

ApresiaLightMC(-PoE)シリーズ

Ver. 1.00

SW マニュアル

**APRESIA Systems 株式会社**

制定・改訂来歴表

No.	年 月 日	内 容
-	2020年5月18日	新規作成
A	2020年5月29日	<ul style="list-style-type: none"> <li>・ 1.2 パラメーター設定手順 アクセス制限の設定を追加</li> <li>・ 3.1.20 RMON Statistics 注意事項を削除</li> <li>・ 3.1.21 RMON History 注意事項を削除</li> <li>・ 3.1.22 RMON Alarm 注意事項を削除</li> <li>・ 3.1.23 RMON Event 注意事項を削除</li> <li>・ 3.2.13 Access Management Statistics 注意事項を削除</li> <li>・ 3.4.1 Restart Device 再起動中の注意事項を追加</li> <li>・ 3.4.3 Software Upload 再起動中の注意事項を追加</li> <li>・ 3.4.8 Activate Configuration 再起動中の注意事項を追加</li> </ul>
B	2020年9月30日	<ul style="list-style-type: none"> <li>・ 2.4 Web ブラウザの注意事項を追加</li> <li>・ 3.1.32 PoE Ping Auto Checking PD 受電機器の注意事項を追加</li> <li>・ 3.4.4 Image select ファームウェアの注意事項を追加</li> </ul>
C	2021年3月31日	<ul style="list-style-type: none"> <li>・ はじめに 製品名(手配品名)に下記を追加 (ApresiaLightMC-FX(APLMCFX), ApresiaLightMC-FX-PoE(APLMCFXPOE))</li> <li>・ はじめに 100BASE-FX 品は受注生産を追加</li> <li>・ 2.4.1 ログイン ログイン画面を変更</li> <li>・ 3.1.7 Ports 100BASE-FX 品の注意事項を追加</li> <li>・ 3.2.25 DDMI Detailed 100BASE-FX 品の注意事項を追加</li> <li>・ 6. 準拠規格 100BASE-FX を追加</li> </ul>
D	2021年8月31日	<ul style="list-style-type: none"> <li>・ はじめに ファームウェアバージョンアップ時の注意事項を追加</li> <li>・ はじめに 登録商標に関する文言を変更</li> <li>・ 1.1 初期 IP アドレス設定は MANAGE ポートのみ対応、注意書きを追加</li> <li>・ 1.2 パラメーター設定手順 IP アドレス設定手順を変更</li> <li>・ 3.1.2 System IP インバンド管理用 IP アドレスと注意書きを追加</li> <li>・ 3.2.3 IP Status インバンド管理用 IP アドレスを追加</li> <li>・ 3.1.32 PoE Ping Auto Checking パラメーター範囲を変更</li> <li>・ 3.1.32 PoE Ping Auto Checking PD reboot に関する注意書きを追加</li> <li>・ 3.4.1 Restart Device 再起動に関する注意事項を追加</li> <li>・ 3.4.3 Software Upload バージョンアップ時の注意事項を追加</li> <li>・ 3.4.4 Image select バージョンアップ時の注意事項を追加</li> <li>・ 6. 準拠規格 RFC954 : FTP Client を追加</li> </ul>

## はじめに

本書(SW マニュアル(ソフトウェアマニュアル))には、メディアコンバーターApresiaLightMC(-PoE)シリーズの Web ベース GUI の説明および操作方法を記述しています。それ以外のハードウェアに関する説明および操作方法については、各適用機種ハードウェアマニュアルを参照ください。

本書適用の機種一覧表

シリーズ名	製品名	手配品名
ApresiaLightMC シリーズ	ApresiaLightMC-SX	APLMCSX
	ApresiaLightMC-LX	APLMCLX
	ApresiaLightMC-BX20D	APLMCBX20D
	ApresiaLightMC-BX20U	APLMCBX20U
	ApresiaLightMC-BX40D	APLMCBX40D
	ApresiaLightMC-BX40U	APLMCBX40U
	ApresiaLightMC-FX	APLMCFX 受注生産品
ApresiaLightMC-PoE シリーズ	ApresiaLightMC-SX-PoE	APLMCSXPOE
	ApresiaLightMC-LX-PoE	APLMCLXPOE
	ApresiaLightMC-BX20U-PoE	APLMCBX20UPOE
	ApresiaLightMC-BX40U-PoE	APLMCBX40UPOE
	ApresiaLightMC-FX-PoE	APLMCFXPOE 受注生産品



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。

## 注意事項

- ❗ 本ファームウェアは ApresiaLightMC(-PoE)シリーズ専用です。その他の ApresiaLight シリーズにインストールすることはできません。  
また、ApresiaLightMC(-PoE)シリーズに ApresiaLightFM シリーズ、ApresiaLightGM シリーズ、ApresiaLightGM152GT 及び ApresiaLightGS シリーズ用のファームウェアをインストールすることはできません。

## ファームウェアバージョンアップ時の注意事項

- ❗ バージョンアップ時における注意事項を記載しています。ご使用前に必ずご一読下さい。

### 【1.00.04 以前から 1.00.05 以降へのファームウェアバージョン変更時】

- ・ Ver. 1.00.05 のファームウェアではバージョンアップ後にコンフィグ設定の追加/変更が必要な機能を追加しております。リリースノートをご確認いただき、十分理解されたのち、バージョンアップを実行ください。
- ・ 遠隔でバージョンアップ作業を実施された場合、リリースノート記載の APLMC-10005-RC004 の仕様変更により、装置にアクセスできなくなる恐れがありますので、事前に通信環境をご確認ください。  
MANAGE ポート経由の IP アドレスはバージョンアップ後も引き継がれますが、USER ポートまたは LH ポート経由の IP アドレスについては引き継がれずに無効となります。

## 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。

- (a) 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。
- (b) 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。

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

JavaScript、Java は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。

Ethernet 及びイーサネットは、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、本書に記載のブランド名は、各所有者の商標もしくは登録商標です。

# 目次

制定・改訂履歴表	1
はじめに	2
1. パラメーター設定手順	8
1.1 初期 IP アドレス設定	8
1.2 パラメーター設定手順	10
1.3 パラメーター設定端末の準備	13
1.4 パラメーター設定端末の接続	14
2. Web ベース GUI 方式の基本操作	16
2.1 表記規則	16
2.2 セッションの終了	16
2.3 オンラインヘルプ	16
2.4 概要	16
2.4.1 ログイン	17
2.4.2 GUI の画面説明	17
2.5 ナビゲーションメニュー	18
2.6 タイトルバーのアイコン	18
3. コマンドの詳細	19
3.1 Configuration	19
3.1.1 System Information	19
3.1.2 System IP	19
3.1.3 System NTP	22
3.1.4 System Time	23
3.1.5 System Log	26
3.1.6 System Alarm Profile	27
3.1.7 Ports	27
3.1.8 Users	29
3.1.9 SSH/TELNET	31
3.1.10 HTTPS	31
3.1.11 Access Management	33
3.1.12 SNMP System	34
3.1.13 SNMP Trap Destination	34
3.1.14 SNMP Trap Sources	36
3.1.15 SNMP Communities	37
3.1.16 SNMPv3 Users	38
3.1.17 SNMP Groups	39
3.1.18 SNMPv3 Views	40
3.1.19 SNMP Access	41
3.1.20 RMON Statistics	42
3.1.21 RMON History	42

3.1.22	RMON Alarm .....	43
3.1.23	RMON Event .....	45
3.1.24	Link OAM Port .....	46
3.1.25	Link OAM Event .....	47
3.1.26	Loop Protection .....	48
3.1.27	LLDP (For PoE Model Only) .....	49
3.1.28	LLDP-MED (For PoE Model Only) .....	51
3.1.29	PoE (For PoE Model Only) .....	57
3.1.30	PoE Power Scheduler (For PoE Model Only) .....	59
3.1.31	PoE Power Reset (For PoE Model Only) .....	60
3.1.32	PoE Ping Auto Checking (For PoE Model Only) .....	60
3.1.33	CPOE (For PoE Model Only) .....	62
3.1.34	Storm Policing .....	64
3.1.35	LPT .....	64
3.2	Monitor .....	66
3.2.1	System Information .....	66
3.2.2	CPU Load .....	67
3.2.3	IP Status .....	67
3.2.4	System Log .....	68
3.2.5	System Detailed Log .....	70
3.2.6	System Alarm .....	70
3.2.7	Ports State .....	71
3.2.8	Traffic Overview .....	72
3.2.9	Detailed Statistics .....	73
3.2.10	Link OAM Statistics .....	74
3.2.11	Link OAM Port Status .....	76
3.2.12	Link OAM Event Status .....	78
3.2.13	Access Management Statistics .....	80
3.2.14	RMON Statistics .....	80
3.2.15	RMON History .....	82
3.2.16	RMON Alarm .....	83
3.2.17	RMON Event .....	84
3.2.18	Loop Protection .....	85
3.2.19	LLDP Neighbors (For PoE Model Only) .....	85
3.2.20	LLDP-MED Neighbors (For PoE Model Only) .....	86
3.2.21	LLDP PoE (For PoE Model Only) .....	90
3.2.22	LLDP Port Statistics (For PoE Model Only) .....	91
3.2.23	PoE (For PoE Model Only) .....	93
3.2.24	DDMI Overview .....	94
3.2.25	DDMI Detailed .....	94

3.3 Diagnostics .....	95
3.3.1 Ping (IPv4) .....	95
3.3.2 Traceroute (IPv4) .....	97
3.4 Maintenance .....	98
3.4.1 Restart Device .....	98
3.4.2 Factory Default .....	99
3.4.3 Software Upload .....	99
3.4.4 Image select .....	100
3.4.5 Save Configuration .....	101
3.4.6 Download Configuration .....	101
3.4.7 Upload Configuration .....	102
3.4.8 Activate Configuration .....	103
3.4.9 Delete Configuration .....	103
4. 使用上の注意事項 .....	105
5. トラブルシューティング .....	106
5.1 表示 LED に関連する現象と対策 .....	106
5.2 コンソール端末に関連する現象と対策 .....	106
5.3 HTTPS に関連する現象と対策 .....	107
5.4 メディアコンバーター機能に関連する現象と対策 .....	107
5.5 SFP に関連する現象と対策 .....	107
5.6 PoE に関連する現象と対策 .....	107
6. 準拠規格 .....	108

# 1. パラメーター設定手順

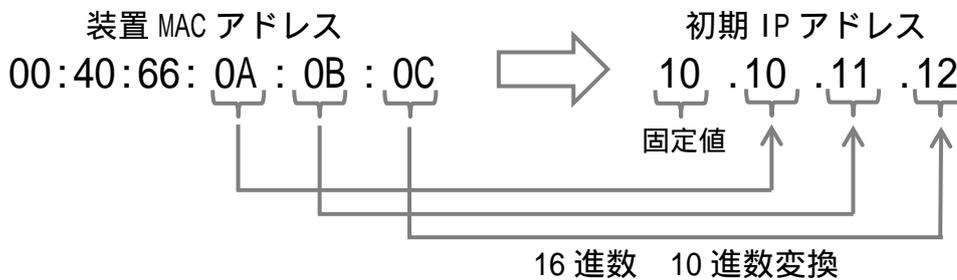
パラメーターの設定は、設定端末の準備、設定端末の接続、パラメーターの設定手順で行います。  
Web ベース GUI 方式によるコマンド詳細については 3 章を参照してください。  
なお、コマンドライン方式については別紙 (CLI マニュアル) を参照してください。

## 1.1 初期 IP アドレス設定

初回起動時に初期 IP アドレスが以下の設定ルールに従って MANAGE ポートに自動設定されます。ご使用の環境に合わせて IP アドレスを変更してください。

### (1) 初期 IP アドレスの設定ルール

初期 IP アドレスの先頭 1 バイトは 10 の固定とし、2 バイトから 4 バイトまでは装置 MAC アドレスの下位 3 バイトを 16 進数から 10 進数に変換した値で自動的に設定されます。  
装置 MAC アドレスが 00:40:66:0A:0B:0C の場合、初期 IP アドレスは 10.10.11.12 となります。

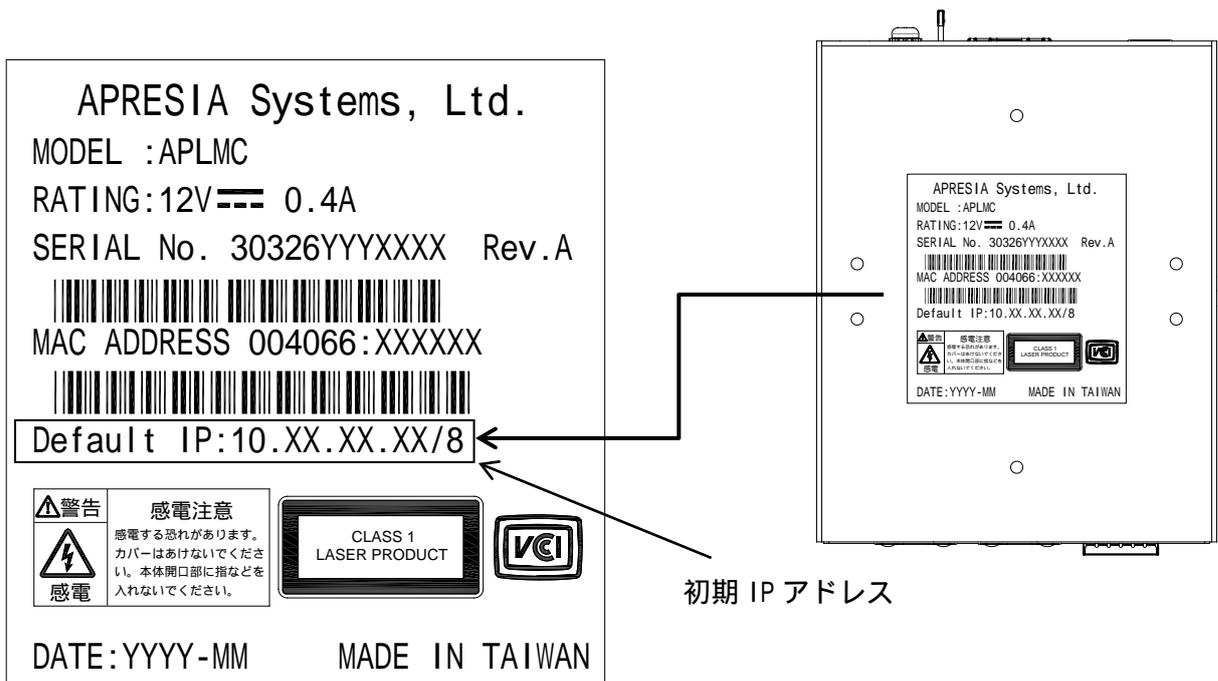


### (2) サブネットマスク

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。

### (3) 初期 IP アドレスの確認方法

初期 IP アドレスは装置底面の機器銘版ラベル上に表記されます。



## 注意事項

-  工場出荷時の初期 IP アドレス(MANAGE ポートのみ)は、内部的に VLAN default(vid=1) に所属します。vid=1 以外の vid に IP アドレスを設定することはできません。タグ付きフレームから本装置にアクセスすることはできません。
-  [APLMC 1.00.04 以前]  
工場出荷時の初期 IP アドレス(MANAGE ポート/USER ポート/LH ポート)は、内部的に VLAN default(vid=1) に所属します。

## 1.2 パラメーター設定手順

### (1) パラメーター設定端末を用いた IP アドレス設定の手順

パラメーター設定端末の準備(1.3 節参照)

パラメーター設定端末の接続(1.4 節参照)

パラメーター設定端末の電源 ON

本装置の電源 ON

LED 表示ランプの確認  
PWR 表示 LED が点灯していることを確認してください。

#### パラメーター設定端末の表示画面の確認

以下のような表示がされていることを確認してください。

表示されない場合、Enter キーを押し、コンソール画面を更新してください。

<表示例>

```
ApresiaLightMC Gigabit Ethernet Media Converter
Command Line Interface
```

```
Firmware: 1.00.05
```

```
Copyright(c) 2020 APRESIA Systems, Ltd. All rights reserved.
```

```
Press the <TAB> or <?> key any time you lose the direction
```

```
Warning for security
```

```
Please change default password for login account as soon after start using.
```

```
And also, please set access-allowed IP address to avoid incorrect access
by using access management function.
```

```
Press ENTER to get started
```

```
Username: adpro
```

```
Password:
```

```
#
```

#### パスワードの設定

例として、アカウント名「adpro」のパスワードを「pass1234」に設定する場合を以下に示します。

```
# configure terminal
```

```
(config)# username adpro privilege 15 password unencrypted pass1234
```

例 1 : MANAGE ポート(アウトバンド管理)に IP アドレスを設定する場合

IP アドレスの設定

例として、IP アドレス 10.1.1.1/8 を MANAGE ポートに設定する場合を以下に示します。

```
(config)# interface manage
(manage-config)# ip address 10.1.1.1 255.0.0.0
(manage-config)# exit
```

例 2 : USER ポート/LH ポート(インバンド管理)に IP アドレスを設定する場合

IP アドレスの設定

例として、IP アドレス 10.1.1.1/8 を USER ポート/LH ポートに設定する場合を以下に示します。

```
(config)# interface inband
(manage-config)# ip address 10.1.1.1 255.0.0.0
(manage-config)# exit
```

アクセス制限の設定

例として、アクセス許可する IP アドレスを 10.1.1.10 に設定する場合を以下に示します。

```
(config)# access management 1 10.1.1.10 all
(config)# access management
```

設定情報の保存

```
# copy running-config startup-config
Building configuration...
% Saving 2220 bytes to flash:startup-config
#
```

本装置からログアウト

```
#logout
```

パラメーター設定端末を電源 OFF とし、本装置から取り外します。

セットアップ完了

(2) Web ベース GUI 方式を用いたパラメーター設定の手順

Web ベース GUI 方式を用いたパラメーターの設定は、本装置の MANAGE ポートが LAN に接続され IP アドレスが設定されている場合のみ可能です。

(Ver. 1.00.05 以降。Ver. 1.00.04 以前は MANAGE ポート/USER ポート/LH ポートから設定可能)

本装置に割り当てられた IP アドレスに HTTPS でアクセスしてください。

例) <https://10.1.1.1>

認証画面が表示されることを確認してください。

システムログイン(2.4.1項参照)

システムパラメーターの設定(2章参照)

セットアップ完了

### 1.3 パラメーター設定端末の準備

本装置のパラメーター設定に必要な端末の条件及び通信条件を表 1-1 に記載します。

表 1-1 パラメーター設定端末の条件及び通信条件

#### (1) パラメーター設定端末の条件

項番	項目	仕様
1	端末の設定	ANSI X3.64/VT100
2	スクリーンサイズ	80 列×24 行/スクリーン以上

#### (2) 通信条件

項番	項目	仕様
1	キャラクター	8 bit/キャラクター
2	ストップビット	1 bit
3	パリティ	なし
4	ボー・レート	9,600 bit/s
5	フロー制御	なし
6	端末接続ケーブル	RS-232 ケーブル (クロス)

## 1.4 パラメーター設定端末の接続

コンソールポートの接続にはRS-232C ケーブルを使用します。ケーブルは製品に添付されておりませんので、事前に準備しておく必要があります。パラメーター設定端末により接続方法が異なりますので、下記を参考に接続してください。



図 1-1 RS-232C ケーブルの接続

本装置のコンソールポートのピン仕様を図 1-2、表 1-2 に記載します。コンソールポートはRJ-45 形状です。パラメーター設定端末により接続方法が異なりますので、下記を参考に接続してください。

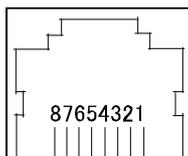


図 1-2 コンソールポートのピン No.

表 1-2 コンソールポートのピン仕様

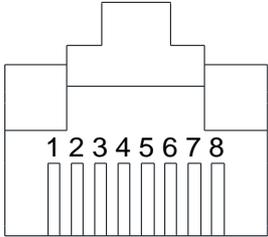
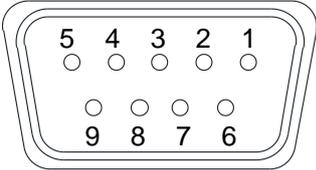
ピン No.	信号名	信号の内容	備考
1	RS(RTS)	送信リクエスト	不使用
2	ER(DTR)	データ端末レディ	不使用
3	SD(TxD)	送信データ	出力
4	SG(GND)	回路アース	-
5	SG(GND)	回路アース	-
6	RD(RxD)	受信データ	入力
7	DR(DSR)	データセットレディ	不使用
8	CS(CTS)	送信可	不使用

### 注意事項

- ❗ コンソールポートには、パラメーター設定時のみ RS-232C ケーブルを接続し、誤入力防止のため通常の運用時には接続しないでください。

本装置とパラメーター設定端末を RS232C ケーブル(装置側 RJ-45/設定端末側 D-SUB9 ピン)で接続する場合の RS-232C ケーブルのピン配置と結線例を表 1-3 に記載します。

表 1-3 RS-232C ケーブル接続結線例(D-SUB9 ピン-9 ピンの場合)

コンソールポート側(RJ-45)		接続	設定端末側(D-SUB9)	
ピン番号	信号名称		ピン番号	信号名称
1	RS(RTS)		7	CS(CTS)
2	ER(DTR)		4	DR(DSR)
3	SD(TxD)		3	RD(RxD)
4	SG(GND)		5	SG(GND)
5	SG(GND)			
6	RD(RxD)		2	SD(TxD)
7	DR(DSR)		6	ER(DTR)
8	CS(CTS)		8	RS(RTS)
		-		
RJ-45 コネクタ(オス)		-	D-SUB9 コネクタ(メス)	

**!** コンソールポートと 10BASE-T/100BASE-TX/1000BASE-T などの Ethernet ポートを接続しないでください。誤って接続した場合、故障の可能性があります。

## 2. Web ベース GUI 方式の基本操作

Web ベース GUI 方式によるパラメーターの表示/設定方法を説明します。

### 2.1 表記規則

3章のコマンドの詳細にて記述される、引数の表記規則を表 2-1 に記載します。

表 2-1 コマンド引数の表記規則

表記規則	説明
[ ]	ボタン、ツールバーアイコン、メニュー、または、メニュー項目を示します。 表示例： [Home]をクリックして初期ページを表示します。
メニュー名 > メニューオプション	メニュー名 > メニューオプションはシステムメニューの構成を示します。 表示例： Configuration > System これは、[Configuration]メニューの下に [System]メニューがあることを意味します。

### 2.2 セッションの終了

セッションを終了するには、Web ブラウザを閉じます。これにより、権限のないユーザーがユーザー名とパスワードを使用してシステムにアクセスすることを防止できます。

### 2.3 オンラインヘルプ

各画面には、画面に関連する情報のページを呼び出すヘルプボタンがあります。新しいウィンドウにヘルプが表示されます。

### 2.4 概要

Web ブラウザを使用して、遠隔から HTTPS プロトコルでメディアコンバーターにアクセスします。Web ベース GUI 方式は、GUI 画面で設定を行います。

#### 注意事項

-  Web ブラウザは Google Chrome での動作を確認しています。  
なお、ブラウザに関する情報は把握しておりませんので、十分な検証の上ご使用いただきますようお願いいたします。
-  Web ベース GUI は、動的な表示を実現するために JavaScript を使用しています。一部の機能を利用するためには Web ブラウザ及び Java の設定を適切に行う必要があります。
-  HTTPS の Web ベース GUI のため、GUI 画面へのアクセス時の CPU 負荷が大きくなり、適用されるセキュリティ方式によっては大幅に CPU 負荷が増加することがあります。

### 2.4.1 ログイン

本装置にアクセスするには、ブラウザのアドレスバーに `https://[本装置の初期 IP アドレス]` を入力します。

初期 IP アドレスは、本装置の筐体底面に貼られているラベルにを記載しています。IP アドレスを変更したい場合は、「パラメーター設定手順」に従いコマンドラインインターフェースから IP アドレスの設定変更を行ってください。

下記の図にあるような認証画面が開きます。



ユーザー名とパスワードを入力し(デフォルトのユーザー名:adpro、パスワード:なし)、OK をクリックします。GUI 画面が開きます。

次に Web ベース GUI 方式の操作方法については記載します。

### 2.4.2 GUI の画面説明

GUI の画面は、下記に示すように 3 つの領域に分割されています。



領域 1	表示するフォルダまたはウィンドウを選択するナビゲーションメニューです。フォルダアイコンを開いて、ハイパーリンクウィンドウボタンとそれに含まれるサブフォルダを表示します。
領域 2	ホームアイコン、ログアウトアイコン、ヘルプアイコンがクリック可能です。
領域 3	初期状態、または領域 2 のホームアイコンをクリックすると、フロントパネルのグラフィック画像により、スイッチのステータスやポート状態などを表示します。 また、領域 1 で選択した構成データおよびエントリーに基づくスイッチ情報を表示します。

## 注意事項

- 
 現在のセッション中に本装置の設定を変更した場合は、Maintenance > Configuration > Save startup-config または、コマンドラインインターフェース (CLI) コマンド `copy running-config startup-config` で設定を保存して下さい。

