

ApresiaLightGM シリーズ

Ver. 1.14

SW マニュアル

APRESIA Systems 株式会社

制定・改訂履歴表

No.	年 月 日	内 容
-	2020年7月15日	Ver.1.13 SW マニュアル(TD61-7159B)より新規作成

はじめに

本書には、スイッチングハブの 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	品名	型式
ApresiaLightGM シリーズ	ApresiaLightGM110GT-SS	APLGM110GTSS
	ApresiaLightGM118GT-SS	APLGM118GTSS
	ApresiaLightGM124GT-SS	APLGM124GTSS
	ApresiaLightGM110GT-PoE	APLGM110GTPOE
	ApresiaLightGM118GT-PoE	APLGM118GTPOE
	ApresiaLightGM124GT-PoE	APLGM124GTPOE
	ApresiaLightGM110GT-PoE2	APLGM110GTPOE2
	ApresiaLightGM118GT-PoE2	APLGM118GTPOE2
	ApresiaLightGM124GT-PoE2	APLGM124GTPOE2



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



ApresiaLightGM シリーズで使用されるファームウェアは、同シリーズの機器用に作成されたものです。上記の機種一覧表に記載した型式以外の機器 (ApresiaLightFM シリーズや ApresiaLightGM152GT など) にインストールすることはできません。また、ApresiaLightGM シリーズの機器に、同シリーズ製品以外の機器用のファームウェア (ApresiaLightFM シリーズや ApresiaLightGM152GT 用のファームウェアなど) をインストールすることはできません。

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全てのソフトウェア(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 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/イーサネットは、富士ゼロックス株式会社の登録商標です。

その他ブランド名は、各所有者の商標もしくは登録商標です。

目次

1. パラメーター設定手順	10
1.1 初期 IP アドレス設定	10
1.2 パラメーター設定手順	11
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 概要	17
2.2.1 ログイン	17
2.2.2 GUI の画面説明	18
3. コマンドの詳細	19
3.1 Device Information	19
3.2 Configuration	20
3.2.1 System Information	20
3.2.2 Serial Port Settings	20
3.2.3 IP Address Settings	21
3.2.4 IPv6 Interface Settings	23
3.2.5 IPv6 Route Settings	24
3.2.6 IPv6 Neighbor Settings	25
3.2.7 Port Configuration	26
3.2.7.1 Port Settings	26
3.2.7.2 Port Description Settings	28
3.2.7.3 Port Error Disabled	29
3.2.7.4 Port Media Type	30
3.2.7.5 Port Green Mode Settings	31
3.2.8 Static ARP Settings	32
3.2.9 User Accounts	33
3.2.10 System Log Configuration	34
3.2.10.1 System Log Settings	34
3.2.10.2 System Log Server	34
3.2.11 DHCP Snooping	36
3.2.11.1 DHCP Snooping Settings	36
3.2.11.2 DHCP Snooping Ports Settings	37
3.2.11.3 DHCP Snooping Entry Settings	38
3.2.11.4 DHCP Snooping Static Entry Settings	38
3.2.12 MAC Address Aging Time	39
3.2.13 Web Settings	39
3.2.14 Telnet Settings	40
3.2.15 CLI Paging Settings	40
3.2.16 Firmware Information	41

3.2.17	SNTP Settings	42
3.2.17.1	Time Settings	42
3.2.17.2	TimeZone Settings	43
3.2.18	SMTP Settings	45
3.2.18.1	SMTP Service Settings	45
3.2.18.2	SMTP Service	46
3.2.19	SNMP Settings	47
3.2.19.1	SNMP View Table	48
3.2.19.2	SNMP Group Table	49
3.2.19.3	SNMP User Table	50
3.2.19.4	SNMP Community Table	51
3.2.19.5	SNMP Host Table	52
3.2.19.6	SNMP Engine ID	52
3.2.19.7	SNMP Trap Configuration	53
3.2.19.8	RMON	54
3.2.20	Command Logging Settings	55
3.2.21	Port LED Testing	56
3.2.22	PoE	57
3.2.22.1	PoE System Settings	57
3.2.22.2	PoE Port Settings	59
3.2.23	SFP Auto Recognition Settings	61
3.3	L2 Features	62
3.3.1	Jumbo Frame	69
3.3.2	802.1Q Static VLAN	69
3.3.3	QinQ	72
3.3.3.1	QinQ Settings	72
3.3.3.2	VLAN Translation CVID Entry Settings	73
3.3.4	802.1v Protocol VLAN	74
3.3.4.1	802.1v Protocol Group Settings	74
3.3.4.2	802.1v Protocol VLAN Settings	75
3.3.5	GVRP Settings	76
3.3.6	Asymmetric VLAN Settings	77
3.3.7	MAC-based VLAN Settings	77
3.3.8	PVID Auto Assign Settings	78
3.3.9	Link Aggregation	79
3.3.9.1	Link Aggregation Settings	80
3.3.9.2	Link Aggregation Settings	81
3.3.10	Traffic Segmentation	82
3.3.11	BPDU Guard Settings	83
3.3.12	IGMP Snooping	84
3.3.12.1	IGMP Snooping Settings	84
3.3.13	MLD Snooping Settings	87

3.3.14	Port Mirror	91
3.3.15	Loopback Detection Settings	92
3.3.16	Spanning Tree	94
3.3.16.1	STP Bridge Global Settings	96
3.3.16.2	STP Port Settings	98
3.3.16.3	MST Configuration Identification	100
3.3.16.4	STP Instance Settings	101
3.3.16.5	MSTP Port Information	101
3.3.17	Forwarding & Filtering	102
3.3.17.1	Unicast Forwarding Settings	102
3.3.17.2	Multicast Forwarding Settings	103
3.3.17.3	Multicast Filtering Mode	104
3.3.18	LLDP	105
3.3.18.1	LLDP Global Settings	105
3.3.18.2	LLDP Port Settings	106
3.3.18.3	LLDP Basic TLVs Settings	107
3.3.18.4	LLDP Dot1 TLVs Settings	108
3.3.18.5	LLDP Dot3 TLVs Settings	109
3.4	サービス品質 (QoS)	110
3.4.1	Bandwidth Control	111
3.4.2	Traffic Control	112
3.4.3	802.1p Default Priority	115
3.4.4	802.1p User Priority	115
3.4.5	QoS Scheduling Settings	116
3.4.6	Priority Mapping	117
3.4.7	TOS Mapping	117
3.4.8	DSCP Mapping	118
3.5	Security	119
3.5.1	Trusted Host	119
3.5.2	Port Security	120
3.5.2.1	Port Security Port Settings	120
3.5.2.2	Port Security FDB Entries	121
3.5.3	Authentication Setting	122
3.5.4	802.1X	123
3.5.4.1	802.1X Settings	123
3.5.4.2	802.1X User	126
3.5.4.3	Authentication RADIUS Server	127
3.5.4.4	Initialize Port(s)	128
3.5.4.5	Reauthenticate Port(s)	129
3.5.5	SSL Settings	130
3.5.6	SSH	133
3.5.6.1	SSH Settings	133

3.5.6.2	SSH Authmode and Algorithm Settings	135
3.5.6.3	SSH User Authentication Lists	136
3.5.7	Access Authentication Control	137
3.5.7.1	Authentication Policy Settings	138
3.5.7.2	Application Authentication Settings	139
3.5.7.3	Authentication Server Group	140
3.5.7.4	Authentication Server	141
3.5.7.5	Login Method Lists	142
3.5.7.6	Enable Method Lists	143
3.5.7.7	Local Enable Password Settings	144
3.5.8	MAC-based Access Control	145
3.5.8.1	MAC-based Access Control Settings	146
3.5.8.2	MAC-based Access Control Local Settings	148
3.5.9	Web Authentication	149
3.5.9.1	Web Authentication Settings	149
3.5.9.2	Web Authentication User Settings	151
3.5.9.3	Web Authentication Port Settings	152
3.5.9.4	Web Authentication Customize	153
3.6	アクセス制御一覧(ACL)	156
3.6.1	ACL Configuration Wizard	156
3.6.2	Access Profile List	157
3.6.3	ACL Finder	172
3.6.4	ACL Flow Meter	172
3.7	Monitoring	174
3.7.1	Cable Diagnostics	174
3.7.2	SFP	175
3.7.2.1	SFP General Information	175
3.7.2.2	SFP Diagnostic Monitoring	175
3.7.3	Utilization Notify	176
3.7.3.1	CPU Utilization Notify	176
3.7.3.2	CPU Utilization	176
3.7.3.3	DRAM Utilization Notify	177
3.7.3.4	DRAM & FLASH Utilization	178
3.7.3.5	Port Utilization	178
3.7.4	Packet Size	179
3.7.5	Packets	180
3.7.6	Errors	181
3.7.6.1	Received (RX)	181
3.7.6.2	Transmitted (TX)	182
3.7.7	Port Access Control	183
3.7.7.1	RADIUS Authentication	183
3.7.7.2	RADIUS Account Client	184
3.7.7.3	Authenticator State	186

3.7.7.4 Authenticator Statistics	187
3.7.7.5 Authenticator Session Statistics	188
3.7.7.6 Authenticator Diagnostics	190
3.7.8 Peripheral	192
3.7.8.1 Device Environment	192
3.7.9 Browse ARP Table	193
3.7.10 Browse VLAN	193
3.7.11 IGMP Snooping	194
3.7.11.1 Browse IGMP Router Port	194
3.7.11.2 IGMP Snooping Group	194
3.7.11.3 IGMP Snooping Host	195
3.7.12 MLD Snooping	195
3.7.12.1 Browse MLD Router Port	195
3.7.12.2 MLD Snooping Group	196
3.7.13 LLDP	196
3.7.13.1 LLDP Statistics System	196
3.7.13.2 LLDP Local Port Information	197
3.7.13.3 LLDP Remote Port Information	198
3.7.14 MBA Authentication State	198
3.7.15 Web Authentication State	199
3.7.16 Browse Session Table	199
3.7.17 MAC Address Table	200
3.7.18 System Log	201
3.7.19 Self-Test	201
3.7.20 PD Monitoring	202
3.7.20.1 PD Monitoring Global Settings	202
3.7.20.2 PD Monitoring Port Settings	203
3.7.20.3 PD Monitoring Port ICMP Settings	204
3.8 セーブ	205
3.8.1 Save Configuration	205
3.8.2 Save Log	205
3.8.3 Save All	205
3.8.4 Show Technical Support	206
3.9 ツール	207
3.9.1 Configuration File Upload & Download	207
3.9.2 Upload Log File	208
3.9.3 Upload Technical Support	208
3.9.4 Reset	209
3.9.5 Ping Test	209
3.9.6 Download Firmware	210
3.9.7 Reboot System	211
4. 使用上の注意事項	212

5. トラブルシューティング	213
5.1 表示 LED に関連する現象と対策	213
5.2 コンソール端末に関連する現象と対策	213
5.3 HTTP に関連する現象と対策	214
5.4 スイッチングハブ機能に関連する現象と対策	214
5.5 VLAN に関連する現象と対策	214
5.6 SFP に関連する現象と対策	214
5.7 PoE に関連する現象と対策	215
5.8 内蔵冷却ファンに関連する現象と対策	215
6. 準拠規格	216

1. パラメーター設定手順

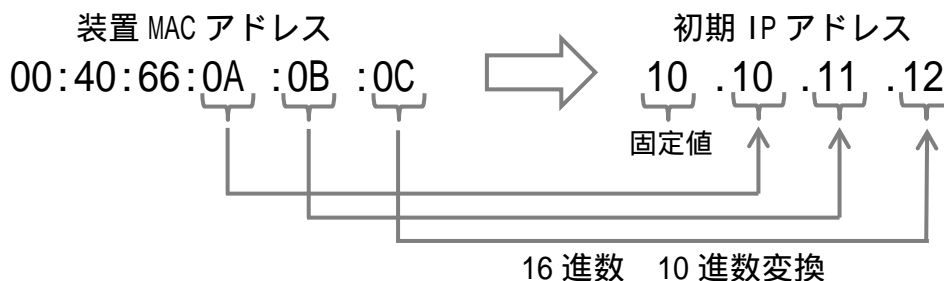
パラメーターの設定は、設定端末の準備、設定端末の接続、パラメーターの設定手順で行います。
Web ベース GUI 方式によるコマンド詳細については 3 章を参照してください。
なお、コマンドライン方式については別紙 (CLI マニュアル) を参照してください。

1.1 初期 IP アドレス設定

Ver.1.08.00 以降のファームウェアでは、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。

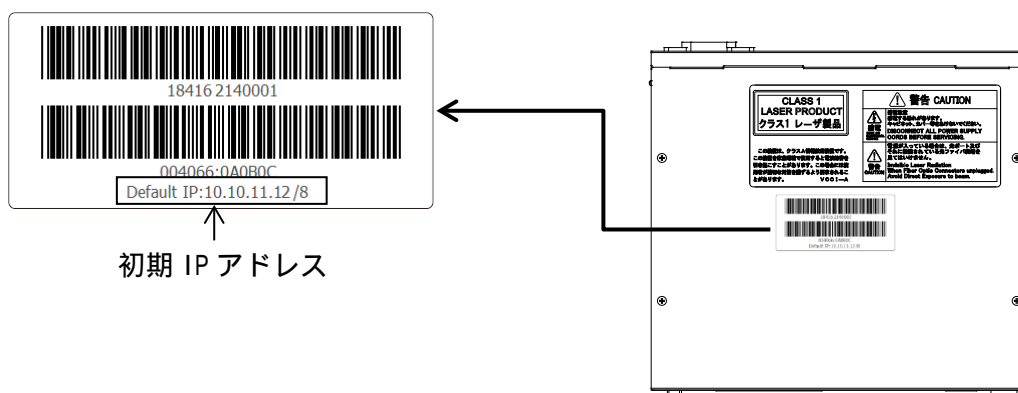


(2) サブネットマスク

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

Ver.1.02 以降のバージョンで出荷された製品では、初期 IP アドレスが装置トップパネルのバーコードラベル上に表記されます。それ以前のバージョンで出荷された製品では初期 IP アドレスの記載がありませんが、バーコードラベル上の MAC アドレス表示あるいは UI 上の MAC アドレス表示を元に、(1)の初期 IP アドレスの設定ルールに従って算出することができます。



注意事項

! 工場出荷時の初期 IP アドレスは、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(1.1 節参照)

パラメーター設定端末の接続(1.1 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。

以下のように表示されたら、何かキーを押して下さい。
表示されない場合、Ctrl+R を押し、コンソール画面を
更新してください。

<表示例>

Press any key to login...

パラメーター設定端末の表示画面の確認

以下のように表示されていることを確認してください。
表示されない場合、Ctrl+R を押し、コンソール画面を
更新してください。

<表示例>

ApresiaLightGM110GT-SS Gigabit Ethernet Switch
Command Line Interface

Firmware: 1.14.00

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

UserName:

システムログイン

login 名 : adpro によりシステムにログインします。初
回立ち上げ時にはパスワードは設定されていませんの
で、そのままリターンを押してログインしてください。

UserName:adpro

PassWord:

#

IP アドレスの設定

例として、IP アドレス 10.0.0.1/24 を設定する場合を以下に示します。

```
#config ipif System ipaddress 10.0.0.1/24  
Command: config ipif System ipaddress 10.0.0.1/24
```

Success.

#

本装置からログアウト

```
#logout
```

Press any key to login...

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。

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

例)http://10.0.0.1

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(2.2.1 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、表 1-2 に記載します。

表 1-1 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 (VT100 互換)

表 1-2 通信条件

項番	項目	仕様
1	キャラクター	8bit/キャラクター
2	ストップビット	1bit
3	パリティ	なし
4	フロー制御	なし
5	ボーレート	9600bps
6	端末接続ケーブル	RS-232C ケーブル(ストレート)、 ただし、本装置側は DB-9 オス型コネクターを使用のこと

1.4 パラメーター設定端末の接続

パラメーター設定端末と本装置のコンソールポートを標準添付されている専用コンソールケーブル(ストレート)を用いて接続します。

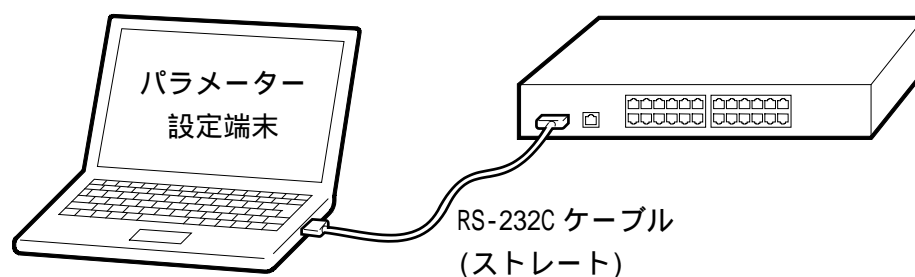


図 1-1 RS-232C ケーブルの接続

表 1-3 に本装置のコンソールポートのピン仕様を記載します。コンソールポートは RS-232C(DTE メス)インターフェース接続となります。

表 1-3 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	-	-	-
2	SD	送信データ	出力
3	RD	受信データ	入力
4	-	-	-
5	SG	回路アース	-
6	-	-	-
7	-	-	-
8	-	-	-
9	-	-	-

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。

RS-232C ケーブルのピン配置を表 1-4 に記載します。

表 1-4 RS-232C ケーブル接続結線例 (D-SUB9 ピン-9 ピンの場合)

本装置側コネクタ 9 ピン D-SUB(オス)	接続	パラメータ設定用端末 コネクタ 9 ピン D-SUB
ピン番号		ピン番号
1	—————	1
2	—————	2
3	—————	3
4	—————	4
5	—————	5
6	—————	6
7	—————	7
8	—————	8
9	—————	9

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： [Apply]をクリックして変更を適用します。 これは、Apply と表記されたボタンを意味します。
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各メニューの構成を示します。 表示例： Device > Port > Port Properties これは、[Device]メニューの下にある[Port]オプションの下に[Port Properties]メニューがあることを意味します。

2.2 概要

Web ブラウザーを使用して、遠隔から HTTP プロトコルでスイッチにアクセスします。Web ベース GUI 方式は、GUI 画面で設定を行います。

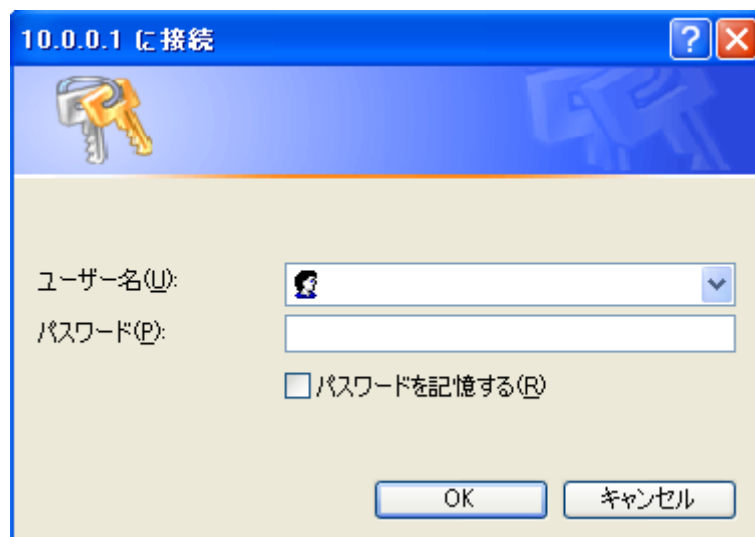
注意事項

- ❗ Web 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 ブラウザーの設定を適切に行う必要があります。
- ❗ HTTPS の Web ベース GUI を使用すると、HTTP の場合よりも 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ー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。
- ❗ Ver.1.12 以前のバージョンでは、動的な GUI 表示を実現するために Java を使用しています。HTTPS の Web ベース GUI では、Web ブラウザーの種類やバージョン、あるいは Java のバージョンによっては、GUI 画面にアクセスできないことや、GUI 上で Java アプレットが正常に動作しないことがあります。

2.2.1 ログイン

スイッチにアクセスするには、ブラウザのアドレスバーに `http://(スイッチの IP アドレス)` を入力します。IP アドレスが設定されていない場合や IP アドレスが不明な場合は、「パラメーター設定手順」などを参考にして、コマンドラインインターフェースから IP アドレスの設定や確認を行ってください。

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。


2.2.2 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	表示するフォルダーまたはウィンドウを選択します。フォルダーアイコンを開いて、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ーを表示します。
領域 2	スイッチの起動時間や各種ステータス等の重要な情報を表示します。また、設定の保存やログアウト等の操作もこの領域で行います。 中央にあるフロントパネルのグラフィック画像では、スイッチのステータスやポート状態などを表示します。 左の APRESIA ロゴをクリックすると APRESIA ウェブサイトへ移動します。
領域 3	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スイッチ設定を変更した場合は、[Save Configuration](メニュー > Save Configuration)または、コマンドラインインターフェース(CLI)コマンド save config で設定を保存して下さい。

3. コマンドの詳細

注意事項

! 本ファームウェア (Ver. 1.14) 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 Device Information

このウィンドウには、スイッチ上の主要機能の主な設定が含まれます。このウィンドウはログオンすると自動的に表示されます。[Device Information]に戻るには、[機種名]をクリックします。

[Device Information]には、スイッチの MAC アドレス (工場出荷時に割り当てられており、変更できません)、ブート PROM バージョン、ファームウェアバージョン、ハードウェアバージョン、および、スイッチ上の異なる設定に関するその他の情報が表示されます。

この情報は、ファームウェアの更新の際に役に立ちます。また、必要に応じて、スイッチの MAC アドレスを取得して、他のネットワークデバイスのアドレステーブルに入力することも可能です。さらに、このウィンドウにはスイッチ上の機能の状態が表示されるので、現在のグローバルステータスに迅速にアクセスできます。

機能によっては、設定ウィンドウにハイパーリンクされているので、[Device Information]から容易にアクセスできます。

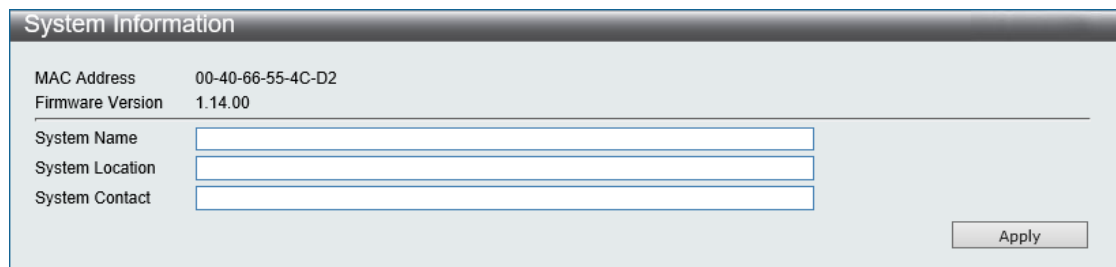
Device Information			
Device Information			
Device Type	APLGM118GTSS	MAC Address	00-40-66-55-4C-D2
System Name		IP Address	10.85.76.210 (Manual)
System Location		Mask	255.0.0.0
System Contact		Gateway	0.0.0.0
Boot PROM Version	1.00.01	Management VLAN	default
Firmware Version	1.14.00	Login Timeout (Minutes)	10 mins
System Time	00 Days 00:46:02	Dual Image	Supported
Device Status and Quick Configurations			
SNTP	Disabled	Jumbo Frame	Enabled
Spanning Tree	Disabled	MLD Snooping	Disabled
RMON	Disabled	IGMP Snooping	Disabled
CLI Paging	Enabled	802.1X	Disabled
Syslog Global State	Disabled	SSH	Disabled
SSL	Disabled	Port Mirror	Disabled
GVRP	Disabled	Web	Enabled (TCP 80)
Telnet	Enabled (TCP 23)		

3.2 Configuration

3.2.1 System Information

このウィンドウには MAC アドレス、ファームウェアバージョンなどのシステム情報が表示されます。システム名、設置場所、連絡先を入力して、目的に合わせてスイッチを定義します。

次のウィンドウを表示するには、Configuration > System Information をクリックします：



下記にパラメーターの説明を記載します。

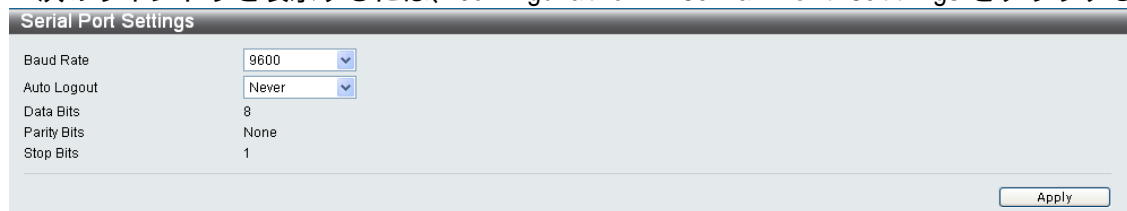
パラメーター	説明
System Name	スイッチのシステム名を入力します(最大 128 文字)。
System Location	スイッチの場所を入力します(最大 128 文字)。
System Contact	スイッチの連絡先名を入力します(最大 128 文字)。

[Apply] をクリックして変更を適用します。

3.2.2 Serial Port Settings

次のウィンドウで、シリアルポート設定を変更します。

次のウィンドウを表示するには、Configuration > Serial Port Settings をクリックします：



下記にパラメーターの説明を記載します。

パラメーター	説明
Baud Rate	このフィールドで、スイッチ上のシリアルポートのボーレートを指定します。9600/19200/38400/115200bps の 4 つのボーレートから選択できます。
Auto Logout	コンソールインターフェースで使用するログアウト時間を選択します。定義したアイドル時間が経過すると、ユーザーを自動的にログアウトします。設定は、2 分/5 分/10 分/15 分/Never から選択します。デフォルト設定は 10 分です。Never を選択した場合は、ログアウトしません。

[Apply] をクリックして変更を適用します。

注意事項



シリアルポートのボーレート設定は、直ちに有効になります。

3.2.3 IP Address Settings

イーサネット経由でスイッチを接続する前に、コンソールインターフェースを使用して IP アドレスを設定してください。このウィンドウでは設定した IP アドレスを変更することができます。

次のウィンドウを表示するには、Configuration > IP Address Settings をクリックします：

The screenshot shows the 'IP Address Settings' configuration window. At the top, there are three radio buttons: 'Static' (selected), 'DHCP', and 'BOOTP'. Below these are several configuration fields: 'IP Interface' (dropdown menu showing 'System'), 'Management VLAN Name' (text box with 'default'), 'Interface Admin State' (dropdown menu with 'Enabled'), 'IPv4 Address' (four input boxes with values 10, 90, 90, 90), 'Subnet Mask' (four input boxes with values 255, 0, 0, 0), and 'Gateway' (four input boxes with values 0, 0, 0, 0). An 'Apply' button is located at the bottom right.

スイッチの IP アドレス、サブネットマスク、および、デフォルトゲートウェイアドレスを手動で割り当てるには以下の手順に従ってください。

- (1) ウィンドウの一番上にある [Static] をクリックします。
- (2) IPv4 アドレスとサブネットマスクを入力します。
- (3) インストールしたサブネット以外のサブネットからスイッチにアクセスする場合は、ゲートウェイの IP アドレスを入力します。インストールしたサブネットからスイッチを管理する場合は、このフィールドはデフォルトアドレス (0.0.0.0) のままにします。

スイッチ上で事前に VLAN を設定していない場合は、管理 VLAN 名に default を使用します。default VLAN には、すべてのスイッチポートがメンバーとして含まれます。

ポートを有効にしたい場合は、Interface Admin State プルダウンメニューから [Enable] を選択します。

DHCP プロトコルまたは BOOTP プロトコルを使用してスイッチに IP アドレス、サブネットマスク、デフォルトゲートウェイアドレスを割り当てるには、[DHCP] または [BOOTP] を選択します。

下記にパラメーターの説明を記載します。

パラメーター	説明
Static	スイッチの IPv4 アドレス、サブネットマスク、デフォルトゲートウェイを入力します。これらのフィールドには、xxx.xxx.xxx.xxx の形式で入力します。xxx はそれぞれ 0~255 の数字です(10 進数で示します)。
DHCP	スイッチの電源を入れると、スイッチは DHCP ブロードキャスト要求を送信します。DHCP プロトコルで、IP アドレス、ネットワークマスク、デフォルトゲートウェイを DHCP サーバーにより割り当てることができます。このオプションに設定すると、スイッチは、デフォルト設定、または、事前に入力した設定を使用する前に、この情報を提供する DHCP サーバーを検索します。
BOOTP	スイッチの電源を入れると、スイッチは BOOTP ブロードキャスト要求を送信します。BOOTP プロトコルで、IP アドレス、ネットワークマスク、デフォルトゲートウェイを BOOTP サーバーによって割り当てることができます。このオプションに設定すると、スイッチは、デフォルト設定、または、前に入力した設定を使用する前に、この情報を提供する BOOTP サーバーを検索します。
IP Interface	IP インターフェース名です。本装置では System 固定になります。
Management VLAN Name	管理ステーションが TCP/IP(HTTP または Telnet 経由)を使用してスイッチを管理できる VLAN 名を入力します。デフォルトで VLAN 名「default」が設定され、すべてのポートに属しています。
Interface Admin State	有効(Enabled)と無効(Disabled)を切り替えます。IP アドレスを設定する場合は、有効(Enabled)に設定します。
IPv4 Address	スイッチの IPv4 アドレスを設定します。
Subnet Mask	スイッチがあるサブネットの拡張を定めるビットマスクです。xxx.xxx.xxx.xxx の形式で入力します。xxx はそれぞれ 0~255 の数字です(10 進数で示します)。クラス A ネットワークの値は 255.0.0.0、クラス B ネットワークの値は 255.255.0.0、クラス C のネットワークの値は 255.255.255.0 です。カスタムサブネットマスクも可能です。
Gateway	送信先アドレスが現在のサブネットの範囲外にあるパケットをどこに送信するかを決める IP アドレスです。通常、これは IP ゲートウェイとして機能するルーターまたはホストのアドレスです。

[Apply]をクリックして変更を適用します。

3.2.4 IPv6 Interface Settings

スイッチの現在の IPv6 インターフェース設定を表示します。

次のウィンドウを表示するには、Configuration > IPv6 Interface Settings をクリックします：

Interface Name	System
VLAN Name	default
Admin. State	Disabled
IPv6 Address	<input type="text"/>
Automatic Link Local Address	Disabled
NS Retransmit Time (0-4294967295)	<input type="text"/> ms

IPv6 Type	IPv6 Address
-----------	--------------

IPv6 インターフェースを設定するには、IPv6 アドレスを入力して、[Apply]をクリックします。新しいエントリーがウィンドウの下部にあるテーブルに表示されます。

下記にパラメーターの説明を記載します。

パラメーター	説明
Interface Name	IPv6 インターフェース名が表示されます。本装置では System 固定になります。
VLAN Name	IPv6 インターフェースの VLAN 名を表示します。
Admin. State	現在の管理者状態を表示します。
IPv6 Address	IPv6 アドレス/サブネットマスクの形式で入力します。
Automatic Link Local Address	有効(Enabled)と無効(Disabled)を切り替えます。有効(Enabled)にすると、ネットワークアドレス情報の外部ソースがない場合に役に立ちます。
NS Retransmit Time (0-4294967295)	0 ~ 4294967295 の間の値を入力します。これはミリ秒単位のネイバーソリシテーションの再送タイマーです。デフォルトは 0 です。

[Apply]をクリックして変更を適用します。

3.2.5 IPv6 Route Settings

スイッチの IPv6 ルートテーブルを設定します。

次のウィンドウを表示するには、Configuration > IPv6 Route Settings をクリックします：

IPv6 Route Settings

IPv6 Default Gateway

IP Interface: System Default Gateway: Metric (1-65535): 1 [Create] [Delete]

Total Entries: 0

Prefix	Next Hop	IP Interface	Protocol	Metric
--------	----------	--------------	----------	--------

下記にパラメーターの説明を記載します。

パラメーター	説明
IP Interface	IPv6 インターフェースが表示されます。本装置では System 固定になります。
Default Gateway	デフォルトゲートウェイとなる IPv6 アドレスを入力します。
Metric	1 ~ 65535 の範囲でメトリック値を入力します。

[Create] をクリックすると、新しい IPv6 ルートがウィンドウ下部のテーブルに表示されます。

[Delete] をクリックすると、対象の IPv6 ルートが削除されます。

3.2.6 IPv6 Neighbor Settings

スイッチの IPv6 ネイバーを設定します。スイッチに現在設定されている IPv6 ネイバーがウィンドウ下部のテーブルに表示されます。

次のウィンドウを表示するには、Configuration > IPv6 Neighbor Settings をクリックします：

IPv6 Neighbor Settings

Interface Name: System
Neighbor IPv6 Address:
Link Layer MAC Address: Add

Interface Name: System
State: All Find Clear

Total Entries: 0

Neighbor	Link Layer Address	Interface	State
----------	--------------------	-----------	-------

ネイバー IPv6 アドレス、および、リンクレイヤー MAC アドレスを入力し、[Add] をクリックします。IPv6 ネイバーテーブルエントリを検索するには、希望する状態 (All/Address/Static/Dynamic) をこのウィンドウの中央にあるセクションで選択して、次に [Find] をクリックします。

ウィンドウの下部にあるテーブルに表示されるすべてのエントリを削除するには、[Clear] をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
Interface Name	IPv6 インターフェイス名が表示されます。本装置では System 固定になります。
Neighbor IPv6 Address	ネイバー IPv6 アドレスを入力します。
Link Layer MAC Address	MAC アドレスを入力します。
State	プルダウンメニューから、All/Address/Static/Dynamic を選択します。

[Add] をクリックして新しいネイバー IPv6 アドレスと Link Layer MAC Address を追加します。

[Find] をクリックして入力された条件で検索します。

[Clear] をクリックして入力されているデータを削除します。

3.2.7 Port Configuration

3.2.7.1 Port Settings

ポートの有効/無効、スピード/デュプレックス、フロー制御、アドレス学習、メディアの種類および MDIX などのポート設定を行います。

次のウィンドウを表示するには、Configuration > Port Configuration > Port Settings をクリックします：

Port	State	Speed/Duplex	Flow Control	Connection	Address Learning	MDIX
01	Enabled	Auto	Disabled	100M/Full/None	Enabled	Auto
02	Enabled	Auto	Disabled	Link Down	Enabled	Auto
03	Enabled	Auto	Disabled	Link Down	Enabled	Auto
04	Enabled	Auto	Disabled	Link Down	Enabled	Auto
05	Enabled	Auto	Disabled	Link Down	Enabled	Auto
06	Enabled	Auto	Disabled	Link Down	Enabled	Auto
07	Enabled	Auto	Disabled	Link Down	Enabled	Auto
08	Enabled	Auto	Disabled	Link Down	Enabled	Auto
09	Enabled	Auto	Disabled	Link Down	Enabled	Auto
10	Enabled	Auto	Disabled	Link Down	Enabled	Auto
11	Enabled	Auto	Disabled	Link Down	Enabled	Auto
12	Enabled	Auto	Disabled	Link Down	Enabled	Auto
13	Enabled	Auto	Disabled	Link Down	Enabled	Auto
14	Enabled	Auto	Disabled	Link Down	Enabled	Auto
15	Enabled	Auto	Disabled	Link Down	Enabled	Auto
16	Enabled	Auto	Disabled	Link Down	Enabled	Auto
17	Enabled	Auto	Disabled	Link Down	Enabled	Auto
18	Enabled	Auto	Disabled	Link Down	Enabled	Auto
19	Enabled	Auto	Disabled	Link Down	Enabled	Auto
20	Enabled	Auto	Disabled	Link Down	Enabled	Auto
21 (C)	Enabled	Auto	Disabled	Link Down	Enabled	Auto
21 (F)	Disabled	Auto	Disabled	Link Down	Enabled	Auto
22 (C)	Enabled	Auto	Disabled	Link Down	Enabled	Auto
22 (F)	Disabled	Auto	Disabled	Link Down	Enabled	Auto
23 (C)	Enabled	Auto	Disabled	Link Down	Enabled	Auto
23 (F)	Disabled	Auto	Disabled	Link Down	Enabled	Auto
24 (C)	Enabled	Auto	Disabled	Link Down	Enabled	Auto

スイッチポートを設定するには、ポートプルダウンメニューから、ポートまたはポート範囲を選択します。

注意事項



相手装置との通信モードをオートネゴシエーションまたは固定に合わせてください。固定モードでは、通信速度や全二重および半二重モードを合わせる必要があります。双方で一致しないと、リンク確立されない場合やリンク確立してもエラー率の高い通信となる場合があります。

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	ポート範囲を選択します。
State	このフィールドを切り替えて、該当するポートまたはポートグループを有効(Enabled)または無効(Disabled)にします。
Speed/Duplex	<p>スピード/デュプレックスフィールドを切り替えて、ポートの速度と全二重/半二重を選択します。Auto設定は、ポートが接続されているデバイスが処理可能な最大速度設定を自動的に設定されます。その他オプションとして、10M half、10M full、100M half、100M full、1000M full master、1000M full slave および1000M full があります。</p> <p>スイッチでは、2種類のギガビット接続(1000M full master および1000M full slave)を設定します。ギガビット接続は、他のポート速度設定とは異なり全二重接続のみ対応します。</p> <p>1000M full master パラメーターと1000M full slave パラメーターは、スイッチポートとギガビット対応のデバイスをUTP接続する際に関係します。マスター設定(1000M full master)は、ポートが、二重、速度、物理レイヤーの種類に関連するキャパシティーをアダプタサイズできるようにします。また、マスター設定は、2つの接続された物理レイヤーのマスターとスレーブの関係を定めます。この関係は2つの物理レイヤーの間のタイミング制御を確立するために必要です。タイミング制御は、マスター物理レイヤー上でローカルソースにより設定されます。スレーブ設定(1000M full slave)は、ループタイミングを使用します。ループタイミングでは、タイミングはマスターから受信したデータストリームから発生します。1つの接続を1000M full master用に設定する場合は、接続のもう一方は1000M full slave用に設定します。それ以外の組み合わせでは、ポートはリンクダウン状態となります。</p>
Flow Control	さまざまなポート構成で使用するフロー制御スキームを表示します。全二重用に構成したポートは802.3xフロー制御を使用します。半二重ポートはバックプレッシャーフロー制御を使用します。自動ポートはその二つのうちから自動選択します。デフォルトは無効です。
Address Learning	有効にすると、送信先MACアドレスと送信元MACアドレスがフォワーディングテーブルに自動的に一覧表示されます。デフォルト設定は有効です。
Medium Type	コンボポートで使用するメディア種類を選択します。SFPを使用する場合は[Fiber]を設定し、1000BASE-Tポートで使用する場合は[Copper]に設定します。
MDIX	MDIX設定は、「auto (自動)」、「normal (MDI-X)」、「cross (MDI)」から選択します。「normal (MDI-X)」に設定した場合、ストレートケーブルを使用してPC(MDI)に接続することが可能です。「cross (MDI)」に設定した場合、ストレートケーブルを使用して他のスイッチ(MDI-X)に接続することが可能です。

