Selverin	
Prefix	12 chars
Source Path	64 chars
Option	no-access-defender no-software
Reboot	
	Restore

本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラ
	ジオボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
Prefix	各ファイルに付加されたプレフィックスを12文字以内で入力します。
Source Path	TFTP サーバー上のファイルのパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。
Reboot	ファイルが復元された後に装置を再起動する場合にチェックします。

一括レストアを開始するには、Restore ボタンをクリックします。

15.5.2 Restore from FTP

Restore from FTP 画面では、FTP サーバーから一括レストアを実施します。

本画面を表示するには、Tools > Restore & Backup > Restore from FTP をクリックします。

Restore from FTP	
FTP Server IP	••••••••••••••••••••••••••••••••••••••
TCP Port (1-65535)	
User Name	32 chars
Password	15 chars
Prefix	12 chars
Source Path	64 chars
Option	no-access-defender no-software
Reboot	
	Restore

本画面の各項目の説明を以下に示します。

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジ
	オボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1~65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Prefix	各ファイルに付加されたプレフィックスを12文字以内で入力します。
Source Path	FTP サーバー上のファイルパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。
Reboot	ファイルが復元された後に装置を再起動する場合にチェックします。

一括レストアを開始するには、Restore ボタンをクリックします。

15.5.3 Restore from SD Card

Restore from SD Card 画面では、装置に挿入した SD カードから一括レストアを実施します。 本画面を表示するには、Tools > Restore & Backup > Restore from SD Card をクリックします。

Restore from SD Card		
Prefix	12 chars	
Source Path	64 chars	
Option	no-access-defender no-software	
Reboot		
	Restore	

パラメーター	説明
Prefix	各ファイルに付加されたプレフィックスを12文字以内で入力します。
Source Path	SD カード上のファイルパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。
Reboot	ファイルが復元された後に装置を再起動する場合にチェックします。

本画面の各項目の説明を以下に示します。

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。

Backup to TFTP	
TFTP Server IP	· · · • • • • • • • • • • • • • • • • •
	O IPv6
Prefix	12 chars
Destination Path	64 chars
Option	no-access-defender no-software
	Backup

本画面の各項目の説明を以下に示します。

パラメーター	説明
TFTP Server IP	TFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラ
	ジオボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
Prefix	各ファイルに付加するプレフィックスを12文字以内で入力します。
Destination Path	TFTP サーバーの保存先ファイルパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。

一括バックアップを開始するには、Backup ボタンをクリックします。

15.5.5 Backup to FTP

Backup to FTP 画面では、FTP サーバーに一括バックアップを実施します。 本画面を表示するには、Tools > Restore & Backup > Backup to FTP をクリックします。

Backup to FTP		
FTF Server IP		
TOD Doct (1 65535)		
TCF F0IL (1-05555)		
User Name	32 chars	
Password	15 chars	
Prefix	12 chars	
Destination Path	64 chars	
Option	no-access-defender no-software	
		Backup

本画面の各項目の説明を以下に示します。

パラメーター	説明
FTP Server IP	FTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。ラジ
	オボタンで IP アドレスの形式(IPv4 / IPv6)を指定します。
TCP Port	FTP 接続に使用する TCP ポート番号を 1~65535 の範囲で入力します。
User Name	FTP 接続に使用するユーザー名を 32 文字以内で入力します。
Password	FTP 接続に使用するパスワードを 15 文字以内で入力します。
Prefix	各ファイルに付加するプレフィックスを 12 文字以内で入力します。
Destination Path	FTP サーバーの保存先ファイルパスを入力します。
no-access-defender	Access Defender ファイルの転送を省略する場合にチェックします。
no-software	ソフトウェアファイルの転送を省略する場合にチェックします。

一括バックアップを開始するには、Backup ボタンをクリックします。

15.5.6 Backup to SD Card

Backup to SD Card 画面では、SD カード上のファイルを SD カード上の別の場所にバックアップします。 本画面を表示するには、Tools > Restore & Backup > Backup to SD Card をクリックします。

Backup to SD Card		
Prefix	12 chars	
Destination Path	64 chars	
Option	no-access-defender no-software	
	Backup	

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

本画面の各項目の説明を以下に示します。

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。

SD Card backup clone
Upload the system operating files to memory card
Backup

クローンファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.6 AAA-local-db Download & Backup

AAA-local-db Download & Backup メニューからは、AAA のローカルデータベースファイルのバック アップ、リストアを実行できます。

AAA-local-db Download & Backup メニューをクリックすると、以下のサブメニューが表示されます。

項番	メニュー名	概要
15.6.1	AAA-local-db Download from TFTP	TFTP サーバーから AAA ローカルデータベースファ イルをダウンロード
15.6.2	AAA-local-db Backup to TFTP	TFTP サーバーに AAA ローカルデータベースファイ ルをバックアップ