## 2.5 ナビゲーションメニュー

Web インターフェースのすべてのメイン画面にアクセスするには、画面の左側(領域 1)にある 4 つのメニューボックスのハイパーリンクをクリックします。



## 2.6 タイトルバーのアイコン



ホームボタン

Web ページが [Port State Overview] ページに戻ります。



ヘルプボタン

より詳細なヘルプについては、各画面のボタンをクリックしてください。  
ヘルプ情報は別のウィンドウに表示されます。



ログアウトボタン

ログアウトボタンをクリックすると、システムは正常にログアウトされます。

### 3. コマンドの詳細

#### 注意事項

- ❗ 本ファームウェア (Ver. 1.00) では、本章に記載している設定のみサポートしております。未記載の設定を行った場合の動作は保証されません。

#### 3.1 Configuration

##### 3.1.1 System Information

Configuration > System > Information

デバイスのシステム情報を設定します。

### System Information Configuration

System Contact	<input type="text"/>
System Name	<input type="text"/>
System Location	<input type="text"/>

オブジェクト	説明
System Contact	この管理対象ノードの連絡先担当者のテキストによる識別情報と、この担当者への連絡方法に関する情報。使用できる文字列の長さは0から255で、使用できる内容は32から126までのASCII文字です。
System Name	この管理対象ノードに管理上割り当てられた名前。慣例により、これはノードの完全修飾名です。名前は、アルファベット (A~Z, a~z)、数字 (0~9)、マイナス記号 (-) からなる文字列です。名前の一部としてスペース文字は使用できません。最初の文字は英字である必要があります。また、最初または最後の文字をマイナス記号にすることはできません。文字列の長さは0から63までです。
System Location	このノードの物理的な場所 (例: telephone closet, 3rd floor)。使用できる文字列の長さは0から255で、使用できる内容は32から126までのASCII文字です。

ボタン	
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

##### 3.1.2 System IP

Configuration > System > IP

IP 基本設定を構成し、IP インターフェースと IP ルートを制御します。  
 サポートされるインターフェースの最大数は 8 で、ルートの最大数は 32 です。

IP Configuration

IP Interfaces

Interface	Enable	DHCPv4				Hostname	Fallback	Current Lease	IPv4	
		Type	IfMac	ASCII	HEX				Address	Mask Length
manage	<input type="checkbox"/>	Auto	Port USER				0		10.249.35.127	23
inband	<input type="checkbox"/>	Auto	Port USER				0			

IP Routes

Delete	Network	Mask Length	Gateway
<input type="checkbox"/>	0.0.0.0	0	10.249.34.1
<input type="checkbox"/>	0.0.0.0	0	10.250.4.3
<input type="checkbox"/>	0.0.0.0	0	10.250.4.4
<input type="checkbox"/>	0.0.0.0	0	10.250.4.8
<input type="checkbox"/>	0.0.0.0	0	10.250.4.10
<input type="checkbox"/>	0.0.0.0	0	10.250.4.40
<input type="checkbox"/>	0.0.0.0	0	10.250.4.77

Add Route

Save Reset

オブジェクト	説明
IP Interfaces	
Interface	[manage]: (アウトバンド管理用)MANAGE ポートのみ、本装置へ IP アクセスが可能です。 [inband]: (インバンド管理用)USER ポート/LH ポートから本装置へ IP アクセスが可能です。デフォルト値は無効です。
DHCPv4/ Enable	このチェックボックスをオンにして、DHCPv4 クライアントを有効にします。このオプションを有効にすると、システムは DHCPv4 プロトコルを使用してインタフェースの IPv4 アドレスとマスクを構成します。
DHCPv4/ Client ID/ Type	クライアント識別子のタイプは選択可能です。オプションは Auto、IF_MAC、ASCII、HEX です。デフォルトは Auto です。タイプが Auto で、ホスト名が設定されている場合(空でない)、ホスト名が DHCP オプション 61 フィールドで使用されます。しかし、hostname が空文字列の場合、xx-xx-xx-xx-xx-xx の形式でシステムの MAC アドレスが使用されます。 Note:上記の 2 つの場合のどちらでも、オプション 61 フィールドの前に余分なバイト 00 が追加されます。 たとえば、xx-xx-xx-xx-xx-xx の場合、オプション 61 の値の長さは 18 になります。 0x00 は Not HW Address を表します。
DHCPv4/ Client ID/ IfMac	DHCP クライアント識別子のインターフェース名。DHCPv4 クライアントが有効で、クライアント識別子タイプが「Ifmac」の場合、設定されたインタフェースのハードウェア MAC アドレスが DHCP オプション 61 フィールドで使用されます。 たとえば、ポート 2 が選択されている場合、オプション 61 の値は、システムの MAC に 2 を加えた値になります。 Note:この場合、01aabbcc010203、長さ 7 のように、オプション 61 フィールドの前に追加バイト 01 が追加されます。

	0x01 は Hardware type Ethernet の略です。
DHCPv4/ Client ID/ ASCII	DHCP クライアント識別子の ASCII 文字列。DHCPv4 クライアントが有効で、クライアント識別子タイプが「ascii」の場合、ASCII 文字列が DHCP オプション 61 フィールドで使用されます。 Note:この場合、オプション 61 フィールドの前にバイト 00 が追加されます。 0x00 は Not HW Address を表します。また、常に小文字を使用します。
DHCPv4/ Client ID/ HEX	DHCP クライアント識別子の 16 進文字列。DHCPv4 クライアントが有効で、クライアント識別子タイプが「HEX」の場合、DHCP オプション 61 フィールドで 16 進数が使用されます。 Note:この場合、オプション 61 の値は、余分なバイトを含まない HEX とまったく同じになります。
DHCPv4/ Hostname	DHCP クライアントのホスト名。DHCPv4 クライアントが有効な場合は、構成されたホスト名が [DHCP option12] フィールドで使用されます。この値が空の文字列の場合、オプション 12 フィールドは system mac を使用します。
DHCPv4/ Fallback	DHCP リースの取得を試行する秒数。この期間が過ぎると、構成済みの IPv4 アドレスが IPv4 インタフェースアドレスとして使用されます。値が 0 の場合はフォールバックメカニズムが無効になり、有効なリースが取得されるまで DHCP が再試行を続けます。有効な値は 0 ~ 4294967295 秒です。
DHCPv4/ Current Lease	アクティブなリースを持つ DHCP インタフェースの場合、この列には、DHCP サーバーによって提供される現在のインタフェースアドレスが表示されます。
IPv4/ Address	インタフェースの IPv4 アドレスをドット 10 進表記で指定します。DHCP が有効な場合、このフィールドはフォールバックアドレスを設定します。インタフェース上で IPv4 操作が望まれない場合、または DHCP フォールバックアドレスが望まれない場合、このフィールドは空欄にしておくことができます。
IPv4/ Mask Length	IPv4 ネットワークマスクのビット数(プレフィックス長)。有効な値は、IPv4 アドレスの 0 から 30 ビットです。DHCP が有効な場合、このフィールドはフォールバックアドレスのネットワークマスクを設定します。インタフェース上で IPv4 操作が望まれない場合、または DHCP フォールバックアドレスが望まれない場合、このフィールドは空欄にしておくことができます。
IP Routes	
Delete	既存の IP ルートを削除するには、このオプションを選択します。
Network	このルートの宛先 IP ネットワークまたはホストアドレス。有効な形式は、ドット付き 10 進表記です。デフォルトルートは次の値を使用できます。0.0.0.0.
Mask Length	ビット数(プレフィックス長)での宛先 IP ネットワークまたはホストマスク。このルートの条件を満たすために一致する必要があるネットワークアドレスの量を定義します。有効な値は、0 から 32 ビットです。デフォルトルートだけが 0(どんなものにも合うので)のマスク長を持ちます。

Gateway	IP ゲートウェイの IP アドレス。有効な形式は、ドット付き 10 進表記です。
---------	---

ボタン	
Add Interface	新しい IP インターフェースを追加するときにクリックします。最大 8 つのインターフェースがサポートされています。
Add Route	新しい IP ルートを追加するときにクリックします。最大 32 のルートがサポートされています。
Save	クリックして変更を保存します。
Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

#### 注意事項

- 
 工場出荷時の初期 IP アドレス(MANAGE ポート用)(アウトバンド管理)は、内部的に VLAN default(vid=1) に所属します。MANAGE ポートには vid=1 以外の vid に IP アドレスを設定することはできません。
- 
 USER ポート/LH ポート用に IP アドレスを設定可能です(インバンド管理)。内部的に VLAN default(vid=2) に所属します。USER ポート/LH ポートには vid=2 以外の vid に IP アドレスを設定することはできません。
- 
 MANAGE ポート(アウトバンド管理用)、USER ポート/LH ポート(インバンド管理用)にはそれぞれに IP アドレスを設定できますが、別セグメントにする必要があります。また、タグ付きフレームから本装置にアクセスすることはできません。

#### 3.1.3 System NTP

Configuration > System > NTP

このページで NTP を構成します。

### NTP Configuration

<b>Mode</b>	Disabled <input type="button" value="v"/>
<b>Server 1</b>	<input type="text"/>
<b>Server 2</b>	<input type="text"/>
<b>Server 3</b>	<input type="text"/>
<b>Server 4</b>	<input type="text"/>
<b>Server 5</b>	<input type="text"/>

オブジェクト	説明
Mode	NTP モードの動作を示します。

	[Enabled] NTP クライアントモードの動作を有効にします。 [Disabled] NTP クライアントモードの動作を無効にします。
Server #	NTP サーバーの IPv4 アドレスを指定します。

ボタン	
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.4 System Time

Configuration > System > Time

このページでは、タイムゾーンを構成できます。

## Time Zone Configuration

Time Zone Configuration	
Time Zone	(UTC+09:00) Osaka, Sapporo, Tokyo ▼
Hours	9 ▼
Minutes	0 ▼
Acronym	JST ( 0 - 16 characters )

## Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled ▼

Start Time settings	
Month	Jan ▼
Date	1 ▼
Year	2014 ▼
Hours	0 ▼
Minutes	0 ▼
End Time settings	
Month	Jan ▼
Date	1 ▼
Year	2097 ▼
Hours	0 ▼
Minutes	0 ▼
Offset settings	
Offset	1 (1 - 1439) Minutes

## Date/Time Configuration

Date/Time settings	
Year	2019 (2000 - 2037)
Month	Oct ▼
Date	21 ▼
Hours	12 ▼
Minutes	41 ▼
Seconds	35 ▼

Save Reset

オブジェクト	説明
Time Zone Configuration	
Time Zone	世界中のさまざまなタイムゾーンを一覧表示します。ドロップダウン・リストから適切なタイム・ゾーンを選択し、 [Save] をクリックして設定します。 [Manual Setting] オプションは、オプションリストから除外される特定のタイムゾーンに使用されます。
Hours	UTC からのオフセット時間。このフィールドは、タイムゾーンが [Manual Setting] で設定されている場合にのみ使用できます。
Minutes	UTC からのオフセット時間 (分)。このフィールドは、タイムゾーンが

	[Manual Setting]で設定されている場合にのみ使用できます。
Acronym	ユーザーはタイムゾーンの頭字語を設定できます。タイムゾーンを識別するためのユーザー設定可能な頭字語です。(範囲:最大 16 文字)文字列 '' は、NULL 入力用に予約された特殊な構文です。
Daylight Saving Time Configuration 夏時間の設定	
Daylight Saving Time	これを使用して、定義された夏時間の間、次の設定に従ってクロックを前後に設定します。[Disable]を選択して、夏時間設定を無効にします。[Recurring]を選択し、設定を毎年繰り返すように夏時間を設定します。[Non-Recurring]を選択し、サマータイムを設定します。(デフォルト:[Non-Recurring])
Recurring Configurations 繰り返し構成	
Start time settings 開始時間の設定	
Week	開始週番号を選択します。
Day	開始日を選択します。
Month	開始月を選択します。
Hours	開始時間を選択します。
Minutes	開始分を選択します。
End time settings 終了時間の設定	
Week	終了週番号を選択します。
Day	終了日を選択します。
Month	終了月を選択します。
Hours	終了時間を選択します。
Minutes	終了分を選択します。
Offset settings オフセット設定	
Offset	夏時間に追加する分数を入力します。(範囲:1 から 1439)
Non Recurring Configurations	
Start time settings 開始時間の設定	
Month	開始月を選択します。
Date	開始日を選択します。
Year	開始年を選択します。
Hours	開始時間を選択します。
Minutes	開始分を選択してください
End time settings 終了時間の設定	
Month	終了月を選択します。
Date	終了日を選択します。
Year	終了年を選択します。
Hours	終了時間を選択します。
Minutes	終了分を選択します。
Offset settings オフセット設定	
Offset	夏時間に追加する分数を入力します。(範囲:1 から 1439)
Date/Time Configuration 日付/時刻構成	
Date/Time Settings 日付/時刻の設定	
Year	現在の日時の年(範囲:2000 から 2037)
Month	現在の日時の月

Date	現在の日時の日付
Hours	現在の日時の時間
Minutes	現在の日時の分
Seconds	現在の日時の秒

ボタン	
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.5 System Log

Configuration > System > Log

このページでシステムログを設定します。

#### System Log Configuration

<b>Server Mode</b>	Disabled <input type="button" value="v"/>
<b>Server Address</b>	<input type="text"/>
<b>Syslog Level</b>	Informational <input type="button" value="v"/>

<input type="button" value="Save"/>	<input type="button" value="Reset"/>
-------------------------------------	--------------------------------------

オブジェクト	説明
Server Mode	サーバーモードの動作を示します。mode 操作を有効にすると、syslog メッセージが syslog サーバに送信されます。syslog プロトコルは UDP 通信に基づいており、UDP ポート 514 で受信されます。また、UDP はコネクションレス型プロトコルであり、確認応答を提供しないため、syslog サーバは確認応答を送信者に返信しません。syslog サーバが存在しない場合でも、syslog パケットは常に送信されます。 使用可能なモードは次のとおりです。 [Enabled]:サーバーモード操作を有効にします。 [Disabled]:サーバーモード操作を無効にします。
Server Address	syslog サーバの IPv4 ホストアドレスを示します。
Syslog Level	syslog サーバに送信するメッセージの種類を示します。 [Error]:重大度コードが Error(3)以下の特定メッセージを送信します。 [Warning]:重大度コードが Warning(4)以下の特定メッセージを送信します。 [Notice]:重大度コードが Notice(5)以下の特定メッセージを送信します。 [Informational]:重大度コードが Informational(6)以下の特定メッセージを送信します。

ボタン	
<input type="button" value="Save"/>	クリックして変更を保存します。

Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。
-------	--

### 3.1.6 System Alarm Profile

Configuration > System > Alarm Profile

アラームを有効/無効にするアラームプロファイルが表示されます。

#### Alarm Profile

No	Description	Enabled
* *		<input checked="" type="checkbox"/>
1	Link down on Port-USER	<input checked="" type="checkbox"/>
2	Link down on Port-LH	<input checked="" type="checkbox"/>
3	Link down on Port-MANAGE	<input type="checkbox"/>

Save	Reset
------	-------

オブジェクト	説明
No	アラームプロファイルエントリのインデックス
Description	アラームタイプの説明
Enabled	<p>チェックボックスが有効になっている場合、アラームが発生するとアラーム履歴/現在値にアラームが表示され、アラーム LED が点灯します。SNMP トラップエントリが存在し有効になっている場合は、SNMP トラップが送信されます。</p> <p>チェックボックスが無効になっている場合、アラームが発生してもアラームは取得されず、アラーム履歴/現在に表示されません。アラーム LED の点灯、および SNMP トラップも送信されません。</p>

ボタン	
Save	クリックして変更を保存します。
Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.7 Ports

Configuration > Ports

このページには、現在のポート構成が表示されます。ポートを設定します。

#### Port Configuration

Refresh

Port	Link	Speed		Adv Duplex		Adv speed			Maximum Frame Size	Excessive Collision Mode	Frame Length Check	MDI/MDIX Mode	Description
		Current	Configured	Fdx	Hdx	10M	100M	1G					
*		<>	<>	<input checked="" type="checkbox"/>	9600	<>	<input type="checkbox"/>	<>					
USER	1Gfdx	Auto	Auto	<input checked="" type="checkbox"/>	9600	Discard	<input type="checkbox"/>	MDI	USER Port				
LH	100fdx Fiber	Auto	Auto	<input type="checkbox"/>	9600		<input type="checkbox"/>		LH Port				
MANAGE	100fdx	Auto	Auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9600	Discard	<input type="checkbox"/>	MDI	Management Port

Save	Reset
------	-------

オブジェクト	説明
--------	----

Port	対象ポートの名称です。
Link	現在のリンク状態がグラフィカルに表示されます。緑色はリンクがアップしていることを示し、赤色はリンクがダウンしていることを示します。
Speed/Current	ポートの現在のリンク速度を示します。
Speed/Configured	指定されたデバイスポートで利用可能なリンク速度を選択します。特定のポートでサポートされている速度のみが表示されます。表示される速度は次のとおりです。 [Disabled] デバイスポートの動作を無効にします。 [Auto] 対向装置のポートとの AutoNegotiation 機能で、互換性のある最高速度が選択されます。 [10Mbps HDX] 対象ポートを強制的に 10Mbps 半二重モードにします。 [10Mbps FDX] 対象ポートを強制的に 10Mbps 全二重モードにします。 [100Mbps HDX] 対象ポートを強制的に 100Mbps 半二重モードにします。 [100Mbps FDX] 対象ポートを強制的に 100Mbps 全二重モードにします。 [1Gbps FDX] 対象ポートを強制的に 1Gbps 全二重にします。
Adv Duplex	Speed/Configured を [Auto] に設定されている場合に、AutoNegotiation 機能で選択可能な Duplex モードを設定しておくことができます。 Fdx : Full Duplex(全二重) Hdx : Half Duplex(半二重)
Adv Speed	Speed/Configured を [Auto] に設定されている場合に、AutoNegotiation 機能で選択可能なリンクスピードを設定しておくことができます。 10Mbps, 100Mbps, 1Gbps Speed と Duplex には規格上決められた組み合わせがあり、無効な組み合わせの場合、Speed を優先して接続モードを決定します。
Maximum Frame Size	FCS を含むデバイス・ポートで許可される最大フレーム・サイズを入力します。範囲は 1518 ~ 9600 バイトです。
Excessive Collision Mode	ポート送信衝突動作を設定します。 [Discard] 16 コリジョン後にフレームを廃棄します。(デフォルト) [Restart] 16 回の衝突後にバックオフアルゴリズムを再開します。
Frame Length Check	EtherType/Length フィールドでフレーム長が正しくないフレームを廃棄するかどうかを設定します。イーサネットフレームにはフィールド EtherType が含まれており、これを使用して 1535 以下の値のフレームペイロードサイズ(バイト単位)を示すことができます。EtherType/Length フィールドが 1535 より大きい場合、フィールドが EtherType として使用されていることを示します(フレームのペイロードにカプセル化されているプロトコルを示します)。「フレーム長チェック」が有効な場合、EtherType/Length フィールドが実際のペイロード長と一致しないと、ペイロードサイズが 1536 バイト未満のフレームは廃棄されます。「フレーム長チェック」を無効にすると、フレーム長の不一致のためにフレームがドロップされません。 Note: フレーム長の不一致によりドロップされたフレーム数をカウントするドロップカウンタはありません。
MDI/MDIX Mode	MDI, MDIX を設定します。 Speed/Configured を [Auto] に設定されている場合には本設定に関わら

	ず AutoNegotiation 機能により自動で決定されます。 Speed/Configured を固定値に設定にした場合は適切に MDI, MDIX を設定してください。
Description	ポートの説明。最大長は 255 文字です。

ボタン	
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。
<input type="button" value="Refresh"/>	クリックすると、ページが更新されます。ローカルで行った変更はすべて元に戻されます。

#### 注意事項

- ❗ Excessive Collision Mode、Frame Length Check は評価未実施のため、サポートの対象外になります。
- ❗ ApresiaLightMC-FX(手配品名：APLMCFX)、ApresiaLightMC-FX-PoE(手配品名：APLMCFXPOE)の LH ポートは 100M Full 固定のみサポートしています。100BASE-FX SFP モジュールを本装置に実装することで、自動的に 100M Full 固定設定になります。
- ❗ ApresiaLightMC-FX(手配品名：APLMCFX)、ApresiaLightMC-FX-PoE(手配品名：APLMCFXPOE)の USER ポートは自動的に 10M/100M に設定されません。必要に応じて設定を変更してください。

#### 3.1.8 Users

Configuration > Security > System > Users

このページには、現在のユーザーの概要が表示されます。現在、Web サーバで別のユーザとしてログインするには、ブラウザを閉じてから再度開いてください。

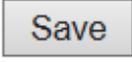
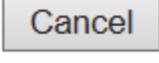
### Users Configuration

User Name	Privilege Level
adpro	15

#### Add User

User Settings	
User Name	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>

オブジェクト	説明
User Configuration ユーザー設定	
User Name	ユーザーを識別する名前。
Privilege Level	ユーザーの権限レベル。指定できる範囲は0から15です。特権レベルの値が15の場合、すべてのグループにアクセスできます。つまり、デバイスの完全な制御が許可されます。しかし、他の値は各グループの権限レベルを参照する必要があります。そのグループにアクセスするには、ユーザーの権限がグループの権限レベル以上である必要があります。デフォルト設定では、ほとんどのグループの権限レベル5は読み取り専用アクセスを持ち、権限レベル10は読み取り/書き込みアクセスを持ちます。また、システムメンテナンス(ソフトウェアのアップロード、工場出荷時のデフォルト設定など。)には、ユーザ権限レベル15が必要です。一般に、特権レベル15は、管理者アカウントに対して、特権レベル10は、標準ユーザアカウントに対して、特権レベル5は、ゲストアカウントに対して使用することができます。
Add User ユーザーの追加	
User Name	このエントリが属するユーザ名を識別する文字列。文字列の長さは1から31までです。有効なユーザー名には、文字、数字、およびアンダースコアを使用できます。
Password	ユーザーのパスワード。文字列の長さは0から31までです。スペースを含む印刷可能な文字はすべて使用できます。ユーザーの権限レベル。指定できる範囲は0から15です。特権レベルの値が15の場合、すべてのグループにアクセスできます。つまり、デバイスの完全な制御が許可されます。しかし、他の値は各グループの権限レベルを参照する必要があります。そのグループにアクセスするには、ユーザーの権限がグループの権限レベル以上である必要があります。デフォルト設定では、ほとんどのグループの権限レベル5は読み取り専用アクセスを持ち、権限レベル10は読み取り/書き込みアクセスを持ちます。また、システムメンテナンス(ソフトウェアのアップロード、工場出荷時のデフォルト設定など)には、ユーザ権限レベル15が必要です。一般に、特権レベル15は、管理者アカウントに対して、特権レベル10は、標準ユーザアカウントに対して、特権レベル5は、ゲストアカウントに対して使用します。
Password (again)	確認のためにパスワードをもう一度入力します。

ボタン	
	新しいユーザーを追加するときにクリックします。ユーザーの最大数は20です。
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。
	クリックすると、ローカルで行ったすべての変更が元に戻され、ユーザーに戻ります。

<b>Delete User</b>	現在のユーザーを削除します。このボタンは、新しい構成(新しいユーザーの追加)では使用できません。
--------------------	--

### 3.1.9 SSH/TELNET

Configuration > Security > System > SSH/TELNET

このページで SSH/TELNET を構成します。

## SSH Configuration

<b>SSH Mode</b>	Enabled ▼
<b>TELNET Mode</b>	Disabled ▼

Save	Reset
------	-------

オブジェクト	説明
Mode	SSH および TELNET モード操作を示します。可能なモードは次のとおりです。 [Enabled] SSH/TELNET モード操作を有効にします。 [Disabled] SSH/TELNET モード操作を無効にします (TELNET はデフォルトで無効になっています)。

ボタン	
Save	クリックして変更を保存します。
Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.10 HTTPS

Configuration > Security > System > HTTPS

このページでは、HTTPS 設定を構成し、デバイスの現在の証明書を維持できます。

## HTTPS Configuration

Refresh
---------

<b>Mode</b>	Enabled ▼
<b>Automatic Redirect</b>	Enabled ▼
<b>Certificate Maintain</b>	None ▼
<b>Certificate Status</b>	System's secure HTTP certificate is presented