[Apply]をクリックして変更を適用します。

[Refresh]をクリックして画面に表示されるリストを更新します。

3.2.7.2 Port Description Settings

各ポートにコメントを記載します。

次のウィンドウを表示するには、Configuration > Port Configuration > Port Description Settings をクリックします：

From Port	To Port	Medium Type	Description
01	01	Copper	

Port	Description
01	
02	
03	
04	
05	
06	
07	
08	
09	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21 (C)	
21 (F)	
22 (C)	

ポートプルダウンメニューからポートまたはポート範囲を選択します。

コンボポートで使用するメディアの種類を Medium Type から選択します。SFP ポートは[Fiber]に設定し、1000BASE-T ポートは[Copper]に設定します。コンボポートの設定状態はスイッチポート番号スロットに表示されます (C は RJ45 ポートを示します。F は光ポートを示します)。

下記にパラメーターの説明を記載します。

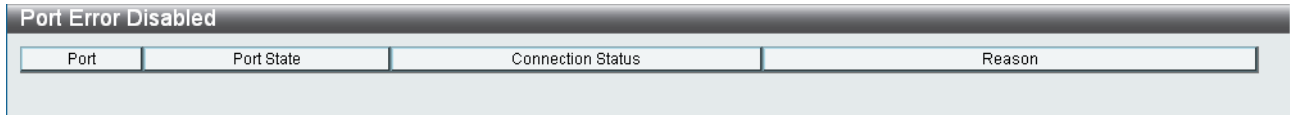
パラメーター	説明
From Port/To Port	ポート範囲を選択します。
Medium Type	コンボポートで使用するメディアの種類を選択します。SFP 使用する場合は [Fiber] を設定し、1000BASE-T ポートとして使用する場合は [Copper] に設定します。
Description	ポートの説明を記載します。

[Apply] をクリックして変更を適用します。

3.2.7.3 Port Error Disabled

ループ検出やリンク切断状態などの理由のために接続状態が無効になったポートに関する情報が表示されます。

次のウィンドウを表示するには、Configuration > Port Configuration > Port Error Disabled をクリックします：



Port	Port State	Connection Status	Reason
------	------------	-------------------	--------

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	エラーで無効になったポートが表示されます。
Port State	ポートの現在の実行状態(有効または無効)が表示されます。
Connection Status	ポートのアップリンク状態(有効または無効)が表示されます。
Reason	ポートがエラーで無効になった理由が表示されます(ループの発生など)。

3.2.7.4 Port Media Type

ポートのメディアタイプを表示します。

このウィンドウを表示するには、Configuration > Port Configuration > Port Media Type をクリックします：

Port	Type
01	100BASE-TX
02	1000BASE-T
03	1000BASE-T
04	1000BASE-T
05	1000BASE-T
06	1000BASE-T
07	1000BASE-T
08	1000BASE-T
09	1000BASE-T
10	1000BASE-T
11	1000BASE-T
12	1000BASE-T
13	1000BASE-T
14	1000BASE-T
15	1000BASE-T
16	1000BASE-T
17	1000BASE-T
18	1000BASE-T
19	1000BASE-T
20	1000BASE-T
21	1000BASE-T
22	1000BASE-T
23	1000BASE-T
24	1000BASE-T

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	ポートの番号が表示されます。
Type	ポートのメディアタイプが表示されます。

3.2.7.5 Port Green Mode Settings

各ポートの省電力機能の状態を表示します。

次のウィンドウを表示するには、Configuration > Port Configuration > Port Green Mode Settings をクリックします：

From Port	To Port	State		
01	01	Enabled	Apply	Refresh

Port	State	Operation State
01	Enable	Power Down
02	Enable	Power Down
03	Enable	Power Down
04	Enable	Power Down
05	Enable	Power Down
06	Enable	Power Down
07	Enable	Power Down
08	Enable	Power Down
09	Enable	Power Down
10	Enable	Power Down
11	Enable	Power Down
12	Enable	Power Down
13	Enable	Power Down
14	Enable	Power Down
15	Enable	Power Down
16	Enable	Power Down
17	Enable	Power Down
18	Enable	Power Down
19	Enable	Power Down
20	Enable	Power Down
21	Enable	Power Down
22	Enable	Power Down
23	Enable	Power Down
24	Enable	Power Down

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	ポート範囲を選択します。
State	選択したポートまたはポート範囲で、この機能を有効/無効にします。 デフォルト設定は有効です。

[Apply]をクリックして変更を適用します。

[Refresh]をクリックして画面に表示されるリストを更新します。

3.2.8 Static ARP Settings

ARP は、TCP/IP ネットワークにおいて、IP アドレスからイーサネット(Ethernet)LAN 上の MAC アドレスを求めるために使われる通信プロトコルです。指定のデバイスの ARP 情報を表示、定義、変更、削除することができます。また、静的 ARP のエントリーには IP アドレスと MAC アドレスを設定します。

次のウィンドウを表示するには、Configuration > Static ARP Settings をクリックします。

Interface	IP Address	MAC Address	Type	Edit	Delete
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast	Edit	Delete
System	10.0.0.1	00-40-66-45-5E-78	Local	Edit	Delete
System	10.0.0.255	FF-FF-FF-FF-FF-FF	Local/Broadcast	Edit	Delete

下記にパラメーターの説明を記載します。

パラメーター	説明
ARP Aging Time (0-65535)	アクセスされない状態でスイッチの ARP テーブルが維持できる最大時間を分単位で設定します。0 ~ 65535 分の範囲で設定することができます。デフォルト設定は 20 分です。
IP Address	ARP エントリーの IP アドレスです。
MAC Address	ARP エントリーの MAC アドレスです。

[Apply] をクリックして変更を適用します。

静的 ARP エントリーの IP アドレスと MAC アドレスを入力した後、[Apply] をクリックして新しいエントリーを適用します。静的 ARP 設定をすべて消去するには、[Delete All] をクリックします。静的 ARP エントリーを変更するには、テーブル内の相応する [Edit] をクリックします。静的 ARP エントリーを削除するには、テーブル内の対応する [Delete] をクリックします。

3.2.9 User Accounts

このウィンドウを使用して、ユーザーアカウントの制御、新しいユーザーの作成、既存のユーザーアカウントの表示を行います。

次のウィンドウを表示するには、Configuration > User Accounts をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
User Name	ユーザーの名前です。15文字までの英数字文字列を入力します。アカウントは8個まで作成することができます。
Password	新しいユーザーのパスワードを入力します(最大15文字)。
Access Right	ユーザー権利には、管理者とユーザーの2つのレベルがあります。管理者権限のあるユーザーが使用できる機能や選択は、ユーザー権限のあるユーザーは使用できないことがあります。
Confirm Password	新しいパスワードをもう一度入力します。

[Apply]をクリックして変更を適用します。既存のユーザーを変更または削除するには、該当するユーザーの[Edit]をクリックします。

管理者権利とユーザー権利

ユーザーアカウントには、管理者とユーザー2つの権限があります。管理者権限のあるユーザーが使用できる機能や選択は、ユーザー権限のユーザーは使用できないことがあります。

次の表は管理者権限とユーザー権限の概要です。


管理	管理者	ユーザー
設定	あり	なし
ネットワーク監視	あり	読み取り専用
コミュニティ名とトラップステーション	あり	読み取り専用
ファームウェアと構成ファイルの更新	あり	なし
システムユーティリティー	あり	なし
工場出荷時設定へのリセット	あり	なし
ユーザーアカウント管理		
ユーザーアカウントの追加/更新/削除	あり	なし
ユーザーアカウントの表示	あり	なし

3.2.10 System Log Configuration

3.2.10.1 System Log Settings

このウィンドウでシステムログ設定の有効/無効、及びシステムログ保存モードを指定します。

次のウィンドウを表示するには、Configuration > System Log Configuration > System Log Settings をクリックします：



下記にパラメーターの説明を記載します。

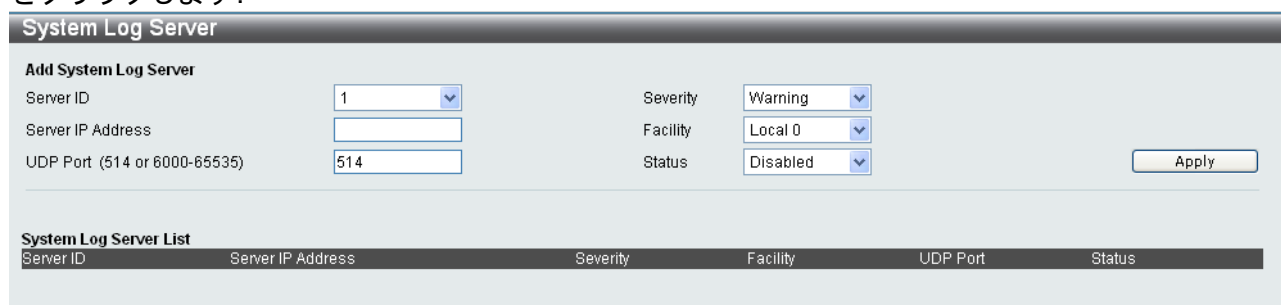
パラメーター	説明
System Log	ラジオボタンで、システムログ機能を有効(Enabled)または無効(Disabled)にします。
System Log Save Mode Settings	プルダウンメニューから、ログエントリーのトリガー方法を選択します。On Demand/Time Interval/Log Trigger から選択します。
min (1-65535)	上記 Mode で Time Interval を選択した場合、ログエントリーを作成するための時間間隔を分単位で入力します。

[Apply]をクリックして変更を適用します。

3.2.10.2 System Log Server

スイッチは、システムログサーバーを使用して最大4つまでの送信先サーバーにシステムログメッセージを送信できます。

次のウィンドウを表示するには、Configuration > System Log Configuration > System Log Server をクリックします：



下記にパラメーターの説明を記載します。

パラメーター	説明																		
Server ID	システムログサーバー設定インデックス(1-4)です。																		
Severity	<p>ブルダウンメニューから、送信するメッセージのレベルを選択できます。 Warning/Information/All から選択します。</p> <p>Warning - 警告的なメッセージをリモートホストに送信する場合に指定します。</p> <p>Informational - 情報的なメッセージをリモートホストに送信する場合に指定します。</p> <p>All - スイッチに生成される現在サポートしている Syslog メッセージのすべてをリモートホストに送信します。</p>																		
Server IP Address	システムログサーバーの IP アドレスです。																		
Facility	<p>オペレーティングシステムのデーモンおよび処理によっては、ファシリティ値が割り当てられていることがあります。ファシリティが明示的に割り当てられていない処理やデーモンは、"ローカル使用"ファシリティのいずれか、または、"ユーザーレベル"ファシリティを使用できます。割り当てられたファシリティは次のように表示されます。スイッチが現在使用しているファシリティ値は、16~23 です。</p> <table border="1"> <thead> <tr> <th>数値</th> <th>ファシリティコード</th> </tr> </thead> <tbody> <tr> <td>16</td> <td>ローカル使用 0 (local0)</td> </tr> <tr> <td>17</td> <td>ローカル使用 1 (local1)</td> </tr> <tr> <td>18</td> <td>ローカル使用 2 (local2)</td> </tr> <tr> <td>19</td> <td>ローカル使用 3 (local3)</td> </tr> <tr> <td>20</td> <td>ローカル使用 4 (local4)</td> </tr> <tr> <td>21</td> <td>ローカル使用 5 (local5)</td> </tr> <tr> <td>22</td> <td>ローカル使用 6 (local6)</td> </tr> <tr> <td>23</td> <td>ローカル使用 7 (local7)</td> </tr> </tbody> </table>	数値	ファシリティコード	16	ローカル使用 0 (local0)	17	ローカル使用 1 (local1)	18	ローカル使用 2 (local2)	19	ローカル使用 3 (local3)	20	ローカル使用 4 (local4)	21	ローカル使用 5 (local5)	22	ローカル使用 6 (local6)	23	ローカル使用 7 (local7)
数値	ファシリティコード																		
16	ローカル使用 0 (local0)																		
17	ローカル使用 1 (local1)																		
18	ローカル使用 2 (local2)																		
19	ローカル使用 3 (local3)																		
20	ローカル使用 4 (local4)																		
21	ローカル使用 5 (local5)																		
22	ローカル使用 6 (local6)																		
23	ローカル使用 7 (local7)																		
UDP Port(514 or 6000-65535)	システムログメッセージを送信する際に使用する UDP ポート番号を入力します。デフォルトは 514 です。																		
Status	システムログサーバーの設定を有効(Enabled)または無効(Disabled)にします。																		

[Apply]をクリックして変更を適用します。

[Edit]をクリックしてエントリーを再設定します。

[Delete]をクリックしてエントリーを削除します。

3.2.11 DHCP Snooping

3.2.11.1 DHCP Snooping Settings

このウィンドウで DHCP Snooping 機能のグローバル設定を指定します。

次のウィンドウを表示するには、Configuration > DHCP Snooping > DHCP Snooping Settings をクリックします：

DHCP Snooping Settings	
DHCP Snooping State	Disabled <input type="button" value="Apply"/>
ARP Inspection	Enabled <input type="button" value="Apply"/>
IPv4 Inspection	Enabled <input type="button" value="Apply"/>
Force Deny Mode	Disabled <input type="button" value="Apply"/>
Current Mode	Permit
Timer (0, 30-604800)	1800 sec <input type="button" value="Apply"/>
Remaining Time	-
DHCP Snooping Option 82 state	Disabled <input type="button" value="Apply"/>

下記にパラメーターの説明を記載します。

パラメーター	説明
DHCP Snooping State	プルダウンメニューから、DHCP Snooping 機能のグローバル設定を有効(Enabled)または無効(Disabled)にします。
ARP Inspection	有効(Enabled)の場合、ARP パケットが DHCP Snooping の検査対象になります。無効(Disabled)の場合は、検査対象になりません。
IPv4 Inspection	有効(Enabled)の場合、IPv4 パケットが DHCP Snooping の検査対象になります。無効(Disabled)の場合は、検査対象になりません。
Force Deny Mode Current Mode	Force Deny Mode を無効(Disabled)にすると、DHCP Snooping 機能は PERMIT モードとして動作し、次項の Timer に定める猶予期間を経て DENY モードに切り替わるまでの間、パケットの検査によるフィルタリングを行いません。DENY モードでは、DHCP Snooping の結果に基づくフィルタリングを実施し、登録されていない IP アドレスが送信元であるパケットをブロックします。Force Deny Mode が有効(Enabled)の場合、直ちに DENY モードとして動作します。 Current Mode では、現在のモード(Permit/Deny)を表示します。
Timer (0, 30-604800) Remaining Time	Force Deny Mode が無効の場合に使用される切替タイマーを秒単位で設定します。0 の場合、DENY モードに移行しません。 Remaining Time は、PERMIT モードから DENY モードへ移行するまでの残り時間を表示します。
DHCP Snooping Option 82 state	有効(Enabled)の場合、DHCP Snooping で Option 82 の情報を追加します。無効(Disabled)の場合、Option 82 の情報を追加しません。

[Apply]をクリックして変更を適用します。

3.2.11.2 DHCP Snooping Ports Settings

このウィンドウで DHCP Snooping 機能を動作させるポート、及び対象 VLAN を指定します。

次のウィンドウを表示するには、Configuration > DHCP Snooping > DHCP Snooping Ports Settings をクリックします：

From Port	To Port	State	<input checked="" type="radio"/> VLAN Name	<input type="radio"/> VID List (e.g.:2-5)	<input type="checkbox"/> All VLANs	Apply
01	01	Enabled				
Port	State	Enabled VLANs				
1	Disabled	-				
2	Disabled	-				
3	Disabled	-				
4	Disabled	-				
5	Disabled	-				
6	Disabled	-				
7	Disabled	-				
8	Disabled	-				
9	Disabled	-				
10	Disabled	-				

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	設定するポート範囲を選択します。
State	有効(Enabled)の場合、対象ポートで DHCP Snooping 機能が動作します。無効(Disabled)の場合、DHCP Snooping 機能が動作しません。
VLAN Name/VID List/ All VLANs	DHCP Snooping を動作させる VLAN を VLAN 名もしくは VID リストで指定します。全ての VLAN を対象にする場合は All VLANs のチェックボックスにチェックします。

[Apply]をクリックして変更を適用します。

3.2.11.3 DHCP Snooping Entry Settings

このウィンドウで DHCP Snooping のダイナミックエントリーを表示します。また、登録されたエントリーをクリアすることもできます。

次のウィンドウを表示するには、Configuration > DHCP Snooping > DHCP Snooping Entry Settings をクリックします：

Port	MAC Address	VID	IP Address	
7	00-40-66-AA-AA-AA	1	192.168.0.10	Delete
7	00-40-66-BB-BB-BB	1	192.168.0.100	Delete

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	エントリーをクリアする場合の対象ポート範囲を選択します。
VLAN Name/VID List/ All VLANs	クリアする対象の VLAN を VLAN 名もしくは VID リストで指定します。 全ての VLAN を対象にする場合は All VLANs のチェックボックスにチェックします。

[Clear] をクリックすると、対象となるエントリーをクリアします。特定の MAC アドレスをクリアする場合、テーブル内の対応する [Delete] をクリックします。

3.2.11.4 DHCP Snooping Static Entry Settings

このウィンドウで DHCP Snooping のスタティックエントリーを作成します。

次のウィンドウを表示するには、Configuration > DHCP Snooping > DHCP Snooping Static Entry Settings をクリックします：

Port	MAC Address	VID	IP Address	
8	00-40-66-AA-AA-AA	1	192.168.0.10	Delete
9	00-40-66-BB-BB-BB	1	192.168.0.100	Delete

下記にパラメーターの説明を記載します。

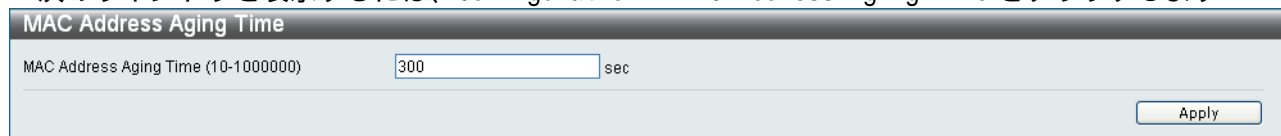
パラメーター	説明
MAC Address	DHCP Snooping スタティックエントリーの MAC アドレスを入力します。
IP Address	DHCP Snooping スタティックエントリーの IP アドレスを入力します。
VLAN Name/VLAN ID(1-4094)	所属する VLAN を VLAN 名もしくは VLAN ID で指定します。

[Create] をクリックして変更を適用します。また、作成済のエントリーを削除する場合は、テーブル内の対応する [Delete] をクリックします。

3.2.12 MAC Address Aging Time

このテーブルで、学習した MAC アドレスをフォーワーディングテーブルに保持する時間を設定します。エージング時間は 10 ~ 1,000,000 秒の範囲で設定します。デフォルト設定は 300 秒です。

次のウィンドウを表示するには、Configuration > MAC Address Aging Time をクリックします：



下記にパラメーターの説明を記載します。

パラメーター	説明
MAC Address Aging Time	MAC address aging time を設定します。値は 10 から 1,000,000 秒の範囲で指定します。デフォルト値は 300 秒です。

[Apply]をクリックして変更を適用します。

注意事項

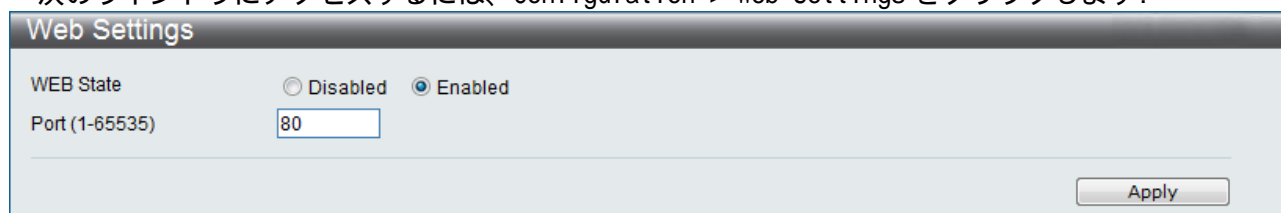


FDB に登録されたエントリーがクリアされる時間は、 $\langle \text{入力値} \rangle \div 2 \sim \langle \text{入力値} \rangle - 1$ までの時間幅があります。

3.2.13 Web Settings

このウィンドウで Web ベース GUI の有効/無効及びポート番号の設定を行います。無効設定にした場合、HTTP 経由でのシステム設定を行うことができなくなります。Web ベース GUI のデフォルト設定は、有効で、TCP ポート番号は 80 です。

次のウィンドウにアクセスするには、Configuration > Web Settings をクリックします：



下記にパラメーターの説明を記載します。

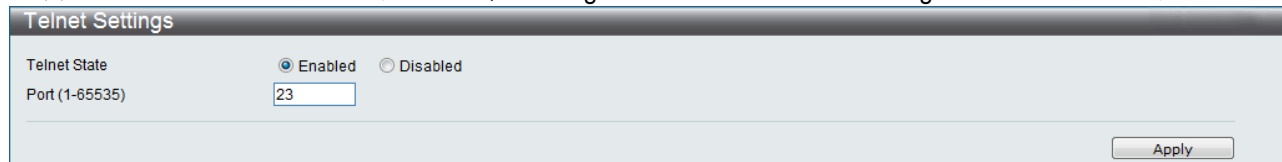
パラメーター	説明
WEB State	Web ベース GUI の有効(Enabled)または無効(Disabled)を設定します。
Port	Web で使用するポート番号を設定します。値は 1 から 65535 の範囲で指定します。デフォルト値は 80 です。

[Apply]をクリックして変更を適用します。

3.2.14 Telnet Settings

Telnet によるスイッチへの接続可否及びポート番号を設定します。デフォルト設定は、Telnet 接続が有効で TCP ポート番号は 23 です。

次のウィンドウにアクセスするには、Configuration > Telnet Settings をクリックします：



下記にパラメーターの説明を記載します。

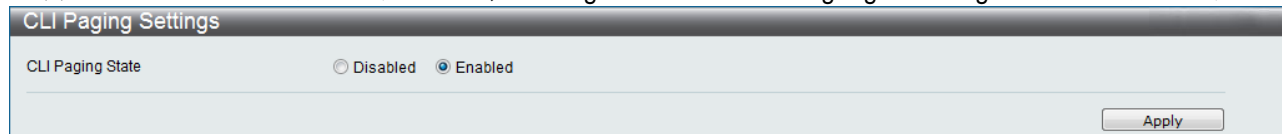
パラメーター	説明
Telnet State	Telnet 設定の有効(Enabled)または無効(Disabled)を設定します。
Port	Telnet で使用するポート番号を設定します。値は 1 から 65535 の範囲で指定します。デフォルト値は 23 です。

[Apply]をクリックして変更を適用します。

3.2.15 CLI Paging Settings

CLI インターフェースにおいて、コマンド表示情報が 1 画面以上となる場合、次画面へのスクローリングを一時停止する CLI ページング機能を設定します。デフォルトでは有効です。

次のウィンドウにアクセスするには、Configuration > CLI Paging Settings をクリックします：



下記にパラメーターの説明を記載します。

パラメーター	説明
CLI Paging State	CLI ページングの有効(Enabled)または無効(Disabled)を設定します。

[Apply]をクリックして変更を適用します。

3.2.16 Firmware Information

スイッチの内蔵メモリーに保管されているファームウェアイメージに関する情報を表示します。

次のウィンドウにアクセスするには、Configuration > Firmware Information をクリックします：

Firmware Information						
ID	Version	Size (B)	Update Time	User		
*1	1.14.00	3580860	0000/00/00 00:01:01	adpro(CONSOLE)	Boot UP	Delete
2	1.14.00	3580860	0000/00/00 00:06:06	adpro(CONSOLE)	Boot UP	Delete

*1 : Boot up firmware
(SSH) : Firmware update through SSH
(WEB) : Firmware update through WEB
(SNMP) : Firmware update through SNMP
(TELNET) : Firmware update through TELNET
(CONSOLE) : Firmware update through CONSOLE

下記にパラメーターの説明を記載します。

パラメーター	説明
ID	スイッチに保存されているファームウェアの ID 番号を表示します。スイッチには 2 つのファームウェアを保存できます。ID 番号に*印あるファームウェアが起動時に使用されます。
Version	ファームウェアのバージョンを表示します。
Size (B)	ファームウェアのサイズを表示します。
Update Time	ファームウェアを保存した時のスイッチ時間を表示します。
User	ファームウェアをダウンロードしたユーザーを表示します。ユーザーを識別できない場合、このフィールドには [Anonymous] または [Unknown] と表示されることがあります。

[Boot UP] をクリックして起動ファームウェアを選択します。

[Delete] をクリックして選択したファームウェアバージョンを削除します。

3.2.17 SNTP Settings

3.2.17.1 Time Settings

このウィンドウで SNTP に関する設定を行います。

次のウィンドウを表示するには、Configuration > SNTP Settings > Time Settings をクリックします：

Time Settings

Status
SNTP State Disabled Enabled
Current Time 00/00/0 05:38:18
Time Source System Clock

SNTP Settings
SNTP First Server 0.0.0.0
SNTP Second Server 0.0.0.0
SNTP Poll Interval In Seconds (30-99999) 720

Set Current Time
Date (DD/MM/YYYY) 00/00/0
Time (HH:MM:SS) 05:38:18

下記にパラメーターの説明を記載します。

パラメーター	説明
Status	
SNTP State	ラジオボタンで、有効または無効を選択して、SNTP を有効(Enabled)または無効(Disabled)にします。
Current Time	スイッチ上に設定されている現在の時間を表示します。
Time Source	システムの時間ソースを表示します。
SNTP Settings	
SNTP First Server	SNTP 情報元となるプライマリーサーバーの IP アドレスです。
SNTP Second Server	SNTP 情報元となるセカンダリーサーバーの IP アドレスです。
SNTP Poll Interval In Seconds (30-99999)	更新した SNTP 情報を要求する間隔です(秒単位)。デフォルト値は 720 です。
Set Current Time	
Date (DD/MM/YYYY)	現在の日付を、日、月、年の順に入力してシステムクロックを更新します。
Time (HH:MM:SS)	現在の時間を、時間、分、秒の順に入力してシステムクロックを更新します。

[Apply]をクリックして変更を適用します。

3.2.17.2 TimeZone Settings

このウィンドウで SNTP のタイムゾーンと夏時間を設定します。

次のウィンドウを表示するには、Configuration > SNTP Settings > TimeZone Settings をクリックします：

TimeZone Settings

Daylight Saving Time State	<input type="text" value="Disabled"/>
Daylight Saving Time Offset In Minutes	<input type="text" value="60"/>
Time Zone Offset:from UTC In +/-HH:MM	+ <input type="text" value="09"/> <input type="text" value="00"/>

DST Repeating Settings

From: Which Week Of The Month	<input type="text" value="First"/>
From: Day Of Week	<input type="text" value="Sun"/>
From: Month	<input type="text" value="Apr"/>
From: Time In HH MM	<input type="text" value="00"/> <input type="text" value="00"/>
To: Which Week Of The Month	<input type="text" value="Last"/>
To: Day Of Week	<input type="text" value="Sun"/>
To: Month	<input type="text" value="Oct"/>
To: Time In HH MM	<input type="text" value="00"/> <input type="text" value="00"/>

DST Annual Settings

From: Month	<input type="text" value="Apr"/>
From: Day	<input type="text" value="29"/>
From: Time In HH MM	<input type="text" value="00"/> <input type="text" value="00"/>
To: Month	<input type="text" value="Oct"/>
To: Day	<input type="text" value="12"/>
To: Time In HH MM	<input type="text" value="00"/> <input type="text" value="00"/>

下記にパラメーターの説明を記載します。

パラメーター	説明
Daylight Saving Time State	夏時間のモード設定を行います。 Disabled - 夏時間を無効にします。 Repeating - 繰り返しモードを使用して、夏時間が有効になります。 Annual - 年間モードを使用して、夏時間が有効になります。
Daylight Saving Time Offset In Minutes	夏時間によるオフセット時間を 30 分、60 分、90 分、120 分に指定します。
Time Zone Offset:from UTC In +/-HH:MM	協定世界時(UTC)からのタイムゾーンオフセットを指定します。

パラメーター	説明
DST Repeating Settings 繰り返しモードを使用して、夏時間の調整を有効にします。 繰り返しモードを使用する場合は、夏時間開始日付と夏時間終了日付を形式に従って指定する必要があります。 例えば、夏時間が4月第2週の日曜日に開始し、10月最終週の日曜日に終了するように指定します。	
From: Which Week Of The Month	夏時間が開始する週を入力します。
From: Day Of Week	夏時間が開始する曜日を入力します。
From: Month	夏時間が開始する月を入力します。
From: Time In HH MM	夏時間が開始する時間を入力します。
To: Which Week Of The Month	夏時間が終了する週を入力します。
To: Day Of Week	夏時間が終了する曜日を入力します。
To: Month	夏時間が終了する月を入力します。
To: Time In HH MM	夏時間が終了する時間を入力します。
DST Annual Settings 年間モードを使用して、夏時間の調整を有効にします。 年間モードを使用する場合は、夏時間開始日付と夏時間終了日付を簡潔に指定する必要があります。 例えば、夏時間が4月3日に開始して、10月14日に終了するように指定します。	
From: Month	各年の夏時間が開始する月を入力します。
From: Day	各年の夏時間が開始する曜日を入力します。
From: Time In HH MM	各年の夏時間が開始する時間を入力します。
To: Month	各年の夏時間が終了する月を入力します。
To: Day	各年の夏時間が終了する日付を入力します。
To: Time In HH MM	各年の夏時間が終了する時間を入力します。

[Apply]をクリックして変更を適用します。

3.2.18 SMTP Settings

SMTP は次のウィンドウで入力された電子メールアドレスに基づいて、スイッチイベントをメールで送信する機能です。スイッチは SMTP のクライアントとして設定されます。サーバーは、スイッチからのメッセージを受信して、正しい情報を電子メールに挿入し、設定した受信者に配信します。スイッチ管理者は、この機能を使用して、小さいワークグループの管理を簡略化したり、クローゼットを配線したり、緊急スイッチイベントを取り扱う際の速度を上げることができます。または、スイッチ上で発生する不確かなイベントを記録して安全性を強化することもできます。

スイッチの SMTP サーバーをセットアップして、スイッチ上で問題が発生した場合にはスイッチログファイルの送信先となる電子メールアドレスを設定します。

3.2.18.1 SMTP Service Settings

このウィンドウで SMTP サービスに関する設定を行います。

次のウィンドウを表示するには、Configuration > SMTP Settings > SMTP Service Settings をクリックします：

The screenshot shows the 'SMTP Service Settings' configuration window. It contains the following elements:

- SMTP Global Settings:**
 - SMTP State: Radio buttons for 'Enabled' and 'Disabled'. 'Disabled' is selected.
 - SMTP Server Address: Text input field containing '0.0.0.0'.
 - SMTP Server Port (1-65535): Text input field containing '0'.
 - Self Mail Address: Text input field with '(Max:64 characters)' label.
 - 'Apply' button.
- SMTP Mail Receiver Address:**
 - 'Add A Mail Receiver' label and text input field with '(Max:64 characters)' label.
 - 'Add' button.
 - Table with 8 rows and 2 columns: 'Index' and 'Mail Receiver Address'. Each row has a 'Delete' button.

下記にパラメーターの説明を記載します。

パラメーター	説明
SMTP State	ラジオボタンで、Enabled または Disabled を選択して、SMTP サービスを有効(Enabled)または無効(Disabled)にします。
SMTP Server Address	リモートデバイス上の SMTP サーバーの IP アドレスを入力します。
SMTP Server Port (1-65535)	SMTP サーバーと通信する TCP ポート番号を入力します。通常、SMTP のポート番号は 25 です。1 ~ 65535 の範囲の値から選択することもできます。
Self Mail Address	メッセージの送信元となる電子メールアドレスを入力します。このアドレスは受信者へ送信する電子メールメッセージの差出人アドレスになります。設定できるのは 1 つのメールアドレスのみです。この文字列は 64 文字内の英数字になります。
Add A Mail Receiver	電子メールの送信先アドレスを指定します。 電子メールアドレスを入力して、[Add] ボタンをクリックします。最大 8 つの電子メールアドレスを追加できます。これらのアドレスをスイッチから削除するには、ウィンドウの一番下にある Mail Receiver Address テーブルの相応する[Delete]をクリックします。

[Apply] をクリックして変更を適用します。

3.2.18.2 SMTP Service

このウィンドウを使用して、前のウィンドウで設定した SMTP サービス設定をテストします。

次のウィンドウを表示するには、Configuration > SMTP Settings > SMTP Service をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
Subject	e-mail の題名を入力します。
Content	e-mail の内容を入力します。

[Send] をクリックしてメールを送信します。

3.2.19 SNMP Settings

SNMP は、ネットワークデバイスの管理と監視用に設計された OSI レイヤー7(アプリケーションレイヤー) プロトコルです。SNMP により、ネットワーク管理ステーションはゲートウェイ、ルーター、スイッチ、および、その他のネットワークデバイスの設定を読み取ったり変更することができます。SNMP を使用して、システム機能が正しく動作するように設定したり、パフォーマンスを監視したり、スイッチ、スイッチグループ、または、ネットワーク内の潜在的な問題を検出します。

SNMP に対応する管理型デバイスには、デバイス上でローカルに動作するソフトウェア(エージェントと呼ばれます)も含まれます。定義した変数のセット(管理オブジェクト)は、SNMP エージェントに維持され、デバイスを管理する際に使用されます。これらのオブジェクトは MIB で定義します。MIB は、SNMP エージェントが制御する情報の標準プレゼンテーションを提供します。SNMP で、MIB 仕様の形式と、ネットワーク経由でこの情報にアクセスする際に使用するプロトコルを定義します。

スイッチは SNMP バージョン 1、2c、3 に対応します。スイッチを監視および制御するバージョンを選択します。SNMP の 3 つのバージョンは、SNMP サーバーとスイッチの間のセキュリティーレベルによって異なります。

SNMP バージョン 1 および 2 では、パスワードのように機能するコミュニティ名を使用して、ユーザーを認証します。SNMP サーバーとスイッチでは同じコミュニティ名を使用します。認証されていない SNMP サーバーからの SNMP パケットは無視されます。

SNMP バージョン 1 および 2c の管理アクセスで使用するスイッチのデフォルトコミュニティ名は次のとおりです:

- public - MIB オブジェクト取得
- private - MIB オブジェクト取得、変更

SNMP バージョン 3 は 2 つの部分に分類され、より高度な認証処理を使用します。最初の部分では、SNMP マネージャーとして機能するユーザーとユーザー属性の一覧を維持します。2 番目の部分では、一覧上の各ユーザーが SNMP マネージャーとして実行できる処理を説明します。

スイッチで、ユーザーグループを一覧表示して、権利の共有セットで設定することができます。SNMP バージョン 3 は、一覧表示された SNMP マネージャーのグループ用に設定することもできます。このように、SNMP バージョン 1 を使用して読み取り専用情報を表示したりトラップを受信できる SNMP マネージャーのグループを作成したり、または、他のグループに SNMP バージョン 3 を使用して読み取り/書き込み権利を与え、高いセキュリティーレベルを割り当てることができます。

SNMP バージョン 3 を使用して、個別ユーザー、または、SNMP マネージャーのグループが指定の SNMP 管理機能を実行できるようにしたり、指定の SNMP 管理機能を実行できないようにすることができます。許可する機能や制限する機能は、指定の MIB に関連するオブジェクト識別子(OID)を使用して定義します。SNMP バージョン 3 では SNMP メッセージを暗号化できる追加セキュリティーレイヤーを使用できます。スイッチの SNMP バージョン 3 設定の設定方法に関する詳細情報は、次のセクションを参照してください。

Trap

トラップは、ネットワーク担当者に、スイッチ上で発生するイベントについて警報するメッセージです。イベントの重要度は、再起動（誰かが間違ってスイッチの電源を切った場合）など高い場合や、または、ポート状態の変更など低い場合があります。スイッチはトラップを生成して、トラップ受信者（またはネットワーク管理者）へ送信します。トラップの例としては、認証エラーやトポロジ－変更のトラップメッセージがあります。

注意事項



工場出荷時の設定状態においては、コミュニティ名が一致する全ての SNMP マネージャーからのアクセスが許可されます。SNMP 機能を使用しない場合、delete snmp community、delete snmp user 設定を行なう必要があります。

3.2.19.1 SNMP View Table

このウィンドウを使用して、リモート SNMP マネージャーでアクセスできる MIB オブジェクトを定義するコミュニティ名、または、SNMP グループにビューを割り当てます。

スイッチの SNMP ビュー設定を設定するには、Configuration > SNMP Settings > SNMP View Table をクリックします：

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

下記にパラメーターの説明を記載します。

パラメーター	説明
View Name	32 文字までの英数字文字列を入力します。View Name を使用して、作成される新しい SNMP ビューを識別します。
Subtree OID	ビューのオブジェクト識別子(OID)サブツリーを入力します。OID で、SNMP マネージャーのアクセスに含める、または、SNMP マネージャーのアクセスから除くオブジェクトツリー(MIB ツリー)を識別します。
View Type	Included を選択して、このオブジェクトを SNMP マネージャーがアクセスできるオブジェクト一覧に含めます。Excluded を選択して、このオブジェクトを SNMP マネージャーがアクセスできるオブジェクト一覧から除きます。

[Apply]をクリックして変更を適用します。エントリーを削除するには、対応する[Delete]をクリックします。

3.2.19.2 SNMP Group Table

このテーブルで作成した SNMP グループで、SNMP ユーザー (SNMP ユーザーテーブルウィンドウで識別します)、または、コミュニティ名を前のウィンドウで作成した SNMP ビューにマップします。

このウィンドウを表示するには、Configuration > SNMP Settings > SNMP Group Table をクリックします：

Group Name	Read View Name	Write View Name	Notify View Name	User-based Security Model	Security Level	
public	CommunityV...		CommunityV...	SNMPv1	NoAuthNoPriv	Delete
public	CommunityV...		CommunityV...	SNMPv2	NoAuthNoPriv	Delete
initial	restricted		restricted	SNMPv3	NoAuthNoPriv	Delete
private	CommunityV...	CommunityV...	CommunityV...	SNMPv1	NoAuthNoPriv	Delete
private	CommunityV...	CommunityV...	CommunityV...	SNMPv2	NoAuthNoPriv	Delete
ReadGroup	CommunityV...		CommunityV...	SNMPv1	NoAuthNoPriv	Delete
ReadGroup	CommunityV...		CommunityV...	SNMPv2	NoAuthNoPriv	Delete
WriteGroup	CommunityV...	CommunityV...	CommunityV...	SNMPv1	NoAuthNoPriv	Delete
WriteGroup	CommunityV...	CommunityV...	CommunityV...	SNMPv2	NoAuthNoPriv	Delete