15.6.1 AAA-local-db Download from TFTP

AAA-local-db Download from TFTP 画面では、TFTP サーバーからローカル AAA データベースファイル をダウンロードします。

本画面を表示するには、Tools > AAA-local-db Download & Backup > AAA-local-db Download from TFTP をクリックします。

AAA-local-db Do	AAA-local-db Download from TFTP		
TFTP Server IP	••••••••••••••••••••••••••••••••••••••		
Source File	64 chars	Download	

本画面の各項目の説明を以下に示します。

TFTP Server IPTFTP サーバーの IPv4 アドレスまたは IPv6 アドレスを入力します。 ジオボタンで IP アドレスの形式 (IPv4 / IPv6)を指定します。Source FileTFTP サーバートのファイル名とパスを 64 文字以内で入力します。	パラメーター	説明
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。	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(I Pv4 / I Pv6)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。

AAA-local-db Ba	AAA-local-db Backup to TFTP		
TFTP Server IP	• • • • • • • • • • • • • • • • • • •		
Destination File	64 chars		
	Backup		

本画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(I Pv4 / I Pv6)を指定します。
Destination File	TFTP サーバーでの保存ファイル名とパスを 64 文字以内で入力します。

ファイルのバックアップを開始するには、Backupボタンをクリックします。

15.7 SSL Files Download & Backup

SSL Files Download & Backup メニューからは、SSL 関連のファイルのバックアップ、リストアを実行できます。

SSL	Files	Down I oad	& Backup	メニューをク	フリック	/すると、	以下のサブメニュ	ーが表示されます。
-----	-------	------------	----------	--------	------	-------	----------	-----------

項番	メニュー名	概要
15.7.1	https-certificate Download from TFTP	TFTP サーバーから HTTPS 証明書をダウンロード
15.7.2	https-certificate Backup to TFTP	TFTP サーバーに HTTPS 証明書をアップロード
15.7.3	https-private-key Download from TFTP	TFTP サーバーから HTTPS 秘密鍵ファイルをダウン ロード
15.7.4	https-private-key Backup to TFTP	TFTP サーバーに HTTPS 秘密鍵ファイルをアップ ロード

15.7.1 https-certificate Download from TFTP

https-certificate Download from TFTP 画面では、TFTP サーバーから装置に HTTPS 証明書をダウン ロードします。

本画面を表示するには、Tools > SSL Files Download & Backup > https-certificate Download from TFTP をクリックします。

https-certificate Download from TFTP		
TFTP Server IP	• • • • • • • • • • • • • • • • • • •	
Source File	64 chars	
	Download	

本画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(I Pv4 / 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。

https-certificate Backup to TFTP		
TFTP Server IP	· · · · • • • • • • • • • • • • • • • •	
	○ IPv6	
Destination File	64 chars	
	Backup	

本画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(I Pv4 / 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。

https-private-key Download from TFTP		
TFTP Server IP	••••••••••••••••••••••••••••••••••••••	
Source File	64 chars]
		Download

本画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(I Pv4 / I Pv6)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。

https-private-key Backup to TFTP		
TETP Soprar IP	© IPv4	
IFIF Serverir		
	○ IPv6	
Destination File	64 chars	
	Backup	

本画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(I Pv4 / IPv6)を指定します。
Destination File	TFTP サーバーの宛先ファイル名とパスを 64 文字以内で入力します。

HTTPS 秘密鍵ファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.8 CSR Files Backup

CSR Files Backup メニューからは、CSR ファイルのバックアップを実行できます。

項番	メニュー名	概要
15.8.1	csr-certificate Backup to TFTP	TFTP サーバーに CSR ファイルをバックアップ
15.8.2	csr-private-key Backup to TFTP	TFTP サーバーに CSR 秘密鍵ファイルをバックアッ プ

CSR Files Backup メニューをクリックすると、以下のサブメニューが表示されます。

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。

csr-certificate Backup to TFTP		
TFTP Server IP	· · · · • • • • • • • • • • • • • • • •	
	○ IPv6	
Destination File	64 chars	
	Backup	

本画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(I Pv4 / 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。

csr-private-key Backup to TFTP		
TFTP Server IP	• • • • • • • • • • • • • • • • • • •	
Destination File	64 chars	
	Backup	

本画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(I Pv4 / IPv6)を指定します。
Destination File	TFTP サーバーの宛先ファイル名とパスを 64 文字以内で入力します。