Save	Reset
------	-------

オブジェクト	説明
Mode	HTTPS モードの動作を示します。使用可能なモードは次のとおりです。 [Enabled] HTTPS モードを有効にします。

	[Disabled] HTTPS モードを無効にします。
Automatic Redirect	<p>HTTPS リダイレクトモード操作を示します。「HTTPS mode Enabled」を選択した場合のみ有効です。リダイレクトモードを有効にすると、HTTP サーバー 続は自動的に HTTPS 接続にリダイレクトされます。デバイス証明書がブラウザに信頼されていない場合は、セキュリティ上の理由から、ブラウザがリダイレクト操作を許可しないことがあります。この場合は、HTTPS 接続を手動で初期化する必要があります。</p> <p>使用可能なモードは次のとおりです。</p> <p>[Enabled] HTTPS リダイレクトモード操作を有効にします。</p> <p>[Disabled] HTTPS リダイレクトモード操作を無効にします。</p>
Certificate Maintain	<p>証明書のメンテナンス操作を行います。可能な操作は次のとおりです。</p> <p>[None] 操作なし。</p> <p>[Delete] 現在の証明書を削除します。</p> <p>[Upload] 証明書 PEM ファイルをアップロードします。[Web Browser]または[URL]を使用できます。</p> <p>[Generate] 新しい自己署名 RSA 証明書を生成します。</p>
Certificate Pass Phrase	アップロード証明書が特定のパスフレーズで保護されている場合は、このフィールドにパスフレーズを入力します。
Certificate Upload	<p>証明書 PEM ファイルをデバイスにアップロードします。ファイルには、証明書と秘密鍵が一緒に含まれている必要があります。証明書と秘密キーを保存するファイルが 2 つに分かれている場合、これらを 1 つの PEM ファイルに結合するには、Linux の cat コマンドを使用します。たとえば、<code>cat my.cert my.key &gt; my.pem</code> などです。Firefox v37 や Chrome v39 のように、新しいバージョンのほとんどのブラウザでは、証明書での DSA のサポートが削除されているので、RSA 証明書が推奨されていることに注意してください。</p> <p>[Web Browser] ブラウザ経由でアップロードします。</p> <p>[URL] URL を使用して証明書をアップロードします。サポートされているプロトコルは HTTP, HTTPS, TFTP, FTP です。</p> <p>HTTP サーバー URL 形式は、&lt;プロトコル&gt;://[:&lt;パスワード&gt;]&lt;ユーザー名&gt;@&lt;ホスト&gt;[:&lt;港&gt;][/&lt;道&gt;]/&lt;ファイル名&gt;です。たとえば、<code>tftp ://10.10.10.10/new_image_path/new_image</code> や、<code>http://username:password@10.10.10.10:80/new_image_path/new_image</code> などとなります。有効なファイル名は、アルファベット(A~Z、a~z)、数字(0~9の)、ドット(.)、ハイフン(-)、アンダースコア(_)です。最大長は 63 で、ハイフンは先頭文字にはできません。ドットのみを含むファイル名は使用できません。</p>
Certificate Status	<p>デバイス上の証明書の現在の状態を表示します。表示されるステータスは次のとおりです。</p> <p>System's secure HTTP certificate is presented.</p> <p>System's secure HTTP certificate is not presented.</p> <p>System's secure HTTP certificate is generating ....</p>

ボタン

<b>Save</b>	クリックして変更を保存します。
<b>Reset</b>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。
<b>Refresh</b>	クリックすると、ページが更新されます。ローカルで行った変更はすべて元に戻されます。

### 3.1.11 Access Management

Configuration > Security > System > Access Management

このページでアクセス管理テーブルを設定します。エントリの最大数は 16 です。アプリケーションのタイプがアクセス管理エントリのいずれかと一致する場合、デバイスへのアクセスが許可されます。

#### Access Management Configuration

**Mode** Disabled ▾

Delete	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
Delete	0.0.0.0	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New Entry

Save Reset

オブジェクト	説明
Mode	アクセス管理モードの動作を示します。使用可能なモードは次のとおりです。 [Enabled] アクセス管理モード操作を有効にします。 [Disabled] アクセス管理モードの操作を無効にします。
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
Start IP address	アクセス管理エントリの開始 IP アドレスを示します。
End IP address	アクセス管理エントリの終了 IP アドレスを示します。
HTTP/HTTPS	ホスト IP アドレスがエントリで指定された IP アドレス範囲と一致する場合、ホストは HTTP/HTTPS インタフェースからデバイスにアクセスできることを示します。
SNMP	ホスト IP アドレスがエントリで指定された IP アドレス範囲と一致する場合、ホストが SNMP インタフェースからデバイスにアクセスできることを示します。
TELNET/SSH	ホスト IP アドレスがエントリで指定された IP アドレス範囲と一致する場合、ホストは TELNET/SSH インターフェイスからデバイスにアクセスできることを示します。

ボタン	
<b>Add New Entry</b>	新しいアクセス管理エントリを追加するときにクリックします。
<b>Save</b>	クリックして変更を保存します。
<b>Reset</b>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.12 SNMP System

Configuration > Security > System > SNMP > System

このページで SNMP を設定します。

## SNMP System Configuration

Mode	Enabled ▼
Engine ID	800016c9030011223344aa

オブジェクト	説明
Mode	SNMP モードの動作を示します。使用可能なモードは次のとおりです。 [Enabled] SNMP モード操作を有効にします。 [Disabled] SNMP モード操作を無効にします。
Engine ID	SNMPv3 エンジン ID を示します。文字列には 10 から 64 までの数字を含む偶数(16 進形式で)を含める必要がありますが、すべてゼロおよびすべて F は使用できません。このエンジン ID のユーザのみがデバイス(ローカルユーザ)にアクセスできるため、エンジン ID を変更すると、現在のすべてのローカルユーザのアクセス権が取り消されます。

ボタン	
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.13 SNMP Trap Destination

Configuration > Security > System > SNMP > Trap > Destination

このページでトラップ送信先を設定します。

## Trap Configuration

### Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
<input type="checkbox"/>	<a href="#">trap-01</a>	Disabled	SNMPv2c	0.0.0.0	162
<input type="checkbox"/>	<a href="#">trap-02</a>	Disabled	SNMPv2c	0.0.0.0	162
<input type="checkbox"/>	<a href="#">trap-03</a>	Disabled	SNMPv2c	0.0.0.0	162
<input type="checkbox"/>	<a href="#">trap-04</a>	Disabled	SNMPv2c	0.0.0.0	162

オブジェクト	説明
Trap Destination Configurations トラップ送信先の設定	
Name	トラップ構成の名前を示します。トラップ送信先の名前を示します。
Enable	トラップ送信先モードの動作を示します。使用可能なモードは次のとおりです。 [Enabled] SNMP トラップモード操作を有効にします。 [Disabled] SNMP トラップモードの動作を無効にします。
Version	サポートされている SNMP トラップのバージョンを示します。 [SNMPv1] SNMPv1 [SNMPv2c] SNMPv2c [SNMPv3] SNMPv3
Destination Address	SNMP トラップの送信先アドレスを示します。有効な IP アドレスをドット区切りの十進表記で指定できます。
Destination port	SNMP トラップ送信先ポートを示します。SNMP エージェントは、このポートを介して SNMP メッセージを送信します。ポート範囲は 1 ~ 65535 です。

[SNMP トラップの設定] ページには、次のフィールドがあります。

### SNMP Trap Configuration

Trap Configuraton Name

Trap Config Name	e345
Trap Mode	Disabled ▼
Trap Version	SNMP v2c ▼
Trap Community	public
Trap Destination Address	
Trap Destination Port	162
Trap Inform Mode	Disabled ▼
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Security Engine ID	8000011603004066e0a71a
Trap Security Name	None ▼

オブジェクト	説明
SNMP Trap Detailed Configuration SNMP トラップ詳細設定	
Trap Config Name	構成するトラップ構成の名前を示します。文字列の長さは 1 から 32 まで、内容は 33 から 126 までの ASCII 文字です。
Trap Mode	SNMP トラップモードの動作を示します。使用可能なモードは次のとおりです。 [Enabled] SNMP モード操作を有効にします。 [Disabled] SNMP モード操作を無効にします。

Trap Version	SNMP トラップのサポートされているバージョンを示します。 [SNMPv1] サポートされている SNMP トラップのバージョンを SNMPv1 に設定します。 [SNMPv2c] サポートされている SNMP トラップのバージョンを SNMPv2c に設定します。 [SNMPv3] サポートされている SNMP トラップのバージョンを SNMPv3 に設定します。
Trap Community	SNMP トラップパケットを送信するときのコミュニティアクセス文字列を示します。使用できる文字列の長さは 0 から 63 で、使用できる内容は ASCII 文字の 33 から 126 です。
Trap Destination Address	SNMP トラップの送信先アドレスを示します。有効な IP アドレスをドット区切りの十進表記で指定できます。
Trap Destination port	SNMP トラップ送信先ポートを示します。SNMP エージェントは、このポートを介して SNMP メッセージを送信します。ポート範囲は 1 ~ 65535 です。
Trap Inform Mode	SNMP トラップ通知モードの動作を示します。使用可能なモードは次のとおりです。 [Enabled] SNMP トラップ通知モード操作を有効にします。 [Disabled] SNMP トラップ通知モードの動作を無効にします。
Trap Inform Timeout (seconds)	SNMP トラップ通知のタイムアウトを示します。指定できる範囲は 0 から 2147 です。
Trap Inform Retry Times	SNMP トラップ通知の再試行回数を示します。指定できる範囲は 0 から 255 です。
Trap Security Engine ID	SNMP トラップセキュリティエンジン ID を示します。SNMPv3 は、認証とプライバシーのために USM を使用してトラップと通知を送信します。これらのトラップと通知の一意のエンジン ID が必要です。文字列には 10 から 64 までの偶数(16 進形式で)を含める必要がありますが、すべてゼロおよびすべて F は使用できません。
Trap Security Name	SNMP トラップのセキュリティ名を示します。SNMPv3 は、USM を使用して認証とプライバシーをトラップおよび通知します。トラップと通知を有効にする場合は、一意のセキュリティ名が必要です。

ボタン	
	新しいユーザーを追加するときにクリックします。
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.14 SNMP Trap Sources

Configuration > Security > System > SNMP > Trap > Sources

このページでは、SNMP トラップのソース構成について説明します。フィルタタイプが含まれているフィルタのうち少なくとも 1 つがフィルタに一致し、フィルタタイプが除外されているフィルタが一致しない場合、指定したトラップソースにトラップが送信されます。

## Trap Configuration

### Trap Source Configurations

Delete	Name	Type	Subset OID
Delete	coldStart ▼	included ▼	

Add New Entry

Save Reset

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
Name	エントリの名前を示します。
Type	エントリのフィルタの種類を指定します。指定可能なタイプは次のとおりです。 [Included] 指定したトラップ条件に合致した際にトラップを送信します。 [excluded] 指定したトラップ条件に合致した際にトラップを送信しません。
Subset OID	エントリのサブセットOID。値は、トラップ名の種類によって異なります。たとえば、ifIndex は linkUp および linkDown のサブセットOIDで、1000001 はポート1を表します。有効なサブセットOIDは、ドットで区切られた(0-4294967295)またはアスタリスクです。最初の文字はアスタリスク(*)で始めてはならず、OID カウントの最大値は 63 を超えてはなりません。

ボタン	
Add New Entry	新しいコミュニティエントリを追加するときにクリックします。最大エントリ数は 32 です。
Save	クリックして変更を保存します。
Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.15 SNMP Communities

Configuration > Security > System > SNMP > Communities

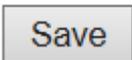
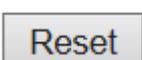
このページで SNMPv3 コミュニティテーブルを設定します。エントリインデックスキーは Community です。

#### SNMPv3 Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix
<input type="checkbox"/>	public	public	0.0.0.0	0
<input type="checkbox"/>	private	private	0.0.0.0	0
Delete				

Add New Entry Save Reset

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
Community Name	コミュニティを SNMP グループ設定にマッピングするセキュリティ名を示します。文字列の長さは1から32まで、内容は33から126までのASCII文字です。
Community Secret	SNMP エージェントへの SNMPv1 および SNMPv2c を使用したアクセスを許可するためのコミュニティシークレット(アクセス文字列)を示します。文字列の長さは1から32まで、内容は33から126までのASCII文字です。
Source IP	SNMP アクセスの送信元アドレスを示します。送信元アドレスの特定の範囲は、送信元プレフィックスと組み合わせて送信元サブネットを制限するために使用できます。
Source Mask	SNMP アクセスの送信元アドレスプレフィックスを示します。

ボタン	
	新しいコミュニティエントリを追加するときにクリックします。
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.16 SNMPv3 Users

Configuration > Security > System > SNMP > Users

このページで SNMPv3 ユーザーテーブルを設定します。エントリインデックスキーは、エンジン ID とユーザー名です。

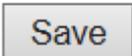
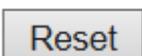
#### SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	80000116030040660a0b0c	<input type="text"/>	Auth, Priv	MD5	<input type="text"/>	DES	<input type="text"/>

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
Engine ID	このエントリが属するエンジン ID を識別するオクテット文字列。文字列には10から64までの偶数(16進形式で)を含める必要がありますが、すべてゼロおよびすべてFは使用できません。SNMPv3 アーキテクチャは、メッセージセキュリティには User-based Security Model (USM) を使用し、アクセス制御には View-based Access Control Model (VACM) を使用します。USM エントリの場合、エントリのキーは usmUserEngineID と usmUserName です。単純なエージェントでは、usmUserEngineID は常にそのエージェント自身の snmpEngineID 値です。この値は、このユーザーが通信できるリモート SNMP エンジンの snmpEngineID の値を取ることでもあります。つまり、ユーザーエンジン ID がシステムエンジン ID と等

	しい場合は、ローカルユーザーです。それ以外の場合はリモートユーザーです。
User name	このエントリが属するユーザ名を識別する文字列。文字列の長さは1から32まで、内容は33から126までのASCII文字です。
Security Level	このエントリが属するセキュリティモデルを示します。可能なセキュリティモデルは、以下の通りです。 [NoAuth,NoPriv] 認証なし、プライバシーなし [Auth,NoPriv] 認証あり、プライバシーなし [Auth,Priv] 認証あり、プライバシーあり エントリがすでに存在する場合、セキュリティレベルの値は変更できません。最初に値が正しく設定されていることを確認する必要があります。
Authentication Protocol	このエントリが属する認証プロトコルを示します。使用可能な認証プロトコルは以下のとおりです。 [MD5] MD5 認証プロトコルを使用 [SHA] SHA 認証プロトコルを使用 エントリがすでに存在する場合、セキュリティレベルの値は変更できません。最初に値が正しく設定されていることを確認する必要があります。
Authentication Password	認証パスワードフレーズを識別する文字列。MD5 認証プロトコルでは、許可される文字列長は8から32です。SHA 認証プロトコルでは、許可される文字列長は8から40です。使用できる内容は、33から126までのASCII文字です。
Privacy Protocol	このエントリが属するプライバシープロトコルを示します。考えられるプライバシー・プロトコルは以下のとおりです。 [DES] DES 認証プロトコルを使用 [AES] AES 認証プロトコルを使用
Privacy Password	プライバシー・パスワード・フレーズを識別するストリング。使用できる文字列の長さは8から32で、使用できる内容はASCII文字の33から126です。

ボタン	
	新しいユーザーエントリを追加するときにクリックします。
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.17 SNMP Groups

Configuration > Security > System > SNMP > Groups

このページでSNMPv3 グループテーブルを設定します。エントリインデックスキーは、セキュリティモデルとセキュリティ名です。

## SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group

Add New Entry

Save

Reset

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
Security Model	このエントリが属するセキュリティモデルを示します。使用可能なセキュリティモデルは次のとおりです。 [v1] SNMPv1 用に予約されています。 [v2c] SNMPv2c 用に予約されています。 [usm] User-based Security Model (USM)
Security Name	このエントリが属するセキュリティ名を識別する文字列。文字列の長さは 1 から 32 まで、内容は 33 から 126 までの ASCII 文字です。
Group Name	このエントリが属するグループ名を識別する文字列。文字列の長さは 1 から 32 まで、内容は 33 から 126 までの ASCII 文字です。

ボタン	
<input type="button" value="Add New Entry"/>	クリックして新しいグループエントリを追加します
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.18 SNMPv3 Views

Configuration > Security > System > SNMP > Views

このページで SNMPv3 ビューテーブルを設定します。エントリインデックスキーは、ビュー名と OID サブツリーです。

## SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included ▼	.1

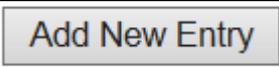
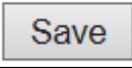
Add New Entry

Save

Reset

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
View Name	このエントリが属するビュー名を識別する文字列。文字列の長さは 1 から 32 まで、内容は 33 から 126 までの ASCII 文字です。
View Type	このエントリが属するビューの種類を示します。使用可能なビューのタ

	<p>イブは次のとおりです。</p> <p>[included] このビューサブツリーを含める必要があることを示します。</p> <p>[excluded] このビューサブツリーを除外することを示します。一般に、ビュー・エントリのビュー・タイプが[excluded]の場合、ビュー・タイプが[included]である別のビュー・エントリが存在し、そのOIDサブツリーが[excluded]ビュー・エントリより優先されます。</p>
OID Subtree	<p>名前付きビューに追加するサブツリーのルートを定義するOIDです。使用できるOIDの長さは1から64です。使用できる文字列の内容は、デジタル番号またはアスタリスク(*)です。</p>

ボタン	
	新しいビューエントリを追加するときをクリックします。
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合をクリックします。

### 3.1.19 SNMP Access

Configuration > Security > System > SNMP > Access

このページで SNMPv3 アクセステーブルを設定します。エントリインデックスキーは、グループ名、セキュリティモデル、およびセキュリティレベルです。

SNMPv3 Access Configuration						
Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name	
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼	
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼	

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
Group Name	このエントリが属するグループ名を識別する文字列。Group Name は 3.1.17 SNMP Groups でエントリ登録したものから選択ください。
Security Model	<p>このエントリが属するセキュリティモデルを示します。使用可能なセキュリティモデルは以下の通りです。</p> <p>[any] 任意のセキュリティモデル</p> <p>[v1] SNMPv1</p> <p>[v2c] SNMPv2c</p> <p>[usm] User-based Security Model (USM)</p>
Security Level	<p>このエントリが属するセキュリティモデルを示します。可能なセキュリティモデルは、以下の通りです。</p> <p>[NoAuth, NoPriv] 認証なし、プライバシーなし</p> <p>[Auth, NoPriv] 認証あり、プライバシーなし</p> <p>[Auth, Priv] 認証あり、プライバシーあり</p>

Read View Name	この要求が現在の値を要求する MIB オブジェクトを定義する MIB ビューの名前。View Name は 3.1.18 Views でエントリ登録したのから選択ください。
Write View Name	この要求が新しい値を設定する可能性のある MIB オブジェクトを定義する MIB ビューの名前です。View Name は 3.1.18 Views でエントリ登録したのから選択ください。

ボタン	
<input type="button" value="Add New Entry"/>	新しいアクセスエントリを追加するときにクリックします。
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.20 RMON Statistics

Configuration > Security > System > RMON > Statistics

このページの RMON 統計テーブルを設定します。エントリインデックスキーは ID です。

## RMON Statistics Configuration

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1. 0

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
ID	エントリのインデックスを示します。範囲は 1 から 65535 です。
Data Source	モニターするポート ID を示します。モニタしたいポートに合わせて下記の番号を登録してください。 USER ポート:1000001 LH ポート:1000002 MANAGE ポート:1000003

ボタン	
<input type="button" value="Add New Entry"/>	新しい RMON 統計エントリを追加するときにクリックします。
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.21 RMON History

Configuration > Security > System > RMON > History

このページの RMON 履歴テーブルを設定します。エントリインデックスキーは ID です。

## RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Delete		.1.3.6.1.2.1.2.2.1.1.	0	1800	50

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
ID	エントリのインデックスを示します。範囲は 1 から 65535 です。
Data Source	モニターするポート ID を示します。モニタしたいポートに合わせて下記の番号を登録してください。 USER ポート : 1000001 LH ポート : 1000002 MANAGE ポート : 1000003
Interval	履歴統計データのサンプリング間隔を秒単位で示します。範囲は 1 から 3600 で、デフォルト値は 1800 秒です。
Buckets	RMON に格納されるこの履歴制御エントリに関連付けられる最大データエントリを示します。範囲は 1 から 65535 で、デフォルト値は 50 です。
Buckets Granted	データ数は RMON に保存される。

ボタン	
<input type="button" value="Add New Entry"/>	新しい RMON 履歴エントリを追加するときにクリックします。
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.22 RMON Alarm

Configuration > Security > System > RMON > Alarm

このページの RMON アラーム表を設定します。エントリインデックスキーは ID です。

#### RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Delete		30	.1.3.6.1.2.1.2.2.1.	0.0	Delta	0	RisingOrFalling	0	0	0

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
ID	エントリのインデックスを示します。範囲は 1 から 65535 です。
Interval	サンプリングおよび上昇しきい値と下降しきい値の比較の間隔を秒単位で示します。範囲は 1 から 2147483647 です。
Variable	[xxx.yyy]形式で入力します。 xxx の範囲は 10 ~ 21 で、yyy の範囲は 1000001 ~ 1000003 です。

	<p>たとえば、10.1000001 は USER ポートの InOctets を、21.1000003 は MANAGE ポートの OutQLen を表します。</p> <p>使用可能な変数 xxx および yyy は次のとおりです。</p> <table border="1"> <thead> <tr> <th>xxx</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>10</td> <td>InOctets: インターフェースで受信されたオクテットの総数 (フレーミング文字を含む)</td> </tr> <tr> <td>11</td> <td>InUcastPkts: 上位層のプロトコルに配信されるユニキャストパケットの数</td> </tr> <tr> <td>12</td> <td>InNUcastPkts: 上位層のプロトコルに配信されるブロードキャストおよびマルチキャストのパケット数</td> </tr> <tr> <td>13</td> <td>InDiscards: パケットが正常であっても破棄される着信パケットの数</td> </tr> <tr> <td>14</td> <td>InErrors: 上位層のプロトコルに配信できないエラーを含む着信パケットの数</td> </tr> <tr> <td>15</td> <td>InUnknownProtos: プロトコルが不明またはサポートされていないために破棄されたインバウンドパケットの数</td> </tr> <tr> <td>16</td> <td>OutOctets: インターフェースから送信されたオクテット数 (フレーミング文字を含む)</td> </tr> <tr> <td>17</td> <td>OutUcastPkts: 送信を要求するユニキャストパケットの数</td> </tr> <tr> <td>18</td> <td>OutNUcastPkts: 送信を要求するブロードキャストパケットとマルチキャストパケットの数</td> </tr> <tr> <td>19</td> <td>OutDiscards: パケットが正常である場合に廃棄されるアウトバウンド・パケットの数</td> </tr> <tr> <td>20</td> <td>OutErrors: エラーのために送信できなかったアウトバウンドパケットの数</td> </tr> <tr> <td>21</td> <td>OutQLen: 出力パケットキューの長さ。(パケット内)</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>yyy</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>1000001</td> <td>USER ポート</td> </tr> <tr> <td>1000002</td> <td>LH ポート</td> </tr> <tr> <td>1000003</td> <td>MANAGE ポート</td> </tr> </tbody> </table>	xxx	説明	10	InOctets: インターフェースで受信されたオクテットの総数 (フレーミング文字を含む)	11	InUcastPkts: 上位層のプロトコルに配信されるユニキャストパケットの数	12	InNUcastPkts: 上位層のプロトコルに配信されるブロードキャストおよびマルチキャストのパケット数	13	InDiscards: パケットが正常であっても破棄される着信パケットの数	14	InErrors: 上位層のプロトコルに配信できないエラーを含む着信パケットの数	15	InUnknownProtos: プロトコルが不明またはサポートされていないために破棄されたインバウンドパケットの数	16	OutOctets: インターフェースから送信されたオクテット数 (フレーミング文字を含む)	17	OutUcastPkts: 送信を要求するユニキャストパケットの数	18	OutNUcastPkts: 送信を要求するブロードキャストパケットとマルチキャストパケットの数	19	OutDiscards: パケットが正常である場合に廃棄されるアウトバウンド・パケットの数	20	OutErrors: エラーのために送信できなかったアウトバウンドパケットの数	21	OutQLen: 出力パケットキューの長さ。(パケット内)	yyy	説明	1000001	USER ポート	1000002	LH ポート	1000003	MANAGE ポート
xxx	説明																																		
10	InOctets: インターフェースで受信されたオクテットの総数 (フレーミング文字を含む)																																		
11	InUcastPkts: 上位層のプロトコルに配信されるユニキャストパケットの数																																		
12	InNUcastPkts: 上位層のプロトコルに配信されるブロードキャストおよびマルチキャストのパケット数																																		
13	InDiscards: パケットが正常であっても破棄される着信パケットの数																																		
14	InErrors: 上位層のプロトコルに配信できないエラーを含む着信パケットの数																																		
15	InUnknownProtos: プロトコルが不明またはサポートされていないために破棄されたインバウンドパケットの数																																		
16	OutOctets: インターフェースから送信されたオクテット数 (フレーミング文字を含む)																																		
17	OutUcastPkts: 送信を要求するユニキャストパケットの数																																		
18	OutNUcastPkts: 送信を要求するブロードキャストパケットとマルチキャストパケットの数																																		
19	OutDiscards: パケットが正常である場合に廃棄されるアウトバウンド・パケットの数																																		
20	OutErrors: エラーのために送信できなかったアウトバウンドパケットの数																																		
21	OutQLen: 出力パケットキューの長さ。(パケット内)																																		
yyy	説明																																		
1000001	USER ポート																																		
1000002	LH ポート																																		
1000003	MANAGE ポート																																		
Sample Type	<p>選択した変数をサンプリングし、しきい値と比較する値を計算する方法。次のサンプル・タイプがあります。</p> <p>[Absolute] サンプルを直接取得します。</p> <p>[Delta] サンプル間の差を計算します。(デフォルト)</p>																																		
Value	最後のサンプリング期間中の統計値																																		
Startup Alarm	<p>選択した変数をサンプリングし、しきい値と比較する値を計算する方法。次のサンプル・タイプがあります。</p> <p>[Rising] 最初の値が上昇しきい値より大きい場合にアラームを発生します。</p> <p>[Falling] 最初の値が下降しきい値より小さいときにアラームを発生します。</p> <p>[RisingOrFalling] 最初の値が上昇しきい値より大きいか、下降しきい</p>																																		