下記にパラメーターの説明を記載します。

パラメーター	説明
Group Name	32 文字までの英数字文字列を入力します。 Group Name を使用して、SNMP ユーザーの新しい SNMP グループを識別します。
Read View Name	SNMP エージェントへの SNMP 読み取り権利が許可されたユーザーの SNMP グループ名を指定します。
Write View Name	SNMP エージェントへの SNMP 書き込み権利が許可されたユーザーの SNMP グループ名を指定します。
Notify View Name	SNMP エージェントが生成した SNMP トラップメッセージを受信できるユーザーの SNMP グループ名を指定します。
User-based Security Model	SNMPv1 - SNMP バージョン 1 を使用することを指定します。 SNMPv2 - SNMP バージョン 2c を使用することを指定します。 SNMPv3 - SNMP バージョン 3 を使用することを指定します。
Security Level	セキュリティレベル設定が適用されるのは SNMPv3 のみです。 NoAuthNoPriv - スイッチとリモート SNMP マネージャーの間で送信されるパケットを認証したり暗号化しないことを指定します。 AuthNoPriv - スイッチとリモート SNMP マネージャーの間で送信されるパケットの認証が必要ですが、暗号化しないことを指定します。 AuthPriv - スイッチとリモート SNMP マネージャーの間で送信されるパケットの認証が必要で、さらに、そのパケットを暗号化することを指定します。

[Apply] をクリックして変更を適用します。

既存の SNMP ユーザーテーブルエントリを削除するには、対応する [Delete] をクリックします。

3.2.19.3 SNMP User Table

このウィンドウには、現在設定されている SNMP ユーザーがすべて表示されます。また、新しいユーザーを追加することができます。

次のウィンドウを表示するには、Configuration > SNMP Settings > SNMP User Table をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
User Name	SNMP ユーザーの識別名です。32 文字までの英数字文字列で指定します。
Group Name	SNMP ユーザーが所属するグループの識別名です。
SNMP Version	V1 - SNMP バージョン 1 を使用していることを示します。 V2 - SNMP バージョン 2 を使用していることを示します。 V3 - SNMP バージョン 3 を使用していることを示します。
SNMP V3 Encryption	None - SNMPv3 暗号化がないことを示します。 Password - パスワード経由 SNMPv3 暗号化があることを示します。 Key - キー経由の SNMPv3 暗号化があることを示します。
Auth-Protocol by Password	SNMP V3 Encryption で Password を選択した場合、下記の指定を行います。 MD5 - HMAC-MD5-96 認証レベルを使用することを示します。 SHA - HMAC-SHA 認証プロトコルを使用することを示します。
Priv-Protocol by Password	SNMP V3 Encryption で Password を選択した場合、下記の指定を行います。 None - 認証プロトコルを使用しないことを示します。 DES - DES 56-bit 暗号化を使用することを示します。
Auth-Protocol by Key	SNMP V3 Encryption で Key を選択した場合、下記の指定を行います。 MD5 - HMAC-MD5-96 認証レベルを使用することを示します。 SHA - HMAC-SHA 認証プロトコルを使用することを示します。
Priv-Protocol by Key	SNMP V3 Encryption で Key を選択した場合、下記の指定を行います。 None - 認証プロトコルを使用しないことを示します。 DES - DES 56-bit 暗号化を使用することを示します。
Password	SNMPv3 暗号化を有効にする場合は、パスワードを入力します。
Key	SNMPv3 暗号化を有効にする場合は、キーを入力します。

[Apply] をクリックして変更を適用します。

選択したエントリーを削除するには、[Delete] をクリックします。

3.2.19.4 SNMP Community Table

このテーブルを使用して、既存の SNMP コミュニティーテーブル設定を表示し、SNMP コミュニティー名を作成して、SNMP マネージャーとエージェント間の関係を定義します。コミュニティ名は、スイッチ上のエージェントへのアクセスを許可するパスワードのように機能します。コミュニティ名は以下の特徴と関連しています。

- (1) すべての MIB オブジェクトのサブセットを定義する MIB ビューはすべて SNMP コミュニティーにアクセスすることができます。
- (2) MIB オブジェクトへの読み取り/書き込み、または読み取り専用レベルを許可し、SNMP コミュニティーにアクセスすることができます。

次のウィンドウを表示するには、Configuration > SNMP Settings > SNMP Community Table をクリックします：

Community Name	View Name	Access Right	
private	CommunityView	read_write	Delete
public	CommunityView	read_only	Delete

下記にパラメーターの説明を記載します。

パラメーター	説明
Community Name	SNMP コミュニティーのメンバーを識別する際に使用する 32 文字までの英数字文字列を入力します。この文字列は、リモート SNMP マネージャーにスイッチの SNMP エージェント内の MIB オブジェクトへのアクセスを許可するパスワードのように使用します。
View Name	リモート SNMP マネージャーがスイッチ上でアクセスできる MIB オブジェクトのグループを識別する際に使用する 32 文字までの英数字文字列を入力します。SNMP ビューテーブルにあるビュー名を使用します。
Access Right	Read Only - 作成したコミュニティ名を使用する SNMP コミュニティーメンバーがスイッチ上の MIB のコンテンツの読み取りしかできないように指定します。 Read Write - 作成したコミュニティ名を使用する SNMP コミュニティーメンバーがスイッチ上の MIB のコンテンツを読み取り/書き込みできるように指定します。

[Apply]をクリックして変更を適用します。

選択したエントリーを削除するには、[Delete]をクリックします。

3.2.19.5 SNMP Host Table

SNMP ホストテーブルウィンドウを使用して、SNMP トラップの受信者を設定します。

次のウィンドウを表示するには、Configuration > SNMP Settings > SNMP Host Table をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
Host IP Address	SNMP トラップを受信するホストの IP アドレスを入力します。
User-based Security Model	SNMPv1 - SNMP バージョン 1 を使用することを指定します。 SNMPv2c - SNMP バージョン 2 を使用することを指定します。 SNMPv3 - SNMP バージョン 3 を使用することを指定します。
Security Level	User-based Security Model で SNMPv3 を指定した場合、下記を選択します。 NoAuthNoPriv - NoAuthNoPriv セキュリティーレベルを指定します。 AuthNoPriv - AuthNoPriv セキュリティーレベルを指定します。 AuthPriv - AuthPriv セキュリティーレベルを指定します。
Community String / SNMPv3 User Name	コミュニティ名または SNMPv3 ユーザー名を入力します。

[Apply] をクリックして変更を適用します。

3.2.19.6 SNMP Engine ID

SNMPv3 では、エンジン ID と呼ばれる識別子を用いてエージェントを一意に識別することができます。

次のウィンドウを表示するには、Configuration > SNMP Settings > SNMP Engine ID をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
Engine ID	SNMP エンジンの ID を指定します。16 進数で 10~64 文字まで入力できます。

エンジン ID を変更するには、所定のスペースに新しいエンジン ID を入力して、[Apply] をクリックします。

3.2.19.7 SNMP Trap Configuration

次のウィンドウを使用して、スイッチ上の SNMP 機能のトラップ設定を有効/無効にします。

次のウィンドウを表示するには、Configuration > SNMP Settings > SNMP Trap Configuration をクリックします：

認証トラップやポートリンク変更トラップ、ログイントラップなどの SNMP トラップを有効または無効に設定します。

下記にパラメーターの説明を記載します。

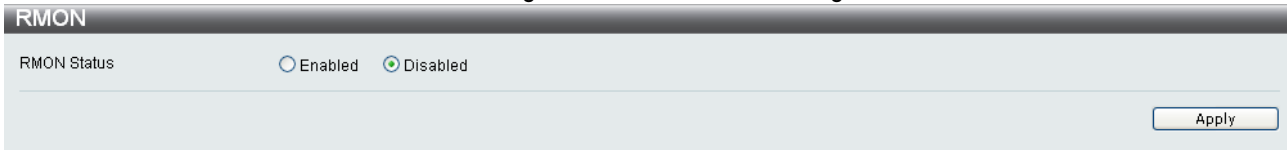
パラメーター	説明
SNMP Trap	SNMP トラップの有効(Enabled)/無効(Disabled)を設定します。
SNMP Authentication Traps	認証トラップの有効(Enabled)/無効(Disabled)を設定します。
SNMP Link Change Traps	リンク変更トラップの有効(Enabled)/無効(Disabled)を設定します。
SNMP Login Trap	ログイントラップの有効(Enabled)/無効(Disabled)を設定します。
SNMP Logout Trap	ログアウトトラップの有効(Enabled)/無効(Disabled)を設定します。
SNMP Login Fail Trap	ログインフェイルトラップの有効(Enabled)/無効(Disabled)を設定します。
From Port/To Port	リンク変更トラップのポート範囲を設定します。
State	リンク変更トラップの有効(Enabled)/無効(Disabled)を設定します。

[Apply]をクリックして変更を適用します。

3.2.19.8 RMON

RMON 機能を有効/無効にします。

次のウィンドウを表示するには、Configuration > SNMP Settings > RMON をクリックします：



下記にパラメーターの説明を記載します。

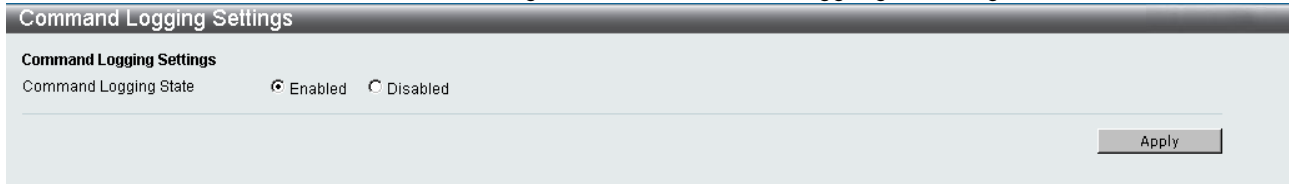
パラメーター	説明
RMON Status	ラジオボタンで、Enabled または Disabled を選択して、RMON を有効 (Enabled) または無効 (Disabled) にします。

[Apply] をクリックして変更を適用します。

3.2.20 Command Logging Settings

Command Logging は、コマンドラインインターフェース上で実行したコマンドの成功および失敗をログに出力する機能です。

次のウィンドウを表示するには、Configuration > Command Logging Settings をクリックします：




下記にパラメーターの説明を記載します。

パラメーター	説明
Command Logging State	ラジオボタンで、Enabled または Disabled を選択して、コマンドログ機能の有効(Enabled)または無効(Disabled)を設定します。デフォルトでは有効となっています。

[Apply] をクリックして変更を適用します。

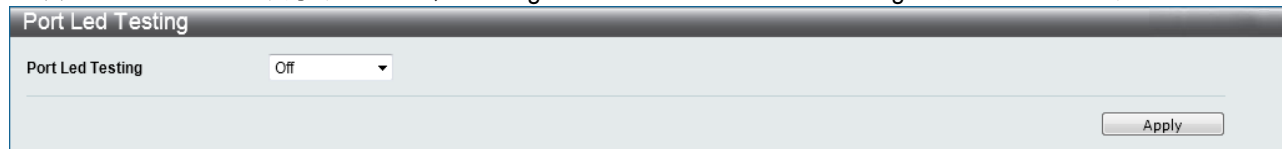
注意事項

-  コマンドログ機能はコマンドラインインターフェース上でのコマンド実行結果をシステムログに出力する機能です。Web ユーザーインターフェース上でのコマンド実行結果については、システムログに出力されません。

3.2.21 Port LED Testing

Port LED Testing は、ポートのリンク状態に関係なく、ポートの LED 表示を点灯または点滅させる機能です。

次のウィンドウを表示するには、Configuration > Port LED Testing をクリックします：



下記にパラメーターの説明を記載します。

パラメーター	説明
Port LED Testing	ポートLED表示の点灯または点滅させる色を指定します。 Off - 全ポートのLED 表示を通常のリンク状態で表示します。 green - 全ポートのLED 表示を緑色点灯で表示します。 amber - 全ポートのLED 表示を橙色点灯で表示します。 blink_green - 全ポートのLED 表示を緑色点滅で表示します。 blink_amber - 全ポートの LED 表示を橙色点滅で表示します。

[Apply]をクリックして変更を適用します。

注意事項



リンクアップしているポートは、実行時に一度リンクダウンが発生します。

3.2.22 PoE

PoE(Power over Ethernet)は、ツイストペアケーブルの指定の組み合わせのペアに直流電圧を重畳させ、通信をしながら受電機器に電源を供給する IEEE802.3at 規格の機能です。

PoE 機能は、APLGM110GTPOE/POE2、APLGM118GTPOE/POE2、APLGM124GTPOE/POE2 の計 6 機種のみで対応しています。

3.2.22.1 PoE System Settings

このウィンドウでスイッチ全体の PoE 給電状態表示および給電制限値、また PoE 給電停止状態からの給電復旧モードを設定します。

次のウィンドウを表示するには、Configuration > PoE > PoE System Settings をクリックします：

PoE System Information					
Power Limit (Watts)	System Total Power Consumption (Watts)	System Power Remained (Watts)	Power Disconnection Method	Recover Mode	Environment Status
375.0	0.0	375.0	Deny Low Priority Port	Auto(Delay:180 sec)	Normal

下記にパラメーターの説明を記載します。

パラメーター	説明
Power Limit	スイッチ全体の給電制限値をワット単位で設定します。値は 20 から 375 の範囲で設定します。APLGM110GTPOE/POE2、APLGM118GTPOE/POE2、APLGM124GTPOE/POE2 で最大値が異なります。APLGM110GTPOE/POE2 の設定範囲は 20 ~ 125(W) です。APLGM118GTPOE/POE2 の設定範囲は 20 ~ 250(W) です。APLGM124GTPOE/POE2 の設定範囲は 20 ~ 375(W) です。
Recover Mode	スイッチの FAN 異常/温度異常による、PoE 給電停止状態からの給電復旧モードを設定します。デフォルト設定は Auto(Delay:180 秒)です。 auto - 正常復帰すると自動でPoE 給電が再開されます。給電再開までの時間を「Delay Time」パラメーターで指定します。 manual - 正常復帰してもPoE 給電は再開されません。給電再開には PoE Manual Recovery の [Apply] をクリックする必要があります。
Delay Time	給電復旧モードの「Recover Mode」パラメーターが auto 設定の場合、給電再開までの時間を180 ~ 600(秒)で指定します。デフォルト設定は180(秒)です。
PoE Manual Recovery	給電復旧モードの「Recover Mode」パラメーターが manual 設定の場合、給電再開には PoE Manual Recovery の [Apply] をクリックします。

[Apply]をクリックして変更を適用します。

[Refresh]をクリックして画面に表示されるリストを更新します。

注意事項

- ❗ スイッチの給電制限値を超過した場合、Deny Low Priority Port プロセスによって、新しく供給を開始するポートよりもプライオリティが低いポートから優先的に給電を停止します。この状態は過負荷が解消されるまで継続されます。
- ❗ APLGM124GTPOE/POE2 装置のみ、PoE 給電総量によって FAN 回転数が動的に制御されます。給電総量が 185W 以上になると FAN 回転が高速になり、155W 以下になると FAN 回転が通常回転に戻ります。
- ❗ ファームウェアバージョンにより、PoE 給電総量の算出方法が異なります。
 - ・バージョン(Ver.1.04)では、受電機器が接続された各ポートの給電制限値(User Define の場合はユーザー設定値、Class Based の場合には PD クラスの給電上限値)を合計して算出します。
 - ・バージョン(Ver.1.05)以降は、受電機器が接続された各ポートで実際に使用している消費電力を合計して算出します。

3.2.22.2 PoE Port Settings

このウィンドウで各ポートの PoE 給電状態表示および PoE 給電設定を行います。

次のウィンドウを表示するには、Configuration > PoE > PoE Port Settings をクリックします：

Port	State	Priority	Power Limit (mW)	Class	Power (mW)	Voltage (Decivolt)	Current (mA)	Status
1	Enabled	Low	---(Class based)	0	0	0	0	OFF : Interim state...
2	Enabled	Low	7770(User Defined)	0	5900	552	108	ON : 802.3af-compl...
3	Enabled	Low	---(Class based)	0	0	0	0	OFF : Interim state...
4	Enabled	Low	---(Class based)	0	0	0	0	OFF : Interim state...
5	Enabled	Low	---(Class based)	0	0	0	0	OFF : Interim state...
6	Enabled	Low	---(Class based)	0	0	0	0	OFF : Interim state...
7	Enabled	Low	---(Class based)	0	0	0	0	OFF : Interim state...
8	Enabled	Low	---(Class based)	0	0	0	0	OFF : Interim state...

下記にパラメーターの説明を記載します。

パラメーター	説明																		
From Port/To Port	設定対象のポートを指定します。																		
State	ポートの PoE ステータスを指定します。デフォルト設定は有効(Enabled)です。無効(Disabled)設定では、ポート接続の PD デバイスに電力を供給しません。																		
Priority	ポートに給電する優先度を指定します。デフォルト設定は(Low)です。Critical, High, Low の優先順位があり、最も高い優先度は Critical です。																		
Power Limit	<p>ポートの給電制限値を設定します。デフォルト設定は 31200(mW) です。この給電制限値は、ユーザー指定(User Define)オプションで 1000 ~ 31200(mW)の範囲で設定します。</p> <p>クラスベース指定(Class Based)の場合は、受電機器が接続されると PD クラスを自動で検出し、そのクラスに応じた給電上限値をポートに割り当てます。</p> <p>各クラスの給電上限値は受電電力範囲より少し大きな値となっており、これは接続ケーブルにおける電力損失等を考慮しているためです。</p> <p>以下のクラスからポート給電上限値を自動で検出します。</p> <table border="1"> <thead> <tr> <th><クラス></th> <th><給電上限値></th> <th><受電電力範囲></th> </tr> </thead> <tbody> <tr> <td>Class 0:</td> <td>16.2(W)</td> <td>0.44 ~ 12.95(W)</td> </tr> <tr> <td>Class 1:</td> <td>4.2(W)</td> <td>0.44 ~ 3.84(W)</td> </tr> <tr> <td>Class 2:</td> <td>7.4(W)</td> <td>3.84 ~ 6.49(W)</td> </tr> <tr> <td>Class 3:</td> <td>16.2(W)</td> <td>6.49 ~ 12.95(W)</td> </tr> <tr> <td>Class 4:</td> <td>31.2(W)</td> <td>12.95 ~ 25.50(W)</td> </tr> </tbody> </table>	<クラス>	<給電上限値>	<受電電力範囲>	Class 0:	16.2(W)	0.44 ~ 12.95(W)	Class 1:	4.2(W)	0.44 ~ 3.84(W)	Class 2:	7.4(W)	3.84 ~ 6.49(W)	Class 3:	16.2(W)	6.49 ~ 12.95(W)	Class 4:	31.2(W)	12.95 ~ 25.50(W)
<クラス>	<給電上限値>	<受電電力範囲>																	
Class 0:	16.2(W)	0.44 ~ 12.95(W)																	
Class 1:	4.2(W)	0.44 ~ 3.84(W)																	
Class 2:	7.4(W)	3.84 ~ 6.49(W)																	
Class 3:	16.2(W)	6.49 ~ 12.95(W)																	
Class 4:	31.2(W)	12.95 ~ 25.50(W)																	

[Apply]をクリックして変更を適用します。

[Refresh]をクリックして画面に表示されるリストを更新します。

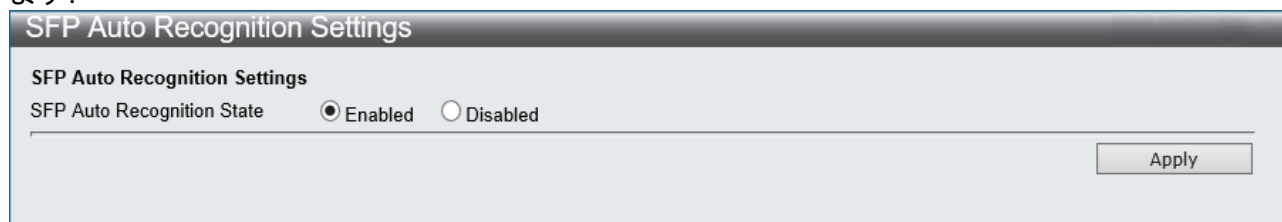
注意事項

- ❗ 最大給電量を超過した場合、プライオリティーの高いポートから電力を供給します。プライオリティーレベルが同じ場合には、若番ポートから優先的に電力を供給します。（新たに接続した受電機器によって給電制限値を超過した場合でも、必ずしも新たに接続した受電機器の電力供給が停止されるわけではありません）
- ❗ パラメーター(State, Priority, Power Limit)を変更した場合、対象ポートの給電を一時的に停止した後に給電を再開します。
- ❗ ユーザー指定(User Define)オプション入力するポートの給電制限値は、200mW 単位での動作となります。
(200mW 未満を入力しても切捨てた値で動作します)
- ❗ Port Setting で、データ通信のポート設定を無効(disabled)にしても電力供給は行われます。
- ❗ ファームウェアバージョンにより、ポート給電制限値のデフォルト値が異なります。
 - ・バージョン(Ver.1.04)では、デフォルト値が(Class Based)です。
 - ・バージョン(Ver.1.05)以降は、デフォルト値が(User Define : 31200mW)です。

3.2.23 SFP Auto Recognition Settings

SFP 自動認識機能を使用すると、コンボポートのメディア種類の設定によらず、SFP ポートのリンク状態によって使用するメディアを自動的に決定します。SFP 自動認識機能はコンボポート全体に適用され、ポート単位で設定することはできません。

次のウィンドウを表示するには、Configuration > SFP Auto Recognition Settings をクリックします：



下記にパラメーターの説明を記載します。

パラメーター	説明
SFP Auto Recognition State	有効(Enabled)が選択された場合は SFP 自動認識機能を使用します。無効(Disabled)が選択された場合は SFP 自動認識機能を使用しません。

[Apply]をクリックして変更を適用します。

注意事項

- ❗ SFP 自動認識機能を有効にすると、全てのコンボポートの state の設定は適用されず、Fiber ポートで光信号を受信する環境では Fiber ポートが、それ以外の場合は UTP ポートが、有効な状態に変更されます。
- ❗ SFP 自動認識機能の設定を切り替えると、コンボポートがリセットされます。

3.3 L2 Features

次のセクションでは、スイッチのレイヤー2 転送に関する機能の設定について説明します。

IEEE 802.1p 優先度について

優先度タギングは、異なる種類のデータを同時に転送できるネットワーク上のトラフィック管理方法を提供するために設計された IEEE802.1p 規格で定義する機能です。この機能は、ネットワークが混雑している場合に、時間に繊細なデータの転送に関連する問題を緩和することを目的とします。通信中のわずかな遅延でも、時間に繊細なデータに左右されるアプリケーション(ビデオ会議など)の品質に甚大な悪影響を及ぼします。

IEEE802.1p 規格に準拠するネットワークデバイスには、データパケットの優先度レベルを認識する機能が備わっています。これらのデバイスはパケットに優先度ラベルを割当てたり、タグすることもできます。対応デバイスは、パケットから優先度タグを取り除くこともできます。この優先度タグで、パケットの迅速性の度数、および、パケットを割り当てるキュー(待ち行列)を定義します。

優先度タグには0~7の値が付いています。0は最低優先度データです。7は最高優先度データに割り当てられます。通常、最高優先度タグ7を使用するのは、わずかな遅延にも敏感なビデオアプリケーションやオーディオアプリケーション、または、データ通信の特別配慮を保証しているエンドユーザーからのデータの場合です。

スイッチにより、優先度タグの付いたデータパケットのネットワーク上での取り扱いを詳細に決めることができます。キューを使用して優先度タグの付いたデータを管理することで、お使いのネットワークのニーズに合わせてその比較優先度を指定することができます。異なるタグの付いたパケットが2つ以上ある場合に、これらのパケットを同じ待ち行列にグループ分けすると便利な場合があります。ただし、一般的に、キュー7(最高優先度の待ち行列)は優先度値7のデータパケット用にします。優先度値のないパケットはキュー0に置かれ、転送の際の優先度は最低になります。

スイッチには、ストリクトモードと加重ラウンドロビンシステムが装備されており、パケットを消去してキューを空にするレートを定義します。キューを空にする比率は4:1です。キュー7(最高優先度の待ち行列)では4つのパケットを消去し、キュー0では1つのパケットを消去します。

スイッチ上の優先度付きキュー設定は、すべてのポート、スイッチに接続されているすべてのデバイスに影響することにご注意ください。お使いのネットワークで優先度タグの割り当て機能のあるスイッチを使用する場合は、この優先度付きキューシステムが特に便利です。

VLAN の説明

VLAN は、物理レイアウトではなく論理スキームに従って構成されたネットワークトポロジーです。VLAN は、パケットが VLAN 内のポート間だけで転送されるように、ネットワークを異なるブロードキャストドメインに論理的にセグメント化します。VLAN でトラフィックを特定のドメインに制限して、帯域のパフォーマンスを強化したり、セキュリティを向上させることができます。

VLAN に関する注記

スイッチは IEEE802.1Q VLAN およびポートベース VLAN に対応します。ポートタグ削除機能を使用して、802.1Q タグをパケットヘッダーから削除して、タグを認識できないデバイスとの互換性を維持することができます。

スイッチのデフォルトでは、すべてのポートは default という名前の単一の 802.1Q VLAN に割り当てられています。default VLAN の VID は 1 です。

IEEE 802.1Q VLAN

次のような関連用語があります：

- ・ タギング - 802.1Q VLAN 情報をパケットのヘッダーに挿入する操作です。
- ・ タグ削除 - 802.1Q VLAN 情報をパケットヘッダーから削除する操作です。
- ・ イングレスポート - パケットがスイッチに流れこみ、VLAN を決める必要があるポートです。
- ・ イーグレスポート - パケットがスイッチから出て、他のスイッチ、または、ホストに流れ、タギングを決める必要があるポートです。

スイッチ上には IEEE 802.1Q(タグ付き)VLAN が装備されています。802.1Q VLAN ではタギングが必要です。タグを付けることによって、VLAN をネットワーク全体に構成できます(ネットワーク上のすべてのスイッチが IEEE 802.1Q に対応する場合)。

VLAN では、ネットワークをセグメント化して、ブロードキャストドメインのサイズを縮小できます。VLAN を入力するパケットはすべて、VLAN のメンバーであるステーションに転送されます(IEEE 802.1Q 対応スイッチ経由)。これには、不明な送信元からのブロードキャストパケット、マルチキャストパケット、ユニキャストパケットが含まれます。

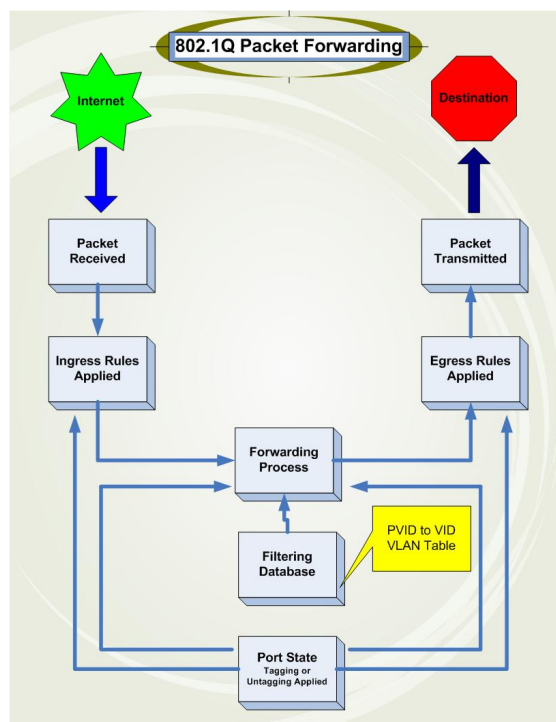
VLAN はネットワークのセキュリティレベルも提供できます。IEEE 802.1Q VLAN は、VLAN のメンバーであるステーション間だけでパケットを配信します。

ポートはタギングまたはタグ削除として設定します。IEEE 802.1Q VLAN のタグ削除機能を使用して、VLAN がパケットヘッダーの VLAN タグを認識しないレガシースイッチでも動作するようにできます。タギング機能により、単一の物理接続によって VLAN が複数の 802.1Q 準拠スイッチを構成し、スパンニングツリーをすべてのポート上で有効にし、正しく動作するようにすることができます。

IEEE 802.1Q 規格では、受信ポートがメンバーである VLAN に対するタグなしパケットの転送を制限します。

IEEE 802.1Q の主な特性は次のとおりです。

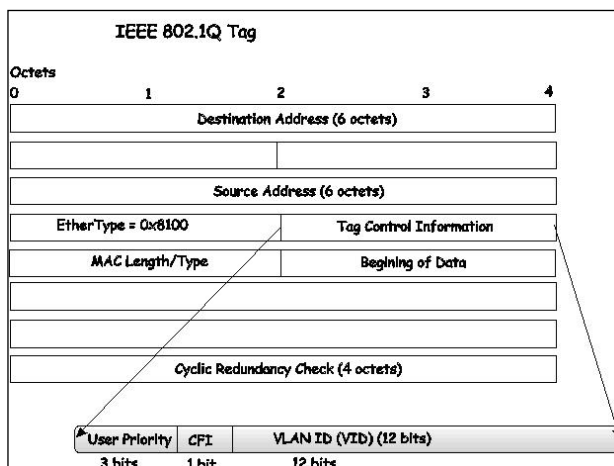
- (1) フィルタリングによってパケットを VLAN に割り当てます。
- (2) 単一のグローバルスパンニングツリーがあることを仮定します。
- (3) 1 レベルタギングの明示的タギングスキームを使用します。
- (4) 802.1Q VLAN パケットフォワーディング
- (5) パケットフォワーディングは、次の 3 種類の規則に基づいて決定します:
 - (a) イングレス規則 - 1 つの VLAN に属する受信フレームの分類に関連する規則です。
 - (b) ポート間のフォワーディング規則 - パケットをフィルターするか、転送するかを決定します。
 - (c) イーグレス規則 - パケットをタグ付き、または、タグなしで送信するかどうかを決定します。



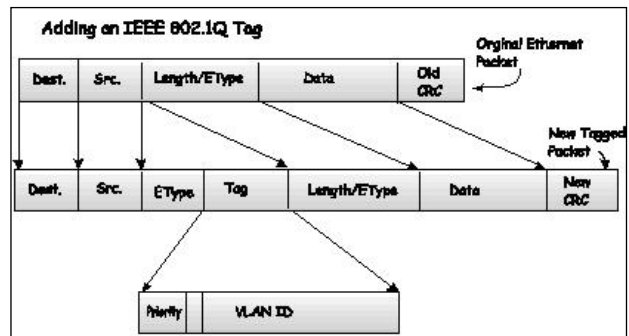
802.1Q VLAN タグ

下の図は 802.1Q VLAN タグを示します。送信元の MAC アドレスの後に挿入する 4 つのオクテットがあります。これらのオクテットは、イーサタイプフィールドの 0x8100 の値で表されます。パケットのイーサタイプフィールドが 0x8100 と同じ場合は、パケットには IEEE 802.1Q/802.1p タグが付きます。タグは次の 2 オクテットに含まれ、ユーザー優先度の 3 ビット、キャノニカル形式の識別子 (CFI - トークンリングパケットのカプセル化のために使用します。これでイーサネットバックボーンで転送できるようにします) の 1 ビット、そして VLAN ID (VID) の 12 ビットから成ります。ユーザー優先度の 3 ビットは 802.1p で使用します。VID は VLAN 識別子であり、802.1Q 規格で使用します。VID の長さは 12 ビットなので、4094 の固有 VLAN を識別できます。

タグをパケットヘッダーに挿入して、パケット全体を 4 オクテット分だけ長くします。パケットに含まれていた情報はすべて維持されます。



イーサタイプと VLAN ID は MAC 送信元アドレスの後、元のイーサタイプ/長さ、または、論理リンク制御の前に挿入します。パケットは元の長さよりも 1 バイト長いので、巡回冗長検査(CRC)を再計算する必要があります。



ポート VLAN ID

タグ付き(および、802.1Q VID 情報のある)パケットは、1 つの 802.1Q 準拠ネットワークデバイスから他の 802.1Q 準拠ネットワークデバイスへ、VLAN 情報が保持された状態で転送されます。これによって、802.1Q VLAN をネットワークデバイスに渡すことができます(すべてのネットワークデバイスが 802.1Q に準拠する場合は、ネットワーク全体に渡すことができます)。

802.1Q VLAN が導入される前には、ポートベースあるいは MAC ベース VLAN が一般的に使用されていました。これらの VLAN は、ポート VLAN ID (PVID) に基づいてパケットを転送します。特定のポートで受信したパケットにはそのポートの PVID が割り当てられ、パケットの送信先アドレス(スイッチのフォワーディングテーブルにあります)に対応するポートに転送されます。パケットを受信したポートの PVID がパケットを転送するポートの PVID と異なる場合は、スイッチはパケットを削除します。

スイッチ内では、異なる PVID は異なる VLAN を意味します(外部ルーターがないと 2 つの VLAN は通信できません)。PVID に基づく VLAN 識別では、特定のスイッチ(またはスイッチスタック)外に拡張する VLAN を作成できません。

スイッチ上の各物理ポートには PVID があります。802.1Q ポートにも、スイッチ内で使用するための PVID が割り当てられます。スイッチ上で VLAN が定義されていない場合は、すべてのポートは PVID を 1 としてデフォルト VLAN が割り当てられます。タグなしパケットには、パケットを受信したポートの PVID が割り当てられます。VLAN では、転送はこの PVID に基づいて決めます。タグ付きパケットは、タグ内に含まれる VID に従って転送されます。タグ付きパケットにも PVID が割り当てられます。ただし、パケットの転送は、PVID ではなく VID に基づいて決めます。

タグを認識できるスイッチでは、スイッチ内の PVID をネットワーク上の VID へ関連付けるためのテーブルを維持する必要があります。スイッチは、転送するパケットの VID とパケットを転送するポートの VID とを比較します。2 つの VID が異なる場合は、ポートはパケットを削除します。タグなしパケット用の PVID とタグ付きパケット用の VID があるので、同じネットワーク上に、タグを認識できるデバイスとタグを認識できないデバイスが共に存在することができます。

スイッチポートの PVID は 1 つのみです。ただし、スイッチの VLAN テーブル内のスイッチのメモリーに保管できるだけの数の VID を持つことができます。

ネットワーク上のデバイスによってはタグを認識できないので、パケットを転送する前に、タグを認識できるデバイス上の各ポートで、転送するパケットにタグを付けるかどうかを決定します。転送するポートがタグを認識できないデバイスに接続されている場合は、パケットにはタグは付きません。転送するポートがタグを認識できるデバイスに接続されている場合は、パケットにタグが付きません。

タグ VLAN とタグなし VLAN

802.1Q 準拠スイッチ上の各ポートはタグ VLAN またはタグなし VLAN として設定します。

タグ VLAN が有効なポートは、ポートを通過するすべてのパケットのヘッダーに、VID 番号、優先度、その他の VLAN 情報を挿入します。パケットに事前にタグがつけられている場合は、ポートはパケットを変更しないので、VLAN 情報はそのまま維持されます。ネットワーク上のその他の 802.1Q 準拠デバイスは、タグにある VLAN 情報を使用して、パケットの転送を決めることができます。

タグ削除が有効なポートは、ポートを通過するすべてのパケットから 802.1Q タグを削除します。パケットに 802.1Q VLAN タグがない場合は、ポートはパケットを変更しません。そのため、タグ削除ポートで受信したり転送したすべてのパケットには 802.1Q VLAN 情報はありません (PVID はスイッチ内部だけで使用します)。タグ削除は、パケットを 802.1Q 準拠ネットワークデバイスから非準拠ネットワークデバイスへ送信する際に使用されます。

イングレスフィルタリング

パケットがスイッチに流れ、VLAN について決める必要のあるスイッチ上のポートは、イングレスポートと呼ばれます。ポートのイングレスフィルタリングが有効な場合は、スイッチはパケットヘッダー内の VLAN 情報(ある場合)を確認して、パケットを転送するかどうかを決定します。

パケットに VLAN 情報がタグされている場合は、イングレスポートは、まずイングレスポート自体がタグ付き VLAN のメンバーであるかどうかを確認します。イングレスポートがタグ付き VLAN のメンバーでない場合、パケットは削除されます。イングレスポートが 802.1Q VLAN のメンバーである場合、スイッチは次に、転送先ポートが 802.1Q VLAN のメンバーであるかどうかを確認します。転送先ポートが 802.1Q VLAN のメンバーでない場合、パケットは削除されます。転送先ポートが 802.1Q VLAN のメンバーである場合、パケットは転送され、転送先ポートは転送されたパケットを接続したネットワークセグメントに転送します。

パケットに VLAN 情報がタグされていない場合、イングレスポートはパケットに独自の PVID を VID としてタグします (ポートがタグングポートの場合)。次に、スイッチは、転送先ポートがイングレスポートと同じ VLAN (同じ VID) のメンバーであるかどうかを確認します。転送先ポートがイングレスポートと同じ VLAN (同じ VID) のメンバーでない場合、パケットは削除されます。VID が同じである場合、パケットは転送され、転送先ポートは転送されたパケットを接続したネットワークセグメント上へ転送します。

イングレスフィルタリングと呼ばるこの処理を使用して、受信ポイントの VLAN がイングレスポートと異なるパケットを削除して、スイッチ内の帯域幅を維持します。これによって、転送先ポートが削除するパケットの処理が不要になります。

デフォルト VLAN

VID 1 の default と呼ばれる VLAN がスイッチ上のすべてのポートがデフォルトで設定されています。

ポートベース VLAN

ポートベース VLAN でスイッチポートを通過するトラフィックを制限します。これによって、スイッチに 1 台のコンピューターあるいは部署全体が直接接続されている場合は、ポートに接続したすべてのデバイスはポートが属する VLAN のメンバーになります。

ポートベース VLAN では、NIC はパケットヘッダー内の 802.1Q タグを識別できる必要はありません。NIC は標準イーサネットパケットを送受信します。パケットの送信先が同じセグメント上にある場合は、標準イーサネットプロトコルを使用して通信します。パケットの送信先が他のスイッチポートにある場合は、VLAN を考慮して、パケットをスイッチで破棄するか転送するかどうかを決めます。

VLAN セグメント化

パケットを、VLAN 2 のメンバーであるポート 1 上のマシンで転送するとします。送信先が他のポート上にある場合(通常のフォワードテーブルのルックアップで検索します)、スイッチは、その他のポート(ポート 10)が VLAN 2 のメンバーであるかどうか(VLAN 2 パケットを受信できるかどうか)を確認します。ポート 10 が VLAN 2 のメンバーでない場合、スイッチはパケットを破棄するため、送信先に転送されません。ポート 10 が VLAN 2 のメンバーの場合、パケットは転送されます。この VLAN に基づく選択的フォワーディング機能で VLAN セグメントをネットワークします。この要点は、ポート 1 は VLAN 2 のみパケットを転送するということです。

ネットワークリソースは VLAN 全体で共有することができます。オーバーラッピング VLAN をセットアップすることでポートは複数の VLAN グループに属することができ、リソースを共有することができます。例えば、VLAN 1 メンバーをポート 1、2、3、4 に設定して、VLAN 2 メンバーをポート 1、5、6、7 に設定すると、ポート 1 は 2 つの VLAN グループに属します。ポート 8、9、10 はどの VLAN グループにも設定されません。つまり、ポート 8、9、10 は同じ VLAN グループになります。