CSR 秘密鍵ファイルのバックアップを開始するには、Backup ボタンをクリックします。

15.9 Ping

Ping 画面では、ネットワーク上の他のデバイスに ping を実行します。 本画面を表示するには、Tools > Ping をクリックします。

Ping			
IPv4 Ping			
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]	
			Start
IPv6 Ping			
Target IPv6 Address	2233::1	7	
Ping Times (1-255)			
Timeout (1-99)	1	sec	
Interval (1-3600)	1	sec	
Size (32-1500)	100	bytes	
Source IPv6 Address]	
			Start
Ping Access-Class			
Ping Access-Class1 Pin	ng Access-Class2 Action	Type ACL Name	
	Add 🗸	IP ACL Please Select	Apply

IPv4 Pingの各項目の説明を以下に示します。

パラメーター	説明
Target IPv4 Address	Ping を実行する IPv4 アドレスを入力します。
Ping Times	IPv4 アドレスへの Ping の試行回数を 1~255 の範囲で入力します。
	手動で停止させるまで、指定した IPv4 アドレスに Ping を実行し続け
	るには、Infiniteをチェックします。
Timeout	Ping のタイムアウトを1~ 99(秒)の範囲で入力します。
Interval	Ping の送信の間隔を1~3600(秒)入力します。
Size	Ping パケットサイズを 32~1500(バイト)の範囲で入力します。
Source IPv4 Address	送信元 IPv4 アドレスを入力します。本装置では指定する必要はありま
	せん。

Ping を実行するには、Start ボタンをクリックします。

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。

IPv6 Pingの各項目の説明を以下に示します。

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	
<pre>[1] Reply from 172.31.132.254, time<10ms [2] Reply from 172.31.132.254, time<10ms [3] Reply from 172.31.132.254, time=10ms [4] Reply from 172.31.132.254, time<10ms Ping Statistics for 172.31.132.254</pre>	
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 172:31:132::110, bytes=56 time<10 ms	
[2] Reply from 172:31:132::110, bytes=56 time<10 ms	<u>^</u>
[3] Reply from 172:31:132::110, bytes=56 time<10 ms	
[4] Reply from 172:31:132::110, bytes=56 time<10 ms	
Ping Statistics for 172:31:132::110	
Packets: Sent =4, Received =4, Lost =0	
	\sim
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)	30	
Port (1-65535)	33434	
Timeout (1-65535)	5 sec	
Probe Times (1-1000)	3	Start
IPv6 Trace Route		
IPv6 Address	2233::1	
Max TTL (1-255)	30	
Port (1-65535)	33434	
Timeout (1-65535)	5 sec	
Probe Times (1-1000)	3	Start

IPv4 Trace Route の各項目の説明を以下に示します。

パラメーター	説明
IPv4 Address	宛先の IPv4 アドレスを入力します。
Max TTL	Traceroute の最大 TTL を 1~255 の範囲で入力します。
Port	Traceroute で使用する TCP/UDP ポート番号を 1~65535 の範囲で入力し ます。
Timeout	Traceroute の各ホップのタイムアウトを 1~65535(秒)の範囲で入力 します。
Probe Times	Traceroute のプローブ回数を1~1000の範囲で入力します。
	• • • • • • • • • • • • • • • • • • • •

Traceroute を実行するには、Start ボタンをクリックします。

IPv6 Trace Routeの各項目の説明を以下に示します。

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

Traceroute を実行するには、Start ボタンをクリックします。

IPv4 Trace RouteのStartボタンをクリックすると、IPv4 Trace Route Resultが表示されます。



IPv6 Trace Route の Start ボタンをクリックすると、IPv6 Trace Route Result が表示されます。



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

15.11 Reset

Reset 画面では、システムをリセットします。システムをリセットし、工場出荷時のデフォルト設定に 戻すこともできます。

本画面を表示するには、Tools > Reset をクリックします。

Reset	
Reset	
Poent System :	
Reset System: Clear the system's configuration to the factory default sattings, including the IP address	
Clear system configuration, save, reboot.	
O 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。

Reboot System	
Reboot System	
Do you want to save the settings ?	Reboot
If you do not save the settings, all changes made in this session will be lost.	

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。

Reboot System	
Saving and rebooting system, please wait	
25%	

ApresiaLightGM200 シリーズ Ver.2.00 SW マニュアル

Copyright(c) 2021 APRESIA Systems, Ltd. 2021年7月初版 2022年6月第3版

APRESIA Systems株式会社 東京都中央区築地二丁目3番4号 築地第一長岡ビル https://www.apresiasystems.co.jp/