	値より小さい場合(デフォルト)にアラームを発します。
Rising Threshold	上昇しきい値(1~2147483647)
Rising Index	上昇イベントインデックス(1~65535)
Falling Threshold	下降しきい値(1~2147483647)
Falling Index	下降イベントインデックス(1~65535)

ボタン	
<input type="button" value="Add New Entry"/>	新しい RMON アラームエントリを追加するときにクリックします。
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.23 RMON Event

Configuration > Security > System > RMON > Event

このページの RMON イベントテーブルを設定します。エントリインデックスキーは ID です。

## RMON Event Configuration

Delete	ID	Desc	Type	Event Last Time
Delete			none ▼	0

オブジェクト	説明
Delete	オンにすると、エントリが削除されます。次回の保存時に削除されます。
ID	エントリのインデックスを示します。範囲は 1 から 65535 です。
Desc	このイベントの概要を示します。文字列の長さは 0 から 127 で、既定は null 文字列です。
Type	イベントの通知を示します。次のタイプがあります。 [none] SNMP ログは作成されず、SNMP トラップも送信されません。 [log] イベントがトリガーされたときに SNMP ログ・エントリを作成します。 [snmptrap] イベントがトリガーされたときに SNMP トラップを送信します。 [logandtrap] SNMP ログエントリを作成し、イベントがトリガーされたときに SNMP トラップを送信します。
Event Last Time	このイベント・エントリが最後にイベントを生成した時点の sysUpTime の値を示します。

ボタン	
<input type="button" value="Add New Entry"/>	新しい RMON イベントエントリを追加するときにクリックします。
<input type="button" value="Save"/>	クリックして変更を保存します。

Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。
-------	--

### 3.1.24 Link OAM Port

Configuration > Link OAM > Port Settings

このページでは、現在の EFM-OAM ポート構成を検査し、変更することもできます。

#### Link OAM Port Configuration

OAM Control Enabled ▾

Port	OAM Mode	Loopback Support	Link Monitor Support	Critical Event Mode Ais
*	<> ▾	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LH	Active ▾	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Save Reset

オブジェクト	説明
OAM Control	システム全体で Link OAM を有効(Enable)にするか無効(disable)にするかを選択します。 リモート OAM アラームを受信すると、OAM LED は赤色で点灯します。DTE が critical event/link fault/dying gasp を含むいずれかのフラグが設定された OAMPDU フレームを受信すると、リモート OAM アラームと見なされます。 Note:LPT 機能は、EFM-OAM 機能が有効な場合のみ動作します。
Port	デバイスのポート番号を示します。Link OAM は、LH ポートに対してのみサポートされています。
OAM Mode	OAM モードをアクティブまたはパッシブに設定します。デフォルトモードはアクティブです。 [Active] アクティブモードに設定すると、ディスカバリープロセスにより OAMPDU による情報の交換が開始されます。ディスカバリープロセスが完了すると、アクティブ DTE は、アクティブモードでリモート OAM ピアエンティティに接続されている間、任意の OAMPDU の送信を許可されます。リモートの OAM エンティティがパッシブモードで動作している場合、アクティブな DTE は限定的に動作します。アクティブデバイスは、パッシブピアからの OAM リモートループバックコマンドおよび変数要求に応答しません。 [Passive]パッシブモードで設定された DTE は、ディスカバリープロセスを開始しません。パッシブ DTE は、リモート DTE によるディスカバリープロセスの開始に反応します。これにより、パッシブリンクへのパッシブの可能性がなくなります。パッシブ DTE は、可変要求またはループバック制御 OAMPDU を送信しません。
Loopback Support	デバイスポートのループバックサポートを有効にするかどうかを選択します。Link OAM リモートループバックは、障害の確認とリンクパフォ

	ーマンスのテストに使用できます。ループバックサポートを有効にすると、DTE は障害検出に役立つリモートループバックコマンドを実行できます。
Link Monitor Support	デバイスポートに対してリンクモニタサポートを有効にするかどうかを設定します。リンクモニタのサポートを有効にすると、DTE は診断情報を含めることができるイベント通知をサポートします。
Critical Event Mode Ais	構成：(USER ポート)[APLMC_1](LH)------(LH)[APLMC_2](USER ポート) APLMC_2 は USER ポートがリンクアップしている間、クリティカル・イベント (bit=0) の OAMPDU を送信します。 APLMC_2 は USER ポートがリンクダウンしている間、クリティカル・イベント (bit=1)の OAMPDU を送信します。 [ケース 1] APLMC_1 の critical-event-mode ais 設定が無効の場合 "show link-oam status"コマンドは、Critical Event にクリティカル・イベント・ビットの結果を表示します。User-port status 項目は常に「-」です。 [ケース 2] APLMC_1 の critical-event-mode ais 設定が有効の場合 "show link-oam status"コマンドは、User-port status にクリティカル・イベント・ビットの結果を表示します。Critical Event 項目は常に「-」です。

ボタン	
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

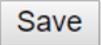
### 3.1.25 Link OAM Event

Configuration > Link OAM > Event Settings

このページでは、現在の EFM-OAM リンク・イベント構成を検査し、変更することもできます。

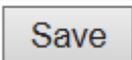
## Link Event Configuration for Port LH

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

オブジェクト	説明
Event Name	構成中のリンク・イベントの名前
Error Window	様々なリンク・イベントを監視するための 1 秒単位のウィンドウ時間を表します。
Error Threshold	対向装置にこのエラーを通知するための、該当するリンク・イベントのウィンドウ時間のしきい値を表します。

Error Frame Event	エラーフレームイベントは、指定された期間中に検出されたエラーフレームの数をカウントします。期間は、時間間隔(1秒単位のウィンドウ)で指定します。このイベントは、エラーフレームカウントがその期間の指定したしきい値(期間のしきい値)以上の場合に生成されます。エラーフレームは、Media Access Control サブレイヤで検出された伝送エラーのあるフレームです。「エラーフレームイベント」のエラーウィンドウは1~60の整数値でなければなりません。デフォルト値は'1'です。一方、エラーしきい値は0~4294967295でなければならず、デフォルト値は'1'です。
Symbol Period Error Event	エラーシンボル期間イベントは、指定された期間中に発生したシンボルエラーの数をカウントします。期間は、基礎となる物理層上の時間間隔で受信可能なシンボルの数によって指定されます。このイベントは、その期間のシンボルエラー数が指定したしきい値以上の場合に生成されます。「シンボル期間エラーイベント」のエラーウィンドウは1~60の整数値でなければなりません。デフォルト値は'1'です。一方、エラーしきい値は0~4294967295でなければならず、デフォルト値は'1'です。
Seconds Summary Event	Errored Frame Seconds Summary Event TLVは、指定された期間中に発生したエラーフレーム秒数をカウントします。期間は時間間隔で指定されます。このイベントは、エラー・フレーム秒数がその期間の指定したしきい値以上の場合に生成されます。エラーフレーム秒は、少なくとも一つのフレームエラーが検出された1/2間隔です。エラーフレームは、Media Access Control サブレイヤで検出された伝送エラーのあるフレームです。「Seconds Summary Event」のエラーウィンドウは10~900の整数値でなければなりません。デフォルト値は'60'です。一方、エラーしきい値は0~65535でなければならず、デフォルト値は'1'です。

ボタン	
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.26 Loop Protection

Configuration > Loop Protection

このページでは、現在のループ保護構成を確認し、設定を変更することもできます。

## Loop Protection Configuration

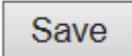
General Settings			
Global Configuration			
Enable Loop Protection	Disable ▾		
Transmission Time	5	seconds	
Shutdown Time	180	seconds	

Port Configuration			
Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<> ▾	<> ▾
USER	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
LH	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾
MANAGE	<input checked="" type="checkbox"/>	Shutdown Port ▾	Enable ▾

Save    Reset

オブジェクト	説明
General Settings 一般設定	
Enable Loop Protection	ループ保護を有効にするかどうかを設定します。
Transmission Time	各ポートで送信される各ループ保護 PDU の間隔を設定します。有効な値は、1 から 10 秒です。デフォルト値は 5 秒です。
Shutdown Time	ループが発生した場合にポートがディセーブル状態のままになる期間 (秒) を設定します。有効な値は、0 から 604800 秒 (7 日間) です。値 0 は次のデバイスの再起動までポートを無効のままにします。デフォルト値は 180 秒です。
Port Configuration ポート設定	
Port	ポートの名称です。
Enable	このポートでループ保護を有効にするかどうかを設定します。
Action	ポートでループが検出されたときに実行されるアクションを設定します。有効な値は、[Shutdown Port] または [Shutdown Port and Log] です。
Tx Mode	ポートがループ保護 PDU をアクティブに生成しているかどうか、またはループしている PDU をパッシブに検索しているかどうかを設定します。

ボタン	
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.27 LLDP (For PoE Model Only)

Configuration > LLDP > LLDP

このページでは、現在の LLDP インタフェース設定を確認・設定できます。

## LLDP Configuration

### LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

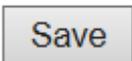
### LLDP Interface Configuration

Interface	Mode	Optional TLVs						
		CDP aware	Trap	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/1	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
GigabitEthernet 1/2	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				
FastEthernet 1/1	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>				

Save Reset

オブジェクト	説明
LLDP Parameters LLDP パラメータ	
Tx Interval	デバイスは、ネットワークディスカバリ情報を最新にするために、隣接ルータに LLDP フレームを定期的に送信します。各 LLDP フレームの間隔は、Tx Interval 値によって決まります。有効な値は 5-32768 秒です。
Tx Hold	各 LLDP フレームには、LLDP フレーム内の情報が有効と見なされる期間に関する情報が含まれます。LLDP 情報の有効期間は、Tx Hold に Tx Interval 秒を掛けた値に設定されます。有効な値は 2-10 回です。
Tx Delay	一部の設定が変更された場合(例: IP アドレス)、新しい LLDP フレームが送信されますが、LLDP フレーム間の時間は常に Tx Delay seconds の値以上になります。Tx Delay は、Tx Interval 値の 1/4 より大きくすることはできません。有効な値は 1-8192 秒です。
Tx Reinit	ポートがディセーブル、LLDP がディセーブル、またはデバイスがリブートされると、LLDP シャットダウンフレームが隣接ユニットに送信され、LLDP 情報が無効になったことを通知します。Tx Reinit はシャットダウンフレームと新しい LLDP 初期化の間の秒数を制御します。有効な値は 1-10 秒です。
LLDP Interface Configuration LLDP インターフェイス設定	
Interface	論理 LLDP インターフェイスのメディアコンバータインターフェイス名
Mode	LLDP モードを選択します。 [Rx only] メディアコンバータは LLDP 情報を送信しませんが、隣接ユニットからの LLDP 情報は分析されます。 [Tx only] メディアコンバータは近隣ルータから受信した LLDP 情報を破棄しますが、LLDP 情報を送信します。 [Disabled] メディアコンバータは LLDP 情報を送信せず、近隣ルータから受信した LLDP 情報を破棄します。 [Enabled] メディアコンバータは LLDP 情報を送信し、近隣ルータから受信した LLDP 情報を分析します。
CDP Aware	CDP Aware を選択します。

	<p>CDP オペレーションは、着信 CDP フレーム(デバイスは CDP フレームを送信しません)のデコードに制限されます。CDP フレームは、インターフェースで LLDP が有効になっている場合にのみデコードされます。LLDP 隣接機器テーブル内の対応するフィールドにマッピングできる CDP TLV のみがデコードされます。他のすべての TLV は破棄されます(認識されない CDP TLV および破棄された CDP フレームは、LLDP 統計には表示されません。)。CDP TLV は、次に示すように LLDP 隣接機器のテーブルにマッピングされます。CDP TLV「デバイス ID」は、LLDP「シャーシ ID」フィールドにマッピングされます。CDP TLV「所在地」は、LLDP「管理アドレス」フィールドにマッピングされます。CDP アドレス TLV には複数のアドレスを含めることができますが、LLDP 隣接機器テーブルには最初のアドレスだけが表示されます。CDP TLV「ポート ID」は、LLDP「ポート ID」フィールドにマッピングされます。CDP TLV「バージョンとプラットフォーム」は、LLDP「システムの説明」フィールドにマッピングされます。CDP と LLDP の両方が「システム機能」をサポートしていますが、CDP 機能は LLDP の一部ではない機能を対象としています。これらの機能は、LLDP 隣接機器テーブルでは「その他」として示されます。すべてのインターフェースで CDP aware が無効になっている場合、デバイスは隣接デバイスから受信した CDP フレームを転送します。少なくとも1つのインターフェースで CDP aware が有効になっている場合、すべての CDP フレームがデバイスによって終端されます。</p> <p>Note:インターフェースの CDP aware が無効にされると、CDP 情報はすぐには削除されませんが、ホールドタイムを超えると削除されます。</p>
Port Descr	オンにすると、送信される LLDP 情報に「Port Descr」が含まれます。
Sys Name	オンにすると、送信される LLDP 情報に「Sys Name」が含まれます。
Sys Descr	オンにすると、送信される LLDP 情報に「Sys Descr」が含まれます。
Sys Capa	オンにすると、送信される LLDP 情報に「Sys Capa」が含まれます。
Mgmt Addr	オンにすると、送信される LLDP 情報に「Mgmt Addr」が含まれます。

ボタン	
	クリックして変更を保存します。
	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.28 LLDP-MED (For PoE Model Only)

Configuration > LLDP > LLDP-MED

このページでは、LLDP-MED を設定できます。この機能は、LLDP-MED をサポートする VoIP デバイスに適用されます。

## LLDP-MED Configuration

### Fast Start Repeat Count

Fast start repeat count

### LLDP-MED Interface Configuration

Interface	Transmit TLVs				Device Type
	Capabilities	Policies	Location	PoE	
*	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<>
GigabitEthernet 1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
GigabitEthernet 1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity
FastEthernet 1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Connectivity

### Coordinates Location

Latitude  ° North Longitude  ° East Altitude  Meters Map Datum WGS84

### Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

### Emergency Call Service

Emergency Call Service

### Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

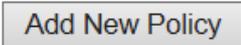
Add New Policy

オブジェクト	説明
Fast start repeat count	ファスト・スタート・リピート・カウント
Fast start repeat count	<p>エンドポイントの迅速な起動と緊急コールサービス位置識別検出は、一般的に VoIP システムの非常に重要な側面です。さらに、制限された LLDPDU スペースを節約し、ネットワークポリシーの不適切な知識に起因するセキュリティおよびシステム整合性の問題を軽減するために、特定のエンドポイントタイプ(たとえば、許可された音声対応デバイスにのみ音声ネットワークポリシーをアドバタイズします。)に特に関連する情報のみをアドバタイズすることが最善です。</p> <p>このことを考慮して、LLDP-MED は、これらの関連する特性を達成するために、プロトコルとプロトコル上のアプリケーション層との間の LLDP-MED Fast Start 相互作用を定義します。最初、ネットワーク接続機器は LLDPDU 内の LLDP TLV のみを送信します。LLDP-MED エンドポイント機器が検出された後にのみ、LLDP-MED 対応ネットワーク接続機器は、関連するインターフェース上の発信 LLDPDU 内の LLDP-MED TLV の通知を開始します。LLDP-MED アプリケーションは、新しい LLDP-MED 情報をできるだけ早く新しいネイバーに共有するために新しい LLDP-MED ネイバーが検出された場合、LLDPDU の送信を一時的に高速化し、1 秒以内に開始します。</p> <p>隣接ルータ間の送信中に LLDP フレームが失われる可能性があるため、隣接ルータが LLDP フレームを受信する可能性を高めるために、ファーストスタート送信を複数回繰り返すことをお勧めします。ファスト・ス</p>

	<p>タート・リピート・カウントでは、ファスト・スタート・トランスミッションを繰り返す回数を指定できません。新しい情報を持つ LLDP フレームを受信したときに、1 秒間隔で 4 つの LLDP フレームが送信されることを考えると、推奨値は 4 回です。</p> <p>LLDP-MED および LLDP-MED ファスト・スタート・メカニズムは、LLDP-MED ネットワーク接続デバイスとエンドポイント・デバイス間のリンク上でのみ動作することを意図しており、ネットワーク接続デバイスを含む LAN インフラストラクチャ要素間のリンク、または他のタイプのリンクには適用されないことに注意してください。</p>
LLDP-MED Interface Configuration LLDP-MED インターフェースの設定	
Interface	構成が適用されるインターフェース名
Transmit TLVs - Capabilities	オンにすると、送信される LLDP-MED 情報にデバイスの機能が含まれます。
Transmit TLVs - Policies	オンにすると、インターフェースに設定されているポリシーが、送信される LLDP-MED 情報に含まれます。
Transmit TLVs - Location	オンにすると、送信される LLDP-MED 情報にデバイスの設定済みロケーション情報が含まれます。
Transmit TLVs - PoE	オンにすると、インターフェースの設定済み PoE(Power over Ethernet) 情報が、送信される LLDP-MED 情報に含まれます。
Device Type	<p>すべての LLDP-MED デバイスは、特定のタイプの LLDP-MED デバイスとして動作しています。これは、以下に定義されているように、ネットワーク接続デバイスまたは特定のクラスのエンドポイントデバイスのいずれかです。</p> <p>ネットワーク接続デバイスは、LLDP-MED エンドポイントデバイス用の IEEE802 ベースの LAN インフラストラクチャへのアクセスを提供する LLDP-MED デバイスです。</p> <p>LLDP-MED ネットワーク接続デバイスは、以下のいずれかの技術に基づく LAN アクセスデバイスです。</p> <ol style="list-style-type: none"> <li>1. LAN スイッチ/ルータ</li> <li>2. IEEE 802.1 ブリッジ</li> <li>3. IEEE 802.3 リピータ(歴史的な理由で含まれる)</li> <li>4. IEEE 802.11 無線アクセスポイント</li> <li>5. IEEE 802.1 AB および MED 拡張をサポートし、任意の方法で IEEE802 フレームをリレーできるデバイス。</li> </ol> <p>エンドポイントデバイス: ネットワークエッジに配置され、IEEE802 LAN テクノロジーに基づいて IP 通信サービスの一部の機能を提供する LLDP-MED デバイス。</p> <p>Network Connectivity Device と Endpoint Device の主な違いは、LLDP-MED 情報交換を開始できるのは Endpoint Device だけであるということです。</p> <p>スイッチは常に Network Connectivity Device である必要がありますが、スイッチをエンドポイント・デバイスとして動作するように構成することで、LLDP-MED 情報交換(2 台のネットワーク接続機器が接続されている場合)を開始できます。</p>
Coordinates Location 座標位置	

Latitude	緯度は最大 4 桁で 0~90 度以内に正規化する必要があります。 赤道の北または南の方向を指定できます。
Longitude	経度は最大 4 桁で 0-180 度以内に正規化する必要があります。 本初子午線の東または本初子午線の西の方向を指定できます。
Altitude	高度は最大 1 桁で -2097151.9 から 2097151.9 の範囲に正規化されるべきです。 高度は二種類(床またはメートル)から選択できます。 メートル:指定した垂直データムによって定義される高度のメートルを表します。 床:床と床の寸法が異なる建物では、より適切な形式で高度を表します。 高度=0.0 は建物の外でも意味があり、与えられた緯度と経度での地面の高さを表します。建物の内部では、0.0 は正面玄関の地面レベルに関連付けられた床レベルを表します。
Map Datum	マップデータムは、次のオプションで指定した座標に使用されます。 WGS84: (地理的 3D)-World Geodesic System1984、CRS Code4327、一次子午線名:グリニッジ。 NAD83/NAVD88:北米データム 1983、CRS コード 4269、一次子午線名:グリニッジ;関連付けられた垂直データムは、1988(海軍 88)の北米垂直データムです。このデータペアは、潮汐水(データム=NAD83/MLLW を使用します。)の近くではなく、陸上の位置を参照するときに使用します。 NAD83/MLLW:北米データム 1983、CRS コード 4269、一次子午線名:グリニッジ;関連する垂直データムは、Mean Lower Low Water (MLLW)です。このデータムペアは、水/海/海洋の位置を参照するときに使用します。
Civic Address Location シビックアドレスの場所	
Country code	大文字の ASCII 文字による二文字の ISO3166 国コード-例:DK,DE または US
State	国の地方区分(州、州、地域、州、県)
County	郡、教区、郡(日本)、地区
City	市、町、市(日本)
City district	市区町村(日本)
Block (Neighborhood)	近所のブロック
Street	街路
Leading street direction	街路方角
Trailing street suffix	末尾の通りの末尾表記
Street suffix	街路種別
House no.	ハウス番号
House no. suffix	家屋番号の末尾表記
Landmark	ランドマーク
Additional location info	追加の位置情報
Name	住居及び事務所の占有者

Zip code	郵便番号
Building	建屋名称
Apartment	ユニット名称
Floor	階
Room no.	部屋番号
Place type	種別
Postal community name	郵便コミュニティ名
P.O. Box	私書箱
Additional code	追加コード
Emergency Call Service 緊急通報サービス	
Emergency Call Service	Emergency Call Service の ELIN 識別子データ形式は、緊急コールのセットアップ中に使用される ELIN 識別子を従来の CAMA または ISDN トランクベースの PSAP に伝送するために定義されています。この形式は、緊急コールに使用される ELIN に対応する数値文字列で構成されています。
Policies ポリシー	
Delete	ポリシーを削除する場合に選択します。次回の保存時に削除されます。
Policy ID	ポリシーの ID。これは自動生成され、特定のインタフェースにマップされるポリシーを選択する時に使用されます。
Application Type	<p>アプリケーションタイプの使用目的:</p> <ol style="list-style-type: none"> <li>1. 音声-専用の IP テレフォニーハンドセットおよび対話型音声サービスをサポートするその他の類似機器で使用します。これらのデバイスは通常、導入を容易にし、データアプリケーションから分離することでセキュリティを強化するために、個別の VLAN に導入されます。</li> <li>2. 音声シグナリング(条件付き): 音声シグナリングと音声メディアで異なるポリシーを必要とするネットワークポートで使用します。Voice アプリケーションポリシーでアドバタイズされたものと同じネットワークポリシーがすべて適用される場合は、このアプリケーションタイプをアドバタイズしないでください。</li> <li>3. ゲストボイス-独自の IP テレフォニーハンドセットおよびインタラクティブな音声サービスをサポートするその他の類似のアプリケーションを使用して、ゲストユーザおよび訪問者向けに個別の「限定機能セット」音声サービスをサポートします。</li> <li>4. ゲスト音声シグナリング(条件付き): ゲスト音声シグナリングとゲスト音声メディアで異なるポリシーを必要とするネットワークポートで使用します。Guest Voice アプリケーションポリシーでアドバタイズされたものと同じネットワークポリシーがすべて適用される場合は、このアプリケーションタイプをアドバタイズしないでください。</li> <li>5. Softphone Voice-PC やラップトップなど、一般的なデータ中心のデバイス上のソフトフォンアプリケーションで使用します。このクラスのエンドポイントは、複数の VLAN をサポートしていない場合が多く、通常、「タグなし」VLAN または単一の「タグ付き」データ固有の VLAN を使用するように設定されます。「タグなし」VLAN(下のタグ付きフラグを参照)で使用するようにネットワークポリシーが定義されている場合、</li> </ol>