VLAN グループとリンクアグリゲーション

リンクアグリゲーションで設定するポートグループの VLAN ID はすべて同一である必要があります。

Q-in-Q VLAN

ネットワークプロバイダーは、Q-in-Q VLAN(ダブル VLAN と呼ばれることもあります)を使用して VLAN 構成を拡張し、大きい包含的 VLAN 内にカスタマー VLAN を置いて、VLAN に新しいレイヤーを追加することができます。こうすることで、大きい ISP で L2 仮想プライベートネットワークを作成し、カスタマー用のトランスペアレント LAN を作成することもできます。これによって、クライアント側で複雑な設定を行うことなく、2 つ以上のカスタマー LAN ポイントを接続できます。複雑性を回避できることに加え、管理者は、それぞれ 4000 以上の VLAN を置くことのできる VLAN を 4000 以上持つこととなり、VLAN ネットワークを大きく拡張したり、ネットワーク上で複数の VLAN を使用するカスタマーのサポートを大きく向上することができます。

基本的に、Q-in-Q VLAN は、SPVID と呼ばれる、既存の IEEE802.1Q VLAN 内にある VLAN タグです。これらの VLAN には TPID(タグ付きプロトコル ID)でマークされ、パケットの VLAN タグ内でカプセル化するため 16 進数で構成されています。これで、パケットをダブルタグとして識別し、ネットワーク上のその他の VLAN から分離して、単一パケット内で VLAN の階層を作成します。

次は Q-in-Q VLAN タグ付きパケットの一例です:

送信先アドレス	送信元アドレス	SPVLAN(TPID + サービスプロバイダー VLAN タグ)	802.1Q CEVLAN タグ (TPID + カスタマー VLAN タグ)	イーサタイプ	ペイロード
---------	---------	-----------------------------------	---	--------	-------

Q-in-Q VLAN の規則

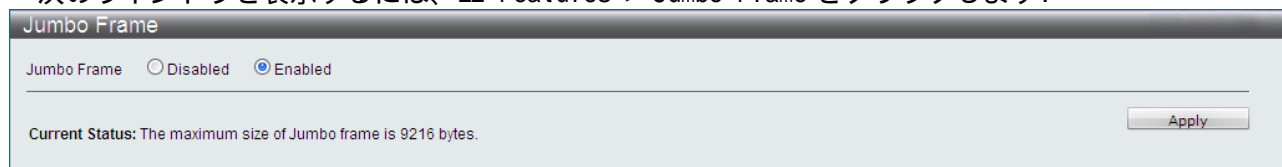
Q-in-Q VLAN をご使用になる際には、以下の規則や規制がございます。

- (1) 全てのポートに対し、SPVLAN において使用する TPID 設定が必要です。TPID は全ポート同じ値の設定になります。
- (2) 全てのポートに対し、アクセスポートまたはアップリンクポートのどちらかに設定する必要があります。
- (3) Q-in-Q VLAN では SPVID タグが付加されますので、ジャンポフレーム機能を有効にしてご使用下さい。
- (4) Q-in-Q のエッジスイッチとして使用する場合、アクセスポートは SPVLAN のタグなしポートとなりアップリンクポートは SPVLAN のタグ付きポートとなります。このときアクセスポートは UNI (User-Network Interface) に、アップリンクポートは NNI (Network-Network Interface) に設定する必要があります。
- (5) 本装置では、Q-in-Q VLAN と標準の VLAN の併用は出来ません。どちらかでのご使用となります。標準の VLAN から Q-in-Q VLAN 有効に変更した場合、それまで設定していた ACL に修正が必要となる場合があります。
- (6) Q-in-Q VLAN を有効にする際には、STP および GVRP を一旦無効にする必要があります。
- (7) アクセスポートより送出される装置 CPU からのパケットは、タグなしになります。

3.3.1 Jumbo Frame

下記ウィンドウのラジオボタンで、Enabled または Disabled を選択して、ジャンボフレームの転送機能を有効(Enabled)または無効(Disabled)にします。デフォルトは有効です。有効にすると、最大サイズ 9216 バイトのジャンボフレーム(1522 バイトの標準イーサネットフレームサイズよりも大きいフレーム)をスイッチで転送できます。

次のウィンドウを表示するには、L2 Features > Jumbo Frame をクリックします：



[Apply]をクリックして変更を適用します。

3.3.2 802.1Q Static VLAN

このウィンドウには、事前に設定したすべての VLAN が、VLAN ID および VLAN 名に従って一覧表示されます。

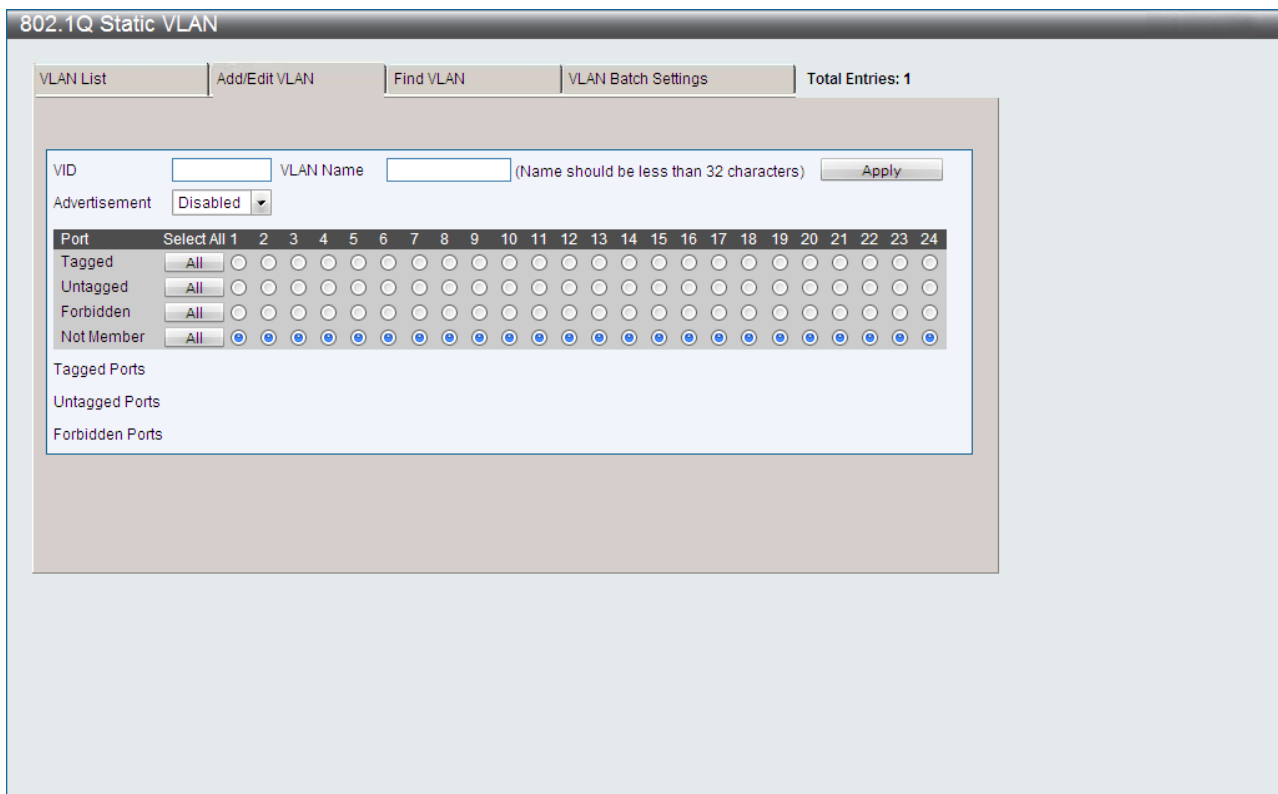
このウィンドウを表示するには、L2 Features > 802.1Q Static VLAN をクリックします：



VID	VLAN Name	Advertisement	Tagged Ports	Untagged Ports	Forbidden Ports
1	default	Enabled		1,2,3,4, 5,6,7,8, 9,10,11,12...	

新しい 802.1Q VLAN エントリーを作成するには、ウィンドウの一番上にある [Add/Edit VLAN] タブをクリックします。次のページの最初の図にあるように、新しいタブが表示されます。ここで、ポートを設定して、新しい VLAN に固有名と番号を割り当てます。

既存の 802.1Q VLAN エントリーを編集するには、上の対応する VLAN エントリーの横にある [Edit] をクリックします。



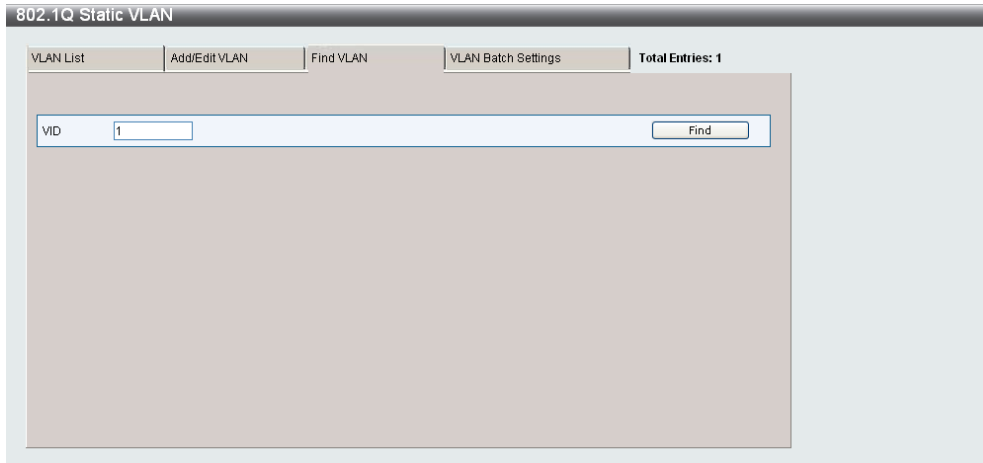
[802.1Q Static VLAN]の最初のウィンドウに戻るには、[VLAN List]タブをクリックします。既存の802.1Q VLAN エントリーを変更するには、相応する[Edit]ボタンをクリックすると、新しいウィンドウが表示されます。ここで、ポートを設定して、新しいVLAN に固有名と番号を割り当てます。新しいウィンドウのパラメーターの説明については、次の表を参照してください。

下記にパラメーターの説明を記載します。

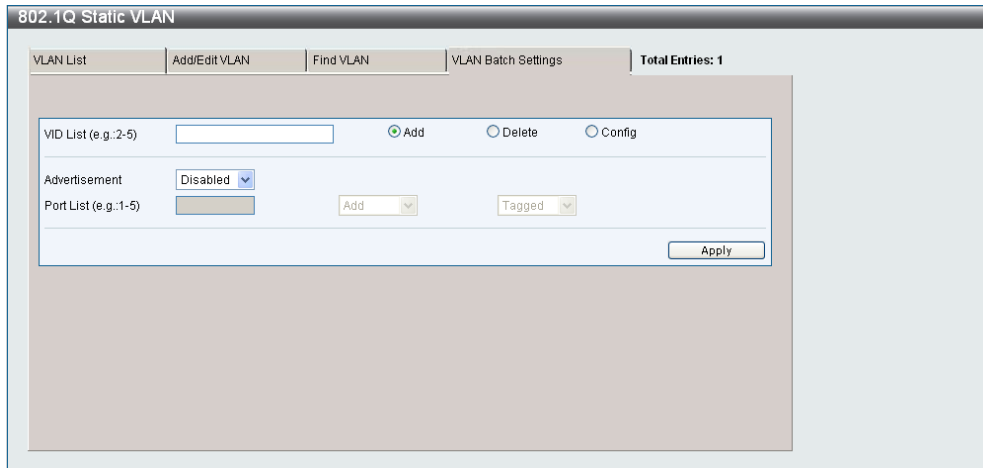
パラメーター	説明
VID	VLAN の[Add/Edit VLAN]タブで、VLAN ID を入力したり、既存のVLAN のVLAN ID を表示します。VLAN はVIDまたはVLAN 名で識別します。
VLAN Name	[Add/Edit VLAN]で、新しいVLAN の名前を入力したり、VLAN の名前を変更します。VLAN 名の長さは32文字以内にします。
Advertisement	この機能を有効にして、スイッチがGVRP パケットを外部ソースに送信して、既存のVLAN を結合できることを通知します。
Port	個別ポートをVLAN のメンバーとして指定します。
Tagged	ポートを802.1Q タグ付きとして指定します。ボックスにチェックを入れると、その対象ポートはタグ付きとして指定されます。
Untagged	ポートを802.1Q タグなしとして指定します。ボックスにチェックを入れると、その対象ポートはタグなしとして指定されます。
Forbidden	この項目を選択することで、対象ポートがダイナミックVLAN のメンバーになることを禁止します。
Not Member	個別ポートをVLAN の非メンバーとして指定します。

[Apply]をクリックして変更を適用します。

VLAN を検索するには、[Find VLAN]タブをクリックし VLAN ID を入力、次に、[Find]をクリックします。VLAN List に事前に設定した VLAN の設定が表示されます。



VLAN バッチエントリーを作成するには、[VLAN Batch Settings]タブをクリックします。次のウィンドウが表示されます：



下記にパラメーターの説明を記載します。

パラメーター	説明
VID List (e.g. :2-5)	VLAN の設定を変更、追加、削除する ID 番号を入力します。
Advertisement	この機能を有効にすることで、スイッチが GVRP パケットを外部ソースに送信し、既存の VLAN を結合できることを通知します。
Port List (e.g. :1-5)	各ポートを VLAN のメンバーとして追加、削除します。
Tagged	ポートを 802.1Q タグ付きとして指定します。ボックスにチェックを入れると、その対象ポートはタグ付きとして指定されます。
Untagged	ポートを 802.1Q タグなしとして指定します。ボックスにチェックを入れると、その対象ポートはタグなしとして指定されます。
Forbidden	この項目を選択して、ポートを VLAN の非メンバーとして指定し、ポートが動的に VLAN のメンバーになることを禁止します。

[Apply]をクリックして変更を適用します。

3.3.3 QinQ

3.3.3.1 QinQ Settings

このウィンドウを使用して、QinQ 機能のパラメーター設定を行います。

次のウィンドウを表示するには、L2 Features> QinQ > QinQ Settings をクリックします：

Port	Role	Outer TPID	VLAN Translation
1	NNI	0x88a8	Disabled
2	NNI	0x88a8	Disabled
3	NNI	0x88a8	Disabled
4	NNI	0x88a8	Disabled
5	NNI	0x88a8	Disabled
6	NNI	0x88a8	Disabled
7	NNI	0x88a8	Disabled
8	NNI	0x88a8	Disabled
9	NNI	0x88a8	Disabled
10	NNI	0x88a8	Disabled
11	NNI	0x88a8	Disabled
12	NNI	0x88a8	Disabled
13	NNI	0x88a8	Disabled
14	NNI	0x88a8	Disabled
15	NNI	0x88a8	Disabled
16	NNI	0x88a8	Disabled
17	NNI	0x88a8	Disabled
18	NNI	0x88a8	Disabled
19	NNI	0x88a8	Disabled
20	NNI	0x88a8	Disabled
21	NNI	0x88a8	Disabled
22	NNI	0x88a8	Disabled
23	NNI	0x88a8	Disabled
24	NNI	0x88a8	Disabled

下記にパラメーターの説明を記載します。

パラメーター	説明
QinQ Global Settings	ラジオボタンで、Enabled または Disabled を選択して、QinQ グローバル設定の有効(Enabled)または無効(Disabled)を設定します。
From Port/To Port	QinQ を設定する対象ポート範囲を指定します。
Role	各ポートのロールを指定します。 UNI - 指定したユーザーと指定したネットワーク間の通信を指定するユーザーネットワークインターフェースを選択します。 NNI - 2つの指定したネットワーク間の通信を指定するネットワーク間インターフェースを指定します。
Outer TPID (hex : 0x1-0xffff)	アウターTPID はパケットの学習と切り替えの際に使用します。アウターTPID で、アウタータグを作成して、VLAN ID と内部優先度に基づいてパケットに挿入します。
VLAN Translation	VLAN 変換を有効(Enabled)または無効(Disabled)にします。これで、プライベートネットワークから受信したデータパックにある VLAN ID を、サービスプロバイダーのネットワークで使用される VLAN ID に変換します。デフォルトは無効(Disabled)です。

[Apply] をクリックして変更を適用します。

3.3.3.2 VLAN Translation CVID Entry Settings

VLAN 変換で、プライベートネットワークから受信したデータパックにある VLAN ID を、サービスプロバイダーのネットワークで使用する VLAN ID に変換します。

次のウィンドウを表示するには、L2 Features > QinQ > VLAN Translation CVID Entry Settings をクリックします：

VLAN Translation CVID Entry Settings

Action: Add (dropdown) | CVID List(1-4094): [] | SVID (1-4094): [] | Apply | Delete All

Total Entries: 0

CVID	SVID	Action
------	------	--------

<<Back | Next>>

下記にパラメーターの説明を記載します。

パラメーター	説明
Action	サービスプロバイダーVLAN ID(SVID)パケットの Add(追加)または Replace(置換)を指定します。
CVID List(1-4094)	タグ付きパケットが追加されるカスタマーVLAN ID 一覧です。
SVID (1-4094)	サービスプロバイダーの VLAN にタグ付きメンバーとして結合するように VLAN を設定します。

[Apply]をクリックして変更を適用します。

[Delete All]をクリックして VLAN 変換エントリーを削除します。

3.3.4 802.1v Protocol VLAN

このウィンドウでプロトコル VLAN グループの作成およびグループへのプロトコル追加の設定を行います。802.1v Protocol Group Settings では、各プロトコルのマルチプル VLAN への対応および同じ物理ポートに対する異なるプロトコルの設定を行います。例えば、ユーザーは 802.1Q と 802.1v を同じ物理ポートにタグなしとして設定することができます。ウィンドウの下側には既に作成した VLAN グループが表示されます。

3.3.4.1 802.1v Protocol Group Settings

次のウィンドウを使用して 802.1v プロトコルグループを設定します。

次のウィンドウを表示するには、L2 Features > 802.1v Protocol VLAN > 802.1v Protocol Group Settings をクリックします：

802.1v Protocol Group Settings

Add Protocol VLAN Group
Group ID (1-16) Group Name
Note: Name should be less than 32 characters .

Add Protocol for Protocol VLAN Group
 Group ID Group Name Protocol Protocol Value (0-FFFF)

Total Entries: 0

Group ID	Group Name	Frame Type	Protocol Value
----------	------------	------------	----------------

下記にパラメーターの説明を記載します。

パラメーター	説明
Group ID (1-16)	グループの ID 番号を 1～16 の範囲で選択します。
Group Name	グループ名によって、新しいプロトコル VLAN グループを識別します。最大 32 文字の英数字文字列を入力します。
Protocol	この機能は、パケットヘッダー内のタイプオクテットを確認して、それに関連するプロトコルの種類を検索することで、パケットをプロトコル定義の VLAN にマップします。プルダウンメニューから、Ethernet または IEEE802.3 SNAP を選択します。(IEEE802.3_LLIC には対応していません)
Protocol Value (0-FFFF)	グループの値を入力します。

[Add]をクリックして新しいエントリーを追加します。

[Delete All]をクリックしてエントリーを削除します。

3.3.4.2 802.1v Protocol VLAN Settings

このウィンドウで、プロトコル VLAN を設定します。ウィンドウの下半分に、事前に作成した設定が表示されます。

次のウィンドウを表示するには、L2 Features > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
Group ID	ラジオボタンをクリックし、事前に設定したグループ ID を選択します。
Group Name	ラジオボタンをクリックして、事前に設定したグループ名を選択します。
VID (1-4094)	ラジオボタンをクリックして VID を入力します。VLAN ID と VLAN 名で、ユーザーが作成したい VLAN を識別します。
VLAN Name	ラジオボタンをクリックして VLAN 名を入力します。VLAN 名と VLAN ID で、ユーザーが作成したい VLAN を識別します。
802.1p Priority	このパラメーターは、スイッチで事前に設定した 802.1p デフォルト優先度を書き直すように指定されています。これを使用して、パケットの転送先となる CoS キューを決めます。このフィールドが指定されると、スイッチが受け入れたこの優先度と一致するパケットが、ユーザーが事前に指定した CoS キューに転送されます。 優先度付きキュー、CoS キュー、および、802.1p のマッピングに関する詳細情報については、本マニュアルの QoS のセクションを参照してください。
Port List (e.g.: 1-6)	All Ports のみ選択できます。
Search Port List	この機能を使用して、事前に設定したポート一覧設定をすべて検索し、テーブルの下半分に表示できます。ポート一覧を検索するには、表示したいポート番号を入力して、[Find] をクリックします。事前に設定したポート一覧をすべてウィンドウの下半分に表示するには、[Show All] をクリックします。事前に設定したポート一覧をすべて消去するには、[Delete All] をクリックします。

[Add] をクリックして新しいエントリーを追加します。

[Find] をクリックして入力された条件で検索します。

[Show All] をクリックして全てのエントリーを表示します。

[Delete All] をクリックして全てのエントリーを削除します。

3.3.5 GVRP Settings

このウィンドウで、スイッチが、その他の GARP VLAN 登録プロトコル(GVRP)対応スイッチと VLAN 設定情報を共有するかどうかを決定します。さらに、イングレスチェックを使用して、PVID がポートの PVID と一致しない受信パケットをフィルタリングすることができます。

このウィンドウを表示するには、L2 Features > GVRP Settings をクリックします：

Port	PVID	Reassigned PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	--	Disabled	Enabled	All
2	1	--	Disabled	Enabled	All
3	1	--	Disabled	Enabled	All
4	1	--	Disabled	Enabled	All
5	1	--	Disabled	Enabled	All
6	1	--	Disabled	Enabled	All
7	1	--	Disabled	Enabled	All
8	1	--	Disabled	Enabled	All
9	1	--	Disabled	Enabled	All
10	1	--	Disabled	Enabled	All
11	1	--	Disabled	Enabled	All
12	1	--	Disabled	Enabled	All
13	1	--	Disabled	Enabled	All
14	1	--	Disabled	Enabled	All
15	1	--	Disabled	Enabled	All
16	1	--	Disabled	Enabled	All
17	1	--	Disabled	Enabled	All
18	1	--	Disabled	Enabled	All
19	1	--	Disabled	Enabled	All
20	1	--	Disabled	Enabled	All
21	1	--	Disabled	Enabled	All
22	1	--	Disabled	Enabled	All
23	1	--	Disabled	Enabled	All
24	1	--	Disabled	Enabled	All

下記にパラメーターの説明を記載します。

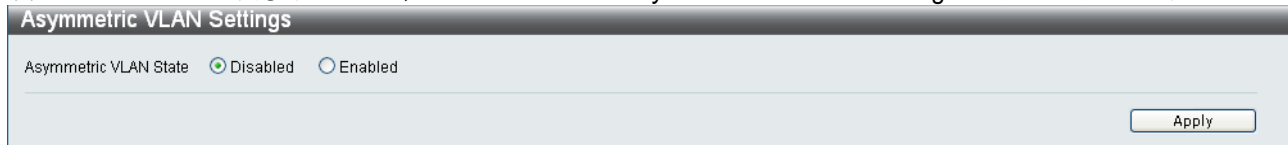
パラメーター	説明
GVRP State Settings	ラジオボタンで、Enabled または Disabled を選択して、GVRP グローバル設定の有効(Enabled)または無効(Disabled)を設定します。
From Port/To Port	作成するポートベース VLAN に含むポート範囲を指定します。
PVID (1-4094)	各ポートの PVID 割り当てを入力します。802.1Q ポート設定テーブルで作成する際に、手動で VLAN に割り当てることができます。スイッチのデフォルトでは、すべてのポートに VID 1 の default VLAN が割り当てられています。
GVRP	グループ VLAN 登録プロトコル(GVRP)で、ポートが動的に VLAN のメンバーになれるようにします。GVRP のデフォルト設定は無効です。
Ingress Checking	Ingress Checking で Enabled を選択すると本装置の全ポートにおいて、受信パケットの VLAN ID と受信ポートの VLAN ID が異なる場合に、パケットが破棄されます。デフォルト設定は「Enabled」有効です。
Acceptable Frame Type	このフィールドで、ポートが受け入れるフレームの種類を決めます。Tagged Only を選択した場合は、タグ付きのフレームのみ受け入れます。All を選択した場合は、タグ付きまたはタグなしフレームを受け入れます。デフォルトでは、All が有効になっています。

[Apply]をクリックして変更を適用します。

3.3.6 Asymmetric VLAN Settings

共有 VLAN 学習は、アシンメトリック VLAN の主要要件の 1 つです。通常の条件では、VLAN 環境内で通信する 2 つのデバイスは、同じ VLAN を使用して送受信します。しかし、2 つの異なる VLAN を使用すると便利な場合があります(クライアントが個別の IP サブネット上にある場合、または、機密性に関連する必要からクライアント間のトラフィックを分割する場合など)。

次のウィンドウを表示するには、L2 Features > Asymmetric VLAN Settings をクリックします：



下記にパラメーターの説明を記載します。

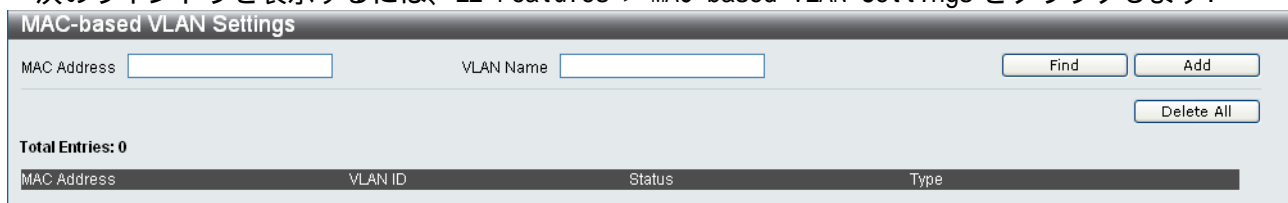
パラメーター	説明
Asymmetric VLAN State	ラジオボタンで、Enabled または Disabled を選択して、asymmetric VLAN の有効(Enabled)または無効(Disabled)を設定します。

[Apply] をクリックして変更を適用します。

3.3.7 MAC-based VLAN Settings

このウィンドウを使用して、スイッチ上に MAC ベース VLAN エントリーを作成します。MAC アドレスは既存の静的 VLAN のいずれかにマップします。複数の MAC アドレスは同じ VLAN にマップされます。静的 MAC ベース VLAN エントリーをユーザー用に作成した場合は、このユーザーからのトラフィックは指定した VLAN に転送されます。そのため、各エントリーで、送信先 MAC アドレスと VLAN の関係を指定します。

次のウィンドウを表示するには、L2 Features > MAC-based VLAN Settings をクリックします：



下記にパラメーターの説明を記載します。

パラメーター	説明
MAC Address	マップする MAC アドレスを指定します。
VLAN Name	事前に設定した VLAN の VLAN 名を入力します。

[Find] をクリックして入力されたパラメーターに関するエントリーを検索します。

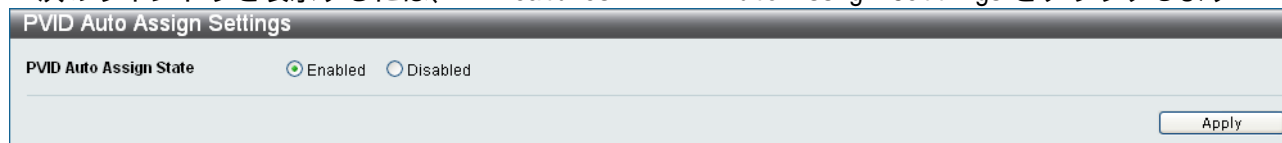
[Add] をクリックして新しいエントリーを追加します。

[Delete All] をクリックして全てのエントリーを削除します。

3.3.8 PVID Auto Assign Settings

スイッチ上の PVID 自動割り当てを有効または無効にします。PVID は、スイッチがフォワーディングおよびフィルタリングを目的に使用する VLAN です。PVID 自動割り当てが有効な場合は、事前に設定した PVID 設定、または、VLAN 設定で PVID を変更することができます。ユーザーがポートを VLAN のタグなしメンバーシップに設定すると、このポートの PVID は、設定した VLAN で更新されます。VLAN 一覧コマンドでは、PVID は VLAN 一覧上の最後の項目で更新されます。ユーザーがポートを PVID の VLAN のタグなしメンバーシップから削除すると、ポートの PVID はデフォルト VLAN に割り当てられます。PVID 自動設定が無効な場合は、PVID は PVID 設定でしか変更できません(ユーザーが明示的に変更します)。VLAN 設定では PVID は自動的に変更されません。デフォルト設定は有効です。

次のウィンドウを表示するには、L2 Features > PVID Auto Assign Settings をクリックします：



下記にパラメーターの説明を記載します。

パラメーター	説明
PVID Auto Assign State	ラジオボタンで、Enabled または Disabled を選択して、PVID Auto Assign の有効(Enabled)または無効(Disabled)を設定します。





[Apply] をクリックして変更を適用します。

3.3.9 Link Aggregation

リンクアグリゲーション(ポートトランク)について

リンクアグリゲーションを使用して、ポートの番号を組み合わせ、単一の高帯域幅データパイプラインを作成します。スイッチは、最大 8 のリンクアグリゲーショングループに対応します。各グループを構成するポート数は 2~8 です。

注意事項

-  GM シリーズのリンクアグリゲーショングループ数の最大は APLGM118GTSS/PoE/PoE2 と APLGM124GTSS/PoE/PoE2 で 8、それ以外は製品搭載ポート数 ÷ 2 となります。
-  メンバーポートとして、ユーザーポートとコンボポートを組み合わせることは出来ません。
-  認証機能 (MAC 認証、Web 認証、802.1X 認証) とのポート併用はできません。
-  GM シリーズではアルゴリズムが ip_source または ip_destination の場合、Unknown unicast、Broadcast、及び Multicast のフレームはロードシェアされません。

リンクアグリゲーションで、複数のポートをグループ化して、単一リンクとして動作するようにできます。これによって、単一リンクの帯域幅をまとめた帯域幅が得られます。

通常、リンクアグリゲーションを使用して、サーバーなどの帯域幅集中ネットワークデバイスあるいは複数のデバイスをネットワークのバックボーンにリンクします。

スイッチでは、最大 8 のリンクアグリゲーショングループを作成できます。各グループは 2~8 のリンク(ポート)で構成されます。グループ内のすべてのポートは同じ VLAN のメンバーである必要があります。また、その STP 状態、静的マルチキャスト、トラフィック制御、トラフィック分布、802.1p デフォルト優先度設定は同じでなければなりません。ポートセキュリティ、ポートミラーリング、802.1X は、リンクアグリゲーショングループ上で有効にできません。さらに、集合されたリンクはすべて同じ速度で、全二重として設定する必要があります。

すべての設定オプション(マスターポートに適用する VLAN 設定を含みます)は、リンクアグリゲーショングループ全体に適用されます。

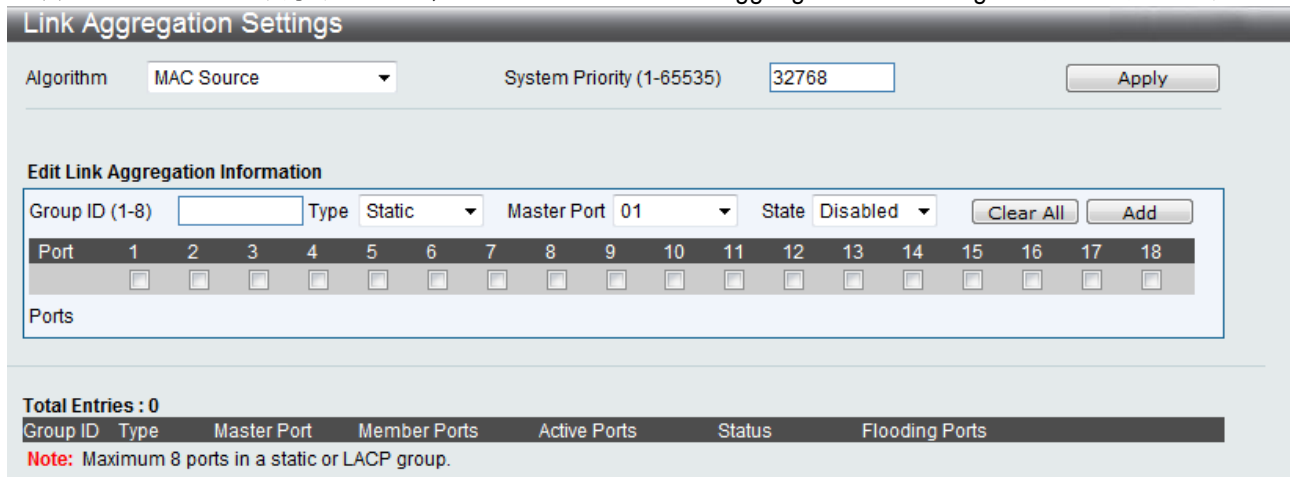
集合したグループ内のポートには、負荷分散が自動的に適用されます。また、グループ内にリンクエラーが発生すると、ネットワークトラフィックはグループ内のその他のポートに割り振ります。

スイッチレベルでは、スパニングツリープロトコルは、リンクアグリゲーショングループを単一リンクとして扱います。ポートレベルでは、スパニングツリープロトコルは、マスターポートのポートパラメーターを使用して、ポートコストを計算したり、リンクアグリゲーショングループの状態を定めます。スイッチ上に 2 つの冗長リンクアグリゲーショングループが設定されている場合は、STP は 1 つのグループ全体をブロックします。STP は冗長リンクのある単一ポートも同様にブロックします。

3.3.9.1 Link Aggregation Settings

このウィンドウを使用して、トランクポートのグループ設定を行います。ウィンドウの下半分に、事前に作成したグループが表示されます。

次のウィンドウを表示するには、L2 Features > Link Aggregation Settings をクリックします：



下記にパラメーターの説明を記載します。

パラメーター	説明
Algorithm	スイッチがトランクグループを構成するポート間で負荷分散する際に使用するアルゴリズムを設定します。 分散アルゴリズムは、MAC Source/MAC Destination/MAC Source Destination/IP Source/IP Destination/IP Source Destination から選択します。
System Priority	LACP の装置優先度を 1 ~ 65535 の範囲で設定します。値が小さいほど優先度が高くなります。デフォルト値は 32768 です。
Group ID	トランクグループの ID 番号を 1 ~ 8 で選択します。 ID の設定範囲は装置によって異なります。
Type	プルダウンメニューで、Static、LACP(リンクアグリゲーション制御プロトコル)のいずれかを選択します。LACP を選択すると、相手装置とネゴシエーションを行いトランクグループを構成します。
Master Port	プルダウンメニューで、トランクグループのマスターポートを選択します。
State	プルダウンメニューから、Enabled または Disabled を選択して、トランクグループの有効(Enabled)または無効(Disabled)を設定します。
Active Ports	トランクグループの動作可能なポートを表示します。
Ports	トランクグループのメンバーポートを選択します。1 つのグループに最大 8 つのポートを割り当てることができます。
Flooding Ports	このポートでは、ブロードキャスト、マルチキャスト、宛先不明パケットを、フラディングします。ポートは自動で選択されます。

[Apply] をクリックして変更を適用します。

[Clear All] をクリックしてフィールドからの全ての入力データをクリアーします。

3.3.9.2 Link Aggregation Settings

このウィンドウを使用して、LACP 制御フレームの処理モード、タイムアウト値、ポート優先度を設定します。

次のウィンドウを表示するには、L2 Features > LACP Port Settings をクリックします：

LACP Port Settings

From Port: To Port: Activity: LACP Timeout: Port Priority (1-65535):

Port	Activity	LACP Timeout	Port Priority
1	Passive	Short	32768
2	Passive	Short	32768
3	Passive	Short	32768
4	Passive	Short	32768
5	Passive	Short	32768
6	Passive	Short	32768
7	Passive	Short	32768
8	Passive	Short	32768
9	Passive	Short	32768
10	Passive	Short	32768
11	Passive	Short	32768
12	Passive	Short	32768
13	Passive	Short	32768
14	Passive	Short	32768
15	Passive	Short	32768
16	Passive	Short	32768
17	Passive	Short	32768
18	Passive	Short	32768

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	選択したポートから始まるポートのグループを設定します。
Activity	Active - アクティブ指定の LACP ポートは、LACP 制御フレームを送信します。これにより、LACP 準拠デバイスはポートグループを必要に応じて動的に調整します。ポートグループを動的に変更するには、相手デバイスも LACP に対応できなければなりません。 Passive - パッシブ指定の LACP ポートでは、始めに LACP 制御フレームを送信することができません。リンクしたポートグループで調整し、動的に変更するには、接続した一方のデバイスがアクティブの必要があります。
LACP Timeout	対向装置から受信する LACP 制御フレームの受信タイムアウト時間を設定します。デフォルト設定は、「short」です。 short - LACP の受信タイムアウト時間を 3 秒に設定します。 long - LACP の受信タイムアウト時間を 90 秒に設定します。
Port Priority (1-65535)	LACP のポート優先度を 1 ~ 65535 の範囲で設定します。値が小さいほど優先度が高くなります。デフォルト値は 32768 です。

[Apply] をクリックして変更を適用します。

3.3.10 Traffic Segmentation

Traffic Segmentation を使用して、スイッチ上の単一ポートからポートのグループへのトラフィックを制限します。このトラフィックフローセグメントは、VLAN を使用してトラフィックを制限する方法と似ていますが、VLAN を使う場合よりもトラフィックを制限します。これは、スイッチ CPU のオーバーヘッドを増加せずにトラフィックを制限する方法です。このウィンドウで、スイッチ上のその他のポートにパケットを転送できるスイッチ上のポートを表示します。特定のポートの新しいフォワーディングポートを設定するには、最初のポートプルダウンメニューと最後のポートプルダウンメニューからポートを選択して、次に、[Apply] をクリックします。

次のウィンドウを表示するには、L2 Features > Traffic Segmentation をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	トラフィックを制限する対象のポートを入力します。
Forward Portlist	パケットを転送できるスイッチ上のポートを選択します。これらのポートは、From Port/To Port で指定したポートからパケットを受信します。

[Clear All] をクリックして全て選択解除します。

[Select All] をクリックして全て選択します。

[Apply] をクリックして変更を適用します。

3.3.11 BPDU Guard Settings

このウィンドウを使用して、BPDU Guardのパラメーターを設定します。

次のウィンドウを表示するには、L2 Features > BPDU Guard Settings をクリックします：



Port	State	Mode	Status
1	Disabled	Shutdown	Normal
2	Disabled	Shutdown	Normal
3	Disabled	Shutdown	Normal
4	Disabled	Shutdown	Normal
5	Disabled	Shutdown	Normal
6	Disabled	Shutdown	Normal
7	Disabled	Shutdown	Normal
8	Disabled	Shutdown	Normal
9	Disabled	Shutdown	Normal
10	Disabled	Shutdown	Normal