	<p>L2 プライオリティフィールドは無視され、DSCP 値のみが関連します。</p> <p>6. ビデオ会議-リアルタイムの対話型ビデオ/オーディオサービスをサポートする専用のビデオ会議機器およびその他の類似機器で使 用します。</p> <p>7. ストリーミングビデオ-ブロードキャストまたはマルチキャストベ ースのビデオコンテンツ配信、および特定のネットワークポリシー処理を 必要とするストリーミングビデオサービスをサポートするその他の類 似アプリケーションで使用します。バッファリングを用いた TCP に依存 するビデオアプリケーションは、このアプリケーションタイプの使用を 意図したものではない。</p> <p>8. ビデオ信号方式(条件付きの)-ビデオメディアとは別のビデオ信号方 式ポリシーを必要とするネットワークポロジで使用します。このアプ リケーションタイプは、ビデオ会議アプリケーションポリシーでアドバ タイズされたものと同じネットワークポリシーがすべて適用される場 合はアドバタイズしないでください。</p>
Tag	<p>指定されたアプリケーションタイプが「タグ付き」または「タグなし」 VLAN のどちらを使用しているかを示すタグ。</p> <p>Untagged は、デバイスがタグなしフレームフォーマットを使用してお り、IEEE 802.1 Q-2003 で定義されているタグヘッダーを含んでいない ことを示します。この場合、VLAN ID とレイヤ 2 プライオリティフィー ルドの両方が無視され、DSCP 値のみが関連します。</p> <p>Tagged は、デバイスが IEEE 802.1 Q タグ付きフレームフォーマットを 使用していること、および VLAN ID とレイヤ 2 プライオリティ値の両方 と DSCP 値が使用されていることを示します。タグ付き書式には、タグ ヘッダーと呼ばれる追加フィールドがあります。タグ付きフレームフォ ーマットは、IEEE 802.1 Q-2003 によって定義されるように、優先タグ 付きフレームも含む。</p>
VLAN ID	IEEE 802.1 Q-2003 で定義されているインターフェイスの VLAN 識別子 (VID)
L2 Priority	L2 優先度は、指定されたアプリケーションタイプに使用されるレイヤ 2 優先度です。L2 プライオリティは、IEEE 802.1 D-2004 で定義されてい るように、八つのプライオリティレベル(0 から 7)のいずれかを指定で きます。値 0 は、IEEE 802.1 D-2004 で定義されているデフォルトの優 先順位の使用を表します。
DSCP	IETF RFC2474 で定義されているように、指定されたアプリケーションタ イプに対して Diffserv ノードの動作を提供するために使用される DSCP 値。DSCP には、64 個のコードポイント値(0 から 63)のいずれかを含め ることができます。値 0 は、RFC2475 で定義されているデフォルトの DSCP 値の使用を表します。
Adding a new policy	<p>新しいポリシーを追加するときにクリックします。新しいポリシーのア プリケーションタイプ、タグ、VLAN ID、L2 プライオリティ、および DSCP を指定します。「保存」をクリックします。</p> <p style="text-align: right;"></p> <p>サポートされているポリシーの数は 32 です。</p>
Port Policies Interface Configuration ポートポリシーインターフェイスの構成	

Interface	構成が適用されるインターフェース名
Policy Id	特定のインターフェースに適用されるポリシーの集合。ポリシーのセットを選択するには、ポリシーに対応するチェックボックスをオンにします。

ボタン	
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.29 PoE (For PoE Model Only)

Configuration > PoE > PoE

このページでは、現在の PoE ポート設定を確認および設定できます。

## Power Over Ethernet Configuration

<b>Reserved Power determined by</b>	<input checked="" type="radio"/> Class	<input type="radio"/> Allocation	<input type="radio"/> LLDP-MED
<b>Power Management Mode</b>	<input checked="" type="radio"/> Actual Consumption	<input type="radio"/> Reserved Power	

## PoE Port Configuration

Port	Mode	Operation	Maximum Power [W]
*	<>	<>	30
1	Auto-Restart	PoE+	30

<input type="button" value="Save"/>	<input type="button" value="Reset"/>
-------------------------------------	--------------------------------------

オブジェクト	説明
Reserved Power determined by 予約電力	
Allocated mode	このモードでは、ユーザーは各ポートが予約できる電力量を割り当てます。各ポート/PD に割り当て/予約された電力は、最大電力フィールドで指定されます。
Class mode	このモードでは、各ポートは、接続された PD が属するクラスに応じて、予約する電力量を自動的に決定し、それに従って電力を予約します。4 つの異なるポートクラスがあり、4、7、15.4、または 30 ワット用のものがあります。 このモードでは、[Maximum Power(最大電力)]フィールドは無効です。
LLDP-MED mode	このモードは、各ポートが LLDP プロトコルを使用して PoE 情報を交換することで予約する電力量を決定し、それに従って電力を予約するという Class モードと似ています。ポートで LLDP 情報が利用できない場合、ポートはクラスモードを使用して電力を予約します。 このモードでは、[最大電力]フィールドは無効です。 すべてのモード: ポートの予約電力を超える電力をポートが使用する場合、ポートはシャットダウンされます。

Power Management Mode 電源管理モード	
Actual Consumption	このモードでは、実際の消費電力が、電源が供給できる電力を超えるか、予約電力を超えると、ポートがシャットダウンされます。
Reserved Power	このモードでは、予約電力がパワーサプライの供給できる電力を超えると、ポートがシャットダウンされます。このモードでは、PDがパワーサプライから利用可能な電力を超える電力を要求した場合、ポートの電源はオンになりません。
Port Configuration ポート設定	
Port	この行の論理ポート番号です。 PoE 対応でないポートはグレー表示され、PoE を設定できません。
PoE Mode PoE モード	
Disable	ポートの PoE が無効になっています。
Enable	ポートの PoE を有効にします。
Schedule	スケジューリングによってポートの PoE を有効にします。
Auto-Restart	スケジューリングによってポートの PoE を有効にし、さらに自動再起動 PD 用の ICMP Ping Detection を提供します。
Maximum Power 最大電力	
[Maximum Power] の値には、リモートデバイスに供給できる最大電力をワット単位で示す数値が含まれます。最大許容値は 30.0 W です。	

ボタン	
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

#### 注意事項

- ❗ PoE 給電異常時、または、PD 受電未対応機器と接続した場合、PoE LED は橙点灯します。

### 3.1.30 PoE Power Scheduler (For PoE Model Only)

Configuration > PoE > Power Scheduler

このページでは、電力スケジューリングを設定します。

エントリーは、PoE ポートのパワーアライブ間隔を制御するために使用されます。

電源のオン/オフを1週間でスケジュールするための特定の間隔を設定できます。

## PoE Power Scheduling Control on Port USER

Port USER ▼

### Power Scheduling Interval Configuration

Day							Interval		Action
Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	Start	End	
<input type="checkbox"/>	00:00 ▼	- 00:29 ▼	<input checked="" type="radio"/> Power ON <input type="radio"/> Power OFF						

Apply

### Power Scheduling During 00:00 ▼ - 05:59 ▼

Time Interval	Day						
	Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
00:00 - 00:29	●	●	●	●	●	●	●
00:30 - 00:59	●	●	●	●	●	●	●
01:00 - 01:29	●	●	●	●	●	●	●
01:30 - 01:59	●	●	●	●	●	●	●
02:00 - 02:29	●	●	●	●	●	●	●
02:30 - 02:59	●	●	●	●	●	●	●
03:00 - 03:29	●	●	●	●	●	●	●
03:30 - 03:59	●	●	●	●	●	●	●
04:00 - 04:29	●	●	●	●	●	●	●
04:30 - 04:59	●	●	●	●	●	●	●
05:00 - 05:29	●	●	●	●	●	●	●
05:30 - 05:59	●	●	●	●	●	●	●

Save

Reset

オブジェクト	説明
Power Scheduling Interval Configuration 電力スケジューリング間隔設定	
Day	チェックマークは、セットのメンバーである日を示します。
Interval	開始: 開始時間と開始分を選択します。 終了: 終了時間と終了分を選択します。
Action	Power On: インターバル中に電源をオンにするラジオ・ボタンを選択します。 電源オフ-インターバル中に電源をオフにするラジオボタンを選択します。
Power Scheduling During 電源スケジューリング中	
Time Interval	1日に48の時間間隔があります。休憩時間は30分です。
Day	現在のスケジュール状態はグラフィカルに表示されます。 緑は電源をONにすること、赤をOFFにすることを示します。 時間間隔のメンバーである日を示すチェックマークを直接変更します。 必要に応じてチェックをオンまたはオフにして、スケジュールテーブル

	を変更します。
--	---------

ボタン	
Apply	クリックすると、電源スケジュールの間隔が適用されます。
Save	クリックして変更を保存します。
Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.31 PoE Power Reset (For PoE Model Only)

Configuration > PoE > Power Reset

このページは、パワーリセットエントリー構成を提供します。

エントリーは、PoE ポートの電源リセット時間を制御するために使用されます。

PoE ポートごとに最大5つのエントリーを作成できます。

## PoE Power Reset Control on Port USER

Port USER ▼

Delete	Day							Time (hh:mm)
	Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	
Delete	<input type="checkbox"/>	00 ▼ : 00 ▼						

Add New

Save

Reset

オブジェクト	説明
Delete	オンにすると、エントリーが削除されます。 指定したエントリーは、次回の保存時に削除されます。
Day	チェックマークは、エントリーのメンバーである日を示します。必要に応じてチェックボックスをオンまたはオフにして、エントリーを変更します。
Time (hh:mm)	hh 時間を選択します。 mm 分を選択します。

ボタン	
Add New	クリックして新しいリセットエントリーを追加します。
Save	クリックして変更を保存します。
Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

### 3.1.32 PoE Ping Auto Checking (For PoE Model Only)

Configuration > PoE > Ping Auto Checking

PoE ICMP Ping Auto Checking

Auto-refresh  Refresh Clear Counters

Port	Enable (*)	Ping IP Address	Interval (sec)	Number of Retries	Failure Action	Power Off Time (sec)	Counters Sent/Rcvd Loss/Reboot	Manual Restart
		IPv4						
*	<input type="checkbox"/>		30	3	<>	60		<input type="checkbox"/>
USER	<input type="checkbox"/>		30	3	Reboot PD	60	0/0 0/0	<input type="checkbox"/>

Save Reset [Note \*: To Enable ICMP Ping, use Configuration/PoE page, select Auto-Restart mode. Other modes will disable ICMP Ping.]

オブジェクト	説明
Port	この行の論理ポート番号です。 PoE に対応していないポートは、ここでは使用できません。
Enable	ICMP Ping Checking 機能を有効/無効を確認できます(この項目は Read Only となっています)。 設定は、PoE の設定画面で行います。 スケジュールオプションの下の[Auto Restart]オプションを選択します。[Auto Restart] が選択されている場合、スケジュールは有効で機能します。そのため、Auto-Restart オプションが選択されている場合は、PoE スケジュールを設定する必要があります。設定されていない場合は、PoE ポートに電力が出力されません。 Note: ping が開始されないには、次の 2 つの条件があります。 1. IP が有効でない場合。(0.0.0.0 など) 2. PoE ポートに電力が出力されない場合は、PD が接続されていないか、スケジュール設定に従って電源がオフになっている可能性があります。
Ping IP Address IPv4	ポートごとの Ping 検出のための PD の IPv4 アドレス。デフォルトは 0.0.0.0 です。
Interval (sec)	ポートごとの秒単位の時間間隔。Ping は、前回のラウンド以降、待機時間がこの間隔を超えたときに開始されますが、他のポートを待機しているために時間どおりにはなりません。範囲:10~1800 秒。
Number of Retries	ping の再試行回数。システムは ping を繰り返し実行します。再試行回数が 5 の場合は、5+1 回 ping します。範囲は 1~5 です。
Failure Action	ping (ping の再試行を含む) がパケットを受信していない場合は、ping 失敗イベントです。障害イベントが発生した場合、システムは何もしないか、このオプションに従って PD をリブートできます。Reboot PD は、PoE ポートが電源出力を停止し、電源オフ時間を待ってから再び電源出力を開始することを意味します。
Power Off Time (sec)	ping 障害イベントが発生した場合の PD の電源切断時間。Failure Action が何もしない場合、この time パラメータは使用されません。 範囲:3~120 秒
Counters Sent/Rcvd/Loss/Reboot	ping パケットの送信/受信/消失および再起動 PD のカウンタ。カウンタは手動でリセットできます。デバイスを再起動すると、カウンタもリセットされます。
Manual Restart	すぐに PD を再起動します。このポートの PoE は、3~5 秒後に無効化および有効化されます。ただし、再起動は再起動番号には含まれません。

	ん。
--	----

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されま す。自動更新は3秒ごとに行われます。
Refresh	クリックすると、ページがすぐに更新されます。
Clear Counters	カウンタをリセットするときにクリックします。
Save	クリックして変更を保存します。
Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリ ックします。

**!** PoE Ping Auto Checking 機能により、PD 受電機器の電源を OFF にする可能性がありますので、ご注意ください。

**!** PoE Ping Auto Checking 機能において、ICMP PING 失敗時のアクションを reboot PD を選択した場合、本装置は PoE 給電のポートリセット(PD 受電機器をリブート)を行います。

その後も PD 受電機器から ping 応答がない場合、本装置は2回目の PoE 給電ポートリセット(PD 受電機器をリブート)を行いますが、さらに3回目のポートリセットでは PoE 給電が停止したままになります。

(Ver. 1.00.05 以降で対応)

### 3.1.33 CPOE (For PoE Model Only)

Configuration > PoE > CPOE configuration

このページで CPOE を設定します。

## CPOE Configuration

Mode  ▼

Save    Reset

オブジェクト	説明
Mode	CPOE モードの動作を示します。可能なモードは次のとおりです。 [Enabled] CPOE モード操作を有効にします。(デフォルト値) [Disabled] CPOE モードの動作を無効にします。

ボタン	
Save	クリックして変更を保存します。
Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリ ックします。

## 注意事項



Continuous PoE 機能(c-poe)の設定を無効にした場合でも、本装置の電源起動途中に一時的に PD 受電機器に対して PoE 給電されます。(約 30 秒)

### 3.1.34 Storm Policing

Configuration > Storm Policing

デバイスのグローバルストームポリサーは、このページで設定します。

ユニキャストストームポリサー、マルチキャストストームポリサー、およびブロードキャストストームポリサーがあります。これは、フラッディングされたフレーム、つまり MAC アドレステーブルに存在しない(VLAN ID、DMAC)ペアを持つフレームにのみ影響します。表示される設定は次のとおりです。

#### Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	<input type="checkbox"/>	1	fps ▼
Multicast	<input type="checkbox"/>	1	fps ▼
Broadcast	<input type="checkbox"/>	1	fps ▼

オブジェクト	説明
Frame Type	次の設定が適用されるフレームタイプ
Enable	特定のフレームタイプに対してグローバルストームポリサーを有効または無効にします。
Rate	グローバルストームポリサーのレートを制御します。この値は、「単位」が fps の場合は 1-1024000 に、Unit「単位」が kfps の場合は 1-1024 に制限されます。このレートは、グローバルストームポリサーがサポートする最も近い値に内部的に切り上げられます。サポートされているレートは Rate が 512fps 以下の場合 1、2、4、8、16、32、64、128、256、512fps です。Rate が 512fps 以上の場合 1、2、4、8、16、64、128、256、512、1024kfps です。
Unit	グローバルストームポリサーレートの測定単位を fps または kfps で制御します。

ボタン	
<input type="button" value="Save"/>	クリックして変更を保存します。
<input type="button" value="Reset"/>	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

#### 注意事項

 本グローバルストームポリサー機能は、サポートの対象外です。

### 3.1.35 LPT

Configuration > LPT

このページで LPT(リンクパススルー)を設定します。

本装置 2 台での対向接続において、LPT が有効設定の場合、対向機の USER ポートのリンク断または LH

ポートのリンク断(片断線も含む)により、USER ポートを強制リンク断(Force Down)します。  
装置間のリンク状態通知は EFM-OAM(IEEE802.3ah OAM)フレームを用いて行われます。

#### 注意事項

- ❗ LPT を有効にするには EFM-OAM(IEEE802.3ah OAM) が有効になっている必要があります。  
(EFM-OAM および LPT のデフォルト値：有効)

### LPT Configuration

Mode	Enabled ▼	
USER port Advertise Wait Time	0	time unit 0.1 sec (100 millisecond)
LH port Advertise Wait Time	0	time unit 0.1 sec (100 millisecond)

Save    Reset

オブジェクト	説明
Mode	LPT モードの動作を示します。 [Enabled] LPT モードを有効にします。 [Disabled] LPT モードを無効にします。 注:LPT 機能を使用するには、EFM-OAM 機能を有効にする必要があります。 OAM LED: リモートアラームが検出されると点灯します。リモートアラームは、リモート APLMC(POE)によって送信された OAMPDU パケットで重大なイベントが発生したことを意味します。クリティカル・イベントのアラームがクリアされるとオフになります。(クリティカル・イベント、フラグ:false)
USER port Advertise Wait Time	ローカルシステムで、USER ポートリンクのダウンを検出したときに送信するリンクフォールトメッセージのガードタイム(遅延時間)を示します。 有効な値の範囲は 0~20(x100 ミリ秒)、つまり 0.1 秒~2 秒です。 デフォルト値:0 (待ち時間なし)
LH port Advertise Wait Time	ローカルシステムで、LH ポートのリンクダウンが検出されたときに送信される Link Fault Message のガードタイム(遅延時間)を示します。 有効な値の範囲は 0~20(x100 ミリ秒)、つまり 0.1 秒~2 秒です。 デフォルト値:0 (待ち時間なし)

ボタン	
Save	クリックして変更を保存します。
Reset	ローカルで行った変更を元に戻し、以前に保存した値に戻す場合にクリックします。

## 3.2 Monitor

### 3.2.1 System Information

Monitor > System > Information

デバイスのシステム情報が表示されます。

#### System Information

Auto-refresh  Refresh

System	
Contact	
Name	
Location	
Hardware	
Product Name	APLMCBX40UPOE
MAC Address	00-40-66-e7-ea-b5
Serial Number	303279000030
Temperature-PSE	53 C
Time	
System Date	2021-08-15 10:05:06+09:00
System Uptime	0days 00:01:22
Software	
Software Version	1.00.05
Software Date	2021-08-03 20:49:15+08:00
Acknowledgments	<a href="#">Details</a>

オブジェクト	説明
Contact	Configuration > System > Information System Contact で設定されているシステムコンタクト
Name	Configuration > System Information > System Name で設定されたシステム名
Location	Configuration > System > Information System Location で設定されているシステムの場所
MAC Address	このデバイスの MAC アドレス
Serial Number	このデバイスのシリアル番号
Temperature-PSE (ApersiaLightMC-PoE シリーズのみ)	PoE 用 LSI の温度測定値
System Date	現在のシステムの日時
System Uptime	デバイスが動作している期間
Product Name	このデバイスの型式
Software Version	このデバイスのソフトウェアバージョン
Software Date	デバイスソフトウェアが作成された日付
Acknowledgements	本デバイスに使用されているソフトウェアのライセンス条件の詳細を表示します。

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。
Refresh	クリックすると、ページが更新されます。

### 3.2.2 CPU Load

Monitor > System > CPU Load

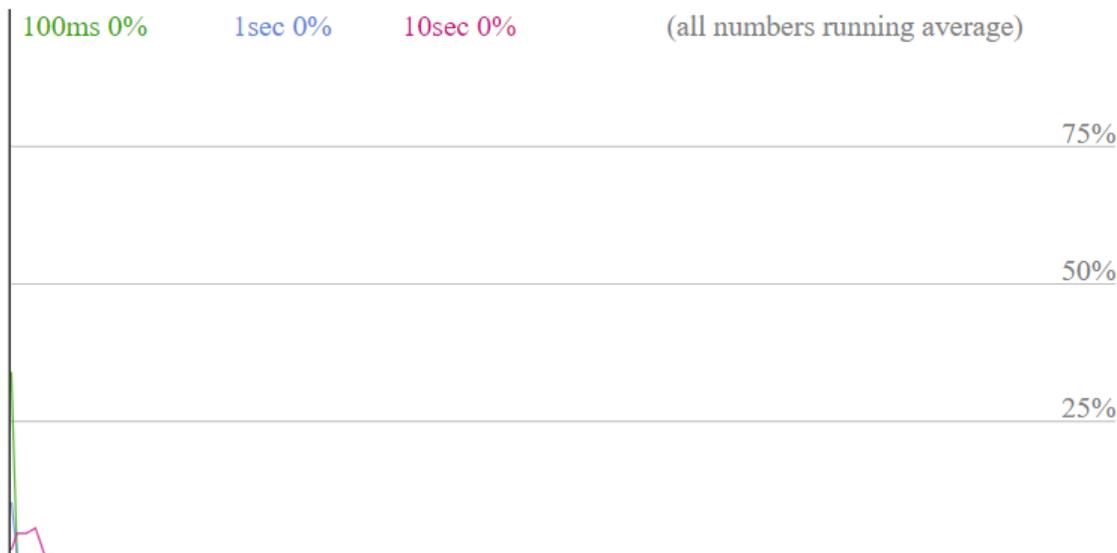
このページには、SVG グラフを使用して CPU 負荷が表示されます。

負荷は、最後の 100 ミリ秒、1 秒、および 10 秒間隔の平均として測定されます。最後の 120 個のサンプルがグラフ化され、最後の数値もテキストとして表示されます。

SVG グラフを表示するには、ブラウザが SVG 形式をサポートする必要があります。一部のブラウザのバージョンでは SVG をサポートするプラグインのインストールが必要となる場合があります。

#### CPU Load

Auto-refresh



ボタン	
Auto-refresh <input checked="" type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。

### 3.2.3 IP Status

Monitor > Systems > IP Status

このページには、IP プロトコル層のステータスが表示されます。ステータスは、IP インターフェイス、IP ルート、および近隣ノードキャッシュ(ARP キャッシュ)のステータスによって定義されます。

## IP Interfaces

Auto-refresh  

Interface	Type	Address	Status
VLAN1	LINK	00-40-66-e7-ea-b5	<UP BROADCAST MULTICAST>
VLAN1	IPv4	10.249.35.127/23	
VLAN2	LINK	00-40-66-e7-ea-b5	<UP BROADCAST MULTICAST>

## Routes

Network	Gateway	Status
0.0.0.0/0	10.249.34.1	<UP GATEWAY>
10.249.34.0/23	VLAN1	<UP>

## Neighbour cache

IP Address	Link Address
10.249.34.1	VLAN1:00-40-66-c7-4b-d5

オブジェクト	説明
IP Interfaces	IP インタフェース
Interface	インタフェースの名前 [VLAN1]: MANAGE ポート用(アウトバンド管理) [VLAN2]: USER ポート/LH ポート用(インバンド管理)
Type	エントリのアドレスタイプ。LINKまたはIPv4です。
Address	インタフェースの現在のアドレス
Status	インタフェースのステータスフラグ
Routes ルート	
Network	このルートの宛先 IP ネットワークまたはホストアドレス
Gateway	このルートのゲートウェイアドレス
Status	ルートのステータスフラグ
Neighbor cache 近隣キャッシュ	
IP Address	エントリの IP アドレス
Link Address	指定された IP アドレスへのバインドが存在するリンク(MAC)アドレス

ボタン	
<input type="button" value="Refresh"/>	クリックすると、ページが更新されます。
Auto-refresh <input checked="" type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されま す。自動更新は3秒ごとに行われます。

### 3.2.4 System Log

Monitor &gt; System &gt; Log

システムログを表示します。

各ページには、「ページあたりのエントリ数(entries per page.)」入力フィールドで選択した最大 999 個のテーブルエントリが表示されます。最初にアクセスしたときに、このテーブルの最初のエントリが Web ページに表示されます。

[Level]入力フィールドは、表示システムログエントリをフィルタするために使用されます。

[Clear Level]入力フィールドを使用して、消去するシステムログエントリを指定します。特定のシステムログエントリをクリアするには、クリアレベルを選択してから **Clear** ボタンをクリックします。

[Start from ID]入力フィールドでは、このテーブルの表示開始エントリを変更できます。

**Refresh** ボタンをクリックすると、表示されているテーブルがそのエントリまたは最も近い次のエントリから更新されます。さらに、これらの入力フィールドは、**Refresh** ボタンをクリックすると、最初に表示されたエントリの値を想定し、同じ開始入力フィールドで継続的に更新できるようになります。

**>>** は、現在表示されているテーブルの最後のエントリを、次のルックアップの基準として使用します。終端に達すると、「これ以上のエントリはありません」というテキストが表示されます。最初からやり直すには **|<<** ボタンを使ってください。

### System Log Information

Auto-refresh  **Refresh** **Clear** **|<<** **<<** **>>** **>>|**

Level	All ▼
Clear Level	All ▼

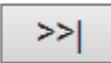
The total number of entries is 7 for the given level.

Start from ID  with  entries per page.

ID	Level	Time	Message
1	Informational	2019-10-17 08:04:06+09:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	2019-10-17 08:04:08+09:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	2019-10-17 08:04:08+09:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Warning	2019-10-17 08:04:19+09:00	SYSTEM: Alarm LED, changed state to ON (stable).
5	Notice	2019-10-17 08:39:11+09:00	LINK-UPDOWN: USER Port Link Up.
6	Notice	2019-10-17 08:39:14+09:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
7	Notice	2019-10-17 08:42:01+09:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.

オブジェクト	説明
ID	システムログエントリの ID
Level	システムログエントリのレベル Informational: システム・ログ・エントリは Informational レベルです。 Warning: システムログエントリは Warning レベルです。 Error: システムログエントリは Error レベルです。
Time	システムログエントリの発生時刻
Message	システムログエントリの詳細メッセージ

ボタン	
Auto-refresh <input checked="" type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は 3 秒ごとに行われます。
<b>Refresh</b>	現在のエントリからテーブルエントリを更新します。
<b>Clear</b>	選択したエントリを削除します。
<b> &lt;&lt;</b>	使用可能な最初のエントリからテーブルエントリを更新します。
<b>&lt;&lt;</b>	現在表示されている最後のエントリで終了するテーブルエントリを更新します。

	現在表示されている最後のエントリからテーブルエントリを更新します。
	テーブルエントリを更新し、最後に使用可能なエントリで終了します。

### 3.2.5 System Detailed Log

Monitor > System > Detailed Log

デバイスシステムの詳細なログ情報がここに表示されます。

#### Detailed System Log Information



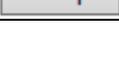



<b>ID</b>	1
-----------	---

#### Message

Level	Notice
Time	2020-01-02 09:00:12+09:00
Message	LINK-UPDOWN: USER Port Link Up(LPT)

オブジェクト	説明
Level	システム・ログ・エントリーの重大度レベル
ID	システム・ログ・エントリの ID(1 以上)
Message	システムログエントリの詳細メッセージ

ボタン	
	システムログエントリを現在のエントリ ID に更新します。
	システムログエントリを最初に使用可能なエントリ ID に更新します。
	システムログエントリを以前に使用可能なエントリ ID に更新します。
	システムログエントリを次に使用可能なエントリ ID に更新します。
	システムログエントリを最後に使用可能なエントリ ID に更新します。

### 3.2.6 System Alarm

Monitor > System > Alarm

このページには、最新のアラームと履歴が表示されます。

#### Alarm Current

Auto-refresh

Alarm Current Alarm History

SeqNo	Description	Time
2	Link down on LH Port	2019-10-17 08:04:20+09:00

## Alarm History

Auto-refresh

SeqNo	Description	State	Time
1	Link down on USER Port	Set	2019-10-17 08:04:20+09:00
2	Link down on LH Port	Set	2019-10-17 08:04:20+09:00
3	Link down on USER Port	Clear	2019-10-17 08:39:11+09:00

オブジェクト	説明
Alarm Current	最新アラーム
SeqNo	アラームシーケンス番号
Description	アラームタイプの説明
Time	アラーム発生日時
Alarm History	アラーム履歴
SeqNo	アラームシーケンス番号
Description	アラームタイプの説明
State	アラーム状態。アラーム発生時の状態を設定する。クリアされたアラームは消えます。
Time	アラーム発生日時

ボタン	
Auto-refresh <input checked="" type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。
<input type="button" value="Refresh"/>	クリックすると、データが更新されます。
<input type="button" value="Clear"/>	クリックしてデータをクリアします。

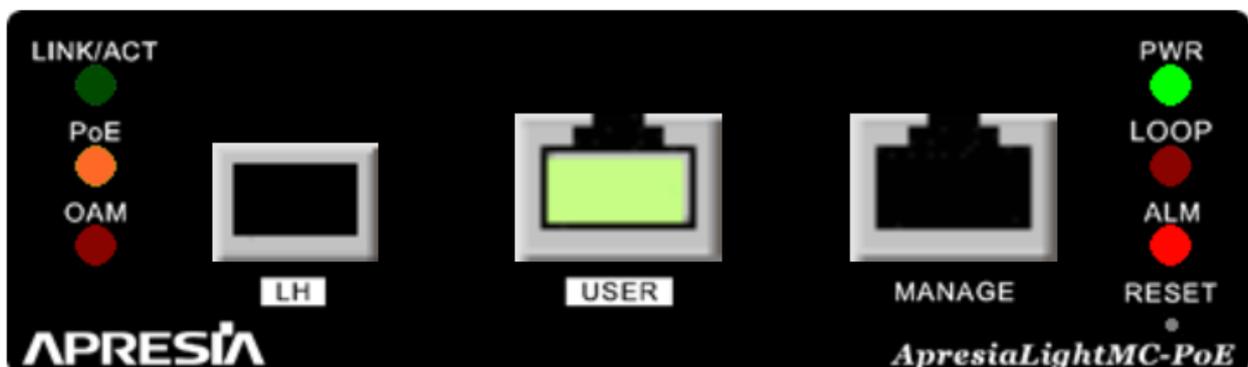
### 3.2.7 Ports State

Monitor > Ports > State

このページには、現在のデバイスポートの状態の概要が表示されます。

## Port State Overview

Auto-refresh



ポートの状態は次のように示されます。

RJ45 ポート			
SFP ポート			
状態	Disabled	Down	Link
PWR		電源供給時に緑点灯します。	
LOOP		ループを検知すると赤点灯し、解消されると消灯します。 (実機は赤点滅します)	
ALM		電源投入、装置リブート時のハードリセット中、あるいは装置起動異常時に赤点灯します。 指定したポートのリンクが切断されると赤点灯します。 (デフォルト値：USER ポートおよび LH ポート)	
LINK/ACT		リンクが確立またはフレームの送受信が行われると緑点灯します。(実機はフレーム送受信時、点滅します)	
PoE (For PoE Model Only)	 	PoE 給電が正常に行われている場合は緑点灯します。 PoE 給電異常時、または、PD 受電未対応機器と接続した場合は橙点灯します。 PoE 給電停止設定時又はPD 受電機器が未接続の場合は消灯します。	
OAM		EFM-OAM 有効時： 対向のメディアコンバーターの USER ポートがリンクダウンする、あるいは電源断通知(dying gasp)を検知した時に赤点灯します。 EFM-OAM 無効時：消灯します。	

ボタン	
Auto-refresh <input checked="" type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。
Refresh	クリックすると、ページが更新されます。

#### 注意事項

 PoE 給電異常時、または、PD 受電未対応機器と接続した場合、PoE LED は橙点灯します。

#### 3.2.8 Traffic Overview

Monitor > Ports > Traffic Overview

このページは、すべてのデバイスポートの一般的な統計情報を表示します。

Port Statistics Overview

Auto-refresh  Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
USER	7719	5838	1218817	1474279	0	0	0	0	2364
LH	0	1	0	68	0	0	0	0	0
MANAGE	0	0	0	0	0	0	0	0	0

オブジェクト	説明
Port	ポート名称
Packets	ポートごとの受信および送信パケットの数
Bytes	ポートごとの受信および送信バイト数
Errors	受信エラー、送信エラーとなったフレーム数
Drops	輻輳のために廃棄された受信および送信フレーム数
Filtered	転送プロセスによってフィルタリングされた受信フレーム数

ボタン	
<input type="button" value="Refresh"/>	クリックすると、ページがすぐに更新されます。
<input type="button" value="Clear"/>	すべてのポートのカウンタをクリアします。
<input checked="" type="checkbox"/> Auto-refresh	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。

3.2.9 Detailed Statistics

Monitor > Ports > Detailed Statistics

このページには、特定のデバイス・ポートの詳細な統計情報が表示されます。ポート選択ボックスを使用して、表示するデバイス・ポートの詳細を選択します。

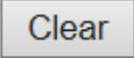
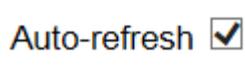
表示されるカウンタは、受信と送信の合計、受信と送信のサイズカウンタ、および受信と送信のエラーカウンタです。

Detailed Port Statistics Port USER

Port USER Auto-refresh  Refresh Clear

Receive Total		Transmit Total	
Rx Packets	8336	Tx Packets	6526
Rx Octets	1340261	Tx Octets	1725070
Rx Unicast	5458	Tx Unicast	6519
Rx Multicast	2372	Tx Multicast	0
Rx Broadcast	506	Tx Broadcast	7
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	3455	Tx 64 Bytes	2039
Rx 65-127 Bytes	3294	Tx 65-127 Bytes	2228
Rx 128-255 Bytes	272	Tx 128-255 Bytes	435
Rx 256-511 Bytes	7	Tx 256-511 Bytes	1037
Rx 512-1023 Bytes	1264	Tx 512-1023 Bytes	197
Rx 1024-1526 Bytes	44	Tx 1024-1526 Bytes	590
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	8336	Tx Q0	6521
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	5
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	2372		

オブジェクト	説明
Receive Total and Transmit Total 受信合計と送信合計	
Rx and Tx Packets	受信および送信されたパケットの数
Rx and Tx Octets	受信および送信されたバイト数。FCS は含まれますが、フレーミングビットは含まれません。
Rx and Tx Unicast	受信および送信されたユニキャストパケットの数
Rx and Tx Multicast	受信および送信されたマルチキャストパケットの数
Rx and Tx Broadcast	受信および送信されたブロードキャストパケットの数
Rx and Tx Pause	受信および送信された PAUSE オペコードを持つ MAC 制御フレームの数
Receive and Transmit Size Counters 受信および送信サイズカウンタ	
それぞれのフレームサイズに基づいてカテゴリに分割された、受信および送信パケットの数	
Receive and Transmit Queue Counters 受信キューカウンタと送信キューカウンタ	
入出力キューごとの受信パケットと送信パケットの数	
Receive Error Counters 受信エラーカウンタ	
Rx Drops	受信バッファの不足または出力輻輳が原因でドロップされたフレームの数
Rx CRC/Alignment	CRC エラーまたはアラインメントエラーのある受信フレームの数
Rx Undersize	有効な CRC で受信されたショートフレームの数
Rx Oversize	有効な CRC で受信されたロングフレームの数
Rx Fragments	無効な CRC で受信したショートフレームの数
Rx Jabber	無効な CRC で受信したロングフレームの数
Rx Filtered	転送プロセスによってフィルタリングされた受信フレームの数
Note: ショートフレームとは、64 バイト未満のフレームのことです。 ロングフレームは、このポートに設定されている最大フレーム長より長いフレームです。	
Transmit Error Counters 送信エラーカウンタ	
Tx Drops	出力バッファの輻輳が原因でドロップされたフレームの数
Tx Late/Exc. Coll.	過剰な輻輳またはレイトコリジョンが原因で廃棄されたフレームの数

ボタン	
	クリックすると、ページがすぐに更新されます。
	選択したポートのカウンタをクリアします。
	このチェックボックスをオンにすると、ページが自動的に更新されません。自動更新は 3 秒ごとに行われます。

### 3.2.10 Link OAM Statistics

Monitor > Link OAM > Statistics

このページには、特定のデバイス・ポートの OAM 統計情報の詳細が表示されます。

表示されるカウンタは、LH ポートで送受信された OAM フレームの合計数を表します。本装置の起動中あるいは対向装置との OAM ディスカバリーが完了する前は、統計情報は取得できません。

Detailed Link OAM Statistics for Port LH

Auto-refresh  Refresh Clear

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

オブジェクト	説明
Rx and Tx OAM Information PDU's	送受信された OAM 情報 PDU の数。
Rx and Tx Unique Error Event Notification	このインタフェースで送受信された一意のイベント OAMPDU の数。送信中にフレームが失われる可能性があることを考慮すると、イベント通知は、正常に受信される可能性を高めるために 2 回送信される場合があります。重複イベント通知送信は、Tx および Rx の重複イベント通知カウンタによってそれぞれカウントされます。固有のイベント通知 OAMPDU は、以前に送信されたイベント通知 OAMPDU シーケンス番号とは異なるシーケンス番号フィールドを持つイベント通知 OAMPDU として示されます。
Rx and Tx Duplicate Error Event Notification	このインタフェースで送受信された重複イベント OAMPDU の数。送信中にフレームが失われる可能性がある場合、イベント通知 OAMPDU は、正常に受信される可能性を高めるために複数回送信される場合があります。重複イベント通知 OAMPDU は、以前に送信されたイベント通知 OAMPDU シーケンス番号と同一のシーケンス番号フィールドを持つイベント通知 OAMPDU として示されます。
Rx and Tx Loopback Control	このインタフェースで送受信されたループバック制御 OAMPDU の数
Rx and Tx Variable Request	このインタフェースで送受信された可変要求 OAMPDU の数
Rx and Tx Variable Response	このインターフェースで送受信された可変応答 OAMPDU の数
Rx and Tx Org Specific PDU's	このインタフェースで送信された組織固有の OAMPDU の数
Rx and Tx Unsupported Codes	サポートされていないオペコードを使用して、このインターフェース上で送信された OAMPDU の数
Rx and Tx Link fault PDU's	このインターフェースで送受信されたリンク障害 PDU の数
Rx and Tx Dying Gasp	このインターフェースで送受信された Dying Gasp イベントの数
Rx and Tx Critical Event PDU's	このインターフェースで送受信されたクリティカルイベント PDU の数

ボタン	
<input type="button" value="Refresh"/>	クリックすると、ページがすぐに更新されます。
<input type="button" value="Clear"/>	選択したポートのカウンタをクリアします。
<input checked="" type="checkbox"/> Auto-refresh	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。

### 3.2.11 Link OAM Port Status

Monitor > Link OAM > Port Status

このページには、EFM-OAM 構成の動作ステータスが表示されます。

表示されるフィールドには、選択したポートのアクティブな設定ステータスが表示されます。

#### Detailed Link OAM Status for Port LH

Auto-refresh

Local		Remote	
MAC Address	00:40:66:e0:a6:fa	MAC Address	00:40:66:e0:a7:42
Vender(OUI)	00:40:66	Vender(OUI)	00:40:66
Discovery status	SEND_ANY_STATE	Discovery status	SEND_ANY_STATE
Power status	-	Power status	Up
User-port status	-	User-port status	-
Critical Event	-	Critical Event	Up
Link status	-	Link status	Up
OAM Version	01	OAM Version	01
OAM Mode	Active	OAM Mode	Active
Unidirectional	Unsupported	Unidirectional	Unsupported
Remote Loopback	Unsupported	Remote Loopback	Unsupported
Link Event	Supported	Link Event	Supported
Variable Retrieval	Supported	Variable Retrieval	Supported

Link Status Information	
Local LH Port Link Fault	-
Remote LH Port Link Fault	-
Remote USER Port Link Fault	-
Remote Power Fault	-

オブジェクト	説明
MAC Address	MAC アドレス
Vender(OUI)	ベンダー識別子(OUI)
Discovery Status	検出プロセスの現在の状態が表示されます。状態には、障害状態、アクティブ状態、パッシブ状態、SEND_LOCAL_REMOTE_STATE、SEND_LOCAL_REMOTE_OK_STATE、SEND_ANY_STATE があります。
Power status	Local 側は常に - が表示されます。 Remote 側は、デバイス電源の状態が表示されます。
User-Port Status	Local 側は常に - が表示されます。 Remote 側は、Critical Event Flag/Bit に依存する Up/Down が表示されます。 (注:このステータスは、LH ポートの「link-oam critical-event-mode ais (クリティカル・イベント・モード ais)」によって変更できます。) Up: クリティカル・イベント (false) のある OAM フレームを受信 Down: クリティカル・イベント (true) を含む OAM フレームを受信

Critical Event	Local 側は常に - が表示されます。 Remote 側は、Critical Event Flag/Bit に依存する Up/Down が表示されます。 Up: Critical Event False を受信 Down: Critical Event True を受信
Link status	Local 側は常に - が表示されます。 Remote 側は、EFM-OAM ステータスまたは LH ポートのステータスにより表示されます。 Up: Link Fault bit=0 のフレームを受信 Down: Link Fault bit=1 のフレームを受信 - : リモートデバイスの EFM-OAM が無効になっているか、このデバイスの LH ポートがリンクダウンしている場合
OAM Version	Link-OAM のバージョン
OAM Mode	OAM のモード
Unidirectional	この機能は、ユーザーが設定することはできません。この設定のステータスは PHY から取得されます。
Remote Loopback	ステータスが有効な場合、デバイスは OAM remote loopback mode をサポートします。
Link Event	ステータスが有効な場合、デバイスは interpreting Link Events をサポートします。
Variable Retrieval	ステータスが有効な場合、デバイスは sending Variable Response OAMPDU をサポートします。
Local LH Port Link Fault	Local 側 LH ポートのリンク障害状態を表示します。 - : Local 側 LH ポートが Link up detect: Local 側 LH ポートが Link down
Remote LH Port Link Fault	Remote 側 LH ポートのリンク障害状態を表示します。EFM-OAM Link Fault フラグを使用します。 - : APLMC が Link Fault (bit=0) の OAMPDU を受信 detect: APLMC が Link Fault (bit=1) の OAMPDU フレームを受信
Remote USER Port Link Fault	Remote 側 USER ポートのリンク障害状態を表示します。EFM-OAM Critical Event フラグを使用します。 - : APLMC がクリティカル・イベント (bit=0) の OAMPDU を受信 detect: APLMC がクリティカル・イベント (bit=1) の OAMPDU を受信
Remote Power Fault	Remote 側デバイスの電源状態を表示します。 - : Local 側で dying gasp フレーム未受信 detect: Local 側で dying gasp フレームを受信 これは、Remote 側デバイスの電源が切れている可能性があることを示します。

ボタン	
<input type="button" value="Refresh"/>	クリックすると、ページがすぐに更新されます。
<input checked="" type="checkbox"/> Auto-refresh	このチェックボックスをオンにすると、ページが自動的に更新されません。自動更新は 3 秒ごとに行われます。

### 3.2.12 Link OAM Event Status

Monitor > Link OAM > Event Status

このページでは、現在の EFM-OAM リンク・イベント構成を検査し、変更することもできます。

左側の枠にはローカル側 OAM ユニットのイベント状態が表示され、右側の枠には LH ポートのリモート側 OAM ユニットのイベント状態が表示されます。

Detailed Link OAM Link Status for Port LH

Auto-refresh  Refresh

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0	Frame Error Event Timestamp	0
Frame Error Event Timestamp	0	Frame error event window	0
Frame error event window	0	Frame error event threshold	0
Frame error event threshold	0	Frame errors	0
Frame errors	0	Total frame errors	0
Total frame errors	0	Total frame error events	0
Total frame error events	0		
Local Frame Period Status		Remote Frame Period Status	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		Remote Symbol Period Status	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Total symbol period errors	0	Total symbol period errors	0
Total Symbol period error events	0	Total Symbol period error events	0
Local Event Seconds Summary Status		Remote Event Seconds Summary Status	
Error Frame Seconds Summary Event Timestamp	0	Error Frame Seconds Summary Event Timestamp	0
Error Frame Seconds Summary Event window	0	Error Frame Seconds Summary Event window	0
Error Frame Seconds Summary Event Threshold	0	Error Frame Seconds Summary Event Threshold	0
Error Frame Seconds Summary Errors	0	Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Errors	0	Total Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Events	0	Total Error Frame Seconds Summary Events	0

オブジェクト	説明
Sequence Number	この 2 オクテットのフィールドは、リモートエンドで発生したイベントの合計数を示します。
Frame Error Event Timestamp	この 2 オクテットのフィールドは、イベントが生成された時間基準を 100ms 間隔で示します。
Frame error event window	この 2 オクテットのフィールドは、期間の長さを 100ms 間隔で示します。 1) デフォルト値は 1 秒です。2) 下限は 1 秒です。3) 上限は 1 分です。
Frame error event threshold	この 4 オクテットのフィールドは、イベントが生成されるために、その期間内に検出されたエラーフレームの数がそれ以上である必要があることを示します。1) デフォルト値は 1 フレームエラーです。2) 下限は 0 フレームエラーです。3) 上限はありません。
Frame errors	この 4 オクテットフィールドは、その期間中に検出されたエラーフレームの数を示します。
Total frame errors	この 8 オクテットのフィールドは、OAM サブレイヤがリセットされてから検出されたエラーフレームの合計を示します。
Total frame error events	この 4 オクテットフィールドは、OAM サブレイヤがリセットされてから生成されたエラーフレームイベント TLV の数を示します。
Frame Period Error Event Timestamp	この 2 オクテットのフィールドは、イベントが生成された時間基準を 100ms 間隔で示します。
Frame Period Error Event Window	この 4 オクテットのフィールドは、フレーム単位で期間を示します。
Frame Period Error Event Threshold	この 4 オクテットのフィールドは、イベントを生成するためには、その期間内にエラーが発生したフレームの数以上である必要があることを

	示します。
Frame Period Errors	この 4 オクテットフィールドは、その期間のフレームエラーの数を示します。
Total frame period errors	この 8 オクテットのフィールドは、OAM サブレイヤがリセットされてから検出されたフレームエラーの合計を示します。
Total frame period error events	この 4 オクテットフィールドは、OAM サブレイヤがリセットされてから生成されたエラーフレーム期間イベント TLV の数を示します。
Symbol Period Error Event Timestamp	この 2 オクテットのフィールドは、イベントが生成された時間基準を 100ms 間隔で示します。
Symbol Period Error Event Window	この 8 オクテットのフィールドは、期間中のシンボルの数を示します。
Symbol Period Error Event Threshold	この 8 オクテットのフィールドは、イベントが生成されるためには、その期間内のエラーシンボルの数がそれ以上でなければならないことを示します。
Symbol Period Errors	この 8 オクテットのフィールドは、期間中のシンボルエラーの数を示します。
Total symbol period errors	この 8 オクテットのフィールドは、OAM 副層がリセットされた後のシンボルエラーの合計を示します。
Total Symbol period error events	この 4 オクテットフィールドは、OAM サブレイヤがリセットされてから生成されたエラーシンボル期間イベント TLV の数を示します。
Error Frame Seconds Summary Event Timestamp	この 2 オクテットのフィールドは、16 ビット符号なし整数として符号化された、100ms 間隔でイベントが生成された時の時間基準を示します。
Error Frame Seconds Summary Event window	この 2 オクテットのフィールドは、16 ビット符号なし整数として符号化された 100ms 間隔の期間を示します。
Error Frame Seconds Summary Event Threshold	この 2 オクテットのフィールドは、16 ビット符号なし整数としてエンコードされたイベントが生成されるためには、その期間内でのエラーフレーム秒数がそれ以上でなければならないことを示します。
Error Frame Seconds Summary Errors	この 2 オクテットのフィールドは、16 ビット符号なし整数として符号化された、その期間の誤りフレーム秒数を示します。
Total Error Frame Seconds Summary Errors	この 4 オクテットフィールドは、OAM サブレイヤがリセットされてから検出されたエラーフレーム秒の合計を示します。
Total Error Frame Seconds Summary Events	この 4 オクテットのフィールドは、OAM サブレイヤがリセットされてから生成された、32 ビット符号なし整数として符号化されたエラーフレーム秒要約イベント TLV の数を示します。

ボタン	
<input type="button" value="Refresh"/>	クリックすると、ページがすぐに更新されます。
<input type="button" value="Clear"/>	クリックすると、データがクリアされます。
<input checked="" type="checkbox"/> Auto-refresh	このチェックボックスをオンにすると、ページが自動的に更新されず、自動更新は 3 秒ごとに行われます。

### 3.2.13 Access Management Statistics

Monitor > Security > Access Management Statistics

このページには、アクセス管理の統計が表示されます。

なお、アクセス管理を有効にした場合のみ統計情報が取得されます。

#### Access Management Statistics

Auto-refresh  Refresh Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

オブジェクト	説明
Interface	リモートホストがデバイスにアクセスできるインターフェースの種類
Received Packets	アクセス管理モードが有効なときにインターフェースから受信したパケットの数
Allowed Packets	アクセス管理モードが有効な場合に、インターフェースから許可されるパケットの数
Discarded Packets	アクセス管理モードが有効なときにインターフェースから廃棄されたパケットの数

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。
Refresh	クリックすると、ページがすぐに更新されます。
Clear	すべての統計をクリアします。

### 3.2.14 RMON Statistics

Monitor > Security > System > RMON > Statistics

このページでは、RMON 統計エントリの概要について説明します。各ページには、「ページあたりのエントリ数」入力フィールドで選択した統計テーブルの最大 99 個のエントリが表示されます。デフォルトは 20 個です。最初にアクセスしたとき、Web ページには統計テーブルの先頭から最初の 20 エントリが表示されます。最初に表示されるのは、統計テーブルで ID が最も小さいものです。

[Start from Control Index] では、統計テーブルの開始点を選択できます。

ボタンをクリックすると、表示されているテーブルが、そのテーブルまたは次に一致する統計テーブルから更新されます。

は、現在表示されているエントリの最後のエントリを、次のルックアップの基準として使用します。終端に達すると、「これ以上のエントリはありません」というテキストが表示されます。最初からやり直すには  ボタンを使ってください。

表示されるカウンタは次のとおりです。

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1518
No more entries																		

オブジェクト	説明
ID	Statistics エントリのインデックスを示します。
Data Source(ifIndex)	監視するポート ID
Drop	リソース不足のためにプローブによってパケットがドロップされたイベントの総数
Octets	ネットワークで受信したデータの総オクテット数 (エラーパケットを含む)
Pkts	受信したパケットの総数 (エラーパケット、ブロードキャストパケット、およびマルチキャストパケットを含む)
Broad-cast	ブロードキャストアドレスに送信された、受信した正常なパケットの総数
Multi-cast	マルチキャストアドレスに送信された、受信した正常なパケットの総数です。
CRC Errors	フレーム長は正常であったが、FCS エラーか Alignment エラーのどちらかを含んでいた受信パケットの総数
Under-size	64 オクテット未満で受信したパケットの合計数
Over-size	最大フレーム長設定値以上で受信したパケットの合計数
Frag.	サイズが 64 オクテット未満で、無効な CRC とともに受信されたフレームの数
Jabb.	最大フレーム長設定値以上で受信したパケットで、無効な CRC を含むフレームの数
Coll.	このイーサネットセグメントでのコリジョンの合計数の推定値
64	長さが 64 オクテットであった受信パケットの総数 (エラーパケットを含む)
65 ~ 127	長さが 65 から 127 オクテットの間であった受信パケットの総数 (エラーパケットを含む)
128 ~ 255	長さが 128 から 255 オクテットの間であった受信パケットの総数 (エラーパケットを含む)
256 ~ 511	長さが 256 から 511 オクテットの間であった受信パケットの総数 (エラーパケットを含む)
512 ~ 1023	長さが 512 から 1023 オクテットの間であった受信パケットの総数 (エラーパケットを含む)
1024 ~ 1518	長さが 1024 から 1518 オクテットの間であった受信パケットの総数 (エラーパケットを含む)