下記にパラメーターの説明を記載します。

パラメーター	説明
BPDU Guard Global State	ラジオボタンで、Enabled または Disabled を選択して、BPDU Guard Global の有効(Enabled)または無効(Disabled)を設定します。
Log Status	BPDU ガードログを設定します。プルダウンメニューで None、Attack Detected、Attack Cleared、Both から選択します。Attack Detected は BPDU フレーム検知時にログを出力します。Attack Cleared は自動復帰時やコマンドでの手動復旧時にログを出力します。Both は両方でログを出力します。
Recovery Time	BPDU ガード状態から自動復帰する時間を 60 ~ 1,000,000 秒の範囲で指定します。デフォルト値は 60 秒です。Infinite を指定すると自動復帰しません。
From Port/To Port	設定するポートの範囲指定をします。
State	プルダウンメニューで Enabled または Disabled を選択して、指定したポートに BPDU ガード機能の有効(Enabled)または無効(Disabled)を設定します。
Mode	BPDU ガードモードを設定します(本バージョンは Shutdown のみ対応)。
Status	ポートの BPDU ガード機能の動作状態が表示されます。通常動作(Normal)またはガード状態(Err-Disabled)が表示されます。

[Apply]をクリックして変更を適用します。

注意事項

-  BPDU ガード機能が有効なポートでは、スパニングツリー機能は設定できません。
-  BPDU ガード機能が対象とするパケットは、スイッチでサポートする IEEE802.1D BPDU(STP/RSTP/MSTP)となります。

3.3.12 IGMP Snooping

IGMP スヌーピングを使用するには、まず、グローバル設定を有効にします。次に、L2 Features > IGMP Snooping ウィンドウを使用して、各 VLAN を設定します。IGMP スヌーピングを有効にすると、スイッチは、デバイスから IGMP ホストへ送信される IGMP メッセージ、または、IGMP ホストからデバイスへ送信される IGMP メッセージに基づいて、特定のマルチキャストグループメンバーへのポートを開いたり閉じることができます。スイッチは、IGMP メッセージを監視して、ホストからの続行の要求が終了すると、マルチキャストパケットの転送を中止します。

3.3.12.1 IGMP Snooping Settings

このウィンドウを使用して、スイッチ上の IGMP スヌーピングのグローバル設定を有効または無効にします。

次のウィンドウを表示するには、L2 Features > IGMP Snooping > IGMP Snooping Settings をクリックします：

VID	VLAN Name	State
1	default	Disabled

[Apply]をクリックして変更を適用します。

[Edit]をクリックして特定入力を再設定します。

[Edit]をクリックして、このウィンドウを開きます：

VLAN ID	1	VLAN Name	default
Querier Expiry Time	0 sec	Querier IP	0.0.0.0
Max Response Time (1-25)	10 sec	Query Interval (1-65535)	125 sec
Last Listener Query Interval (1-25)	1 sec	Robustness Value (1-255)	2
Querier State	Disabled	Fast Done	Disabled
State	Disabled	Querier Role	Non-Querier
Version	3		

下記にパラメーターの説明を記載します。

パラメーター	説明
VLAN ID	VLAN ID と VLAN 名で、ユーザーが IGMP スヌーピング設定を変更したい VLAN を識別します。
VLAN Name	VLAN 名と VLAN ID で、ユーザーが IGMP スヌーピング設定を変更したい VLAN を識別します。
Querier Expiry Time	クエリー有効時間を表示します。
Querier IP	ネットワークの IGMP クエリーとして動作するデバイスの IP アドレスです。

パラメーター	説明
Max Response Time (1-25)	メンバーからのレポートを待つ最大時間を秒単位で決めます。1~25秒の値を設定します。デフォルトは10秒です。
Query Interval (1-65535)	IGMP クエリーを送信する時間間隔を秒単位で設定します(1~65535秒)。デフォルトは125秒です。
Last Listener Query Interval (1-25)	グループ特有クエリーメッセージの最大時間間隔を指定します。応答としての送信でグループメッセージを残したものを含みます。デフォルトは1です。
Robustness Value (1-255)	推定されるパケットロスに従って、この変数を調整します。VLAN上のパケットロスが高いことが推定される場合は、ロバストネス変数を高くして、パケットロスの増加に対応できるようにします。1~255の値を設定します。デフォルトは2です。
Querier State	プルダウンメニューから、Enabledを選択して、IGMP クエリーパケットの送信を有効にします。または、Disabledを選択して、IGMP クエリーパケットの送信を無効にします。デフォルトは無効(Disabled)です。
Fast Done	プルダウンメニューから、Enabledを選択すると、Fast Doneが有効となり、スイッチがIGMP 脱退レポートパケットを受信すると、マルチキャストグループのメンバーがグループを直ちに脱退できるようになります(最終メンバークエリータイマーは必要ありません)。デフォルトは無効(Disabled)です。
State	プルダウンメニューから、Enabledを選択して、IGMP スヌーピングが有効になります。デフォルトは無効(Disabled)です。
Querier Role	この読み取り専用フィールドは、クエリーパケット送信用のスイッチの動作を説明します。クエリーは、スイッチがIGMP クエリーパケットを送信することを意味します。Non-Querierは、スイッチがIGMP クエリーパケットを送信しないことを示します。クエリー状態フィールドと状態フィールドを有効に切り替えると、このフィールドはクエリーだけを読み取ります。
Version	スイッチ上で使用するIGMPバージョンを設定します。デフォルト値は3です。

[<<Back]をクリックして以前のウィンドウに戻ります。

[Apply]をクリックして変更を適用します

IGMP スヌーピングルーターポート設定を変更するには、[Modify Router Port] ハイパーリンクをクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
Static Router Port	このセクションはマルチキャスト対応のルーターに接続される一連のポートを指定するために使用されます。 これは、ルーターの宛先を備えたパケットが全てのプロトコルに関わらずマルチキャスト対応のルーターに到達することを保証します。
Forbidden Router Port	このセクションはマルチキャスト対応のルーターに接続されない一連のポートを指定するために使用されます。 これは、禁止されたルーターポートがルーティングパケットを転送しないことを保証します。
Dynamic Router Port	ダイナミックに設定されたルーターポートを表示します。
Ports	ルーターポート配置にそれらを含めるために適切なポートを個々に選択してください。

[Select All]をクリックして全て選択します。

[Clear All]をクリックして全て選択解除します。

[Apply]をクリックして設定を適用します

[<<Back]をクリックして以前のウィンドウに戻ります。

3.3.13 MLD Snooping Settings

MLD スヌーピングは IPv6 におけるスヌーピング機能で、IPv4 における IGMP スヌーピングのように使用します。これを使用して、マルチキャストデータを要求している VLAN 上のポートを探索します。選択した VLAN 上にあるすべてのポートにマルチキャストトラフィックをフラッドする代わりに、MLD スヌーピングでは、要求しているポートとマルチキャストトラフィックの送信元により作成されたクエリーとレポートを使い、受信を希望するポートだけにマルチキャストデータを転送します。

MLD スヌーピングを実行するには、エンドノードと MLD ルーターの間で送信される MLD 制御パケットのレイヤー3 部分を確認します。このルートがマルチキャストトラフィックを要求していることが分かると、スイッチは、そのルートに直接接続されているポートを正しい IPv6 マルチキャストテーブルに挿入して、そのポートにマルチキャストトラフィックを転送します。マルチキャストルーティングテーブルのこのエントリーは、ポート、VLAN ID、および、関連するマルチキャスト IPv6 マルチキャストグループアドレスを記録して、このポートをアクティブな待ち受けポートとみなします。アクティブな待ち受けポートは、マルチキャストグループデータを受信できるもののみです。

本装置は、MLD スヌーピングバージョン 1 とバージョン 2 に対応しています。

注意事項



MLD スヌーピングバージョン 2 のソースフィルタリング機能は未サポートです。

MLD 制御メッセージ

MLD スヌーピングバージョン 1 では、デバイス間で 3 種類のメッセージが送信されます。これらの 3 つのメッセージはすべて、3 つの ICMPv6 パケットヘッダー (130、131、132 のラベルが付いています) で定義します。

- (1) マルチキャストリスナークエリー、バージョン 1 - IPv4 の IGMPv2 ホストメンバーシップクエリーと似ています。ICMPv6 パケットヘッダー内で 130 のラベルが付いています。ルーターはこのメッセージを送信して、マルチキャストデータを要求しているリンクの有無を照会します。ルーターは、2 種類の MLD クエリーメッセージを生成します。一般クエリーを使用して、マルチキャストデータをすべての待ち受けポートに送信する準備が完了したマルチキャストアドレスをすべてアドバタイズします。マルチキャスト特有クエリーは、準備が完了した特定のマルチキャストアドレスをアドバタイズします。これら 2 種類のメッセージは、IPv6 ヘッダーにあるマルチキャスト送信先アドレスとマルチキャストリスナークエリーメッセージ内のマルチキャストアドレスで識別します。
- (2) マルチキャストリスナーレポート、バージョン 1 - IGMPv2 のホストメンバーシップレポートと似ています。ICMPv6 パケットヘッダー内で 131 のラベルが付いています。待ち受けポートは、マルチキャストリスナークエリーメッセージへの応答で、マルチキャストアドレスからマルチキャストデータを受信することを希望する旨をスイッチに対して送信します。
- (3) マルチキャストリナー脱退 - IGMPv2 のグループ脱退メッセージと似ています。ICMPv6 パケットヘッダー内で 132 のラベルが付いています。このメッセージを送信するのは、特定のマルチキャストグループアドレスからのマルチキャストデータの受信を希望せず、このアドレスからのマルチキャストデータに関し、脱退の旨を伝えるマルチキャスト待ち受けポートです。このメッセージを受信すると、特定のマルチキャストグループアドレスからのマルチキャストトラフィックをこの待ち受けポートへ転送することを中止します。

MLD スヌーピングバージョン 2 では、デバイス間で 2 種類のメッセージが送信されます。これらの 2 つのメッセージは、2 つの ICMPv6 パケットヘッダー (130 および 143 のラベルが付いています) で定義します。

- (1) マルチキャストリスナークエリー、バージョン 2 - IPv4 の IGMPv3 メンバーシップクエリーと似ています。ICMPv6 パケットヘッダー内で、130 のラベルが付いています。ルーターはこのメッセージを送信して、マルチキャストデータを要求しているリンクの有無を照会します。MLD スヌーピングバージョン 2 では、ルーターは次の 3 種類の MLD クエリーメッセージを生成します。

- 1) ルーターは、一般クエリーメッセージを送信して、接続したリンク上にリスナーがあるマルチキャストアドレスを学習します。一般クエリーでは、マルチキャストアドレスフィールドと送信元の数フィールドは 0 に設定されています。
- 2) ルーターは、マルチキャストアドレス特有クエリーメッセージを送信して、接続したリンク上に特定のマルチキャストアドレスのリスナーがあるかどうかを学習します。マルチキャストアドレス特有クエリーでは、マルチキャストアドレスフィールドに、ルーターが関心のあまるマルチキャストアドレスが含まれます。送信元の数フィールドは 0 に設定されています。

3) ルーターは、マルチキャストアドレスおよび送信元特有クエリーを送信して、接続したリンク上に、特定のマルチキャストアドレスの指定した一覧にある送信元のリスナーがあるかどうかを学習します。マルチキャストアドレスおよび送信元特有クエリーでは、マルチキャストアドレスフィールドに、ルーターが関心のあるマルチキャストアドレスが含まれます。送信元アドレスフィールドには、ルーターが関心のある送信元アドレスが含まれます。

(2) マルチキャストリスナーレポート、バージョン 2 - IGMPv3 のホストメンバーシップレポートと似ています。ICMP パケットヘッダー内で 143 のラベルが付いています。待ち受けポートは、マルチキャストリスナークエリーメッセージへの応答で、スイッチに対し、マルチキャストアドレスからマルチキャストデータを受信することを希望するメッセージを送信します。

このウィンドウを使用して、スイッチ上で MLD スヌーピングを有効にして、MLD スヌーピングの設定を設定します。MLD スヌーピング状態を有効にするには、MLD スヌーピンググローバル設定にある [Enabled] を選択し、次に、[Apply] をクリックします。

このウィンドウを表示するには、L2 Features > MLD Snooping Settings をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
MLD Snooping State	ラジオボタンで、Enabled または Disabled を選択して、MLD Snooping Global Settings を有効(Enabled) または無効(Disabled) に設定します。

[Apply] をクリックして変更を適用します。

[Edit] をクリックして入力済みのエントリーを修正します。

既存のエントリーを設定するには、相応する [Edit] をクリックします。次のウィンドウが表示されます。

下記にパラメーターの説明を記載します。

パラメーター	説明
VLAN ID	MLD スヌーピング設定を変更する VLAN ID を識別します。
VLAN Name	MLD スヌーピング設定を変更する VLAN 名を識別します。
Query Interval (1-65535)	クエリー間隔フィールドを使用して、MLD クエリーを送信する時間間隔を秒単位で設定します(1~65535 秒)。デフォルトは、125 秒です。
Max Response Time (1-25)	メンバーからのレポートを待つ最大時間を秒単位で決めます(1~25 秒)。デフォルトは 10 秒です。
Robustness Value (1-255)	VLAN 上のパケットロスが高いと推定される場合は、ロバストネス変数を高くして、パケットロスの増加に対応できるようにします。デフォルトは 2 です。
Last Listener Query Interval (1-25)	グループ特有クエリーメッセージの最大時間間隔を指定します。応答としての送信でグループメッセージを残したものを含みます。デフォルトは 1 です。
Fast Done	プルダウンメニューから、Enabled を選択すると、Fast Done が有効となり、スイッチが MLD 脱退レポートパケットを受信すると、マルチキャストグループのメンバーがグループを直ちに脱退できるようになります(最終メンバークエリータイマーは必要ありません)。デフォルトは無効(Disabled)です。
State	プルダウンメニューから、Enabled を選択すると、MLD スヌーピングが有効になります。デフォルトは無効(Disabled)です。
Version	MLD バージョンが表示されます(ここでは、変更不可)。
Querier Role	このフィールドは、クエリーパケット送信用のスイッチの動作を説明します。クエリーは、スイッチが MLD クエリーパケットを送信することを意味します。Non-Querier は、MLD クエリーパケットを送信しないことを意味します。

[Apply]をクリックして変更を適用し、[<<Back]をクリックして初期[MLD Snooping Settings]ウィンドウに戻ります。

[MLD Snooping Router Ports Settings]を変更するには、[Modify Router Port]ハイパーリンクをクリックします。

希望するルーターポートを選択し、[Apply]をクリックして変更を適用します。選択したすべてのルーターポートを消去する場合は、相応する[Clear All]をクリックします。[<<Back]をクリックして、[MLD Snooping Settings]ウィンドウに戻ります。

3.3.14 Port Mirror

スイッチのポート上で送受信したフレームをコピーして、コピーを他のポートにリダイレクトすることが可能です。 スニファーマーやRMONプロンプなどの監視デバイスをミラーポートに取り付けて、対象ポートを通過するパケットに関する詳細を表示します。この機能は、ネットワーク管理やトラブルシューティングの際に役に立ちます。

次のウィンドウを表示するには、L2 Features > Port Mirror をクリックします：

Sniffer Mode	Ports
Tx	
Rx	
Both	
None	

Sniffer Mode	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tx	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Rx	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Both	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
None	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

下記にミラーポートの設定手順を記載します。

- (1) ミラーポートの設定を有効に変更します。
- (2) ターゲットポートを選択します。ターゲットポートは送信元ポートからコピーを受信します。
- (3) 送信元ポートを選択します。送信元ポートからフレームを送信します。
- (4) [Apply]をクリックして変更を有効にします。

注意事項

- ❗ リンクアグリゲーションポートをミラーリングする場合、LAG 所属ポートの全てをミラー元として設定してください。
- ❗ 送信フレームのミラーリングでは、タグなしフレームの場合も送信フレームのVLAN タグ付きフレームでミラーリングします。
- ❗ Target ポートに VLAN がアサインされている場合、Target ポートに接続したデバイスからのフレームは VLAN 内に送出されます。アサイン VLAN を削除することにより Target ポートからのフレーム送出を回避することができます。

3.3.15 Loopback Detection Settings

ループ防止機能を設定します。


次のウィンドウを表示するには、L2 Features > Loopback Detection Settings をクリックします：


下記にパラメーターの説明を記載します。


パラメーター	説明
State(Global)	ラジオボタンで、Enabled または Disabled を選択して、スイッチの Loopback Detection 機能の有効(Enabled)または無効(Disabled)を設定します。デフォルト設定は無効(Disabled)です。ループ防止機能によりループを検知している状態では、本装置の console LED を点滅させる LED 点滅可視化機能を実装しています。
Interval (1-32767)	ループ防止機能が有効なポートから送信されるループ検知パケット(CTP : Configuration Test Protocol)の送信間隔(秒)を設定します。設定範囲は 1 ~ 32767 です。デフォルト値は 10 秒です。
Mode	ポートベースモードとしてループ防止機能が動作します。ポートベースモードでは、ループが検出されると、ポートは無効になります。
Recover Time (0 or 60-1000000)	ループ発生状態から自動復旧までの時間(秒)を設定します。 [0]を設定した場合、自動復旧が無効になるため手動による復旧が必要になります。手動で復旧させる場合は、Loop Port State 「Disabled」(無効)および「Enabled」(有効)の設定で初期化します。 設定範囲は、60 ~ 1000000 です。デフォルト値は 60 秒です。
From Port/To Port	ループ防止機能を設定するポート範囲を指定します。
State (Port)	プルダウンメニューから、Enabled または Disabled を選択して、指定したポートの Loopback Detection 機能を有効(Enabled)または無効(Disabled)に設定します。デフォルト設定は無効(Disabled)です。
Method	プルダウンメニューから、ループ防止機能を設定したポートのループ検知動作を shutdown(ポート閉塞する)または drop(ループ検知するが、ポート閉塞しない)のどちらかを指定します。

[Apply]をクリックして変更を適用します。

注意事項

-  ループ防止機能は、機器毎に識別されたループ検知パケットを自装置内ポートで受信することでループ検知と判断します。このループ検知パケットは、Tag VLANには対応しておりません。(TagポートでもTag付与されずに送出されます)そのため、対向機器で転送するにはNative VLANを設定する必要があります。
 - ・ver.1.00.00以前では、ループ検知パケットを「自送出ポートで受信」することでループを検知します。
 - ・ver.1.01.00以降では、ループ検知パケットを「自装置内ポートで受信」することでループを検知します。

-  LED点滅可視化機能により、ループ検知時にCONSOLE LED点滅状態が変わります。
(ループ検知が解除された場合にはLED点滅も同時に解除されます)
 - ・ver.1.02.00以前では、ループ検知してもCONSOLE LEDは点滅しません。
 - ・ver.1.03.00以降では、ループ検知している状態でCONSOLE LEDが点滅します。

-  ループ防止機能にてループ検知した場合、速やかにループ原因を取り除いて下さい。ループ検知状態からリカバリー時間(デフォルト60秒)経過すると自動復旧が行われます。ループ状態である場合、次のループ検知まで一時的なループ再発となり、ネットワーク全体が不安定な状態になります。ループ発生源を早期に特定できない場合には、自動復旧を無効とするリカバリー時間(0秒)を設定として、手動復旧に設定されることを推奨します。

3.3.16 Spanning Tree

スイッチは、STP、RSTP、MSTP に対応しています。

802.1Q-2005 MSTP

MSTP は、IEEE802 で定義されている規格です。MSTP により、複数の VLAN を単一のツリーインターフェースにマップすることができます。これにより、ネットワーク全体で複数のパスウェイを提供します。したがって、これらの MSTP 構成で、トラフィック負荷を分散し、単一のスパニングツリーインターフェースが故障しても、失敗したインスタンスの新しいトポロジーを高速収束できます。これらの VLAN 用のフレームは、インターコネクトブリッジ経由で、3つのスパニングツリープロトコル (STP、RSTP、MSTP) のいずれかを使用して、すばやく処理されます。

また、このプロトコルは、BPDU パケットにタグを付けるので、受信デバイスは、スパニングツリーインスタンス、スパニングツリー範囲、および、それらに関連する VLAN を識別できます。MSTI ID でこれらのインスタンスを分類します。MSTP で、マルチプルスパニングツリーをコモンアンドインターナルスパニングツリー (CIST) と接続します。CIST は、各 MSTP 範囲とその最大拡張を自動的に決めて、シングルスパニングツリーを実行する 1つの仮想ブリッジとして表示されます。そのため、異なる VLAN に割り当てられたフレームは、ネットワーク上の管理上確立された範囲内で異なるデータルートを流れるので、VLAN またはその対応スパニングツリーを定義する際の管理上のエラーに関わらず、フレームを簡単な方法で処理できます。

ネットワーク上で MSTP を使用する各スイッチには、単一の MSTP 構成があります。この構成には、次の 3つの属性があります：

- (1) 最大 32 文字の英数字文字列で定義する構成名(構成名フィールドにある [MST Configuration identification]で定義します)。
- (2) 構成レビジョン番号(ここでは、レビジョンレベルという名前が付いています。[MST Configuration identification]ウィンドウにあります)。
- (3) 4094 エlementテーブル(ここでは、[MST Configuration identification]ウィンドウ内で VID 一覧として定義されています)。このテーブルで、スイッチが対応する 4094 個の VLAN をそれぞれ該当するインスタンスに関連付けます。

スイッチ上で MSTP 機能を使用するには、次の 3つの手順に従います：

- (1) スイッチを MSTP に設定します(STP バージョンフィールドの[STP Bridge Global Settings]ウィンドウにあります)。
- (2) MSTP インスタンスの正しいスパニングツリー優先度を入力します(ここでは、MSTI ID 設定する際に、[MSTI Config Information]ウィンドウで優先度として定義されています)。
- (3) 共有する VLAN は MSTP インスタンス ID に追加します(ここでは、MSTI ID 設定する際に、[MST Configuration Identification]ウィンドウで VID 一覧として定義されています)。

ポート遷移状態

3つのプロトコルの主な違いは、転送状態へのポートの遷移方法と、この遷移をトポロジ内のポートの役割(転送する、または転送しない)に関係付ける方法です。MSTPとRSTPでは、STPで使用する遷移状態(無効、ブロッキング、待ち受け)を組み合わせ、単一の状態(ディスカーディング)を作成します。いずれの場合も、ポートはパケットを転送しません。STPポート遷移状態(無効、ブロッキング、待ち受け)、または、RSTP/MSTPポート状態(ディスカーディング)には、機能上の違いはありません。ポートは、ネットワークトポロジ内でアクティブではありません。下の表は、3つのプロトコルにおけるポート遷移状態の違いを示しています。

3つのプロトコルは、同じ方法で安定するトポロジを計算します。各セグメントにはルートブリッジへの単一パスがあります。すべてのブリッジはBPDUパケットを待ち受けます。ただし、BPDUは、各Helloパケットと一緒に、頻繁に送信されます。1つのBPDUパケットが受信されなかった場合でも、BPDUパケットは送信されます。そのため、ブリッジ間の各リンクは、リンクの状態の影響を受けます。最終的にはこの違いによって、リンクの失敗を素早く検出し、トポロジの迅速な調整につながります。

MSTP	RSTP	STP	フォワーディング	学習
無効	無効	無効	なし	なし
ディスカーディング	ディスカーディング	ブロッキング	なし	なし
ディスカーディング	ディスカーディング	待ち受け	なし	なし
学習	学習	学習	なし	あり
フォワーディング	フォワーディング	フォワーディング	あり	あり

RSTPでは、フォワード状態へのより高速な遷移が可能です。タイマー設定には左右されません。RSTP準拠ブリッジは、その他のRSTP準拠ブリッジリンクからのフィードバックに左右されます。ポートは、フォワード状態に遷移する前に、トポロジが安定化するのを待つ必要はありません。この高速遷移のために、プロトコルは次の2つの新しい変数を生成します(エッジポートおよびポイントツーポイント(P2P)ポート)。

エッジポート

エッジポートは、ループを作成できないセグメントに直接接続されているポートです。例えば、単一のワークステーションに直接接続されているポートなどです。エッジポートとして指定されているポートは、待ち受け状態や学習状態にならずに、直ちにフォワード状態に遷移します。エッジポートは、BPDUパケットを受信すると、直ちに通常のスパニングツリーポートになります。

P2P ポート

P2Pポートも高速遷移に対応します。P2Pを使用してその他のブリッジに接続します。RSTP/MSTPでは、全二重モードで動作するすべてのポートは、設定変更しない限り、P2Pポートとみなされます。

STP/RSTP/MSTP 互換性

MSTP または RSTP は、レガシー装置と互換性があります。また、必要な場合は、BPDU パケットを STP 形式に自動調整します。ただし、STP を使用するセグメントでは、MSTP または RSTP の高速遷移、および高速トポロジ変更検出の利点はありません。また、プロトコルは、セグメント上のレガシー装置を更新して RSTP または MSTP を使用する場合に、マイグレーションで使用する変数を提供します。

STP は次の 2 つのレベルで動作します：

- (1) スイッチレベルでは、設定はグローバルに適用されます。
- (2) ポートレベルでは、設定は、ポートのユーザー定義グループ毎に適用されます。

3.3.16.1 STP Bridge Global Settings

このウィンドウでは、STP ブリッジのグローバル設定を行います。

次のウィンドウを表示するには、L2 Features > Spanning Tree > STP Bridge Global Settings をクリックします：

パラメーター	説明
STP State	ラジオボタンで、Enabled または Disabled を選択して、STP を有効(Enabled) または無効(Disabled)に設定します。
STP Version	プルダウンメニューから、スイッチ上で使用する STP のバージョンを選択します。次の 3 つから選択します。 STP - STP をグローバルに設定します。 RSTP - RSTP をグローバルに設定します。 MSTP - MSTP をグローバルに設定します。
Forwarding BPDU	プルダウンメニューから、BPDU パケットの転送を有効(Enabled)または無効(Disabled)にします。デフォルト設定は有効(Enabled)です。

下記にパラメーターの説明を記載します。

パラメーター	説明
STP State	ラジオボタンで、Enabled または Disabled を選択して、STP を有効(Enabled) または無効(Disabled)に設定します。
STP Version	プルダウンメニューから、スイッチ上で使用する STP のバージョンを選択します。次の 3 つから選択します。 STP - STP をグローバルに設定します。 RSTP - RSTP をグローバルに設定します。 MSTP - MSTP をグローバルに設定します。
Forwarding BPDU	プルダウンメニューから、BPDU パケットの転送を有効(Enabled)または無効(Disabled)にします。デフォルト設定は有効(Enabled)です。

パラメーター	説明
Bridge Max Age (6-40)	Max Age を設定して、古い情報がネットワーク内の冗長パスを通して永続的に循環することのないよう、新しい情報が有効に転送されるようにすることができます。この値はルートブリッジで設定します。この値を使用して、スイッチのスパニングツリー設定値が、ブリッジした LAN 上のその他のデバイスと同じかどうかを判断します。値の期限が切れるまでに BPDU がルートブリッジから受信されない場合は、スイッチは、自身の BPDU をその他のスイッチへ送信して、ルートブリッジになることを許可します。お使いのスイッチのブリッジ識別子が最小の場合は、そのスイッチがルートブリッジになります。6~40 秒から選択します。デフォルト値は 20 秒です。
Bridge Hello Time (1-2)	Hello Time は 1 秒または 2 秒で設定します。この値は Root Bridge から他のスイッチに送信される 2 つの BPDU パケットの時間間隔です。Global Bridge Hello Time は STP/RSTP モードで動作している場合にのみ設定可能です。デフォルト値は 2 秒です。
Bridge Forward Delay (4-30)	転送遅延は 4~30 秒の範囲で設定します。スイッチ上のポートは、ブロッキング状態からフォワーディング状態に遷移する間、この設定時間待ち受け状態となります。デフォルト値は 15 秒です。
Tx Hold Count (1-10)	間隔毎に送信される Hello パケットの最大数を設定します(1~10)。デフォルトは 6 です。
Max Hops (6-40)	スイッチが送信する BPDU パケットを廃棄する前のスパニングツリー範囲内のデバイス間のホップの数を設定します。ホップカウント上のスイッチは、値が 0 になるまで、ホップカウントを 1 ずつ減らします。0 になった場合、BPDU パケットを廃棄して、ポート用に保留していた情報は無効になります。ホップカウントは 6~40 の範囲で設定します。デフォルトは 20 です。

[Apply]をクリックして変更を適用します。

注意事項



Hello 時間は、最大エージより長くすることはできません。最大エージよりも長くすると、エラーが発生します。上記のパラメーターを設定する際には、次の計算式に従います。

最大エージ $2 \times (\text{送信遅延} - 1 \text{ 秒})$

最大エージ $2 \times (\text{Hello 時間} + 1 \text{ 秒})$

3.3.16.2 STP Port Settings

このウィンドウで STP のポート設定を行います。

次のウィンドウを表示するには、L2 Features > Spanning Tree > STP Port Settings をクリックします：

STP Port Settings

From Port: 01 To Port: 01

External Cost (0=Auto): 0 Migrate: Yes Edge: Auto

P2P: Auto Port STP: Enabled Restricted Role: False

Restricted TCN: False Forward BPDUs: Enabled

Apply

Port	External Cost	Edge	P2P	Port STP	Restricted Role	Restricted TCN	Forward BPDUs	Hello Time
1	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
2	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
3	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
4	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
5	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
6	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
7	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
8	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2

Port field : M=Trunk Master ; T= Trunk Member External Cost, Edge, P2P and Hello Time fields : Value1/Value2 (Value1=Configured value ; Value2=Actual value)

MST が選択されている場合は、次のウィンドウが表示されます。

STP Port Settings

From Port: 01 To Port: 01

External Cost (0=Auto): 0 Migrate: Yes Edge: Auto

P2P: Auto Port STP: Enabled Restricted Role: False

Restricted TCN: False Forward BPDUs: Enabled Hello Time (1-2): 2 sec

Apply

Port	External Cost	Edge	P2P	Port STP	Restricted Role	Restricted TCN	Forward BPDUs	Hello Time
1	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
2	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
3	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
4	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
5	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
6	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
7	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
8	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2

Port field : M=Trunk Master ; T= Trunk Member External Cost, Edge, P2P and Hello Time fields : Value1/Value2 (Value1=Configured value ; Value2=Actual value)

スイッチで使用するスパンニングツリーは、各ポートでグループを構成します。STP グループのルートポートは、ポート優先度とポートコストに基づき選択され、STP グループ内の冗長リンクをブロックします。STP グループは、VLAN グループに対応するように定義することを推奨します。

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	プルダウンメニューで選択して設定するポート範囲を指定します。
External Cost (0=Auto)	External Cost - パケットを指定したポート一覧に転送する際の相対コストを表すメトリックを定義します。ポートコストは自動的に設定するか、または、メトリック値で設定します。デフォルト値 0 です(Auto)。 0 (Auto) - 外部コストの設定 0 は、パケットを一覧内の指定したポートへ転送する速度を自動的に設定して、効率性を最適化します。デフォルトのポートコスト: 100 Mbps ポート = 200000 ギガビットポート = 20000 1 ~ 200,000,000 の値に定義して、外部コストを決めます。数字が小さいほど、パケット転送を選択するポートの優先度が高くなります。
Migrate	このパラメーターを YES に設定すると、ポートは BPDU パケットを他のブリッジへ送信し、STP 情報を要求するように設定されます。RSTP に設定されている場合、ポートは 802.1D STP から 802.1w RSTP まで移行できます。
Edge	このパラメーターを True に設定すると、ポートはエッジポートとして指定されます。ただしトポロジーの変更によってループ発生の可能性が生じると、エッジポートとしての資格を失います。また、エッジポートで BPDU パケットを受信すると、そのポートはエッジポートとしての資格を失います。False に設定するとエッジポートとして指定されません。Auto に設定すると BPDU パケットを受信しない場合などで自動的にエッジポートになります。
P2P	このパラメーターを True に設定すると、ポイントツーポイント(P2P)共有リンクになります。P2P ポートはエッジポートと同様にフォワーディング状態に高速転移可能のため、RSTP の利点を活用できますが、ポートは全二重で動作している必要があります。False は、ポートを P2P 状態にできません。Auto の場合、いつでもポートを P2P 状態にして、P2P 状態が True である場合と同様に動作するようにできます。ポートがこの状態を維持できない場合は(ポートが強制的に半二重動作になった場合など)、P2P 状態が False であるのと同様に動作するように変更されます。デフォルト設定は Auto です。
Port STP	プルダウンメニューから、Enabled あるいは Disabled を選択し、STP をポート単位で有効(Enabled)または無効(Disabled)にします。
Restricted Role	プルダウンメニューでパケットの制限付き役割(Restricted Role)状態を真(True)あるいは偽(False)に設定します。デフォルト値は False です。
Restricted TCN	プルダウンメニューでパケットの制限付き TCN(Restricted TCN)を真(True)あるいは偽(False)に設定します。デフォルト値は False です。
Forward BPDU	プルダウンメニューで、受信した BPDU パケットを転送するか(Enabled)、破棄するか(Disabled)かを設定します。デフォルトは有効(Enabled)です。
Hello Time	BPDU パケットを送信する間隔を 1 秒または 2 秒で設定します。デフォルト値は 2 秒です。本設定は MST を選択した場合のみ表示されます。

[Apply]をクリックして変更を適用します。

注意事項



認証機能 (MAC 認証、Web 認証、802.1X 認証) とのポート併用はできません。

3.3.16.3 MST Configuration Identification

MST Configuration Identification にある次のウィンドウで、スイッチ上の MSTI インスタンスを設定します。これらの設定で、スイッチ上に設定されたマルチプルスパニングツリーインスタンスを固有識別します。スイッチには 1 つの CIST(コモンインターナルスパニングツリー)があります。ユーザーは、CIST のパラメーターを変更することができます。ただし、CIST の MSTI ID を変更したり、削除することはできません。

次のウィンドウを表示するには、L2 Features > Spanning Tree > MST Configuration Identification をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
Configuration Name	スイッチ上に事前に設定した名前です。MSTI を固有識別します。設定されていない場合は、このフィールドには、MSTP を実行するデバイスへの MAC アドレスが表示されます。
Revision Level (0-65535)	スイッチ上に設定された MSTP 範囲を識別します。0 ~ 65535 の値から選択します。デフォルト設定は 0 です。
MSTI ID (1-4)	スイッチ上に現在設定されている MSTI ID が表示されます。このフィールドには CIST MSTI があります。CIST MSTI は設定しますが、削除することはできません。
Type	MSTI 設定変更方法を選択できます。次の 2 つの方法から選択します。 Add VID - VID を VID 一覧パラメーターと併せて MSTI ID に追加します。 Remove VID - VID を VID 一覧パラメーターと併せて MSTI ID から削除します。
VID List (1-4094)	このフィールドには、特定の MSTI に関連する VLAN ID が表示されます。

[Apply]をクリックして変更を適用します。

[Edit]をクリックして入力済みのエントリーを修正します。

[Delete]をクリックして選択したエントリーを削除します。

3.3.16.4 STP Instance Settings

次のウィンドウには、スイッチ上に現在設定されている MSTI が表示されます。

次のウィンドウを表示するには、L2 Features > Spanning Tree > STP Instance Settings をクリックします：

Instance Type	Instance Status	Instance Priority
CIST	Disabled	32768(Bridge Priority : 32768, SYS ID Ext : 0)

STP Instance Operational Status			
MSTP ID	--	Designated Root Bridge	--
External Root Cost	--	Regional Root Bridge	--
Internal Root Cost	--	Designated Bridge	--
Root Port	--	Max Age	--
Forward Delay	--	Remaining Hops	--
Last Topology Change	--	Topology Changes Count	--

下記にパラメーターの説明を記載します。

パラメーター	説明
MSTI ID	変更するインスタンスの MSTI ID を表示します。0 は CIST(デフォルト MSTI) を意味します。
Priority	プルダウンメニューから、優先度を入力します。優先度の値は 0 ~ 61440 の範囲で設定します。

[Apply]をクリックして変更を適用します。

[Edit]をクリックして入力済みのエントリーを修正します。

[View]をクリックして指定したエントリーの情報を表示します。

3.3.16.5 MSTP Port Information

このウィンドウには、現在の MSTP ポート情報が表示されます。このウィンドウを使用して、MSTI ID のポート設定を更新します。ループが発生する場合は、MSTP 機能はポート優先度を使用して、フォワーディング状態にするインターフェースを選択します。最初に転送するインターフェースの優先度値は高く設定します。インスタンスの優先度が同じ場合は、MSTP 機能は最も小さい MAC アドレスをフォワーディング状態にします。その他のインターフェースはブロックされます。優先度値が低いと、パケット転送の優先度は高くなります。

次のウィンドウを表示するには、L2 Features > Spanning Tree > MSTP Port Information をクリックします：

MSTI	Designated Bridge	Internal Path Cost	Priority	Status	Role
0	8000/00ae32002400	200000	128	Forwarding	Designated

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	プルダウンメニューからポートを選択します。
Instance ID	設定されているインスタンスの MSTI ID を表示します。0 は CIST(デフォルト MSTI)を示します。
Internal Path Cost (1-200000000)	インターフェースを STP インスタンス内で選択した場合に、このパラメーターを設定して、パケットを指定したポートに転送する際の相対コストを表すようにします。内部コストが低いと、送信は速くなります。
Priority	プルダウンメニューから、0~240 の値を選択して、ポートインターフェースの優先度を設定します。優先度が高いインターフェースは、パケットを最初に転送するインターフェースです。数字が小さいと、優先度は高くなります。

[Find]をクリックして入力された条件で検索します。

[Apply]をクリックして変更を適用します。

[Edit]をクリックして入力済みのエントリーを修正します。

3.3.17 Forwarding & Filtering

3.3.17.1 Unicast Forwarding Settings

次のウィンドウを表示するには、L2 Features > Forwarding & Filtering > Unicast Forwarding Settings をクリックします：

エントリーを追加したり編集するには、下記のパラメーターを定義して、次に、[Add/Modify]をクリックします。

パラメーター	説明
VLAN ID (1-4094)	MAC アドレスに割り当てる VLAN ID を指定します。
MAC Address	ユニキャスト FDB に登録したい MAC アドレスを指定します。登録するアドレスはユニキャスト MAC アドレスである必要があります。
Port	プルダウンメニューから、上記で入力した MAC アドレスがあるポート番号を選択します。

[Apply]をクリックして変更を適用します。新しいエントリーがウィンドウの下半分に表示されます。

3.3.17.2 Multicast Forwarding Settings

次のウィンドウを表示するには、L2 Features > Forwarding & Filtering > Multicast Forwarding Settings をクリックします:

下記にパラメーターの説明を記載します。

パラメーター	説明
VLAN ID (1-4094)	MAC アドレスに割り当てる VLAN ID を指定します。
MAC Address	マルチキャスト FDB に登録したい MAC アドレスを指定します。登録するアドレスはマルチキャスト MAC アドレスである必要があります。
Port Settings	静的マルチキャストグループのメンバーにするポートを選択します。次のオプションがあります: None - マルチキャストグループを動的に結合するポート上には制限はありません。None を選択すると、ポートは静的マルチキャストグループのメンバーにはなりません。 Egress - ポートはマルチキャストグループの静的メンバーです。 [All] をクリックすると、選択したすべてのポートを None、または、Egress として選択できます。 [Clear All] をクリックすると、このウィンドウの一番上にある設定をすべて消去します。

[Apply] をクリックして変更を適用します。

[Clear All] をクリックしてフィールドからの全ての入力データをクリアーします。

[All] をクリックして全てのポートを選択します。

3.3.17.3 Multicast Filtering Mode

マルチキャストフィルタリングモードを設定します。

次のウィンドウを表示するには、L2 Features > Forwarding & Filtering > Multicast Filtering Mode をクリックします：

Port	Multicast Filtering Mode
1	Forward Unregistered Groups
2	Forward Unregistered Groups
3	Forward Unregistered Groups
4	Forward Unregistered Groups
5	Forward Unregistered Groups
6	Forward Unregistered Groups
7	Forward Unregistered Groups
8	Forward Unregistered Groups
9	Forward Unregistered Groups
10	Forward Unregistered Groups
11	Forward Unregistered Groups
12	Forward Unregistered Groups
13	Forward Unregistered Groups
14	Forward Unregistered Groups
15	Forward Unregistered Groups
16	Forward Unregistered Groups
17	Forward Unregistered Groups
18	Forward Unregistered Groups
19	Forward Unregistered Groups
20	Forward Unregistered Groups
21	Forward Unregistered Groups
22	Forward Unregistered Groups
23	Forward Unregistered Groups
24	Forward Unregistered Groups

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	設定するポートの範囲を選択します。
Filtering Mode	ポートへの転送を要求するマルチキャストパケットを受信した際のアクションを指定します。 Forward Unregistered Groups - 送信先が上で指定したポート範囲内にある非登録マルチキャストグループであるマルチキャストパケットを転送します。 Filter Unregistered Groups - 送信先が上で指定したポート範囲内にある非登録マルチキャストグループであるマルチキャストパケットをフィルターします。

[Apply]をクリックして変更を適用します。

3.3.18 LLDP

LLDP で、IEEE 802 LAN に接続されているその他のステーションにアドバタイズできるようにします。このシステムの主な機能は、ステーション、管理アドレス、または、これらの機能を管理するエンティティのアドレス、および、それらの管理エンティティにより要求されるステーションの IEEE 802 LAN への取り付けポイントの識別を組み入れることです。

このプロトコル経由で配信される情報は、受信先の MIB に保管されるので、ネットワーク管理システム(NMS)は、SNMP などの管理プロトコル経由で情報にアクセスできます。

3.3.18.1 LLDP Global Settings

このウィンドウを表示するには、L2 Features > LLDP > LLDP Global Settings をクリックします：

LLDP Global Settings

LLDP State Disabled Enabled Apply

LLDP Forward Message Disabled Enabled Apply

Message Tx Interval (5-32768) sec

Message Tx Hold Multiplier (2-10)

LLDP Reinit Delay (1-10) sec

LLDP Tx Delay (1-8192) sec

LLDP Notification Interval (5-3600) sec Apply

LLDP System Information

Chassis ID Subtype	MAC Address
Chassis ID	00-40-66-45-5E-78
System Name	
System Description	Fast Ethernet Switch
System Capabilities	Repeater, Bridge

下記にパラメーターの説明を記載します。

パラメーター	説明
LLDP State	ラジオボタンで LLDP を有効(Enabled)または無効(Disabled)にします。
LLDP Forward Message	ラジオボタンで、LLDP Forward Message を有効(Enabled)または無効(Disabled)に設定します。有効の場合には受信した LLDP パケットを透過して他のポートに転送します。この機能は LLDP が有効の場合には動作しません。
Message Tx Interval (5-32768)	この間隔で、アクティブポートがネイバーにアドバタイズメントを再送する頻度を制御します(5 ~ 32768 秒)。デフォルト値は 30 秒です。
Message Tx Hold Multiplier (2-10)	この機能で、LLDP スイッチで使用するマルチプライヤーを変更して、LLDP アドバタイズメントを作成して LLDP ネイバーへ送信するための生存時間を計算します。アドバタイズメントの生存時間が切れると、アドバタイズしたデータはネイバースイッチの MIB から削除されます。デフォルト値は 4 です。
LLDP Reinit Delay (1-10)	LLDP 再初期化遅延間隔は LLDP 無効コマンドを受信した後、LLDP ポートが再初期化を始めるまでに待つ最小時間です(1 ~ 10 秒)。デフォルト値は 2 秒です。
LLDP Tx Delay (1-8192)	LLDP 送信遅延で、LLDP MIB コンテンツが変更された場合に、連続する LLDP アドバタイズを遅らせる LLDP ポートの最小遅延間隔を変更します(1 ~ 8192 秒)。デフォルト値は 2 秒です。

パラメーター	説明
LLDP Notification Interval (5-3600)	LLDP 通知間隔を使用して、LLDP ネイバーからポートに受信したアドバタイズメント内に LLDP 変更が検出された場合に、設定した SNMP トラップ先に送信します。LLDP 通知間隔は、5 ~ 3600 秒で設定可能です。デフォルト値は 5 秒です。

[Apply]をクリックして変更を適用します。

3.3.18.2 LLDP Port Settings

次のウィンドウを表示するには、L2 Features > LLDP > LLDP Port Settings をクリックします：

LLDP Port Settings

From Port: 01 To Port: 01 Notification: Disabled Admin Status: Tx and Rx
Subtype: IPv4 Action: Disabled Address:

Note: The IPv4/IPv6 Address should be the Switch's Address.