ボタン

Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。
Refresh	クリックすると、ページがすぐに更新されます。
<<	統計テーブルの最初のエントリ (ID が最も小さいエントリ) からテーブルを更新します。
>>	現在表示されている最後のエントリの後のエントリからテーブルを更新します。

### 3.2.15 RMON History

Monitor > Security > Access Management Statistics

このページでは、RMON 履歴エントリの概要について説明します。各ページには、「entries per page (ページあたりのエントリ数)」入力フィールドで選択した履歴テーブルの最大 99 個のエントリが表示されます。デフォルトは 20 個です。最初にアクセスしたとき、Web ページには「履歴 (History) テーブル」の先頭から最初の 20 エントリが表示されます。

「Start from History Index (履歴インデックスから開始)」と「Sample Index (サンプルインデックス)」では、履歴テーブルで開始点を選択できます。

Refresh ボタンをクリックすると、表示されているテーブルが更新されます。

>> は、現在表示されているエントリの最後のエントリを、次のルックアップの基準として使用します。終端に達すると、「これ以上のエントリはありません」というテキストが表示されます。最初からやり直すには |<< ボタンを押してください。

#### RMON History Overview

Auto-refresh  Refresh |<< >>

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

オブジェクト	説明
History Index	履歴コントロールエントリのインデックスを示します。
Sample Index	コントロールエントリに関連付けられたデータエントリのインデックスを示します。
Sample Start	このサンプルが測定された間隔の開始時の sysUpTime の値
Drop	リソース不足のためにプローブによってパケットがドロップされたイベントの総数
Octets	ネットワークで受信したデータの総オクテット数。(エラーパケットを含む)
Pkts	受信したパケットの総数。(不正なパケット、ブロードキャストパケット、およびマルチキャストパケットを含む)
Broad-cast	ブロードキャストアドレスに送信された、受信した正常なパケットの総数
Multi-cast	マルチキャストアドレスに送信された、受信した正常なパケットの総数です。
CRCErrors	長さ(フレーミングビットを除くが、FCS オクテットは含む)が 64 オクテット以上 1518 オクテット以下であったが、オクテットの整数倍での不

	良 Frame Check Sequence(FCS)(FCS エラー)か、またはオクテットの整数倍でない不良 FCS(アライメントエラー)のどちらかを含んでいた受信パケットの総数
Under-size	64 オクテット未満で受信したパケットの合計数
Over-size	最大フレームサイズ以上で受信したパケットの合計数
Frag.	サイズが 64 オクテット未満で、無効な CRC とともに受信されたフレームの数
Jabb.	最大フレームサイズ以上で受信し、無効な CRC とともに受信されたフレームの数
Coll.	このイーサネットセグメントでのコリジョンの合計数の推定値
Utilization	このサンプリング間隔中の、このインターフェース上の平均物理層ネットワーク使用率の推定値。(1/100%単位)

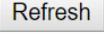
ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は 3 秒ごとに行われます。
	クリックすると、ページがすぐに更新されます。
	履歴テーブルの最初のエントリ (履歴インデックスとサンプルインデックスが最も小さいエントリ) からテーブルを更新します。
	現在表示されている最後のエントリの後のエントリからテーブルを更新します。

### 3.2.16 RMON Alarm

Monitor > Security > System > RMON > Alarm

このページでは、RMON アラームエントリの概要について説明します。各ページには、「entries per page (ページあたりのエントリ数)」入力フィールドで選択したアラームテーブルのエントリが最大 99 個表示されます。デフォルトは 20 個です。最初にアクセスしたとき、Web ページにはアラームテーブルの先頭から 20 個のエントリが表示されます。最初に表示されるのは、アラーム表で ID が最も小さいものです。

「Start from Control Index (コントロールインデックスから開始)」では、アラームテーブルの開始点を選択できます。

 ボタンをクリックすると、表示されているテーブルが更新されます。

 は、現在表示されているエントリの最後のエントリを、次のルックアップの基準として使用します。終端に達すると、「これ以上のエントリはありません」というテキストが表示されます。

最初からやり直すには  ボタンを押してください。

#### RMON Alarm Overview

Auto-refresh    

Start from Control Index  with  entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

オブジェクト	説明
ID	アラーム制御エントリのインデックスを示します。
Interval	サンプリングおよび上昇いきい値と下降いきい値の比較の間隔を秒単

	位で示します。
Variable	サンプリングする特定の変数を示します。
Sample Type	選択した変数をサンプリングし、しきい値と比較する値を計算する方法
Value	最後のサンプリング期間中の統計値。
Startup Alarm	このエントリが最初に有効に設定されたときに送信されるアラーム
Rising Threshold	上昇しきい値
Rising Index	上昇イベントインデックス
Falling Threshold	下降しきい値
Falling Index	下降イベントインデックス

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。
Refresh	クリックすると、ページがすぐに更新されます。
<<	アラームテーブルの最初のエントリ(IDが最も小さいエントリ)からテーブルを更新します。
>>	現在表示されている最後のエントリの後のエントリからテーブルを更新します。

### 3.2.17 RMON Event

Monitor > Security > System > RMON > Event

このページでは、RMON イベントテーブルエントリの概要について説明します。各ページには、イベントテーブルから最大 99 個のエントリが表示されます。デフォルトは 20 個で「entries per page (ページあたりのエントリ数)」入力フィールドで選択します。最初にアクセスしたとき、Web ページには「イベント」(Event) テーブルの先頭から最初の 20 エントリが表示されます。最初に表示されるのは、テーブルで検出されたイベントインデックスとログインデックスが最も小さいものです。

「Start from Event Index (イベントインデックスから開始)」と「Log Index (ログインデックス)」では、ユーザーはイベントテーブルで開始点を選択できます。

ボタンをクリックすると、表示されているテーブルが更新されます。

は、現在表示されているエントリの最後のエントリを、次のルックアップの基準として使用しません。終端に達すると、「これ以上のエントリはありません」というテキストが表示されます。最初からやり直すには  ボタンを押してください。

#### RMON Event Overview

Auto-refresh

Start from Control Index  and Sample Index  with  entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

オブジェクト	説明
Event Index	イベントエントリのインデックスを示します。
Log Index	ログエントリのインデックスを示します。
Log Time	イベントログの時刻を示します。

Log Description	イベントの説明を示します。
-----------------	---------------

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は3秒ごとに行われます。
Refresh	クリックすると、ページがすぐに更新されます。
<<	イベントテーブルの最初のエントリ(イベントインデックスとログインデックスが最小のエントリ)からテーブルを更新します。
>>	現在表示されている最後のエントリの後のエントリからテーブルを更新します。

### 3.2.18 Loop Protection

Monitor > Loop Protection

このページは、デバイスのポートのループ保護ポートステータスを表示します。

#### Loop Protection Status

Auto-refresh  Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
<i>No ports enabled</i>						

オブジェクト	説明
Port	論理ポートのデバイスポート番号
Action	現在設定されているポートアクション
Transmit	現在設定されているポート送信モード
Loops	このポートで検出されたループの数
Status	ポートの現在のループ保護ステータス
Loop	ポートでループが現在検出されているかどうか。
Time of Last Loop	最後に検出されたループイベントの時刻

ボタン	
Refresh	クリックすると、ページがすぐに更新されます。
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、定期的なページの自動更新が有効になります。

### 3.2.19 LLDP Neighbors (For PoE Model Only)

Monitor > LLDP > Neighbors

このページは、すべての LLDP 隣接機器のステータス概要を提供します。表示されたテーブルには、LLDP 隣接機器が検出された各ポートの行が含まれています。

#### LLDP Neighbor Information

Auto-refresh  Refresh

LLDP Remote Device Summary						
Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
GigabitEthernet 1/1	Switch	GigabitEthernet0/1			Other(+)	10.249.31.2 (IPv4)
GigabitEthernet 1/1	18-33-9D-C8-FA-00	Gi0/1	GigabitEthernet0/1	Switch	Bridge(+)	10.249.31.2 (IPv4) - sys-port.1

オブジェクト	説明
Local Interface	LLDP フレームを受信したインターフェイス
Chassis ID	隣接機器の LLDP フレームの ID です。
Port ID	ポート ID は、隣接ポートの ID です。
Port Description	Port Description は、隣接ユニットによってアドバタイズされるポートの説明です。
System Name	システム名は、隣接ユニットによってアドバタイズされる名前です。
System Capabilities	システム機能は、隣接ユニットの機能を記述します。可能な機能は次のとおりです。 1. Other : その他 2. Repeater : リピータ 3. Bridge : ブリッジ 4. WLAN Access Point : WLAN アクセスポイント 5. Router : ルータ 6. Telephone : 電話機 7. DOCSIS cable device : DOCSIS ケーブルデバイス 8. Station only : ステーション 9. Reserved : 予約済み 機能が有効になっている場合、機能の後に (+) が続きます。機能が無効になっている場合は、機能の後に (-) が続きます。
Management Address	管理アドレスは、ネットワーク管理による検出を支援するために上位層エンティティに使用される隣接ユニットのアドレスです。これは、たとえば、ネイバーの IP アドレスを保持することができます。

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は 3 秒ごとに行われます。
<input type="button" value="Refresh"/>	クリックすると、ページが更新されます。

### 3.2.20 LLDP-MED Neighbors (For PoE Model Only)

Monitor > LLDP > LLDP-MED Neighbors

このページには、すべての LLDP-MED ネイバーのステータス概要が表示されます。表示されたテーブルには、LLDP 隣接機器が検出された各ポートの行が含まれています。この機能は、LLDP-MED をサポートする VoIP デバイスに適用されます。

GigabitEthernet 1/1					
Device Type		Capabilities			
Network Connectivity		LLDP-MED Capabilities, Network Policy, Location Identification, Inventory			
Application Type	Policy	Tag	VLAN ID	Priority	DSCP
Voice	Unknown	Untagged	-	-	-
Voice Signaling	Unknown	Untagged	-	-	-
Location					
Country code:					
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities		MAU Type	
Supported	Enabled	100BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 100BASE-T full duplex mode, 10BASE-T half duplex mode		1000BaseTFD - Four-pair Category 5 UTP, full duplex mode	

オブジェクト	説明
Interface	LLDP フレームを受信したインターフェイス
Device Type	<p>LLDP-MED デバイスは、ネットワーク接続デバイスとエンドポイントデバイスという 2 つの主要なデバイスタイプで構成されています。</p> <p>[LLDP-MED ネットワーク接続デバイス定義] TIA-1057 で定義されている LLDP-MED ネットワーク接続機器は、LLDP-MED エンドポイントデバイス用の IEEE802 ベースの LAN インフラストラクチャへのアクセスを提供します。LLDP-MED ネットワーク接続デバイスは、以下のいずれかの技術に基づく LAN アクセスデバイスです。</p> <ol style="list-style-type: none"> <li>1. LAN スイッチ/ルータ</li> <li>2. IEEE 802.1 ブリッジ</li> <li>3. IEEE 802.3 リピータ(歴史的な理由で含まれる)</li> <li>4. IEEE 802.11 無線アクセスポイント</li> <li>5. TIA-1057 で定義されている IEEE 802.1 AB および MED 拡張をサポートし、任意の方法で IEEE802 フレームをリレーできるデバイス</li> </ol> <p>[LLDP-MED エンドポイントデバイス定義] TIA-1057 で定義されている LLDP-MED エンドポイントデバイスは、IEEE802LAN ネットワークエッジにあり、LLDP-MED フレームワークを使用して IP 通信サービスに参加します。</p> <p>LLDP-MED エンドポイントデバイスカテゴリ内で、LLDP-MED スキームは、下記で定義されるように、さらなるエンドポイントデバイスクラスに分割される。</p> <p>各 LLDP-MED エンドポイントデバイスクラスは、前のエンドポイントデバイスクラスのために定義された能力の上に構築されるように定義される。例として、メディアエンドポイント(二類)としての準拠を主張するすべての LLDP-MED エンドポイントデバイスは、汎用エンドポイント(クラス I)に適用可能な TIA-1057 のすべての側面もサポートし、通信デバイス(クラス III)としての準拠を主張するすべての LLDP-MED エンドポイントデバイスは、メディアエンドポイント(二類)および汎用エンドポイント(クラス I)の両方に適用可能な TIA-1057 のすべての側面もサポートするであろう。</p> <p>[LLDP-MED 汎用エンドポイント(クラス I)]</p>

	<p>LLDP-MED 汎用エンドポイント(クラス I)定義は、TIA-1057 で定義されている基本 LLDP 検出サービスを必要とするすべてのエンドポイント製品に適用できますが、IP メディアをサポートしないか、エンドユーザー通信アプライアンスとして動作しません。そのようなデバイスは、(しかしそれだけに限らない)IP 通信コントローラ、他の通信関連サーバ、または TIA-1057 で定義されるような基本サービスを必要とする任意のデバイスを含むことができる。</p> <p>このクラスで定義される検出サービスには、LAN 構成、デバイスの場所、ネットワークポリシー、電源管理、およびインベントリ管理があります。</p> <p>[LLDP-MED メディアエンドポイント(クラス II) ]</p> <p>LLDP-MED メディアエンドポイント(クラス II)定義は、IP メディア機能を持つすべてのエンドポイント製品に適用可能ですが、特定のエンドユーザーに関連付けられる場合と関連付けられない場合があります。機能には、前の汎用エンドポイント・クラス(クラス I)に定義されたすべての機能が含まれ、メディア・ストリーミングに関連する局面を含むように拡張されています。このクラスに準拠する製品カテゴリーの例としては、(しかしそれだけに限らない)音声/メディアゲートウェイがあります。会議 ブリッジ、メディアサーバなどがあります。</p> <p>このクラスで定義される検出サービスには、メディアタイプ固有のネットワーク層ポリシー検出が含まれます。</p> <p>[LLDP-MED 通信エンドポイント(クラス III)]</p> <p>LLDP-MED 通信エンドポイント(クラス III)定義は、IP メディアをサポートするエンドユーザー通信アプライアンスとして機能するすべてのエンドポイント製品に適用できます。機能には、以前の Generic Endpoint(クラス I)および Media Endpoint(二類)クラスに定義されたすべての機能が含まれており、エンドユーザーのデバイスに関連する側面を含むように拡張されています。このクラスに準拠する製品カテゴリーの例としては、IP Phone、PC ベースのソフトフォン、またはエンドユーザを直接サポートするその他の通信アプライアンスなどの(しかしそれだけに限らない)エンドユーザ通信アプライアンスがあります。</p> <p>このクラスで定義される検出サービスには、Location Identifier(ECS/E911 情報含む)の提供、内蔵 L2 スイッチのサポート、インベントリ管理などがあります。</p>
LLDP-MED Capabilities	<p>LLDP-MED Capabilities は、隣接ユニットの LLDP-MED 機能を記述します。可能な機能は次のとおりです。</p> <ol style="list-style-type: none"> <li>1. LLDP-MED 機能</li> <li>2. ネットワークポリシー</li> <li>3. 場所の識別</li> <li>4. MDI-PSE による拡張電力</li> <li>5. MDI による拡張電力-PD</li> <li>6. インベントリ</li> <li>7. 予約済み</li> </ol>
Application Type	エンドポイントまたはネットワーク接続機器によって広告される、この

	<p>ネットワークポリシーのために定義されたアプリケーションの主要機能を示すアプリケーションタイプ。使用可能なアプリケーションの種類を次に示します。</p> <ol style="list-style-type: none"> <li>1. 音声-専用の IP テレフォニーハンドセットおよび対話型音声サービスをサポートするその他の類似機器で使します。これらのデバイスは通常、導入を容易にし、データアプリケーションから分離することでセキュリティを強化するために、個別の VLAN に導入されます。</li> <li>2. 音声シグナリング: 音声シグナリングと音声メディアで異なるポリシーを必要とするネットワークトポロジで使します。</li> <li>3. ゲストボイス-独自の IP テレフォニーハンドセットおよび対話型音声サービスをサポートするその他の類似のアプリケーションを使用しているゲストユーザおよび訪問者に対して、個別の限定機能セット音声サービスをサポートします。</li> <li>4. ゲスト音声シグナリング: ゲスト音声シグナリングとゲスト音声メディアで異なるポリシーを必要とするネットワークトポロジで使します。</li> <li>5. Softphone Voice-PC やラップトップなど、一般的なデータ中心のデバイス上のソフトフォンアプリケーションで使します。</li> <li>6. ビデオ会議-リアルタイムの対話型ビデオ/オーディオサービスをサポートする専用のビデオ会議機器およびその他の類似機器で使します。</li> <li>7. ストリーミングビデオ-ブロードキャストまたはマルチキャストベースのビデオコンテンツ配信、および特定のネットワークポリシー処理を必要とするストリーミングビデオサービスをサポートするその他の類似アプリケーションで使します。バッファリングを用いた TCP に依存するビデオアプリケーションは、このアプリケーションタイプの使用を意図したものではない。</li> <li>8. ビデオシグナリング-ビデオメディアとは別のポリシーをビデオシグナリングに必要とするネットワークトポロジで使します。</li> </ol>
Policy	<p>ポリシーは、エンドポイント・デバイスが、そのポリシーがデバイスに必要であることを明示的に通知したいことを示します。[定義済み] または [不明] のいずれかです。</p> <p>不明: 指定されたアプリケーションの種類ネットワークポリシーは、現在不明です。</p> <p>定義済み: ネットワークポリシーが定義されています。</p>
TAG	<p>TAG は、指定されたアプリケーション・タイプがタグ付きまたはタグなし VLAN のどちらを使用しているかを示します。タグ付きまたはタグなしを指定できます。</p> <p>Untagged: デバイスはタグなしフレームフォーマットを使用しているため、IEEE 802.1 Q-2003 で定義されているタグヘッダーを含みません。</p> <p>タグ付き: デバイスは IEEE 802.1 Q タグ付きフレームフォーマットを使用しています。</p>
VLAN ID	<p>VLAN ID は、IEEE 802.1 Q-2003 で定義されているインターフェースの VLAN 識別子 (VID) です。1 から 4094 の値は、有効な VLAN ID を定義するために使用されます。0 (タグ付き優先度) の値は、デバイスが IEEE 802.1</p>

	Q-2003 で定義されたプライオリティタグ付きフレームを使用している場合に使用されます。これは、IEEE 802.1 D プライオリティレベルのみが重要であり、入力インターフェースのデフォルトの PVID が代わりに使用されることを意味します。
Priority	Priority は、指定したアプリケーションタイプに使用されるレイヤ 2 の優先順位です。八つの優先レベル(0 から 7)のいずれか。
DSCP	DSCP は、IETF RFC2474 で定義されているように、指定されたアプリケーションの種類に対して Diffserv ノードの動作を提供するために使用される DSCP 値です。64 個のコードポイント値のいずれかを含みます。(0 から 63)
Auto-negotiation	オートネゴシエーションは、リンクパートナーが MAC/PHY オートネゴシエーションをサポートしているかどうかを識別します。
Auto-negotiation status	自動ネゴシエーションステータスは、リンクパートナーで現在自動ネゴシエーションが有効になっているかどうかを示します。オートネゴシエーションがサポートされ、オートネゴシエーション・ステータスが無効になっている場合、802.3 PMD の動作モードでは、オートネゴシエーションではなく、動作中の MAU タイプのフィールド値が決定されます。
Auto-negotiation Capabilities	オートネゴシエーション機能は、リンクパートナーの MAC/PHY 機能を示します。

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は 3 秒ごとに行われます。
<input type="button" value="Refresh"/>	クリックすると、ページが更新されます。

### 3.2.21 LLDP PoE (For PoE Model Only)

Monitor > LLDP > PoE

このページは、すべての LLDP PoE 隣接機器のステータスの概要を提供します。表示されたテーブルには、LLDP PoE 隣接機器が検出された各インターフェースの行が含まれています。

#### LLDP Neighbor Power Over Ethernet Information

Auto-refresh

Local Interface	Power Type	Power Source	Power Priority	Maximum Power
No PoE neighbor information found				

オブジェクト	説明
Local Interface	LLDP フレームを受信したこのデバイスのインターフェース
Power Type	電力タイプは、デバイスが PSE または PD のどちらであることを表します。電力タイプが不明な場合は、「Reserved」と表示されます。
Power Source	電源は、PSE または PD デバイスによって使用されている電源を表します。デバイスが PSE デバイスの場合は、プライマリ電源またはバックアップ電源のいずれかで実行できます。PSE デバイスがプライマリ電源とバッ

	<p>クアッパ電源のどちらを使用しているかが不明な場合は、「Unknown」と表示されます。</p> <p>デバイスがPD デバイスの場合は、ローカル電源で動作するか、PSE を電源として使用できます。また、ローカル電源と PSE の両方を使用できます。</p> <p>PD デバイスが使用している電源が不明な場合は、「不明」と表示されま</p>
Power Priority	<p>電力優先度は、PD デバイスの優先度、または電力を供給している PSE タイプデバイスのインターフェースに関連付けられた電力優先度を表します。電力の優先順位には 3 つのレベルがあります。3 つのレベルは、Critical、High、Low です。</p> <p>電源の優先順位が不明な場合は、「不明」と表示されます。</p>
Maximum Power	<p>最大電力値は、PD デバイスが PSE デバイスから必要とする最大電力をワット単位で示す数値、または PSE デバイスが現在の構成に基づいて最大長のケーブルから供給できる最小電力を含みます。</p> <p>最大許容値は 30.0 W です。デバイスが 30.0 W を超える値を示す場合は、「予約済み」と表示されます。</p>

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は 3 秒ごとに行われます。
Refresh	クリックすると、ページが更新されます。

#### 注意事項



本装置の Power Type は PSE タイプです。LLDP PoE 隣接機器は PD になります。

#### 3.2.22 LLDP Port Statistics (For PoE Model Only)

Monitor > LLDP > PoE Statistics

このページでは、すべての LLDP トラフィックの概要について説明します。

2 種類のカウンタを示します。グローバルカウンタはデバイス全体を参照するカウンタで、ローカルカウンタは現在選択されているデバイスのインターフェースごとのカウンタを参照します。

##### LLDP Global Counters

Auto-refresh  Refresh Clear

Global Counters	
Clear global counters	<input checked="" type="checkbox"/>
Neighbor entries were last changed	2019-10-17 08:03:51+09:00 (24080 secs. ago)
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

##### LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
FastEthernet 1/1	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>

オブジェクト	説明
Global Counters グローバルカウンタ	
Clear global counters	 を押した際にクリアにする項目を選択します。
Neighbor entries were last change	最後にエントリが削除または追加された時刻が表示されます。また、最後の変更が検出されてから経過した時間も表示されます。
Total Neighbors Entries Added	デバイスの再起動後に追加された新しいエントリーの数を示します。
Total Neighbors Entries Deleted	デバイスの再起動後に削除された新しいエントリーの数を示します。
Total Neighbors Entries Dropped	エントリテーブルが最大になったためにドロップされた LLDP フレームの数を示します。
Total Neighbors Entries Aged Out	有効期限が切れたために削除されたエントリーの数を示します。
Local Counters ローカルカウンタ	
Local Interface	LLDP フレームが送受信されるインターフェース
Tx Frames	インターフェースで送信された LLDP フレームの数
Rx Frames	インターフェースで受信した LLDP フレームの数
Rx Errors	何らかのエラーを含む受信 LLDP フレームの数
Frames Discarded	インターフェースで LLDP フレームが受信され、デバイスの内部テーブルがいっぱいになった場合、LLDP フレームはカウントされ、廃棄されます。この状況は、LLDP 標準では「Too Many Neighbors」として知られています。シャーシ ID またはリモートポート ID がまだテーブルに含まれていない場合、LLDP フレームにはテーブル内に新しいエントリが必要です。特定のインターフェースのリンクがダウンしたとき、LLDP シャットダウンフレームを受信したとき、またはエントリがエージングアウトしたときに、エントリはテーブルから削除されます。
TLVs Discarded	各 LLDP フレームには、TLV (TLV は「Type Length Value」の略です。) と呼ばれる複数の情報を含めることができます。TLV が不正な場合は、カウントされて廃棄されます。
TLVs Unrecognized	未知のタイプ値を持つ、整形式 TLV の数
Org. Discarded	LLDP フレームが組織的な TLV で受信されたが、TLV がサポートされていない場合、TLV は破棄され、カウントされます。
Age-Outs	各 LLDP フレームには、LLDP 情報が有効な期間(エイジアウト時間)に関する情報が含まれています。エイジアウト時間内に新しい LLDP フレームが受信されない場合、LLDP 情報は削除され、エイジアウトカウンタが増分されます。
Clear	 ボタンを押したときにクリアされる項目を選択します。

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は 3 秒ごとに行われます。
	クリックすると、ページが更新されます。

<b>Clear</b>	対応するチェックボックスがオンになっているカウンタをクリアします。
--------------	-----------------------------------

### 3.2.23 PoE (For PoE Model Only)

Monitor > PoE

このページでは、すべての PoE ポートの現在のステータスを確認できます。

#### Power Over Ethernet Status

Auto-refresh  **Refresh**

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Port Status
1	-	30 [W]	0 [W]	0 [W]	0 [mA]	No PD detected
Total		30 [W]	0 [W]	0 [W]	0 [mA]	

オブジェクト	説明
Local Port	この行の論理ポート番号です。
PD Class	各 PD は、PD が使用する最大電力を定義するクラスに従って分類されます。「PD クラス」には、PD クラスが表示されます。 次の 5 つのクラスが定義されています。 Class 0 : 最大 15.4 W Class 1 : 最大 4.0 W Class 2 : 最大 7.0 W Class 3 : 最大 15.4 W Class 4 : 最大 30.0 W
Power Requested	PD が予約したい要求電力量が表示されます。
Power Allocated	デバイスが PD に割り当てた電力量が表示されます。
Power Used	使用電力は、PD が現在使用している電力を示します。
Current Used	使用電力は、PD が現在使用している電流を示します。
Port Status	ポートのステータスが表示されます。status には、次のいずれかの値が指定されます。 PoE turned ON - PoE ポートに電力が出力されている。 PoE not available - ポートで PoE がサポートされていない。 PoE turned OFF - PoE disabled - PoE はユーザーによって無効にされています。 No PD detected - ポートで PD が検出されませんでした。 PoE turned OFF - PD overload - PD がポートに供給できる電力を超える電力を要求または使用しており、電源が切れている。 PoE turned OFF - PD がオフになっている。 Invalid PD - PD が検出されましたが、正しく動作していません。

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は 3 秒ごとに行われます。
<b>Refresh</b>	クリックすると、ページが更新されます。

注意事項



PoE 給電異常時、または、PD 受電未対応機器と接続した場合、PoE LED は橙点灯します。

### 3.2.24 DDMI Overview

Monitor > DDMI > Overview

このページに DDMI の概要情報を表示します。

#### DDMI Overview

Auto-refresh  Refresh

Port	Vendor	Part Number	Serial Number	Revision	Date Code	Transceiver
LH	-	-	-	-	-	-

オブジェクト	説明
Port	DDMI ポート
Vendor	SFP ベンダー名を示します。
Part Number	SFP ベンダーから提供されたベンダーPN パーツ番号を示します。
Serial Number	ベンダーによって提供されたベンダーSN シリアル番号を示します。
Revision	ベンダーが提供する部品番号のベンダーリビジョンリビジョンレベルを示します。
Date Code	日付コードベンダーの製造日付コードを示します。
Transceiver	トランシーバの種類を示します。

### 3.2.25 DDMI Detailed

Monitor > DDMI > Detailed

このページに DDMI の詳細情報を表示します。

#### Transceiver Information

Port LH ▾ Auto-refresh  Refresh

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Date Code	-
Transceiver	-

#### DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	-	-	-	-	-
Voltage(V)	-	-	-	-	-
Tx Bias(mA)	-	-	-	-	-
Tx Power(dBm)	-	-	-	-	-
Rx Power(dBm)	-	-	-	-	-

オブジェクト	説明
Transceiver Information	トランシーバ情報
Vendor	SFP ベンダー名を示します。
Part Number	SFP ベンダーから提供されたベンダーPN パーツ番号を示します。
Serial Number	ベンダーによって提供されたベンダーSN シリアル番号を示します。
Revision	ベンダーが提供する部品番号のベンダーリビジョンリビジョンレベル

	を示します。
Date Code	日付コードベンダーの製造日付コードを示します。
Transceiver	トランシーバの種類を示します。
DDMI Information DDMI 情報	
Current	温度、電圧、TX バイアス、TX 電力、および RX 電力の現在値
High Alarm Threshold	温度、電圧、TX バイアス、TX 電力、および RX 電力の高アラームしきい値。
High Warn Threshold	温度、電圧、TX バイアス、TX 電力、および RX 電力の高警告しきい値
Low Warn Threshold	温度、電圧、TX バイアス、TX 電力、および RX 電力の低警告しきい値
Low Alarm Threshold	温度、電圧、TX バイアス、TX 電力、および RX 電力の低いアラームしきい値

ボタン	
Auto-refresh <input type="checkbox"/>	このチェックボックスをオンにすると、ページが自動的に更新されます。自動更新は 3 秒ごとに行われます。
Refresh	クリックすると、ページが更新されます。

#### 注意事項



ApresiaLightMC-FX(手配品名：APLMCFX)、ApresiaLightMC-FX-PoE(手配品名：APLMCFXPOE)は、光パワーモニター機能(DDMI)をサポートしていません。

### 3.3 Diagnostics

#### 3.3.1 Ping (IPv4)

##### Diagnostics > Ping (IPv4)

このページでは、ICMP(IPv4)PING パケットを発行して、IP 接続の問題をトラブルシューティングできます。

を押すと ICMP パケットが送信され、応答受信時にシーケンス番号とラウンドトリップ時間が表示されます。

ICMP ECHO\_REPLY タイプの IP パケット内で受信されたデータの量は、常に要求されたペイロードデータサイズ(違いは ICMP ヘッダー)よりも 8 バイト多くなります。

ページは、すべてのパケットへの応答が受信されるまで、またはタイムアウトが発生するまで、自動的に更新されます。

コマンドの出力は次のようになります。

## Ping (IPv4) Output

```
PING 10.250.4.4 (10.250.4.4) from 10.249.31.10: 56 data bytes
64 bytes from 10.250.4.4: seq=0 ttl=124 time=18.439 ms
64 bytes from 10.250.4.4: seq=1 ttl=124 time=12.872 ms
64 bytes from 10.250.4.4: seq=2 ttl=124 time=14.646 ms
64 bytes from 10.250.4.4: seq=3 ttl=124 time=42.163 ms
64 bytes from 10.250.4.4: seq=4 ttl=124 time=27.276 ms
```

--- 10.250.4.4 ping statistics ---

```
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 12.872/23.079/42.163 ms
```

Ping session completed.

New Ping

## Ping (IPv4)

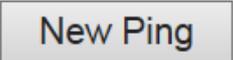
Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address	<input type="text"/>	
Payload Size	<input type="text" value="56"/>	bytes
Payload Data Pattern	<input type="text" value="0"/>	(single byte value; integer or hex with prefix '0x')
Packet Count	<input type="text" value="5"/>	packets
TTL Value	<input type="text" value="64"/>	
Source Port Number	<input type="text"/>	
IP Address for Source Interface	<input type="text"/>	
Quiet (only print result)	<input type="checkbox"/>	

Start

オブジェクト	説明
Hostname or IP Address	シンボリックホスト名または IP アドレスとしての宛先ホストのアドレス
Payload Size	ICMP データペイロードのサイズをバイト単位で決定します。(イーサネット、IP および ICMP ヘッダーのサイズを除く) デフォルト値は 56 バイトです。有効範囲は 2 ~ 1452 バイトです。
Payload Data Pattern	ICMP データペイロードで 사용되는パターンを決定します。 デフォルト値は 0 です。有効範囲は 0 ~ 255 です。
Packet Count	送信する PING 要求の数を指定します。デフォルト値は 5 です。有効範囲は 1 ~ 60 です。
TTL Value	IPv4 ヘッダーの Time-To-Live(TTL)フィールド値を決定します。デフォルト値は 64 です。有効範囲は 1 ~ 255 です。
Source Port Number	入力は不要です。
IP Address for Source Interface	入力不要です。

Quiet (only print result)	このオプションをチェックすると、各 ping 要求の結果は出力されず、最終結果のみが表示されます。
---------------------------	---

ボタン	
	クリックすると、ICMP パケットの送信が開始されます。
	クリックして診断を再起動します。

### 3.3.2 Traceroute (IPv4)

Diagnostics > Traceroute (IPv4)

このページでは、リモートホストに対して IPv4 経由の traceroute テストを実行できます。traceroute は、ルートを表示し、IPv4 ネットワーク上のパケットの通過遅延を測定する診断ツールです。

#### Traceroute (IPv4)

Fill in the parameters as needed and press "Start" to initiate the Traceroute session.

Hostname or IP Address	<input type="text"/>	
DSCP Value	<input type="text" value="0"/>	
Number of Probes Per Hop	<input type="text" value="3"/>	packets
Response Timeout	<input type="text" value="3"/>	seconds
First TTL Value	<input type="text" value="1"/>	
Max TTL Value	<input type="text" value="30"/>	
IP Address for Source Interface	<input type="text"/>	
Use ICMP instead of UDP	<input type="checkbox"/>	
Print Numeric Addresses	<input type="checkbox"/>	



オブジェクト	説明
Hostname or IP Address	宛先 IP アドレス
DSCP Value	この値は、IPv4 ヘッダーの DSCP 値に使用されます。デフォルト値は 0 です。有効範囲は 0~63 です。
Number of Probes Per Hop	ホップごとに送信されるプローブ(パケット)の数を決定します。デフォルト値は 3 です。有効範囲は 1~60 です。
Response Timeout	送信された要求に対する応答を待機する秒数を指定します。デフォルト値は 3 です。有効範囲は 1~86400 です。
First TTL Value	最初に送信されるパケットの IPv4 ヘッダーの Time-To-Live(TTL)フィールドの値を決定します。デフォルト値は 1 です。有効範囲は 1~30 です。
Max TTL Value	IPv4 ヘッダーの Time-To-Live(TTL)フィールドの最大値を指定します。指定したリモートホストに到達する前にこの値に達すると、テストは停止します。デフォルト値は 30 です。有効範囲は 1~255 です。
IP Address for	このフィールドを使用すると、指定した IP アドレスをソースインタフ

Source Interface	エースとして持つ特定のローカルインタフェースをテストで使用できます。指定した IP アドレスは、ローカルインターフェイスで構成する必要があります。ルーティング設定に基づいて自動選択する場合は、このフィールドを空のままにします。 Note:送信元インターフェイスの IP アドレスのみを指定できます。
Use ICMP instead of UDP	デフォルトでは、tracert コマンドは UDP データグラムを使用します。このオプションを選択すると、代わりに ICMP ECHO パケットが使用されます。
Print Numeric Addresses	デフォルトでは、tracert コマンドは、取得したホスト IP アドレスの逆引き DNS 検索を使用してホップ情報を出力します。DNS 情報が利用できない場合は、表示が遅くなることがあります。このオプションを選択すると、DNS の逆引き参照が行われず、tracert コマンドによって代わりに数値の IP アドレスが出力されます。

ボタン	
	tracert テストを実行するときにクリックします。

### 3.4 Maintenance

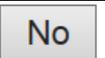
#### 3.4.1 Restart Device

Maintenance > Restart Device

このページでデバイスを再起動できます。再起動後、デバイスは正常に起動します。

#### Restart Device



ボタン	
	デバイスを再起動するときにクリックします。
	クリックすると再起動せずに、Port State ページに移動します。

#### 注意事項

-  本装置の再起動中は、USER ポート/LH ポート/MANAGE ポートの全ての通信が一時的に停止します。
-  本装置の再起動(restart Device)では、EFM-OAM の電源断通知(dying gasp フレーム)を発生しない仕様です。(1.00.05 以降)

### 3.4.2 Factory Default

Maintenance > Factory Defaults

デバイスの構成をリセットできます。

新しい構成はすぐに適用されるため、再起動は必要ありません。

#### Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Yes

No

ボタン	
Yes	クリックすると、設定が工場出荷時のデフォルトにリセットされます。
No	クリックするとリセットせずに、Port State ページに移動します。

### 3.4.3 Software Upload

Maintenance > Software > Upload

このページは、デバイスを制御するファームウェアを更新します。

ファームウェアのアップロードを行うと、現在の Active イメージが Backup イメージに退避され、新たにアップロードされたイメージが Active イメージに格納されます。

#### Software Upload

Choose File No file chosen

Upload

ボタン	
Choose File	ソフトウェアイメージの場所を選択します。
Upload	クリックすると、ファームウェアアップグレードプロセスが開始します。

ソフトウェアイメージがアップロードされると、ファームウェア更新が開始されたことを示すページが表示されます。数分後、ファームウェアが更新され、デバイスが再起動します。

警告:ファームウェアの更新中に、Web アクセスが機能しなくなります。この時点でデバイスを再起動したり電源を切ったりしないでください。ファームウェアが破損し、デバイスが機能しなくなる可能性があります。

#### 注意事項



本装置の再起動中は、USER ポート/LH ポート/MANAGE ポートの全ての通信が一時的に停止します。

❗ LHポート間で対向接続させる本装置(2台)は、同一のファームウェアバージョンでご使用ください。

❗ Ver. 1.00.05 のファームウェアではバージョンアップ後にコンフィグ設定の追加/変更が必要な機能を追加しています。十分理解されたのち、バージョンアップを実行してください。

遠隔でバージョンアップ作業を実施された場合、Ver. 1.00.05 リリースノート記載の APLMC-10005-RC004 の仕様変更により、装置にアクセスできなくなる恐れがありますので、事前に通信環境をご確認ください。

MANAGE ポート経由の IP アドレスはバージョンアップ後も引き継がれますが、USER ポートまたは LH ポート経由の IP アドレスについては引き継がれずに無効となります。

#### 3.4.4 Image select

Maintenance > Software > Image Select

このページでは、デバイスの Active(アクティブ) および Backup(バックアップ)ファームウェアイメージに関する情報を表示します。また、バックアップイメージに戻すことができます。

Web ページには、アクティブなファームウェアイメージとバックアップファームウェアイメージに関する情報を示す 2 つのテーブルが表示されます。

Note:

1. アクティブなファームウェアイメージが Backup イメージの場合は、「Active Image」テーブルだけが表示されます。この場合、[Active Backup Image] ボタンも無効になります。
2. Backup イメージがアクティブな場合(Active イメージの破損の場合など)、新しいファームウェアイメージをデバイスにアップロードすると、Active イメージスロットが自動的に使用され、これがアクティブになります。

### Software Image Selection

Active Image	
Image	APLMC_1.00.05.img
Version	1.00.05
Date	2021-08-03 20:49:15+08:00

Backup Image	
Image	APLMC_1.00.05.img
Version	1.00.05
Date	2021-08-03 20:49:15+08:00

Activate Backup Image Cancel

オブジェクト	説明
Image	イメージが最後に更新されたときからのファームウェアイメージのファイル名

Version	ファームウェアイメージのバージョン
Data	ファームウェアが作成された日付

ボタン	
	代替イメージを使用する場合にクリックします。このボタンは、システムの状態によって無効になる場合があります。
	バックアップイメージのアクティブ化をキャンセルします。このページから移動します。

#### 注意事項

-  本装置の再起動中は、USER ポート/LH ポート/MANAGE ポートの全ての通信が一時的に停止します。
-  LH ポート間で対向接続させる本装置(2台)は、同一のファームウェアバージョンでご使用ください。
-  Ver. 1.00.05 のファームウェアではバージョンアップ後にコンフィグ設定の追加/変更が必要な機能を追加しています。十分理解されたのち、バージョンアップを実行してください。

遠隔でバージョンアップ作業を実施された場合、Ver. 1.00.05 リリースノート記載の APLMC-10005-RC004 の仕様変更により、装置にアクセスできなくなる恐れがありますので、事前に通信環境をご確認ください。

MANAGE ポート経由の IP アドレスはバージョンアップ後も引き継がれますが、USER ポートまたは LH ポート経由の IP アドレスについては引き継がれずに無効となります。

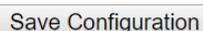
#### 3.4.5 Save Configuration

Maintenance > Configuration > Save startup-config

これにより、running-config が startup-config にコピーされ、次回のリブート時に現在アクティブな設定が使用されます。

##### Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.



#### 3.4.6 Download Configuration

Maintenance > Configuration > Download

デバイス上の任意のファイルを Web ブラウザにダウンロードできます。

ファイルを選択し、 をクリックします。この操作は、ファイルをダウンロードする準備が必要なため、完了までに少し時間がかかる場合があります。

## Download Configuration

Select configuration file to save.

Please note: running-config may take a while to prepare for download.

File Name
<input type="radio"/> running-config
<input type="radio"/> .ca
<input type="radio"/> default-config
<input type="radio"/> shiftTime
<input type="radio"/> history_cmd_log
<input type="radio"/> startup-config

Download Configuration

### 3.4.7 Upload Configuration

Maintenance > Configuration > Upload

Web ブラウザからデバイス上のすべてのファイルにファイルをアップロードできます。ただし、default-config は読み取り専用です。

アップロードするファイルを選択し、ターゲット上のデスティネーション・ファイルを選択して、**Upload Configuration** をクリックします。

宛先が running-config の場合、ファイルはデバイス設定に適用されます。これには 2 つの方法があります。

置き換えモード:現在のコンフィギュレーションは、アップロードされたファイル内のコンフィギュレーションに完全に置き換えられます。

マージモード:アップロードされたファイルは running-config にマージされます。

フラッシュ・ファイル・システムの容量が十分でない場合、新しいファイルを作成できません。代わりに、既存のファイルを上書きするか、別のファイルを削除する必要があります。

## Upload Configuration

### File To Upload

Choose File No file chosen

### Destination File

File Name	Parameters
<input type="radio"/> running-config	<input checked="" type="radio"/> Replace <input type="radio"/> Merge
<input type="radio"/> .ca	
<input type="radio"/> shiftTime	
<input type="radio"/> history_cmd_log	
<input type="radio"/> startup-config	
<input type="radio"/> Create new file	

Upload Configuration

### 3.4.8 Activate Configuration

Maintenance > Configuration > Activate

現在アクティブな設定を表す running-config を除いて、デバイスに存在する設定ファイルをアクティブにすることができます。

アクティブ化するファイルを選択し、**Activate Configuration** をクリックします。これにより、既存の構成を選択したファイルの構成に完全に置き換えるプロセスが開始され、デバイスが再起動します。

**警告:** アクティブ切替中に、Web アクセスが機能しなくなります。この時点でデバイスを再起動したり電源を切ったりしないでください。ファームウェアが破損し、デバイスが機能しなくなる可能性があります。

#### Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

File Name
<input type="radio"/> .ca
<input type="radio"/> default-config
<input type="radio"/> shiftTime
<input type="radio"/> history_cmd_log
<input type="radio"/> startup-config

Activate Configuration

#### 注意事項

**!** 本装置の再起動中は、USER ポート/LH ポート/MANAGE ポートの全ての通信が一時的に停止します。

### 3.4.9 Delete Configuration

Maintenance > Configuration > Delete

startup-config など、フラッシュに保存されている書き込み可能なファイルはすべて削除できます。この操作を実行した後、セーブ・オペレーションを実行せずにデバイスを再起動すると、デバイスはデフォルトの構成にリセットされます。

#### Delete Configuration File

Select configuration file to delete.

File Name
<input type="radio"/> .ca
<input type="radio"/> shiftTime
<input type="radio"/> history_cmd_log
<input type="radio"/> startup-config

Delete Configuration File

## 注意事項

 電源を再投入する場合、電源切断後 5 秒以上間隔を空けて電源を入れてください。

#### 4. 使用上の注意事項

- (1) コンソールポートには、パラメータ設定時のみに RS-232C ケーブルを接続し、通常の運用時には接続しないでください。

## 5. トラブルシューティング

### 5.1 表示 LED に関連する現象と対策

現象	対策
「PWR」 LED が点灯しない。	電源コードが本装置の AC インレットと電源コンセントに正常に接続されていることを確認してください。
ツイストペアケーブルを接続しても「LINK/ACT」 LED が点灯しない。	ケーブルに異常がないかどうか確認してください。
	接続相手の端末が正常に動作しているかどうか確認してください。
	モジュラプラグ(RJ-45)の接続に異常がないかどうか確認してください。
	接続相手が NIC またはハブのカスケードポートである場合、ケーブルがストレートケーブルであることを確認してください。また、接続相手がハブの MDI-X ポートの場合、ケーブルがクロスケーブルであることを確認してください。
	SFP モジュールが正しく挿入されていることを確認してください。

### 5.2 コンソール端末に関連する現象と対策

現象	対策
電源投入しても Login プロンプトが出力されない。	コンソール端末の通信条件が正しいことを確認してください。通信条件は、ボーレート(9600bps)、データ(8bit)、ストップ(1bit)、パリティ(none)、フロー制御(none)、RS, ER は常時(ON)です。
	「CONSOLE」とコンソール端末との RS-232C 接続ケーブルが正しいことを確認してください。
	「CONSOLE」への接続が正常かどうか確認してください。
	「POWER」 LED が点灯していることを確認してください。
設定値が正常に入力されていない。	正常な文字数であれば、内部のメモリーに異常が発生していると考えられます。サポート対応窓口にお問い合わせください。

### 5.3 HTTPS に関連する現象と対策

現象	対策
端末から HTTPS によりログインすることができない。	本装置の IP アドレス、ネットマスク、デフォルトルートの設定が正常であることを確認してください。また設定後にリセットもしくは電源再投入がされていることも確認してください。
	接続しているポートの通信設定が ENABLE 状態になっていることを確認してください。ENABLE 状態ならば、ツイストペアケーブルの接続を確認してください。
	HTTPS アクセスしようとするアドレスが本装置のアドレスであることを確認してください。
	本装置が正常に起動し、動作していることを確認してください。

### 5.4 メディアコンバーター機能に関連する現象と対策

現象	対策
端末から別の端末にデータの中継ができない。	各端末が別々のポート VLAN グループに所属していないかどうか確認してください。
	各端末と本装置間のツイストペアケーブルの接続が正常であることを確認してください。
	各端末の接続されているポートが ENABLE 状態であるかどうか確認してください。
パケットロスが発生する。	特定のポートから出力されるフレームの負荷が 100% を超えていないかどうか確認してください。(特定のポートに 100% を超える負荷が集中した場合、別ポートにも影響を及ぼし、パケットロスが発生する場合があります。)

### 5.5 SFP に関連する現象と対策

現象	対策
SFP を認識している状態で通信しない。	SFP を認識している状態で通信しない場合は、SFP が不完全装着になっている可能性があります。SFP を再度装着し直してください。現象が再発する場合は SFP 又は装置の異常が考えられます。

### 5.6 PoE に関連する現象と対策

現象	対策
端末へ給電されない	給電の Status が Enable になっているかを確認してください。
	ツイストペアケーブルに異常がないかどうか確認してください。
	モジュラープラグ(RJ-45)の接続に異常がないかどうか確認してください。
	端末の給電クラスと合致しているかを確認してください。
	スイッチの給電制限を超えていないかを確認してください。

## 6. 準拠規格

No.	項目	準拠規格
1	LAN インターフェース	IEEE802.3 : 10BASE-T IEEE802.3u : 100BASE-TX, 100BASE-FX IEEE802.3z : 1000BASE-X IEEE802.3ab : 1000BASE-T IEEE802.3u : Auto-Negotiation IEEE802.3at : PoE Plus (For PoE Model Only)
2	コンソールインターフェース	ITU-T 勧告 V.24/V.28
3	ネットワーク管理 プロトコル	RFC1157 : Simple Network Management Protocol (SNMP) RFC1901 : Introduction to Community-based SNMPv2 RFC1905 : Protocol Operations for Version 2 of the SNMP RFC1908 : Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework RFC2570 : Introduction to Version 3 of the Internet-standard Network Management Framework RFC2575 : View-based Access Control Model (VACM) for SNMP IEEE802.3ah : Ethernet OAM (Ethernet in the first mile) IEEE802.1ab : LLDP (For PoE Model Only)
4	ネットワーク管理対象	RFC1213 : Internet 標準 MIB RFC1493 : Bridge MIB (IEEE8021-BRIDGE-MIB) RFC1757 : RMON 1, 2, 3, 9 RFC2674 : Q-Bridge MIB (IEEE8021-Q-BRIDGE-MIB) RFC2819 : RMON MIB (STATISTICS, HISTORY, ALARM, EVENT) RFC2233 : ifMIB IEEE802.3ah : DOT3-OAM-MIB ベンダー独自 MIB
5	通信プロトコル	RFC793 : TCP(Transmission Control Protocol) RFC768 : UDP(User Datagram Protocol) RFC1350 : THE TFTP PROTOCOL (REVISION 2) RFC783 : TFTP Client RFC791 : IP(Internet Protocol) RFC792 : ICMP(Internet Control Message Protocol) RFC826 : ARP(Address Resolution Protocol) RFC854 : TELNET RFC954 : FTP Client RFC1305 : NTP(Network Time Protocol version) RFC3164 : SYSLOG RFC951/RFC1541 : BootP/DHCP Client
6	セキュリティープロトコル	RFC4250 : The Secure Shell(SSh) Protocol Assigned Numbers RFC4251 : The Secure Shell(SSh) Protocol Architecture RFC4252 : The Secure Shell(SSh) Authentication Protocol RFC4253 : The Secure Shell(SSh) Transport Layer Protocol

No.	項目	準拠規格
		RFC4254 : The Secure Shell (SSH) Connection Protocol RFC4256 : Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)

ApresiaLightMC(-PoE)シリーズ

Ver.1.00 SW マニュアル

Copyright(c) 2020 APRESIA Systems, Ltd.

2020年5月 初版

2021年8月 第5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8階)

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