Port ID	Notification	Admin Status	Subtype	Address
1	Disabled	Tx and Rx	IPv4	
2	Disabled	Tx and Rx	IPv4	
3	Disabled	Tx and Rx	IPv4	
4	Disabled	Tx and Rx	IPv4	
5	Disabled	Tx and Rx	IPv4	
6	Disabled	Tx and Rx	IPv4	
7	Disabled	Tx and Rx	IPv4	
8	Disabled	Tx and Rx	IPv4	
9	Disabled	Tx and Rx	IPv4	
10	Disabled	Tx and Rx	IPv4	
11	Disabled	Tx and Rx	IPv4	
12	Disabled	Tx and Rx	IPv4	
13	Disabled	Tx and Rx	IPv4	
14	Disabled	Tx and Rx	IPv4	
15	Disabled	Tx and Rx	IPv4	
16	Disabled	Tx and Rx	IPv4	
17	Disabled	Tx and Rx	IPv4	
18	Disabled	Tx and Rx	IPv4	
19	Disabled	Tx and Rx	IPv4	
20	Disabled	Tx and Rx	IPv4	
21	Disabled	Tx and Rx	IPv4	
22	Disabled	Tx and Rx	IPv4	
23	Disabled	Tx and Rx	IPv4	
24	Disabled	Tx and Rx	IPv4	

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	設定するポート範囲を選択します。
Notification	プルダウンメニューで LLDP の SNMP トラップ通知を有効(Enabled)または無効(Disabled)にします。無効の場合、SNMP トラップを送信しません。
Admin Status	プルダウンメニューでポートごとの LLDP 動作を指定します。以下から動作を選択することができます。 Tx: LLDP フレームの送信のみ行います。 Rx: LLDP フレームの受信のみ行います。 Tx and Rx: LLDP フレームの送受信を行います。 Disabled: LLDP フレームの送受信を行いません。 デフォルト値は Tx and Rx です。
Subtype	IPv4 (IP アドレスの種類)が表示されます。
Action	プルダウンメニューで、LLDP フレームにより装置の管理アドレスを通知するか(Enabled)、通知しないか(Disabled)を選択します。
Address	アドレスは管理 IP アドレスである必要があります。

[Apply]をクリックして変更を適用します。

3.3.18.3 LLDP Basic TLVs Settings

このウィンドウを使用して、基本 TLV の設定を有効にします。

次のウィンドウを表示するには、L2 Features > LLDP > LLDP Basic TLVs Settings をクリックします：

Port	Port Description	System Name	System Description	System Capabilities
1	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled	Disabled

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	設定するポート範囲を選択します。
Port Description	プルダウンメニューから、Enabled あるいは Disabled を選択し、port Description TLV を有効(Enabled)または無効(Disabled)にします。
System Name	プルダウンメニューから、Enabled あるいは Disabled を選択し、System Name TLV を有効(Enabled)または無効(Disabled)にします。
System Description	プルダウンメニューから、Enabled あるいは Disabled を選択し、System Description TLV を有効(Enabled)または無効(Disabled)にします。
System Capabilities	プルダウンメニューから、Enabled あるいは Disabled を選択し、System Capabilities TLV を有効(Enabled)または無効(Disabled)にします。

[Apply]をクリックして変更を適用します。

3.3.18.4 LLDP Dot1 TLVs Settings

LLDP Dot1 TLV は IEEE 802.1 で定められた拡張 TLV で、PVID、VLAN 名、プロトコル VLAN ID、プロトコル ID の情報が含まれます。LLDP Dot1 TLV の設定により、ポート単位で各情報を通知するかどうかを指定することができます。

次のウィンドウを表示するには、L2 Features > LLDP > LLDP Dot1 TLVs Settings をクリックします：

Port	PVID State	Port and Protocol VID State	VID	VLAN Name State	VID	Protocol Identity State	Protocol Identity
1	Disabled	Disabled		Disabled		Disabled	Disabled
2	Disabled	Disabled		Disabled		Disabled	Disabled
3	Disabled	Disabled		Disabled		Disabled	Disabled
4	Disabled	Disabled		Disabled		Disabled	Disabled
5	Disabled	Disabled		Disabled		Disabled	Disabled
6	Disabled	Disabled		Disabled		Disabled	Disabled
7	Disabled	Disabled		Disabled		Disabled	Disabled
8	Disabled	Disabled		Disabled		Disabled	Disabled
9	Disabled	Disabled		Disabled		Disabled	Disabled
10	Disabled	Disabled		Disabled		Disabled	Disabled

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	設定するポート範囲を選択します。
PVID	PVID 情報の通知を有効(Enabled)または無効(Disabled)にします。
Protocol VLAN ID	プロトコル VLAN ID 情報の通知を有効(Enabled)または無効(Disabled)にします。右のプルダウンメニューから VLAN Name、VLAN ID、あるいは ALL を選択して適用する VLAN を指定します。VLAN Name を選択した場合、右のフィールドに VLAN 名を指定します。VLAN ID を選択した場合、右のフィールドに VLAN ID のリストを指定します。ALL を選択すると全ての VLAN が指定されます。
VLAN Name	VLAN 名情報の通知を有効(Enabled)または無効(Disabled)にします。右のプルダウンメニューから VLAN Name、VLAN ID、あるいは ALL を選択し適用する VLAN を指定します。VLAN Name を選択した場合、右のフィールドに VLAN 名を指定します。VLAN ID を選択した場合、右のフィールドに VLAN ID のリストを指定します。ALL を選択すると全ての VLAN が指定されます。
Protocol Identity	プロトコル ID 情報の通知を有効(Enabled)または無効(Disabled)にします。右のプルダウンメニューから EAPOL、LACP、GVRP、STP、あるいは ALL を選択し、通知するプロトコルを指定します。ALL を指定するとすべてのプロトコルが通知されます。

[Apply]をクリックして変更を適用します。

3.3.18.5 LLDP Dot3 TLVs Settings

LLDP Dot3 TLV は IEEE 802.3 で定められた拡張 TLV で、MAC/PHY 設定状態、リンクアグリゲーション、PoE 状態、最大フレームサイズの情報が含まれます。LLDP Dot3 TLV の設定により、ポート単位で各情報を通知するかどうかを指定することができます。

次のウィンドウを表示するには、L2 Features > LLDP > LLDP Dot3 TLVs Settings をクリックします：

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

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	設定するポート範囲を選択します。
MAC/PHY Configuration Status	MAC/PHY 設定状態情報の通知を有効(Enabled)あるいは無効(Disabled)にします。この情報には IEEE802.3 リンクの 2 つの異なる通信設定で、ポートがオートネゴシエーション機能に対応するか、機能が有効か、自動通知機能および動作 MAU タイプが含まれます。デフォルトは無効(Disabled)です。
Link Aggregation	リンクアグリゲーション情報の通知を有効(Enabled)あるいは無効(Disabled)にします。この情報には、ポートがリンクアグリゲーションをできるか、ポートがグループ内に集合されているか、集合されたポート ID が含まれます。デフォルトは無効(Disabled)です。
Power Via MDI	PoE 状態の通知を有効(Enabled)あるいは無効(Disabled)にします。3 つの IEEE 802.3 PMD (10BASE-T、100BASE-TX および 1000BASE-T) では、接続された未供給のシステムにリンク上で電力を供給することができます。MDI TLV 経由の電力供給は、ネットワーク管理により送信する IEEE 802.3 LAN ステーションの MDI パワーサポート機能をアダプタイズし検出することができます。デフォルトは無効(Disabled)です。
Maximum Frame Size	最大フレームサイズ情報の通知を有効(Enabled)あるいは無効(Disabled)にします。デフォルトは無効(Disabled)です。

[Apply]をクリックして変更を適用します。

3.4 サービス品質 (QoS)

802.1p 優先度付きキュー-QoS に対応します。次のセクションでは、QoS の使用、および、802.1p 優先度付きキューを使用する利点について説明します。

QoS の利点

QoS は、ネットワーク管理者が、広い帯域幅が必要な重要な機能、または、優先度が高い重要な機能のために帯域幅を確保できるようにする IEEE 802.1p 規格の機能です。このような機能には、VoIP、Web 検索アプリケーション、ファイルサーバーアプリケーション、ビデオ会議などがあります。広い帯域幅を作成することに加え、重要度の低いトラフィックを制限することもできます。これによって、余剰帯域幅を節約できます。スイッチでは、各物理ポート上に独立したハードウェアキューがあります。さまざまなアプリケーションからのパケットをこのキューにマップして、優先順位を付けます。

クラス 3 の優先度は、スイッチ上の 4 つの優先度付きキューの中で最も高くなっています。QoS を使用するには、パケットのヘッダーを検証し、正しい識別タグが付いていることを確認するようにスイッチで確認します。次に、これらのタグ付きパケットをスイッチ上の送信先キューへ転送します。ここで、優先度に基づいてパケットを空にします。

例えば、2 つの遠隔設定したコンピューター間でビデオ会議を開催したい場合は、管理者はアクセスプロファイルコマンドを使用して、送信するビデオパケットに優先度タグを追加できます。次に、受信側で、管理者は、パケットにこのタグが付いているかどうかを検証するようにスイッチで確認し、タグ付きパケットを取得し、スイッチ上のクラスキューにマップします。次に、管理者は、その他のパケットを転送する前に空にするために、このキューの優先度を設定します。エンドユーザーは送信されたすべてのパケットを可能な限り迅速に受信して、キューに優先順位を付け、パケットの連続ストリームを可能にできます。こうすることで、ビデオ会議で使用できる帯域幅を最適化します。

QoS について

スイッチには 4 つの優先度付きキューがあります。これらの優先度付きキューには 0~3 のラベルが付いています。3 は最高優先度のキューであり、0 は最低優先度のキューです。次のように、IEEE 802.1p で指定された 8 つの優先度タグが、スイッチの優先度タグにマップされています。

- 優先度 0 はスイッチの Q1 キューに割り当てられています。
- 優先度 1 はスイッチの Q0 キューに割り当てられています。
- 優先度 2 はスイッチの Q0 キューに割り当てられています。
- 優先度 3 はスイッチの Q1 キューに割り当てられています。
- 優先度 4 はスイッチの Q2 キューに割り当てられています。
- 優先度 5 はスイッチの Q2 キューに割り当てられています。
- 優先度 6 はスイッチの Q3 キューに割り当てられています。
- 優先度 7 はスイッチの Q3 キューに割り当てられています。

絶対優先に基づいたスケジューリングでは、優先度の高いキューにあるパケットが最初に転送されます。複数の絶対優先キューは優先度タグに基づいて空にします。これらのキューが空になったら、優先度の低いパケットが転送されます。

加重ラウンドロビン方式のキューでは、各優先度付きキューから送信されるパケットの数は、割り当てたウエイトによって異なります。

スイッチには、各ポートに 4 つの優先度付きキュー(8 つのサービスクラス)があります。

3.4.1 Bandwidth Control

このウィンドウで、選択したポートのデータ転送レートと受信レートの上限を設定します。

次のウィンドウを表示するには、QoS > Bandwidth Control をクリックします：

Bandwidth Control

From Port: 01 To Port: 01 Type: Rx No Limit: Disabled Rate (64-1024000): Kbit/sec Apply

Bandwidth Control Table

Port	Rx Rate (Kbit/sec)	Tx Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
1	No Limit	No Limit	No Limit	No Limit
2	No Limit	No Limit	No Limit	No Limit
3	No Limit	No Limit	No Limit	No Limit
4	No Limit	No Limit	No Limit	No Limit
5	No Limit	No Limit	No Limit	No Limit
6	No Limit	No Limit	No Limit	No Limit
7	No Limit	No Limit	No Limit	No Limit
8	No Limit	No Limit	No Limit	No Limit
9	No Limit	No Limit	No Limit	No Limit
10	No Limit	No Limit	No Limit	No Limit

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	帯域幅制限を設定するポート範囲を選択します。
Type	プルダウンメニューから、Rx(受信)、Tx (送信)、Both から選択します。この設定で、帯域幅上限をパケット受信、パケット送信、パケット送受信に適用するか選択します。
No Limit	プルダウンメニューから、選択したポートの帯域幅を制限(Disabled)するか、無制限(Enabled)にするか指定します。
Rate (64-1024000)	選択したポートの制限するデータレートを Kbits/秒単位で入力します。この値は 64 ~ 1,024,000 の整数で設定します。

[Apply]をクリックして変更を適用します。ウィンドウの下半分にある[Bandwidth Control Table]に、設定した帯域幅設定が表示されます。

注意事項



設定範囲は 64-1024000Kbps となりますが、実際に設定される値は 64Kbps の倍数となるように自動的に調整されます。

rx_rate パラメーターの forwarding rate が一定にならないときがあります。

3.4.2 Traffic Control

コンピュータネットワーク上にはマルチキャストやブロードキャストなどのパケットが絶えずラッドしています。このトラフィックはネットワーク上の端末の不良や、故障したネットワークカードなどの誤動作によって増加することもあります。その結果、スイッチの処理能力問題が発生し、ネットワーク全体のパフォーマンスに影響を与えることがあります。本スイッチではこのパケットストーム状況を監視し制御することが可能です。

パケットストーム制御では、スイッチに入力されたパケットのスキャンを行い、ユーザーが指定した閾値を監視し制御します。動作モードには「drop」または「shutdown」を指定することができます。

「drop」オプションでは、インターバル時間毎に監視対象のトラフィックが閾値を超えた場合、閾値を超えた分の監視対象トラフィックを破棄します。監視の対象となるパケットストームは、ブロードキャストとマルチキャスト、宛先不明のユニキャストパケットです。

「Shutdown」オプションでは、インターバル時間毎にブロードキャストとマルチキャストの監視対象パケットが閾値を超え、「countdown」オプションで指定した時間内（0秒～1800秒）もパケットストームが継続すると、ポート閉塞し、警告メッセージを出力します。

閉塞したポートの復旧には、(1)10秒から300秒後の自動リカバリーを待つか、(2)手動コマンドにより復旧させる方法があります。手動コマンドで復旧するには、[Configuration]フォルダにある[Port Configuration]ウィンドウを使って、対象ポートのステータスを無効、有効に切り替える必要があります。

次のウィンドウを表示するには、QoS > Traffic Control をクリックします：



Port	Storm Control Type	Action	Threshold	Count Down	Interval	Recover Time
1	Broadcast	Shutdown	64	0	10	60
2	Broadcast	Shutdown	64	0	10	60
3	Broadcast	Shutdown	64	0	10	60
4	Broadcast	Shutdown	64	0	10	60
5	Broadcast	Shutdown	64	0	10	60
6	Broadcast	Shutdown	64	0	10	60
7	Broadcast	Shutdown	64	0	10	60
8	Broadcast	Shutdown	64	0	10	60
9	Broadcast	Shutdown	64	0	10	60
10	Broadcast	Shutdown	64	0	10	60
11	Broadcast	Shutdown	64	0	10	60
12	Broadcast	Shutdown	64	0	10	60
13	None	Drop	64	0	5	300
14	None	Drop	64	0	5	300
15	None	Drop	64	0	5	300
16	None	Drop	64	0	5	300
17	None	Drop	64	0	5	300
18	None	Drop	64	0	5	300

下記にパラメーターの説明を記載します。

パラメーター 説明	
Traffic Control Settings	
From Port/To Port	トラフィック制御を設定するポート範囲を選択します。
Action	<p>スイッチでパケットストームを検知した際の動作モードを設定します。動作モードには、プルダウンメニューから、「drop」または「shutdown」を指定することが出来ます。</p> <p>Drop - スwitchのハードウェアによるトラフィック制御により、パケットストームの発生を検知します。パケットストームが検知されると、状態が改善するまで閾値を超えた分のパケットを廃棄します。</p> <p>Shutdown - スwitchのソフトウェアによるトラフィック制御により、パケットストームの発生を検知します。パケットストームが検出されると、ブロードキャストとマルチキャストを対象にスイッチ内のカウンターをカウントダウン時間監視します。さらにカウントダウンタイマー経過後もパケットストームが続く場合には、そのポートを閉塞します。ポートは 10 秒から 300 秒の間でユーザーが設定した時間を経過すると自動的に回復します。手動コマンドで復旧するには、[Configuration]フォルダにある [Port Configuration]ウィンドウを使って、対象ポートのステータスを無効、有効に切り替える必要があります。</p>
Count Down (0 to 1800)	<p>カウントダウンタイマーを設定して、パケットストームが継続発生しているポートをシャットダウンするまでの待機時間を設定します。カウントダウン時間が経過すると、スイッチはポートをシャットダウンします。このパラメーターを使用できるのは、アクションフィールドでシャットダウン設定を選択したポートのみです。ハードウェアベースのトラフィック制御では使用できません。このフィールドの時間は 0~1800 秒の範囲で設定します。デフォルト値は 0 です。0 に設定すると、ポートはシャットダウンされません。</p>
Time Interval (5-30)	<p>トラフィック制御機能へ送信されるマルチキャストおよびブロードキャストパケットの監視間隔の時間を設定します。監視したパケットカウントにより、受信パケットが閾値を超えているかどうかを判断します。間隔は 5~30 秒の範囲で設定します。デフォルト設定は 5 秒です。</p>
Threshold (64- 1000000)	<p>トラフィック制御機能を開始するための閾値を指定します。ドロップモードの単位は Kbit/秒です。シャットダウンモードの単位は packets/秒です。閾値は 64~1,000,000 の範囲で設定します。デフォルト設定は 64 です。</p>
Recover Time (10-300)	<p>パケットストームによってシャットダウンしたポートの自動復旧までの時間を設定します。このフィールドの時間は 10~300 秒の範囲で設定します。デフォルト設定は 300 秒です。</p>
Storm Control Type	<p>検出するストームの種類をプルダウンメニューから、次を選択できます： Broadcast、Multicast、Unknown Unicast。 選択後、ストーム検出を有効または無効にします。</p>

[Apply]をクリックして設定を適用します。

注意事項

-  リンクアグリゲーション(ポートトランク)用に設定されているポートでは、トラフィック制御は使用できません。
-  シャットダウン休止モードのポートは、ユーザーがこれらのポートを回復するか、または、ユーザーが設定した 10 秒から 300 秒の時間が経過してポートが自動的に回復するまで、すべてのウィンドウと画面でリンク切断として表示されます。

3.4.3 802.1p Default Priority

スイッチでは、デフォルトの 802.1p 優先度を、スイッチ上の各ポートに割り当てます。

次のウィンドウを表示するには、QoS > 802.1p Default Priority をクリックします：

Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0

このウィンドウで、デフォルトの 802.1p 優先度を、スイッチ上の指定したポートに割り当てます。優先度値には番号が付いています。0 は最低優先度を示し、7 は最高優先度を示します。[Apply] をクリックして設定を適用します。

3.4.4 802.1p User Priority

スイッチでは、ユーザー優先度を各 802.1p 優先度に割り当てることができます。

次のウィンドウを表示するには、QoS > 802.1p User Priority をクリックします：

Priority	Class ID
0	Class-1
1	Class-0
2	Class-0
3	Class-1
4	Class-2
5	Class-2
6	Class-3
7	Class-3

優先度をスイッチ上のポートグループに割り当てた後、このクラスを 802.1p 優先度の 8 つのレベルに割り当てます。

下記にパラメーターの説明を記載します。

パラメーター	説明
Class ID	プルダウンメニューから、Class-0~3 のクラス ID を入力します。

[Apply] をクリックして変更を適用します。

3.4.5 QoS Scheduling Settings

スイッチ内のハードウェアキューで使用する出力スケジューリングを変更して、QoS をカスタマイズします。QoS を変更する場合と同様に、優先度の低いキュー内のネットワークトラフィックへの影響に配慮します。スケジューリングを変更すると、許容範囲を超えるパケットロスや大幅な転送遅延につながる可能性があります。この設定をカスタマイズする場合は、QoS 設定が適切でないとボトルネックが発生するため、特にピーク時にネットワーク性能を監視することが重要です。

次のウィンドウを表示するには、QoS > QoS Scheduling Settings をクリックします：

Class ID	Mechanism	Weight (1-55)
Class-0	Strict	1
Class-1	Strict	2
Class-2	Strict	4
Class-3	Strict	8

下記にパラメーターの説明を記載します。

パラメーター	説明
Scheduling Mechanism	プルダウンメニューから、Strict と Weight Fair を切り替えます。Strict は、サービスの最優先クラスであり、最初にトラフィックを処理します。つまり、サービスの最優先クラスが完了してから、その他のキューを空にします。Weight Fair では、加重ラウンドロビンアルゴリズムを使用して、サービスの優先クラス内に均等に分配されたパケットを取り扱います。
Weight (1-55)	1～55 のウエイト値を入力します。

[Apply] をクリックして変更を適用します。

3.4.6 Priority Mapping

このウィンドウを使用して、優先度マッピングをセットアップします。

次のウィンドウを表示するには、QoS > Priority Mapping をクリックします：

Priority Mapping

From Port: 01 To Port: 01 Priority: None Ethernet Priority: 802.1p IP Priority: TOS Apply

Port	Ethernet Priority	IP Priority
1	802.1p	Off
2	802.1p	Off
3	802.1p	Off
4	802.1p	Off
5	802.1p	Off
6	802.1p	Off
7	802.1p	Off
8	802.1p	Off
9	802.1p	Off
10	802.1p	Off
11	802.1p	Off
12	802.1p	Off
13	802.1p	Off
14	802.1p	Off
15	802.1p	Off
16	802.1p	Off
17	802.1p	Off
18	802.1p	Off
19	802.1p	Off
20	802.1p	Off
21	802.1p	Off
22	802.1p	Off
23	802.1p	Off
24	802.1p	Off

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	設定するポートの範囲を選択します。
Priority	[None]チェックボックスにチェックを入れると、イーサネット優先度および IP 優先度マッピングは実行されません。
Ethernet Priority	[Ethernet Priority]チェックボックスにチェックを入れて、802.1p マッピングをセットアップします。
IP Priority	[IP Priority]チェックボックスにチェックを入れ、プルダウンメニューから、TOS マッピング、DSCP マッピングを選択します。

[Apply]をクリックして変更を適用します。

3.4.7 TOS Mapping

このウィンドウを使用して、サービスタイプ(ToS)マッピングをセットアップします。

次のウィンドウを表示するには、QoS > ToS Mapping をクリックします：

TOS Mapping

TOS Value	Class ID
0	Class-0
1	Class-0
2	Class-0
3	Class-0
4	Class-0
5	Class-0
6	Class-0
7	Class-0

Apply

下記にパラメーターの説明を記載します。

パラメーター	説明
Class ID	プルダウンメニューから、Class-0~3のクラス ID を入力します。

[Apply]をクリックして変更を適用します。

3.4.8 DSCP Mapping

このウィンドウを使用して、DSCP マッピングをセットアップします。

次のウィンドウを表示するには、QoS > DSCP Mapping をクリックします：

DSCP	Class ID
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0

下記にパラメーターの説明を記載します。

パラメーター	説明
DSCP Value	プルダウンメニューから、優先値 0~63 の DSCP 値を入力します。スイッチは、各パケットヘッダーの DiffServ コード部分を確認して転送します。
Class ID	プルダウンメニューから、Class-0~3のクラス ID を入力します。

[Apply]をクリックして変更を適用します。

3.5 Security

3.5.1 Trusted Host

セキュリティーIP管理を使用して、遠隔ステーションがスイッチを管理できるようにします。1つまたは複数の管理ステーションを定義した場合は、Web ベース GUI、Telnet、SNMP マネージャー経由の管理権が許可されるのは、IP アドレスで定義し選択したホストのみです。管理ステーション IP 設定を定義するには、IP アドレスと正しいサブネットマスクを入力して、[Add]をクリックします。

次のウィンドウを表示するには、Security > Trusted Host をクリックします：

The screenshot shows a web interface for configuring trusted hosts. At the top, there are two input fields: 'Permitted Access IP' and 'Net Mask', each followed by an 'Add' button. Below these fields is a 'Delete All' button. Underneath is a table titled 'Trusted Host Table' with two columns: 'Group' and 'Permitted Access'. A red note below the table reads: 'Note: Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.'

下記にパラメーターの説明を記載します。

パラメーター	説明
Permitted Access IP	信頼できるホストの IP アドレスを設定します。
Net Mask	信頼できるホストのネットマスクを設定します。

[Add]をクリックして新しいエントリーを追加します。

[Delete All]をクリックして全てのエントリーを削除します。

3.5.2 Port Security

ポートセキュリティは、スイッチが認識しない非認証の(送信元 MAC アドレスのある)コンピューターがスイッチのポートに接続してネットワークにアクセスすることを防止する機能です。

3.5.2.1 Port Security Port Settings

指定したポートまたはポート範囲の動的 MAC アドレス学習をロックし、MAC アドレスフォワーディングテーブルに入力されている現在の送信元 MAC アドレスを変更できないようにします。Admin State のプルダウンメニューを有効に設定し、[Apply]をクリックして、ポートをロックします。

次のウィンドウを表示するには、Security > Port Security > Port Security Port Settings をクリックします：

Port Security Port Settings

From Port To Port Admin State Max Learning Address (0-64) Lock Address Mode

01 01 Disabled 0 Delete on Reset

Port Security Port Table

Port	Admin State	Max Learning Address	Lock Address Mode
1	Disabled	1	DeleteOnTimeout
2	Disabled	1	DeleteOnTimeout
3	Disabled	1	DeleteOnTimeout
4	Disabled	1	DeleteOnTimeout
5	Disabled	1	DeleteOnTimeout
6	Disabled	1	DeleteOnTimeout
7	Disabled	1	DeleteOnTimeout
8	Disabled	1	DeleteOnTimeout
9	Disabled	1	DeleteOnTimeout
10	Disabled	1	DeleteOnTimeout

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	ポートセキュリティを設定するポート範囲を選択します。
Admin State	プルダウンメニューから、Enabled あるいは Disabled を選択し、ポートセキュリティ(選択したポート用のロックした MAC アドレステーブル)を有効(Enabled)または無効(Disabled)にします。
Max. Learning Address (0-64)	ポートセキュリティで MAC アドレステーブルに登録できる最大 MAC アドレス数を指定します。
Lock Address Mode	スイッチ上で選択したポートグループ用に MAC アドレステーブルロックを適用する方法をプルダウンメニューから選択します。 次のオプションがあります: DeleteOnTimeout - FDB テーブルのエージアウト時間までアドレスをロックします。 DeleteOnReset - 再設定または装置の再起動までアドレスをロックします。 Permanent - ポートセキュリティ機能の無効化までアドレスをロックします。(装置の再起動後もロックされたアドレスは保持されます)

[Apply]をクリックして変更を適用します。

注意事項



認証機能 (MAC 認証、Web 認証、802.1X 認証) とのポート併用はできません。

3.5.2.2 Port Security FDB Entries

このウィンドウを使用して、各ポート別にポートロックエントリーを消去します。エントリーを消去するには、ポートの範囲を入力して、[Clear]をクリックします。

次のウィンドウを表示するには、Security > Port Security > Port Security FDB Entries をクリックします:

Port Security FDB Entries

Clear Locked Entries

From Port To Port

Total Entries: 0

VID	VLAN Name	MAC Address	Port	Type
-----	-----------	-------------	------	------

3.5.3 Authentication Setting

ユーザーはこのページを使用して、ポートの認証モードを設定します。もし装置が複数の認証をサポートする場合、複数の認証コマンドに依って設定された認証モードに基づき、ポートは動作します。

次のウィンドウを表示するには、Security > Authentication Settings をクリックします：

The screenshot shows the 'Authentication Settings' configuration window. At the top, there is a section for 'Configure Authorized Mode' with three dropdown menus: 'From Port' (01), 'To Port' (24), and 'Authorized Mode' (Host-based). An 'Apply' button is located to the right of these settings. Below this is a table titled 'Multiple Authentication Table' with 24 rows. Each row has two columns: 'Port' (numbered 1 to 24) and 'Authorized Mode' (all set to 'Host-based').

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	本設定に使用されるポートのリストが表示されます。このリストは使用している全てのポートに固定されています
Authorized Mode	<p>プルダウンメニューから使用される認証モードを指定します</p> <p>Host-based - 各ユーザーは個々に認証可能です。</p> <p>Host-based port-vlan-mode - 複数のホストに対して認証を行いますが、認証属性に VLAN ID を持つホストだけを原則として認証許可します。各ポートで最初に認証成功したホストの認証属性(VLAN ID)に基づき、ポートの PVID を変更します。追加で認証を受けるホストは、その PVID と同じ VLAN ID の認証属性を持つ必要があります。認証ホストが存在しなくなった場合、PVID は設定値に戻ります。VLAN タグつきフレームのみで通信を行うホストに対しても認証属性を参照しますが、認証属性を持たない場合には上記の動作の範囲外として取り扱われ、正当なユーザーであれば認証も許可されます。このモードは 802.1X 認証と MAC ベース認証のみで対応します。</p> <p>Port-based - 接続されているホストの 1 台が認証をパスさせると、同一ポート上にある全てのホストがネットワークへのアクセスを承認されます。もしそのユーザーが認証に失敗すると、このポートは次回の認証への試行を維持します。デフォルトは Host-based です。</p>

[Apply]をクリックして変更を適用します。

3.5.4 802.1X

802.1X認証は、ポートまたはホストベースによる認証が可能です。

ユーザーは、ネットワークへのアクセスを許可される前に認証する必要があります。認証方法は、ローカル認証とRADIUSサーバー認証および強制認証に対応します。なお、ローカル認証においては、ダイナミックVLANにより動的VLANを割り当てることは出来ません。

注意事項



動的 VLAN を使用する場合、割り当て可能な最大収容数は 64 端末です。最大数 64 には、MAC/Web/802.1X の各認証で使用する動的 VLAN の端末数を含みます。（動的 VLAN を使用しない端末は、この最大収容数には含まれません）

3.5.4.1 802.1X Settings

次のウィンドウを表示するには、Security > 802.1X > 802.1X Settings をクリックします：

802.1X Settings

802.1X State Disabled Enabled Apply

Auth Mode None ▼

Auth Protocol RADIUS EAP ▼ Apply

Auth Failover Disable ▼ Permit VLAN ID [] Apply

802.1X Port Access Control

From Port 01 ▼ To Port 01 ▼

QuietPeriod (0-65535) 60 sec SuppTimeout (1-65535) 30 sec

ServerTimeout (1-65535) 30 sec MaxReq (1-10) 2 times

TxPeriod (1-65535) 30 sec ReAuthPeriod (1-65535) 3600 sec

ReAuthentication Disabled ▼ Port Control Auto ▼ Refresh

Capability None ▼ Direction Both ▼ Apply

Port	AdmDir	Port Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuthentication	Capability
1	Both	Auto	30	60	30	30	2	3600	Disabled	None
2	Both	Auto	30	60	30	30	2	3600	Disabled	None
3	Both	Auto	30	60	30	30	2	3600	Disabled	None
4	Both	Auto	30	60	30	30	2	3600	Disabled	None
5	Both	Auto	30	60	30	30	2	3600	Disabled	None
6	Both	Auto	30	60	30	30	2	3600	Disabled	None
7	Both	Auto	30	60	30	30	2	3600	Disabled	None
8	Both	Auto	30	60	30	30	2	3600	Disabled	None
9	Both	Auto	30	60	30	30	2	3600	Disabled	None
10	Both	Auto	30	60	30	30	2	3600	Disabled	None
11	Both	Auto	30	60	30	30	2	3600	Disabled	None
12	Both	Auto	30	60	30	30	2	3600	Disabled	None
13	Both	Auto	30	60	30	30	2	3600	Disabled	None
14	Both	Auto	30	60	30	30	2	3600	Disabled	None
15	Both	Auto	30	60	30	30	2	3600	Disabled	None
16	Both	Auto	30	60	30	30	2	3600	Disabled	None
17	Both	Auto	30	60	30	30	2	3600	Disabled	None
18	Both	Auto	30	60	30	30	2	3600	Disabled	None
19	Both	Auto	30	60	30	30	2	3600	Disabled	None

下記にパラメーターの説明を記載します。






パラメーター	説明
802.1X State	ラジオボタンで、Enabled または Disabled を選択して、802.1X を有効 (Enabled) または無効 (Disabled) にします。
Auth Mode	Authentication Setting で選択した認証モードとして、[Port Based] または [MAC Based] が表示されます。
Auth Failover	プルダウンメニューから、RADIUS サーバーからの認証応答がない場合、ローカルデータベースによる認証 (Local) する、強制的に認証許可を行う (Permit)、もしくは failover を行わない (Disable) 設定を行います。 Permit - RADIUS サーバーの応答がない時、強制的に認証許可を行います。 Local - RADIUS サーバーの応答がない時、ローカルデータベースによる認証を行います。 Disable - RADIUS サーバーの応答がない時、failover を行いません。 デフォルト設定は無効です。
Permit VLAN ID	Auth Failover で認証許可 [Permit] 後に所属する VLAN ID を設定します。
Auth Protocol	プルダウンメニューから、認証プロトコルとして、[Local] または [RADIUS EAP] を選択します。
From Port/To Port	設定するポート範囲を選択します。
QuietPeriod (0-65535)	サブリカントの認証に失敗した後、新しく認証を開始するまでの間隔を設定します。デフォルト設定は 60 秒です。
SuppTimeout (1-65535)	EAP Request/Identity パケットを除くすべての EAP パケットに対するサブリカントからの応答を待つ時間を設定します。デフォルト設定は 30 秒です。
ServerTimeout (1-65535)	RADIUS サーバーからの応答を待つ時間を設定します。デフォルト設定は 30 秒です。
MaxReq (1-10)	サブリカントに送信する EAP Request/Identity パケットの最大回数を設定します。デフォルト設定は 2 です。
TxPeriod (1-65535)	EAP Request/Identity パケットの送信間隔を設定します。tx_period で設定した時間、サブリカントからの応答が無かった場合、装置は EAP Request/Identity パケットを再送します。デフォルト設定は 30 秒です。
ReAuthPeriod (1-65535)	サブリカントの定期的な再認証の間隔を設定します (1 ~ 65535 秒)。デフォルト設定は 3600 秒です。
ReAuthentication	プルダウンメニューから Enabled あるいは Disabled を選択し、定期的に再認証する (Enabled) かどうかを決めます。デフォルト設定は無効 (Disabled) です。
Port Control	プルダウンメニューから、ForceAuthorized、Auto、ForceUnauthorized を選択し、ポート認証状態を制御します。 [ForceAuthorized] を選択するとポートは 802.1X の認証プロセスを行わず強制的に認証済みの状態となります。スイッチを経由するネットワークアクセスは許可されます。 [Auto] を選択すると、802.1X が有効になります。ポートは非認証状態で起動します。ポート経由で送受信できるのは EAPOL フレームのみです。ポートがリンクアップし、サブリカントからの EAPOL start フレームを受信すると、認証処理が始まります。スイッチは、クライアントの識別を要求して、認証メッセージをクライアントと認証サーバーの間で転送します。

パラメーター	説明
	[ForceUnauthorized]を選択すると、ポートは 802.1X の認証プロセスを行わず強制的に非認証状態となります。スイッチを経由するネットワークアクセスはブロックされます。 デフォルト設定は Auto です。
Capability	プルダウンメニューから、Authenticator、None を選択し、802.1X オーセンティケーター設定をポート毎に適用します。 [Authenticator]を選択して、設定をポートに適用します。設定を有効にすると、ユーザーは認証処理に合格して、ネットワークへのアクセスを取得しなければなりません。 [None]を選択すると、ポート上の 802.1X 機能が無効になります。
Direction	プルダウンメニューから、Both、In を選択し、管理制御方向を双方向(Both)または受信(In)に設定します。 [Both]を選択すると、最初のフィールドで選択したポート経由の送受信トラフィックを制御します。 [In]を選択すると、最初のフィールドで選択したポート経由の受信トラフィックしか制御されません。

[Apply]をクリックして、設定変更を適用します。

[Refresh]をクリックして画面に表示されるリストを更新します。

注意事項

- 
 フェイルオーバー機能における強制的な認証許可(Permit)は、セキュリティー上問題となる可能性があるため、十分検討の上、使用してください。
- 
 フェイルオーバー機能における強制的な認証許可(Permit)は、設定されている RADIUS サーバー全てがタイムアウトの時に、サブリカントに EAP-Success を返します。しかし、サブリカントの仕様によっては EAP-Success 受信後も認証成功状態にならず、通信出来ない場合や認証成功後も EAPOL-Start 送信を繰り返し、認証処理を繰り返す場合もあります。
- 
 フェイルオーバー機能は、RADIUS サーバーの認証応答がユーザー名、パスワード誤りにより認証失敗した場合は強制認証へ移行しません。RADIUS サーバーの認証応答がタイムアウトした際は強制認証へ移行します。
- 
 フェイルオーバー機能設定時、RADIUS サーバーのタイムアウト時間は 30 秒以内に設定してください。デフォルト設定は 15 秒です。
- 
 802.1X のローカル認証は、MD5 のみサポートします。

3.5.4.2 802.1X User

新しい802.1X ユーザーを作成するには、ユーザー名とパスワードを入力して、次に、パスワードを確定し、[Apply]をクリックします。テーブルの下半分に、新しいユーザーが表示されます。エントリーを削除するには、対応する[Delete]をクリックします。

次のウィンドウを表示するには、Security > 802.1X > 802.1X User をクリックします：

802.1X User

802.1X User Password Confirm Password

Apply

Note: Password/User Name should be less than 15 characters.

802.1X User Table Total Entries: 0

User Name	Password
-----------	----------

下記にパラメーターの説明を記載します。下記はすべて 15 文字以内で入力します。

パラメーター	説明
802.1X User	802.1X ユーザー名を入力します
Password	802.1X パスワードを入力します
Confirm Password	802.1X 確認パスワードを入力します

[Apply]をクリックして変更を適用します。

3.5.4.3 Authentication RADIUS Server

スイッチの RADIUS 機能で、集中ユーザー管理を容易にして、盗聴するアクティブなハッカーから保護します。

次のウィンドウを表示するには、Security > 802.1X > Authentication RADIUS Server をクリックします：

Index	IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Key
1	0.0.0.0	1812	1813	5	2	
2						
3						

下記にパラメーターの説明を記載します。

パラメーター	説明
Index	RADIUS 認証サーバーのインデックス番号を割り当てます。最大 3 つまでスイッチに登録できます。スイッチでは登録したインデックス番号の若い順に RADIUS の応答を確認し、最初に応答した RADIUS を認証サーバーとして認識します。
IP Address	RADIUS 認証サーバーの IP アドレスを設定します。
Authentic Port (1-65535)	RADIUS 認証サーバーの UDP ポートを設定します。デフォルトポート番号は 1812 です。
Accounting Port (1-65535)	RADIUS 認証サーバーの UDP ポートを設定します。デフォルトポート番号は 1813 です。
Timeout (1-255)	タイムアウト値を秒単位で入力します(1~255)。デフォルト値は 5 です。
Retransmit (1-255)	再送信値を秒単位で入力します(1~255)。デフォルト値は 2 です。
Key(Max. length 32 characters)	RADIUS 認証サーバーのキーと同じキーを設定します。エントリーの最大長さは 32 文字です。
Confirm Key	Key で入力したものと同一キーを入力します。

[Apply]をクリックして変更を適用します。

3.5.4.4 Initialize Port(s)

ポートの初期化

802.1X のポート側のポートを初期化するには、[802.1X Settings]ウィンドウで 802.1X をポート別に有効にします。

次のウィンドウを表示するには、Security > 802.1X > Initialize Port(s)をクリックします：

Port	Auth PAE State	Backend_State	Port Status
------	----------------	---------------	-------------

このウィンドウで、ポート、または、ポートのグループを初期化します。ウィンドウの下半分にあるポートの初期化テーブルに、ポートの現在の状態が表示されます。ポートを初期化するには、最初のポートフィールドと最後のポートフィールドで、ポートの範囲を選択します。初期化を開始するには、[Apply]をクリックします。

MAC ベース側のポートを初期化するには、まず、[802.1X Settings]ウィンドウで 802.1X を MAC アドレス別に有効にします。

次のウィンドウを表示するには、Security > 802.1X > Initialize Port(s)をクリックします：

Port	Auth PAE State	Backend_State	Port Status
------	----------------	---------------	-------------

ポートを初期化するには、最初のポートフィールドと最後のポートフィールドで、ポートの範囲を選択します。次に、MAC アドレスフィールドに MAC アドレスを入力し、初期化する MAC アドレスを指定します。初期化を開始するには、[Apply]をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	初期化するポート範囲を選択します。
Port	スイッチ上のポートを表す読み取り専用フィールドです。
Auth PAE State	次のいずれかのオーセンティケーター PAE 状態が表示されます。 [Initialize]初期化、[Disconnected]切断済、[Connecting]接続中、 [Authenticating]認証中、[Authenticated]認証済、[Aborting]中断、[Hold]保留、 [ForceAuth]強制認証、[ForceUnauth]強制非認証、[N/A]該当なし。
Backend_State	次のいずれかのバックエンド認証状態が表示されます： [Request]要求、 [Response]応答、[Success]成功、[Fail]失敗、[Timeout]タイムアウト、 [Idle]アイドル、[Initialize]初期化、[N/A]該当なし。
Port Status	制御されているポートの状態は、[Authorized]認証済み、[Unauthorized]非認証、 [N/A]該当なしのいずれかとなります。
MAC Address	対応するポートに接続されているクライアントがある場合、その MAC アドレスです。

[Apply]をクリックして変更を適用します。

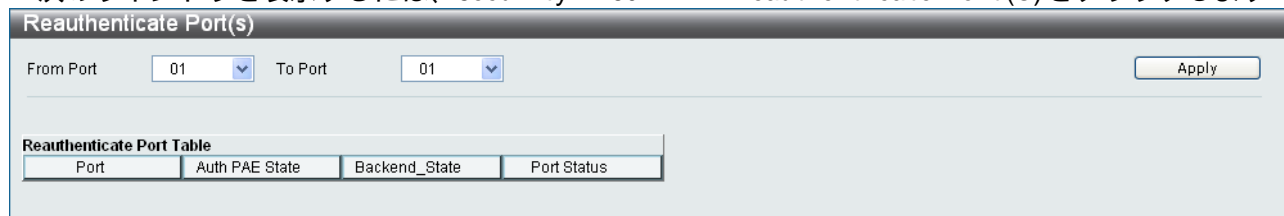
3.5.4.5 Reauthenticate Port(s)

ポートの再認証

下の 2 つのウィンドウを使用して、802.1X ポートを再認証します。

802.1X ポートを再認証するには、[802.1X Settings]ウィンドウで 802.1X をポート別に有効にします。

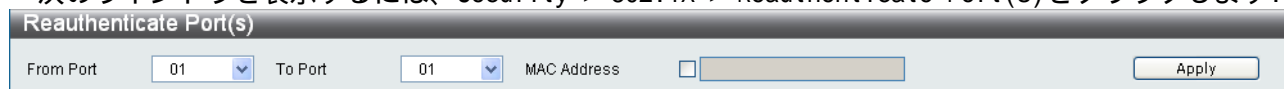
次のウィンドウを表示するには、Security > 802.1X > Reauthenticate Port(s)をクリックします：



このウィンドウで、ポート範囲を指定して[Apply]をクリックします。 [Apply]をクリックすると、ポートの再認証テーブルに、再認証されたポートの現在の状態が表示されます。

MAC ベース側のポートを再認証するには、まず、[802.1X Settings]ウィンドウで 802.1X を MAC アドレス別に有効にします。

次のウィンドウを表示するには、Security > 802.1X > Reauthenticate Port(s)をクリックします：



ポートを再認証するには、まず、最初のポートプルダウンメニューと最後のポートプルダウンメニューから、ポート範囲を選択します。 次に、MAC アドレスフィールドに MAC アドレスを入力し、相応するチェックボックスにチェックを入れて、再認証する MAC アドレスを指定します。 再認証を開始するには、[Apply]をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	再認証するポート範囲を選択します。
MAC Address	ポートがあるスイッチの物理アドレスを表示します。
Auth PAE State	次のいずれかのオーセンティケーター PAE 状態が表示されます。 [Initialize]初期化、[Disconnected]切断済、[Connecting]接続中、 [Authenticating]認証中、[Authenticated]認証済、[Aborting]中断、[Hold]保留、 [ForceAuth]強制認証、[ForceUnauth]強制非認証、[N/A]該当なし。
Backend_State	次のいずれかのバックエンド状態が表示されます： [Request]要求、 [Response]応答、[Success]成功、[Fail]失敗、[Timeout]タイムアウト、 [Idle]アイドル、[Initialize]初期化、[N/A]該当なし。
Port Status	制御されているポートの状態は、[Authorized]認証済み、[Unauthorized]非認証、 [N/A]該当なしのいずれかになります。

[Apply]をクリックして変更を適用します。

3.5.5 SSL Settings

SSL は、認証、デジタル署名、暗号化を使用して、ホストとクライアント間の安全な通信を提供するセキュリティ機能です。これらのセキュリティ機能を適用するには、サイファースイートを使います。サイファースイートは、認証セッションで使用する正確なクリプトグラフィックパラメーター、特定の暗号化アルゴリズム、および、キーサイズを決めるセキュリティ文字列です。次の3つのレベルで構成されます：

- (1) キー交換：サイファースイート文字列の最初の部分で、使用するパブリックキーアルゴリズムを指定します。このスイッチでは Rivest Shamir Adleman(RSA)パブリックキーアルゴリズムとデジタル署名アルゴリズム(DSA)をサポートしています。ここでは、DHE DSS Diffie-Hellman(DHE)パブリックキーアルゴリズムとして指定されています。これは、クライアントとホストの間の最初の認証処理です。クライアントとホストはキーを交換して一致を検索し、受け入れの認証を求めて、次のレベルで暗号化を調整します。

- (2) 暗号化：サイファースイートの二番目の部分には、クライアントとホストの間で送信されるメッセージを暗号化するために使用する暗号化が含まれます。スイッチは次の2つの種類のクリプトロジアルゴリズムに対応します。
 - 1) ストリームサイファー - スイッチ上には、128 ビットキーの RC 4 のストリームサイファーがあります。このキーを使用して、メッセージを暗号化します。また、最適利用のため、クライアントとホストの間で一貫している必要があります。
 - 2) CBC ブロックサイファー - 暗号化したテキストの事前に暗号化したブロック部分を、現在のブロックの暗号化で使用します。スイッチは、データ暗号化標準(DES)で定義された 3DES EDE 暗号化コードと AES(Advanced Encryption Standard)に対応し暗号化テキストを作成します。

- (3) ハッシュアルゴリズム：メッセージ認証コードを決めるメッセージダイジェスト機能を選択できます。このメッセージ認証コードは、送信したメッセージにより暗号化され、統合性を提供し、再生攻撃を防止します。MD5 と SHA の2つのハッシュアルゴリズムをサポートしています。SHA は、SHA-1 及び SHA-2 をサポートしています。

スイッチ上の3つの選択でこれら3つのパラメーターを固有に組み合わせて、サーバーとホストの間で安全に通信できるように3層の暗号化コードを作成します。使用できるサイファースイートの1つあるいはその組み合わせを適用できます。異なるサイファースイートは、セキュリティレベルと安全な接続の性能に影響します。サイファースイートにある情報は、スイッチには含まれません。また、証明書と呼ばれるファイル形式で第三者ソースからダウンロードする必要があります。証明書ファイルがないと、スイッチのこの機能は実行できません。証明書ファイルは、TFTP サーバーを使用してスイッチにダウンロードできます。スイッチは SSLv3.0、TLSv1.0~1.2 に対応しています。SSL のその他のバージョンは互換性がない場合があります。また、認証、および、クライアントからホストへのメッセージの転送に際し、問題が発生することがあります。

証明書のダウンロード

このウィンドウを使用して、SSL 機能用の証明書ファイルを TFTP サーバーからスイッチにダウンロードします。証明書ファイルは、ネットワーク上の認証デバイスで使用するデータレコードです。証明書には、所有者、認証用のキー、デジタル署名に関する情報が含まれます。SSL 機能を最適利用するには、サーバーとクライアントに同じ証明書ファイルが必要です。スイッチが対応するのは、.der ファイル拡張子のある証明書ファイルのみです。1 つの証明書のみプリロードされます。ユーザーは、状況に応じて複数の証明書をダウンロードする必要があります。

サイファースイート

このウィンドウで、スイッチ上で SSL を有効にして、一覧表示されたサイバースイートの 1 つまたはその組み合わせを適用します。サイファースイートは、認証セッションで使用する正確なクリプトグラフィックパラメーター、特定の暗号化アルゴリズム、キーサイズを決めるセキュリティー文字列です。スイッチでは、SSL 機能用に 9 つのサイファースイートを使用できます。デフォルトでは、これらすべてのサイファースイートは有効です。特定のサイファースイートを使用するには、認証の際に使用するサイファースイート以外の不要なサイファースイートを無効にします。

SSL 機能を有効にすると、HTTP は無効になります。SSL 機能を使用中に Web ベース GUI 経由でスイッチを管理するには、Web ブラウザーが SSL 暗号化に対応しなければなりません。また、URL のヘッダーは https:// で始まる必要があります (例 https://10.90.90.90)。その他の方法では、エラーが発生します。また、Web ベース GUI へのアクセスは認証されません。

次のウィンドウを表示するには、Security > SSL Settings をクリックします:

The screenshot shows the 'SSL Settings' configuration page. It is divided into several sections:

- SSL Settings:** Contains radio buttons for 'SSL State' (Disabled is selected), and 'TLS 1.0', 'TLS 1.1', and 'TLS 1.2' (all Enabled are selected).
- Note:** A red message states 'Web will be disabled if SSL is enabled.' with an 'Apply' button.
- SSL Ciphersuite Settings:** Lists nine cipher suites, all with 'Enabled' selected.
- SSL Certificate Download:** Includes input fields for 'Server IP Address', 'Certificate File Name', and 'Key File Name', with a 'Download' button.
- Current Certificate:** Shows the status 'Loaded with RSA Certificate!'.

スイッチ上で SSL 機能をセットアップするには、次のパラメーターを構成して、[Apply]をクリックします。下記にパラメーターの説明を記載します。

パラメーター	説明
SSL Settings	
SSL Status	ラジオボタンで、Enabled または Disabled を選択して、SSL を有効(Enabled)または無効(Disabled)にします。デフォルトは無効(Disabled)です。
TLS 1.0 / TLS 1.1 / TLS 1.2	ラジオボタンで、Enabled または Disabled を選択して、TLSv1.0/1.1/1.2 を個別に有効(Enabled)または無効(Disabled)にします。デフォルトは有効(Enabled)です。
SSL Ciphersuite Settings	
RSA_WITH_RC4_128_MD5/ RSA_WITH_3DES_EDE_CBC_SHA/ DHE_DSS_WITH_3DES_EDE_CBC_SHA/ RSA_WITH_AES_128_CBC_SHA/ RSA_WITH_AES_256_CBC_SHA/ RSA_WITH_AES_128_CBC_SHA256/ RSA_WITH_AES_256_CBC_SHA256/ DHE_DSS_WITH_AES_256_CBC_SHA/ DHE_RSA_WITH_AES_256_CBC_SHA	ラジオボタンで、Enabled または Disabled を選択して、左記を個別に有効(Enabled)または無効(Disabled)にします。デフォルトは有効(Enabled)です。
SSL Certificate Download	
Server IP Address	証明書ファイルがある TFTP サーバーの IP アドレスを入力します。
Certificate File Name	ダウンロードする証明書ファイルのパスとファイル名を入力します。ファイル名は .der 拡張子でなければなりません(例 c:/cert.der)。
Key File Name	ダウンロードするキーファイルのパスとファイル名を入力します。ファイル名は .der 拡張子でなければなりません(例 c:/pkey.der)。

[Download]をクリックして SSL 証明書をダウンロードします。

[Apply]をクリックして変更を適用します。

注意事項



スイッチの SSL 機能を有効にすると、スイッチは Web マネージャー用のポート(ポート 80)を無効にします。Web マネージャーにログインするためには、URL のエントリーは「https://」で始まる必要があります。



ダウンロード可能な証明書及び秘密鍵のファイルサイズは以下の通りです。
 証明書ファイル：8192 バイト
 秘密鍵ファイル：4096 バイト

3.5.6 SSH

SSH は、リモートホストコンピューターに安全にログインして、安全な方法でリモートエンドノード上でコマンドを実行します。また、信頼されないホスト間の通信を暗号化および認証して、安全性を提供します。ネットワーク通信を脅かすセキュリティ上の危険に対する強力な保護を提供します。

次の手順に従って、SSH プロトコルを使用して、リモート PC (SSH クライアント) とスイッチ (SSH サーバー) 間の通信の安全性を確保します。

- (1) [Configuration] フォルダの [User Accounts] ウィンドウを使用して、管理者レベルアクセスのあるユーザーアカウントを作成します。これは、管理者アカウントを作成する方法と同じです。パスワードの指定方法も同様です。SSH プロトコルを使用して安全な通信パスを確立したら、パスワードを使用してスイッチにログオンします。
- (2) [SSH User Authentication] ウィンドウを使用して、ユーザーアカウントが、スイッチとの SSH 接続を確立できるユーザーを識別する際に指定した認証方法を使用するように設定します。SSH では、次の 3 つの方法のいずれかを使用してユーザーを認証します。ホストベース、パスワード、パブリックキーのいずれかです。
- (3) [SSH Authmode and Algorithm Settings] ウィンドウを使用して、SSH クライアントと SSH サーバーの間で送信されるメッセージを暗号化したり、暗号化を解除する際に、SSH が使用する暗号化アルゴリズムを設定します。
- (4) 最後に、[SSH Settings] ウィンドウを使用して、スイッチ上で SSH を有効にします。

上記の手順を完了したら、安全な帯域内接続を使用してスイッチを管理できるように、リモート PC 上の SSH クライアントを設定します。

3.5.6.1 SSH Settings

次のウィンドウを使用して、SSH サーバーを設定します。

次のウィンドウを表示するには、Security > SSH > SSH Settings をクリックします：

SSH Settings	
SSH Server State	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled Apply
SSH Global Settings	
Max. Session (1-8)	<input type="text" value="8"/>
Connection Timeout (120-600)	<input type="text" value="120"/> sec
Authfail Attempts (2-20)	<input type="text" value="2"/> times
Rekey Timeout	<input type="button" value="Never"/>
<input type="button" value="Apply"/>	

下記にパラメーターの説明を記載します。

パラメーター	説明
SSH Server State	SSH を有効または無効に設定します。デフォルトは無効です。
Max Session (1-8)	1~8 の値を入力して、スイッチに同時にアクセスできるユーザーの数を設定します。デフォルト設定は 8 です。
Connection Timeout (120-600)	接続タイムアウトを設定します。120 ~ 600 秒の範囲で設定します。デフォルト設定は 120 秒です。
Authfail Attempts (2-20)	管理者は、SSH 認証を使用してユーザーが SSH サーバーへのログオンを試みることのできる最大回数を設定します。最大試行回数を超えると、スイッチは切断されます。もう一度ログインを試みる場合は、スイッチに接続し直す必要があります。最大試行回数は 2 ~ 20 の範囲で設定します。デフォルト設定は 2 です。
Rekey Timeout	プルダウンメニューから、スイッチがセキュリティーシェル暗号化を切り替える時間を設定します。Never、10min、30min、または、60min から選択します。デフォルト設定は Never です。

[Apply]をクリックして変更を適用します。

3.5.6.2 SSH Authmode and Algorithm Settings

次のウィンドウを表示するには、Security > SSH > SSH Authmode and Algorithm Settings をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
SSH Authentication Mode Settings	
Password	認証用にローカル設定したパスワードを使用したい場合は、このパラメーターを有効にします。デフォルトは有効です。
Public Key	認証用に SSH 上のパブリックキー設定を使用したい場合は、このパラメーターを有効にします。デフォルトは有効です。
Host-based	認証用にホストコンピューターを使用したい場合は、このパラメーターを有効にします。このパラメーターは、SSH 認証技術が必要な Linux ユーザー向けです。またホストコンピューターは、既にインストールした SSH プログラムのある Linux オペレーティングシステムを実行しているものとして扱われます。デフォルトは有効です。
Encryption Algorithm	
3DES-CBC	3DES 暗号化アルゴリズムを有効にします。デフォルトは有効です。
Blow-fish CBC	Blow-fish 暗号化アルゴリズムを有効にします。デフォルトは有効です。
AES128-CBC	AES128 暗号化アルゴリズムを有効にします。デフォルトは有効です。
AES192-CBC	AES192 暗号化アルゴリズムを有効にします。デフォルトは有効です。
AES256-CBC	AES-256 暗号化アルゴリズムを有効にします。デフォルトは有効です。
ARC4	ARC4 暗号化アルゴリズムを有効にします。デフォルトは有効です。
Cast128-CBC	Cast128 暗号化アルゴリズムを有効にします。デフォルトは有効です。
Twofish128	Twofish128 暗号化アルゴリズムを有効にします。デフォルトは有効です。
Twofish192	Twofish192 暗号化アルゴリズムを有効にします。デフォルトは有効です。
Twofish256	Twofish256 暗号化アルゴリズムを有効にします。デフォルトは有効です。
Data Integrity Algorithm	
HMAC-SHA1	SHA1 を有効にします。デフォルトは有効です。
HMAC-MD5	MD5 を有効にします。デフォルトは有効です。
Public Key Algorithm	
HMAC-RSA	RSA を有効にします。デフォルトは有効です。
HMAC-DSA	DSA を有効にします。デフォルトは有効です。

[Apply]をクリックして変更を適用します。

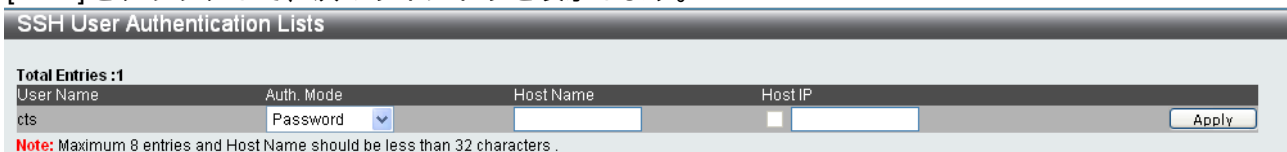
3.5.6.3 SSH User Authentication Lists

次のウィンドウを使用して、SSH 経由でスイッチへのアクセスを試みるユーザー用のパラメーターを構成します。

次のウィンドウを表示するには、Security > SSH > SSH User Authentication Lists をクリックします：



上の例では、[Configuration]フォルダにある[User Accounts]ウィンドウを使用して、ユーザーアカウント「adpro」を設定しています。SSH ユーザー用のパラメーターを設定するには、事前にユーザーアカウントを設定する必要があります。SSH ユーザー用のパラメーターを編集するには、対応する[Edit]をクリックして、次のウィンドウを表示します。



下記にパラメーターの説明を記載します。

パラメーター	説明
User Name	SSH ユーザーを識別するユーザー名を 15 文字以内で入力します。このユーザー名は、事前に構成したユーザーアカウントでなければなりません。
Auth. Mode	管理者は、プルダウンメニューから、次のいずれかを選択して、スイッチへのアクセスを試みるユーザーの認証を設定します。 Host Based - 認証用にリモート SSH サーバーを使用したい場合は、このパラメーターを選択します。このパラメーターを選択する場合は、Host Name、Host IP を入力して SSH ユーザーを識別します。 Password - 認証用にローカルのパスワードを使用したい場合は、このパラメーターを選択します。このパラメーターを入力すると、に再度パスワードを要請され、パスワードをもう一度入力して確定します。 Public Key - 認証用にパブリックキー SSH サーバーに使用したい場合は、このパラメーターを選択します。
Host Name	リモート SSH ユーザーを識別する 32 文字以内の英数字文字列を入力します。このパラメーターを使用するのは、認証モードフィールドでホストベースを選択した場合のみです。
Host IP	SSH ユーザーの対応する IP アドレスを入力します。このパラメーターを使用するのは、認証モードフィールドでホストベースを選択した場合のみです。

[Apply]をクリックして変更を適用します。

3.5.7 Access Authentication Control

Access Authentication Control コマンドで、TACACS/XTACACS/TACACS+/RADIUS プロトコルを使用して、安全にスイッチにアクセスします。ユーザーが、スイッチにログインしたり、管理者レベル権利へのアクセスを試みると、パスワードの入力を要請されます。スイッチ上で TACACS/XTACACS/TACACS+/RADIUS 認証が有効な場合は、スイッチは TACACS/XTACACS/TACACS+/RADIUS サーバーに連絡して、ユーザーを認証します。認証されたユーザーは、スイッチにアクセスできます。

TACACS セキュリティー制御には 3 つのバージョンがあります。それぞれ、独立エンティティーです。スイッチのソフトウェアは次の TACACS バージョンに対応します。

- (1) TACACS - 1 台または複数の集中型 TACACS サーバー経由で UDP プロトコルを使用してパケットを転送し、セキュリティ目的のために、パスワードの確認、認証、ユーザーアクションの通知を提供します。
- (2) XTACACS - TACACS プロトコルの拡張仕様です。TACACS よりも種類の多い認証要求と応答コードを提供します。このプロトコルでも UDP を使用してパケットを転送します。
- (3) TACACS+ - ネットワークデバイスの認証用の詳細なアクセス制御を提供します。TACACS+では、1 台または複数の集中型サーバー経由の認証コマンドを使います。TACACS+プロトコルは、TCP プロトコルを使用してスイッチと TACACS+デーモン間のすべてのトラフィックを暗号化し、配信の信頼性を確保します。

TACACS/XTACACS/TACACS+/RADIUS セキュリティー機能が正しく動作するには、TACACS/XTACACS/TACACS+/RADIUS サーバーをスイッチ以外のデバイス(認証サーバーと呼ばれます)上で構成する必要があります。また、認証用のユーザー名とパスワードが含まれていなければなりません。スイッチがユーザーに認証用のユーザー名とパスワードの入力を要請すると、スイッチは TACACS/XTACACS/TACACS+/RADIUS サーバーに認証要求し、サーバーは次の 3 つのメッセージのいずれかで応答します。

- (1) サーバーはユーザー名とパスワードを認証します。ユーザーはスイッチ上でユーザー権限を取得します。
- (2) サーバーはユーザー名とパスワードを受け入れません。ユーザーはスイッチにアクセスできません。
- (3) サーバーは認証クエリーに応答しません。この時点で、スイッチはサーバーからタイムアウトを受信し、次の認証方法へ移動します。

スイッチには次の 4 つの認証サーバーグループが内蔵されています。それぞれ、TACACS プロトコル、XTACACS プロトコル、TACACS+ プロトコル、RADIUS プロトコル用です。これらの内蔵認証サーバーグループを使用して、スイッチへのアクセスを試みるユーザーを認証します。ユーザーは、認証サーバーを希望する順序で内蔵認証サーバーグループに設定します。ユーザーがスイッチへのアクセスを試行すると、スイッチは、まず、最初の認証サーバーに認証を問い合わせます。認証されないと、2 番目のサーバーにクエリーします。以下、同様に続きます。内蔵認証サーバーグループに設定できるのは、指定したプロトコルを実行しているホストのみです。例えば、TACACS 認証サーバーグループに設定できるのは、TACACS 認証サーバーのみです。

スイッチ管理者は、認証用に、ユーザー定義の方法一覧(TACACS/XTACACS/TACACS+/RADIUS/ローカル/なし)毎に、最大6つの異なる認証技術をセットアップします。これらの技術は希望する順序で一覧表示できます。ユーザーは、これらの技術をスイッチ上の標準ユーザー認証用に定義し、最大8つの認証技術を含めることができます。ユーザーがスイッチへのアクセスを試みると、スイッチは認証用の一覧にある最初の技術を選択します。最初の技術が認証サーバーホストを通過して、認証が返らない場合は、スイッチは、認証用のサーバーグループ内の次の技術へ移動します。この動作は、認証が受け入れられるか、または、拒否されるまで、一覧の最後まで続きます。

TACACS/XTACACS/TACACS+/RADIUS サーバー経由、または、いずれの方法も使わずに正常にデバイスにログインした場合は、ユーザー権限が唯一の割り当てられるレベルとなります。ユーザーが管理者権限を取得したい場合は、[Enable Admin] で権利レベルを高くする必要があります。

3.5.7.1 Authentication Policy Settings

このウィンドウで、スイッチへのアクセスを試みるユーザー用に管理者定義の認証ポリシーを設定します。有効にすると、デバイスはログイン方法一覧を確認して、ログインの際のユーザー認証用の技術を選択します。

次のウィンドウにアクセスするには、Security > Access Authentication Control > Authentication Policy Settings をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
Authentication Policy	プルダウンメニューから、EnabledあるいはDisabledを選択し、スイッチ上の認証ポリシーを有効(Enabled)または無効(Disabled)にします。デフォルト設定は無効(Disabled)です。
Response Timeout (0-255)	スイッチがユーザーからの認証の応答を待つ時間を設定します。0～255秒の範囲で設定します。デフォルト設定は30秒です。
User Attempts (1-255)	スイッチが認証試行を受け入れる最大回数を構成します。設定した最大回数試行しても認証されなかったユーザーは、スイッチへのアクセスが拒否されます。また、認証を試みることができなくなります。コンソールで接続するユーザーは、認証を再試行する前に60秒間待つようにしてください。TelnetとWebベースGUIのユーザーは、スイッチから切断されません。試行回数は1～255の範囲で設定します。デフォルト設定は3です。

[Apply]をクリックして変更を適用します。

3.5.7.2 Application Authentication Settings

このウィンドウで、事前に設定した[Login Method Lists]を使用して、ユーザー権限および管理者権限(管理者の有効化)でログインする際に使用するスイッチ構成アプリケーション(コンソール、Telnet、SSH、HTTP)を設定します。

次のウィンドウを表示するには、Security > Access Authentication Control > Application Authentication Settings をクリックします:

Application	Login Method List	Enable Method List
Console	default	default
Telnet	default	default
SSH	default	default
HTTP	default	default

Apply

下記にパラメーターの説明を記載します。

パラメーター	説明
Application	スイッチ上の構成アプリケーションが一覧表示されます。コンソール、Telnet、SSH、および、HTTP を使用するユーザー用に、ログイン方法一覧と有効化方法一覧を設定します。
Login Method List	プルダウンメニューで、事前に設定した Method List を使用して、ユーザー権限のログイン方法を設定します。デフォルトの Method List、または、ユーザーが構成したその他の Method List を使用します。詳細情報については、本セクションにある[Login Method Lists]ウィンドウを参照してください。
Enable Method List	プルダウンメニューで、事前に設定した Method List を使用して、管理者権限のログイン方法を設定します。デフォルトの方法一覧、または、ユーザーが構成したその他の Method List を使用します。詳細情報については、本セクションにある[Enable Method Lists]ウィンドウを参照してください。

[Apply]をクリックして変更を適用します。

3.5.7.3 Authentication Server Group

このウィンドウで、スイッチ上に認証サーバーグループをセットアップします。サーバーグループは TACACS/XTACACS/TACACS+/RADIUS サーバーをユーザー定義のカテゴリにグループ分けできます。

次のウィンドウを表示するには、Security > Access Authentication Control > Authentication Server Group をクリックします：

The screenshot shows the 'Authentication Sever Group' configuration window with the 'Sever Group List' tab selected. At the top, there are two tabs: 'Sever Group List' and 'Edit Sever Group'. Below the tabs is a form with a 'Group Name (Max: 15 characters)' input field and an 'Add' button. Underneath, a table displays the current list of server groups:

Total Entries: 4		
Group Name	Edit	Delete
radius	Edit	Delete
tacacs	Edit	Delete
tacacs+	Edit	Delete
xtacacs	Edit	Delete

スイッチには 4 つの内蔵認証サーバーグループがあります。これらの内蔵認証サーバーグループは削除できませんが、変更することはできます。

特定のグループを変更するには、対応する [Edit] をクリックするか、または、このウィンドウの一番上にある [Edit Sever Group] タブをクリックします。次のタブが表示されます：

The screenshot shows the 'Authentication Sever Group' configuration window with the 'Edit Sever Group' tab selected. The form includes a 'Group Name (Max: 15 characters)' input field. Below it, the 'Server Host' section contains an 'IP Address' input field, a 'Protocol' dropdown menu (set to 'TACACS'), and an 'Add' button. At the bottom, there is a 'Host List' table with columns for 'IP Address' and 'Protocol'.

認証サーバーを追加するには、認証サーバーの IP アドレスを入力し、プロトコルを選択して、[Add] をクリックします。これで、この認証サーバーがグループに追加されます。

3.5.7.4 Authentication Server

このウィンドウで、スイッチ上の TACACS/XTACACS/TACACS+/RADIUS セキュリティプロトコル用に、ユーザー定義の認証サーバーを設定します。認証ポリシーを有効にしてスイッチへのアクセスを試みると、スイッチは、リモートホスト上のリモート TACACS/XTACACS/TACACS+/RADIUS サーバーに認証パケットを送信します。TACACS/XTACACS/TACACS+/RADIUS サーバーは要求を認証または拒否して、スイッチに正しいメッセージを返します。同じ物理サーバー上で複数の認証プロトコルを実行できます。ただし、TACACS/XTACACS/TACACS+/RADIUS は独立エンティティであり、相互互換性はありません。

サーバーの最大対応数は 16 です。

次のウィンドウを表示するには、Security > Access Authentication Control > Authentication Server をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
IP Address	リモートサーバーの IP アドレスを入力します。
Port (1-65535)	1～65535 の数字を入力して、サーバー上の認証プロトコルの仮想ポート番号を定義します。TACACS/XTACACS/TACACS+サーバーのデフォルトのポート番号は 49 です。RADIUS サーバーのデフォルトのポート番号は 1812 です。高いセキュリティ用に固有のポート番号を設定します。
Protocol	サーバーが使用するプロトコルです。プルダウンメニューから、次のいずれかを選択します。 TACACS - サーバーが TACACS プロトコルを使用する場合に選択します。 XTACACS - サーバーが XTACACS プロトコルを使用する場合に選択します。 TACACS+ - サーバーが TACACS+プロトコルを使用する場合に選択します。 RADIUS - サーバーが RADIUS プロトコルを使用する場合に選択します。
Timeout (1-255)	スイッチの認証要求に対するサーバーからの応答を待つ時間を秒単位で入力します。デフォルト値は 5 です。
Key	設定した TACACS+サーバーまたは RADIUS サーバーと共有する認証キーです。最大 254 文字の英数字文字列を指定します。
Retransmit (1-255)	再送フィールドに値を入力して、サーバーが応答しない場合に、デバイスが認証要求を再送する回数を変更します。デフォルト設定は 2 です。

[Apply]をクリックして、サーバーを追加します。このウィンドウの下半分にあるテーブルに、エントリーが表示されます。

3.5.7.5 Login Method Lists

このウィンドウを使用して、スイッチにログオンするユーザー認証のログインを構成します。このコマンドで適用する認証プロトコルの順序は、認証結果に影響します。例えば、認証プロトコルの順番を TACACS、XTACACS、ローカルとして入力すると、スイッチは、サーバーグループ内の最初の TACACS サーバーへ認証要求を送信します。サーバーから応答がない場合は、スイッチは、サーバーグループ内の 2 番目の TACACS サーバーへ認証要求を送信します。XTACACS 一覧を使用して認証されない場合は、スイッチ内に設定したローカルアカウントデータベースを使用してユーザーを認証します。

TACACS/XTACACS/TACACS+/RADIUS サーバー経由、または、いずれの方法も使わずに、正常にデバイスにログインした場合は、ユーザー権限が割り当てられます。ユーザーが管理者権限を取得したい場合は、[Enable Admin]ウィンドウを使用して、権限を高くする必要があります。

次のウィンドウを表示するには、Security > Access Authentication Control > Login Method Lists をクリックします：

ログイン Method List を変更するには、相応する[Edit]をクリックします。

ログイン方法を定義するには、次のパラメーターを設定して、[Apply]をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
Method List Name	Method List 名を入力します(最大 15 文字)。
Priority 1, 2, 3, 4	この Method List には、プルダウンメニューから、次の組み合わせを最大 4 つまで追加できます： tacacs - TACACS プロトコルを使用してユーザーを認証します。 xtacacs - XTACACS プロトコルを使用してユーザーを認証します。 tacacs+ - TACACS+ プロトコルを使用してユーザーを認証します。 radius - RADIUS プロトコルを使用してユーザーを認証します。 server_group - スイッチ上で事前に構成したユーザー定義のサーバーグループを使用してユーザーを認証します。 local - スイッチ上のローカルユーザーアカウントデータベースを使用してユーザーを認証します。 none - スイッチにアクセスする際の認証は必要ありません。

[Apply]をクリックして変更を適用します。

3.5.7.6 Enable Method Lists

このウィンドウで、スイッチ上の認証方法を使用して Method List をセットアップし、ユーザー権限を管理者(Admin) にします。それには、管理者が定義した方法で認証されなければなりません。最大 8 つの有効な Method List を適用できます。その内の 1 つはデフォルトの Method List です。このデフォルトの Method List は削除できませんが、変更することはできます。

次のウィンドウを表示するには、Security > Access Authentication Control > Enable Method Lists をクリックします：

Enable Method Lists

Method List Name (Max: 15 characters)

Priority 1: Priority 2:
 Priority 3: Priority 4:

Total Entries: 1

Method List Name	Priority 1	Priority 2	Priority 3	Priority 4	
default	local_enable	----	----	----	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

ユーザーが定義した Method List を削除するには、相応する [Delete] をクリックします。 Method List を変更するには、相応する [Edit] をクリックします。

ログイン Method List を定義するには、次のパラメーターを設定して、 [Apply] をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
Method List Name	Method List 名を入力します(最大 15 文字)。
Priority 1, 2, 3, 4	プルダウンメニューから、次の組み合わせを最大 4 つまで追加できます： tacacs - TACACS プロトコルを使用してユーザーを認証します。 xtacacs - XTACACS プロトコルを使用してユーザーを認証します。 tacacs+ - TACACS+ プロトコルを使用してユーザーを認証します。 radius - RADIUS プロトコルを使用してユーザーを認証します。 server_group - スイッチ上で事前に構成したユーザー定義のサーバーグループを使用してユーザーを認証します。 local - スイッチ上のローカルユーザーアカウントデータベースを使用してユーザーを認証します。 none - スイッチにアクセスする際の認証は必要ありません。

[Apply] をクリックして変更を適用します。

3.5.7.7 Local Enable Password Settings

このウィンドウで、[enable admin]コマンド用のローカルに有効化したパスワードを構成します。
"local_enable"を選択して、ユーザーレベル権利を管理者権利にすると、ユーザーはここで構成したパスワードの入力を要請されます。このパスワードはスイッチ上にローカル設定されます。

次のウィンドウを表示するには、Security > Access Authentication Control > Local Enable Password Settings をクリックします:



ローカルパスワードを設定するには、次のパラメーターを構成して、[Apply]をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
Old Local Enable Password (Max: 15 characters)	事前に設定したパスワードを入力します。パスワードの最大長さは 15 文字です。
New Local Enable Password	管理者権限に変更する際に使用する新しいパスワードを入力します。パスワードの最大長さは 15 文字です。
Confirm Local Enable Password	上で入力した新しいパスワードを確定します。違うパスワードを入力すると、エラーメッセージが表示されます。

[Apply]をクリックして変更を適用します。

3.5.8 MAC-based Access Control

MACベースアクセス制御は、ポートまたはホストベースによる認証が可能です。

ユーザーは、ネットワークへのアクセスを許可される前に認証する必要があります。認証方法は、ローカル認証とRADIUSサーバー認証および強制認証に対応します。MACベースアクセス制御では、ローカルデータベースまたはRADIUSサーバーデータベース内のMACユーザー情報を認証のために検索します。

注意事項

- ❗ Ver.1.05以降のファームウェアより、MACベースアクセス制御と組み合わせたローミング機能をサポートします。認証されたホストが同一装置内の別の認証ポートへローミングする場合、新しいポートで認証状態が引き継がれます。
- ❗ ダイナミック VLAN により動的 VLAN を割り当てる場合、ローミングするポートの VLAN ID が異なるため、ポートの Ingress checking 設定を無効にする必要があります。この設定は「GVRP Settings」ウィンドウで行います。
- ❗ 動的 VLAN を使用する場合、割り当て可能な最大収容数は 64 端末です。最大数 64 には、MAC/Web/802.1X の各認証で使用する動的 VLAN の端末数を含みます。（動的 VLAN を使用しない端末は、この最大収容数には含まれません）

MAC ベースアクセス制御に関する注記

MAC ベースアクセス制御には特定の制限および規制があります。

この機能をポート用に有効にすると、スイッチはそのポートの FDB を消去します。

また、リングアグリゲーション、ポートセキュリティー、GVRP を有効にしたポートでは、MAC ベース認証を有効にすることはできません。

3.5.8.1 MAC-based Access Control Settings

このウィンドウを使用して、スイッチ上の MAC ベースアクセス制御機能のパラメーターを設定します。

次のウィンドウを表示するには、Security > MAC-based Access Control > MAC-based Access Control Settings をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
設定	
MBA Global State	ラジオボタンで、Enabled または Disabled を選択して、MAC ベースアクセス制御機能をグローバルに有効(Enabled)または無効(Disabled)にします。
Method	指定したポートで MAC 認証する際の認証の種類としてプルダウンメニューから、RADIUS、Local を選択します。 RADIUS - リモート RADIUS サーバーを MAC ベースアクセス制御用のオーセンティケーターとして使用します。MAC アドレス一覧は事前に RADIUS サーバー上に設定し、サーバーの設定はまずスイッチ上で最初に構成する必要があります。 Local - この方法を使用して、ローカル設定した MAC アドレスデータベースを MAC ベースアクセス制御用のオーセンティケーターとして使用します。この MAC アドレス一覧は、MAC ベースアクセス制御ローカルデータベース設定ウィンドウで構成できます。

パラメーター	説明
設定	
Password	MAC ベースアクセス制御の認証時に使用する RADIUS サーバーのパスワードを入力します。デフォルトパスワードは default です。
Authentication Failover	プルダウンメニューから、RADIUS サーバーからの認証応答がない場合、ローカルデータベースによる認証(Local)する、強制的に認証許可を行う(Permit)、または failover を行わない(Disable)設定を行います。 Permit - RADIUS サーバーの応答がない時、強制的に認証許可を行います。 Local - RADIUS サーバーの応答がない時、ローカルデータベースによる認証を行います。 Disable - RADIUS サーバーの応答がない時、failover を行いません。 デフォルト設定は無効です。
Permit VLAN ID	Auth Failover で強制認証許可[Permit]後に所属する VLAN ID を設定します。
Authorization Network	プルダウンメニューから、Enabled あるいは Disabled を選択します。有効(Enabled)な場合は、RADIUS サーバーまたはローカルデータベースに従って割り当てた認証済み属性(VLAN など) となっています。どの属性を受け入れるかは、各モジュールの設定によって異なります。 デフォルトでは、属性の認証は無効(Disabled)になっています。
Max User (1-128)	装置全体で収容可能な端末数を 1~128 で入力します。デフォルトは 128 です。ポート毎の収容数(初期値 128)設定と併せて No Limit 指定した場合、使用環境下によりませんが、目安として 512 端末程度の利用が可能です。
Password Type	プルダウンメニューから、MAC ベースアクセス制御のパスワードタイプを設定します。 manual_string - RADIUS 認証時に装置に設定したパスワードを使用します。 client_mac_address - RADIUS 認証時にクライアントの MAC アドレスをパスワードとして使用します。
MAC Format	プルダウンメニューから、MAC ベースアクセス制御の MAC アドレスフォーマットを設定します。 Uppercase, None - 区切り文字を使用せず大文字を使用する場合に設定します。 Uppercase, Hyphen - 区切り文字を使用し大文字を使用する場合に設定します。 Lowercase, None - 区切り文字を使用せず小文字を使用する場合に設定します。 Lowercase, Hyphen - 区切り文字を使用し小文字を使用する場合に設定します。
From Port/ To Port	MAC ベースアクセス制御を設定するポート範囲を選択します。
State	プルダウンメニューから、Enabled あるいは Disabled を選択し、各ポート上の MAC ベースアクセス制御機能を有効(Enabled)または無効(Disabled)にします。
Aging Time (1-1440)	1~1440 分のエイジング値を入力します。デフォルトは 1440 です。エイジングタイムがない場合は、Infinite チェックボックスにチェックを入れます。
Hold Time (1-300)	1~300 秒の保留値を入力します。デフォルトは 300 です。保留時間がない場合は、Infinite チェックボックスにチェックを入れます。
Max User (1-128)	ポート毎の収容可能な端末数を 1~128 で入力します。デフォルトは 128 です。装置全体の収容数(初期値 128)設定と併せて No Limit 指定した場合、使用環境下によりませんが、目安として 512 端末程度の利用が可能です。

[Apply]をクリックして変更を適用します。

注意事項

- ❗ フェイルオーバー機能における強制的な認証許可(Permit)は、セキュリティー上問題となる可能性があるため、十分検討の上、使用してください。
- ❗ フェイルオーバー機能設定時、RADIUS サーバーのタイムアウト時間は 30 秒以内に設定してください。デフォルト設定は 15 秒です。

3.5.8.2 MAC-based Access Control Local Settings

次のウィンドウを使用して、ローカル認証で使用する MAC アドレス、VLAN を登録します。認証を要求する MAC アドレスがこのテーブルと一致すると関連する VLAN がアサインされます。スイッチ管理者は、最大 128 の MAC アドレスを入力することでこれらの端末をローカル認証することができます。

次のウィンドウを表示するには、Security > MAC-based Access Control > MAC-based Access Control Local Settings をクリックします：

MAC Address	VLAN Name	VLAN ID
00-11-22-33-44-55	default	1

[Add]をクリックして新しいエントリーを追加します。

[Delete By MAC]をクリックして入力 MAC アドレスに基づくエントリーを消去します。

[Delete By VLAN]をクリックして入力 VLAN 名又は ID に基づくエントリーを消去します。

[Find By MAC]をクリックして入力 MAC アドレスに基づくエントリーを検索します。

[Find By VLAN]をクリックして入力 VLAN 名又は ID に基づくエントリーを検索します。

[View All]をクリックしてスイッチで有効な全てのエントリー一覧を表示します。

[Edit By Name]をクリックして指定エントリーの VLAN 名を再設定します。

[Edit By ID]をクリックして指定エントリーの VLAN ID を再設定します。

3.5.9 Web Authentication

Web認証は、ポートまたはホストベースによる認証が可能です。

ユーザーは、ネットワークへのアクセスを許可される前に認証する必要があります。認証方法は、ローカル認証とRADIUSサーバー認証および強制認証に対応します。IPv6のWeb認証は未サポートです。

注意事項

- ❗ Ver.1.05 以降のファームウェアより、Web 認証と組み合わせたローミング機能をサポートします。認証されたホストが同一装置内の別の認証ポートへローミングする場合、新しいポートで認証状態が引き継がれます。
- ❗ ダイナミック VLAN により動的 VLAN を割り当てる場合、ローミングするポートの VLAN ID が異なるため、ポートの Ingres checking 設定を無効にする必要があります。この設定は「GVRP Settings」ウィンドウで行います。
- ❗ Web 認証前の最大同時セッション数は 63 です。
- ❗ 動的 VLAN を使用する場合、割り当て可能な最大収容数は 64 端末です。最大数 64 には、MAC/Web/802.1X の各認証で使用する動的 VLAN の端末数を含みます。（動的 VLAN を使用しない端末は、この最大収容数には含まれません）

3.5.9.1 Web Authentication Settings

次のウィンドウで Web 認証の設定を行います。

スイッチの Web 認証を設定するためには Security > Web Authentication > Web Authentication Settings をクリックします。



Web Authentication Settings			
State	Disabled ▼	Method	Local ▼
Authentication Failover	Disabled ▼	Permit VLAN ID	<input type="text"/>
Virtual IP	0.0.0.0	Port Number(1-65535)	80 <input type="radio"/> HTTP <input type="radio"/> HTTPS
RADIUS Authorization	Enabled ▼	Redirection Path	<input type="text"/>
Local Authorization	Enabled ▼	Session Timeout(0-120)	120
Redirect Action	Enabled ▼		
			<input type="button" value="Apply"/>

下記にパラメーターの説明を記載します。

パラメーター	説明
State	プルダウンメニューから、Enabled あるいは Disabled を選択し、Web 認証機能を有効(Enabled)または無効(Disabled)にします。
Method	プルダウンメニューから RADIUS あるいは Local を選択し、Web 認証方法を設定します。RADIUS を選択した場合は RADIUS プロトコルで Web 認証が行われます。Local を選択した場合はローカルデータベースで Web 認証が行われます。
Authentication Failover	プルダウンメニューから RADIUS サーバーからの認証応答がない場合、ローカルデータベースによる認証(Local)する、強制的に認証許可を行う(Permit)、または failover を行わない(Disable)設定を行います。 Permit - RADIUS サーバーの応答がない時、強制的に認証許可を行います。 Local - RADIUS サーバーの応答がない時、ローカルデータベースによる認証を行います。 Disable - RADIUS サーバーの応答がない時、failover を行いません。
Permit VLAN ID	Auth Failover で認証許可[Permit]後に所属する VLAN ID を設定します。
Virtual IP	仮想 IP の IP アドレスを指定します。 仮想 IP に "0.0.0.0" を設定した場合、Web 認証機能を有効にできません。
Port Number	HTTP ポート番号を設定します。デフォルトは 80 です。 HTTP - Web 認証を HTTP プロトコルで実行します。ポート番号のデフォルトは 80 です。TCP ポート番号を 443 にすることはできません。 HTTPS - Web 認証を HTTPS プロトコルで実行します。ポート番号のデフォルトは 443 です。TCP ポート番号を 80 にすることはできません。
RADIUS Authorization	RADIUS サーバーによる認証時に、認証属性情報を使用するか(Enabled)、使用しないか(Disabled)を指定します。
Redirection Path	認証が成功した後、ここに設定した URL にリダイレクトされます。この URL がクリアされると、他の URL にリダイレクトされません。
Local Authorization	ローカルデータベースでの認証時に、認証属性情報(VLAN 情報)を使用するか(Enabled)、使用しないか(Disabled)を指定します。
Session Timeout(0-120)	Web 認証ポートのセッションタイムアウト時間を指定します。未認証端末が短期間に多数のセッションを確立する場合の装置の負荷を緩和することができます。
Redirect Action	プルダウンメニューから、Enabled あるいは Disabled を選択します。有効(Enabled)の場合、未認証端末が Web 認証用の仮想 IP アドレス以外のサイトにアクセスした際に、強制的に仮想 IP アドレスにリダイレクトさせます。無効(Disabled)の場合、リダイレクトは行われず、Web 認証をクリアするためには明示的に仮想 IP アドレスを指定して Web アクセスする必要があります。

[Apply]をクリックして変更を適用します。

注意事項

-  フェイルオーバー機能における強制的な認証許可(Permit)は、セキュリティー上問題となる可能性があるため、十分検討の上、使用してください。
-  フェイルオーバー機能設定時、RADIUS サーバーのタイムアウト時間は 30 秒以内に設定してください。デフォルト設定は 15 秒です。

3.5.9.2 Web Authentication User Settings

以下のウィンドウはスイッチによって使用されている Web 認証ユーザー設定を行う時に用います。

スイッチの Web 認証を設定するためには Security > Web Authentication > Web Authentication User Settings をクリックします

Web Authentication User Settings

Create User

User Name VLAN Name VLAN ID(1-4094) Password Confirmation

Total Entries: 0

User Name	VLAN Name	VID Password
-----------	-----------	--------------

下記にパラメーターの説明を記載します。

パラメーター	説明
User Name	Web ベースアクセス制御アカウント用のユーザー名を指定します。
VLAN Name	Web ベースアクセス制御アカウント用の VLAN 名を指定します。
VLAN ID	Web ベースアクセス制御アカウント用の VLAN ID を指定します。
Password	Web ベースアクセス制御アカウント用のパスワードを指定します。
Confirmation	Web ベースアクセス制御アカウント用の確認パスワードを指定します。

[Apply]をクリックして変更を適用します。

[Delete All]をクリックしてリストから全ての設定されたアカウントを削除します。

3.5.9.3 Web Authentication Port Settings

以下のウィンドウはスイッチによって使用されている Web 認証設定を行う時に用います

スイッチの Web 認証設定を行うには、Security > Web Authentication > Web Authentication Port Settings をクリックします。

Port	State	Aging Time	Block Time
1	Disabled	1440	60
2	Disabled	1440	60
3	Disabled	1440	60
4	Disabled	1440	60
5	Disabled	1440	60
6	Disabled	1440	60
7	Disabled	1440	60
8	Disabled	1440	60
9	Disabled	1440	60
10	Disabled	1440	60
11	Disabled	1440	60
12	Disabled	1440	60
13	Disabled	1440	60

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	この設定で使用するポート範囲を選択します
State	プルダウンメニューから、Enabled あるいは Disabled を選択し、ポートに対する Web 認証を有効(Enabled)または無効(Disabled)に設定します。
Aging Time	認証されたホストが認証状態を保持する時間を設定します。Infinite を設定すると、ポート上で認証されたホストがエージアウトされなくなります
Block Time	認証に失敗すると、block time で設定された間隔の間ブロックされます。

[Apply]をクリックして変更を適用します。

注意事項

- ❗ Web 認証が有効なポートで認証の対象となるフレームは、イーサネットフレームタイプが IP かつ IP プロトコルタイプが TCP のフレームとなります。認証の対象外となるフレーム（例えば ICMP, UDP など）は、認証テーブルへ登録されますが、認証による廃棄は行われませんのでご注意ください。また、IPv6 についても対象外フレームのため認証されずに装置中継します。

3.5.9.4 Web Authentication Customize

以下のウィンドウはスイッチによって使用されている Web 認証ログイン画面およびログアウト画面のカスタマイズ設定を行う時に用います。

スイッチの Web 認証ログイン画面のカスタマイズ設定を行うには、Security > Web Authentication > Web Authentication Customize をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
English/Japanese	カスタマイズ画面に表示する言語を英語または日本語から選択します。
Login/Logout	ログイン画面またはログアウト画面のどちらをカスタマイズするか指定します。
Customize Textbox(1-8)	ログイン画面下にある 1 番から 8 番のユーザーテキストボックスに文字を登録します。 登録可能な任意の文字列は最大で半角 70 文字です。全角の場合は最大 35 文字となります。

[Clear]をクリックして登録内容を初期化します。

[Apply]をクリックして変更を適用します。

[Preview]をクリックして登録されている内容の確認画面を表示します。

ログインプレビュー画面

現状ステータス: **未認証**

Web認証ログイン

ユーザー名	<input type="text"/>
パスワード	<input type="password"/>
<input type="button" value="入力"/> <input type="button" value="クリア"/>	

ご利用方法がわからない方は下記へご連絡ください。

[問い合わせ先]

情報システム統括部 ネットワーク運用担当
担当者名: Network Manager
TEL : 123-4567
MAIL : network.manager.ab@apresiasystems.com

スイッチの Web 認証ログアウト画面のカスタマイズ設定を行うには、Security > Web Authentication > Web Authentication Customize をクリックし、画面左上のプルダウンメニューで Logout を選択します。

Japanese ▾ Logout ▾

現状ステータス: **認証済**

Web認証ログイン

ログイン成功！
このウィンドウを閉じるか、下記のボタンを押して下さい。

Thank you!

Note: Each line in Customize Textbox should be less than 70 octets.

Customize Textbox	
1.	ご利用方法がわからない方は下記へご連絡ください。
2.	
3.	[問い合わせ先]
4.	
5.	情報システム統括部 ネットワーク運用担当
6.	担当者名: Network Manager
7.	TEL : 123-4567
8.	MAIL : network.manager.ab@apresiasystems.com

下記にパラメーターの説明を記載します。

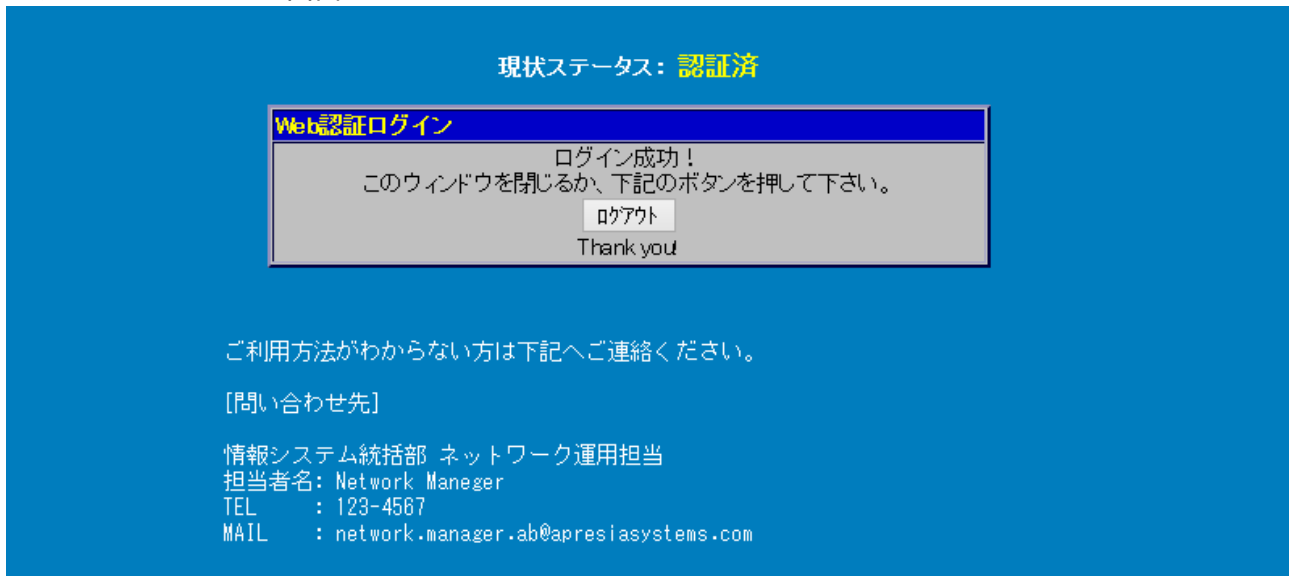
パラメーター	説明
English/Japanese	カスタマイズ画面に表示する言語を英語または日本語から選択します。
Login/Logout	ログイン画面またはログアウト画面のどちらをカスタマイズするか指定します。
Customize Textbox(1-8)	ログアウト画面下にある 1 番から 8 番のユーザーテキストボックスに文字を登録します。 登録可能な任意の文字列は最大で半角 70 文字です。全角の場合は最大 35 文字となります。

[Clear]をクリックして登録内容を初期化します。

[Apply]をクリックして変更を適用します。

[Preview]をクリックして登録されている内容の確認画面を表示します。

ログアウトプレビュー画面



現状ステータス: **認証済**

Web認証ログイン

ログイン成功!
このウィンドウを閉じるか、下記のボタンを押して下さい。

Thank you

ご利用方法がわからない方は下記へご連絡ください。

[問い合わせ先]

情報システム統括部 ネットワーク運用担当
担当者名: Network Manager
TEL : 123-4567
MAIL : network.manager.ab@apresiasystems.com

3.6 アクセス制御一覧(ACL)

アクセスプロファイルで、スイッチが各パケットのヘッダーにある情報に基づいてパケットを転送するかどうかを決める際の基準を設定します。これらの基準は、パケット内容、MAC アドレス、または、IP アドレスに基づいて指定します。

3.6.1 ACL Configuration Wizard

ACL Configuration Wizard を使用すると、ACL によるアクセス制御を簡単に設定することができます。ただし、本設定画面で設定可能な ACL はホストベースの簡易的な内容のみです。より細かいルールを設定する場合は、次節に説明する Access Profile List の画面を使用してください。

次のウィンドウを表示するには、ACL > ACL Configuration Wizard をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
Profile ID (1-256)	プロファイル ID を指定します。当該 ID のプロファイルが登録されていない場合、新規プロファイルが登録されます。この値は 1 ~ 256 の範囲で設定します。
Access ID (1-65535)	登録するルールのアクセス ID を設定します。この値は 1 ~ 65535 の範囲で設定します。Auto Assign がチェックされている場合、自動的に採番されます。
From/To	プルダウンメニューで、From(送信元)および To(送信先)の識別方式を[MAC Address]、[IPv4 Address]、[IPv6]、[Any]から選択します。[IPv6] は送信元のみ選択できます。[Any]以外を選択した場合、右側に入力ボックスが出現しますので、識別方式に応じた形式で識別子(アドレス)を入力します。
Action	プルダウンメニューから、[Permit][Deny][Mirror]を選択します。 [Permit]を選択すると、合致するパケットを転送するルールを構成します。 [Deny]を選択すると、合致するパケットをドロップするルールを構成します。 [Mirror]を選択すると、合致するパケットを、ミラーポートの設定で指定したポートにミラーすることを指定します。この場合、ポートミラーリングを有効にして、ターゲットポートを設定する必要があります。
Option	プルダウンメニューで、[Rate Limiting]、[1P Priority]、[Replace DSCP]から選択します。
Ports	ルールを適用するポートの範囲を入力します。

[Apply]をクリックして変更を適用します。

3.6.2 Access Profile List

アクセスプロファイルを作成するには2つの基本手順に従います。まず、スイッチが確認するフレームの部分を指定します(MAC 送信元アドレスや IP 送信先アドレスなど)。次に、フレームの処理について決める際にスイッチが使用する基準を入力します。

次のウィンドウを表示するには、ACL > Access Profile Lists をクリックします：

Profile ID	Profile Type	Owner Type	Show Details	Add/View Rules	Delete
1	Ethernet	ACL	Show Details	Add/View Rules	Delete
2	IP	ACL	Show Details	Add/View Rules	Delete
3	IPv6	ACL	Show Details	Add/View Rules	Delete
4	Packet Content	ACL	Show Details	Add/View Rules	Delete

ACL プロファイルを新規作成するには、[Add ACL Profile]をクリックします。既存 ACL プロファイルの設定を表示するには、相応する[Show Details]をクリックします。ACL プロファイルにルールを追加するには、相応する[Add/View Rules]をクリックします。既存の ACL プロファイルを削除するには、相応する[Delete]をクリックします。すべての ACL プロファイルエントリーを削除するには、[Delete All]をクリックします。

ACL プロファイルを追加するには、[Add ACL Profile]をクリックします。

Select Profile ID: 1

Select ACL Type

Ethernet ACL IPv4 ACL

IPv6 ACL Packet Content ACL

Select

<<Back Create

アクセスプロファイルを作成する際、以下の4種類のACLタイプからいずれかを選択します。

- (1) Ethernet ACL
- (2) IPv4 ACL
- (3) IPv6 ACL
- (4) Packet Content ACL

ACL タイプを選択し、[Select]をクリックすると、ACL タイプに応じた設定画面が出現します。以下の画面は、ACL タイプとして Ethernet ACL を選択した場合のもので、フレームフォーマットを模した図はフィールド毎にボタンになっており、ボタンをクリックするとボタンが赤色に変わり、当該フィールドが検査対象になります。また、設定用のパラメーターが下の枠内に表示されます。

Add ACL Profile

Select Profile ID

Select ACL Type

Ethernet ACL IPv4 ACL Packet Content ACL

IPv6 ACL

You can select the field in the packet to create filtering mask

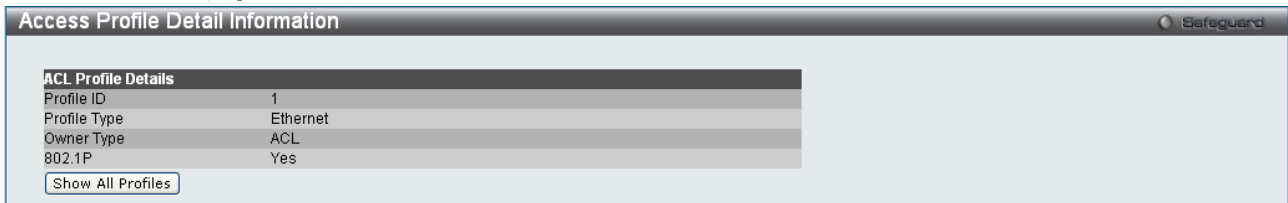
MAC Address	VLAN	802.1p	Ethernet Type	PayLoad
-------------	------	--------	---------------	---------

注意事項

- !** APLGM シリーズでは ACL の各タイプに対してルールを書き込むグループが装置内部に割り当てられ、独立して動作します。
受信パケットが同一グループ内の複数ルールに該当する場合、最も低いプロファイル ID 及びアクセス ID をもつ ACL ルールが優先と判断されますが、該当するルールが複数のグループに存在する場合、対象となる全てのグループに対して調査し、最終的な優先順位は permit 及び deny (deny が上位) によって判断されません。
- !** IPv6 ACL と Packet Content ACL、及び DHCP Snooping 機能は、最大でも 2 個までしか併用できません。また、2 個併用した場合は、一つのタイプに対して設定可能な ACL の最大ルール数が、最大合計登録数の約半分に制限されます。
- !** APLGM シリーズで設定可能なルール数は Ethernet ACL、IPv4 ACL、IPv6 ACL、Packet Content ACL の全てのタイプの合計で最大 256 です。一つの ACL タイプに対して設定可能なルール数は、最大合計登録数を超えない範囲内では原則として制限はありませんが、以下の場合に登録数が制限されることがあります。

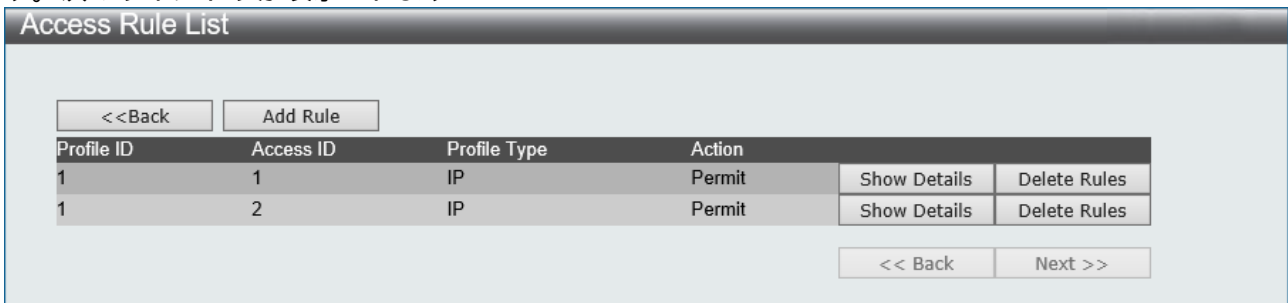
 - DHCP スヌーピング機能を有効にしている場合
 - IPv6 ACL もしくは Packet Content ACL のルールを使用している場合

事前に構成したエントリーの構成を表示するには、相応する[Show Details]をクリックします。次のウィンドウが表示されます：



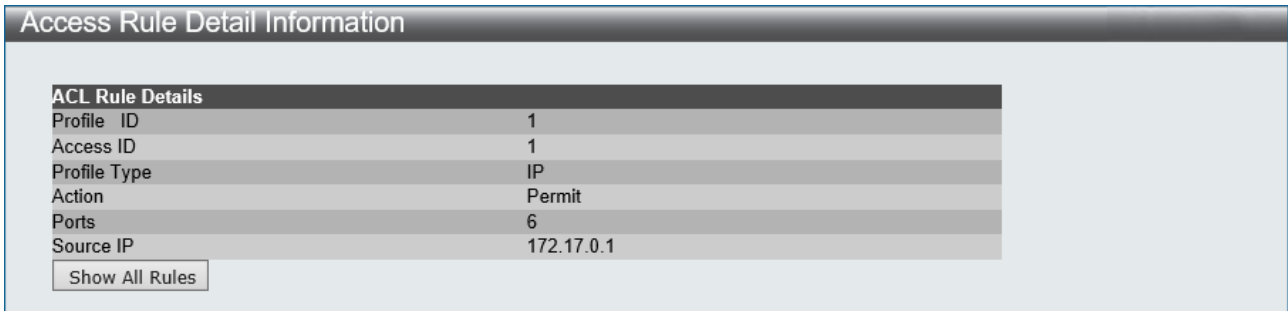
[Access Profile List]ウィンドウに戻るには、[Show All Profiles]をクリックします。

事前に構成したエントリーにルールを追加するには、相応する[Add/View Rules]をクリックします。次のウィンドウが表示されます：



[Add Rule]をクリックすると、ルール設定の画面に移行します（ルール設定画面はACLタイプによって異なります。詳細は次ページ以降の各タイプ別設定の記載を確認してください）。設定されているルールを確認する場合、相対する[Show Details]をクリックします。ルールを削除するには、相対する[Delete Rules]をクリックします。

事前に構成したルールを表示するには、相応する[Show Details]をクリックします。次のウィンドウが表示されます：



[Access Rule List]ウィンドウに戻るには、[Show All Rules]をクリックします。

(1) Ethernet ACL の設定

[Add ACL Profile]画面から Ethernet ACL を選択した場合、Ethernet ACL プロファイル設定用の画面になります。

下記に Ethernet ACL タイプのプロファイル設定パラメーターの説明を記載します。

パラメーター	説明
Select ACL Type	下記に示す各 ACL タイプからプロファイルを設定します。選択した種類のプロファイルの要件に従ってウィンドウが変わります。 [Ethernet ACL]各パケットのヘッダー内のレイヤー2 部分を対象にします。 [IPv4 ACL]各フレームのヘッダー内の IPv4 アドレスを対象にします。 [IPv6 ACL]各フレームのヘッダー内の IPv6 アドレスを対象にします。 [Packet Content ACL]各パケットのヘッダー内の指定マスクを対象にします。
MAC Address	どちらかの[Source MAC Mask]にチェックを入れて、送信元 MAC アドレスマスクまたは[Destination MAC Mask]を入力し、次に、送信先 MAC アドレスマスクを入力します。
802.1Q VLAN	VLAN - VLAN を指定します。 VLAN Mask (0-FFF) - VLAN マスクを指定します。 このオプションを選択して、スイッチが各パケットヘッダーの VLAN 識別子を確認し、これを転送用の基準、または、基準の一部として使用します。
802.1p	このオプションを選択して、スイッチが各パケットヘッダーの 802.1p 優先度値を確認し、これを転送用の基準、または、基準の一部として使用します。
Ethernet Type	このオプションを選択して、スイッチが各フレームのヘッダーにあるイーサネットタイプの値を確認します。

各設定を入力して[Create]をクリックすると、[Access Profile List]ウィンドウに新しいACL プロファイルエントリーが挿入されます。

ACL プロファイルエントリーにルールを追加するには、[Access Profile List]から相対する [Add/View Rules]をクリックし、[Access Rules List]から[Add Rule]をクリックします。次のウィンドウが表示されます：

下記に Ethernet ACL タイプのルール設定のパラメーターの説明を記載します。

パラメーター	説明
Access ID (1-65535)	アクセス用の固有識別子番号を入力します。この値は 1 ~ 65535 の範囲で設定します。 Auto Assign - このチェックボックスにチェックを入れ、作成しているルールに対し、スイッチが自動的にアクセス ID を割当てます。
VLAN Name	スイッチが各パケットヘッダーの VLAN 識別子を確認し、これを転送用の基準、または基準の一部として使用します。
VLAN ID (1-4094)	事前に設定した VLAN ID を指定します。
VLAN ID	事前に設定した VLAN の VLAN ID を入力します。
Source MAC Address	送信元 MAC アドレスの MAC アドレスを指定します。
Source MAC Mask	送信元 MAC アドレスの MAC アドレスマスクを指定します。このマスクは 16 進数形式で入力します。

パラメーター	説明
Destination MAC Address	送信先 MAC アドレスの MAC アドレスを指定します。
Destination MAC Mask	送信先 MAC アドレスの MAC アドレスマスクを指定します。このマスクは 16 進数形式で入力します。
802.1p (0-7)	0~7 の値を入力して、この 802.1p 優先値のあるパケットだけにアクセスプロファイルを適用するように指定します。
Ethernet Type (0-FFFF)	値を入力することで、パケットヘッダーにこの 16 進数 802.1Q イーサネットタイプのあるパケットだけにアクセスプロファイルを適用するように指定します。
Action	プルダウンメニューから、[Permit][Deny][Mirror]を選択します。 [Permit]を選択すると、合致するパケットを転送するルールを構成します。 [Deny]を選択すると、合致するパケットをドロップするルールを構成します。 [Mirror]を選択すると、合致するパケットを、ミラーポートの設定で指定したポートにミラーすることを指定します。この場合、ポートミラーリングを有効にして、ターゲットポートを設定する必要があります。
Priority (0-7)	パケットの 802.1p ユーザー優先度を、優先度フィールドに入力した値(このコマンドで事前に指定した基準を満たす値)に書き直す場合は、指定した CoS キューに転送する前に優先度値を入力します。 優先度付きキュー、CoS キュー、および、802.1p のマッピングに関する詳細情報については、本マニュアルの QoS のセクションを参照してください。
Replace Priority	指定した CoS キューに転送する前に、ボックスをクリックしてこのオプションを有効にし、優先度フィールドに入力した 802.1p ユーザー優先度値(このコマンドで前に指定した基準を満たす値)を書き直す際に使用する置換値を手動で入力します。そうしないと、パケットの受信 802.1p ユーザー優先度は、スイッチで転送される前に元の値に書き直されます。
Replace DSCP (0-63)	スイッチが DSCP 値(選択した基準を満たすパケットにある値)を隣接するフィールドに入力した値で置き換えます。
Counter	プルダウンメニューでカウンター機能の有効(Enabled)または無効(Disabled)を指定します。デフォルト設定は無効(Disabled)です。
Ports	ルールを適用するポート範囲を入力します。

各設定項目を入力し、[Apply]をクリックすると ACL ルールが追加されます。

(2) IPv4 ACL の設定

[Add ACL Profile]画面から IPv4 ACL を選択すると、IPv4 ACL 設定用の画面になります。

IPv4 ACL ラジオボタンをチェックすると、右にプロトコル ([ICMP]、[IGMP]、[TCP]、[UDP]、[Protocol ID]) を選択するプルダウンメニューが出現します。プロトコルを選択後、[Select]をクリックすると、次のウィンドウが表示されます(このウィンドウは、[ICMP]、[IGMP]、[TCP]、[UDP]、[Protocol ID]のどれを選択したかによって異なります):

The screenshot shows the 'Add ACL Profile' configuration window. At the top, 'Select Profile ID' is set to 2. Under 'Select ACL Type', 'IPv4 ACL' is selected with a radio button, and 'ICMP' is chosen from the protocol dropdown menu. A 'Select' button is visible. Below this, a row of tabs allows selecting the field in the packet to create a filtering mask: 'L2 Header', 'VLAN', 'IPv4 DSCP', 'IPv4 Address', and 'ICMP'. The 'ICMP' tab is active, showing the following settings:

- 802.1Q VLAN**
 - VLAN
 - VLAN Mask (0-FFF) []
- IPv4 DSCP**
 - DSCP
- IPv4 Address**
 - Source IP Mask []
 - Destination IP Mask []
- ICMP**
 - ICMP
 - ICMP Type ICMP Code

At the bottom of the window, there are '<- Back' and 'Create' buttons.

下記に IPv4 ALC タイプのプロファイル設定パラメーターの説明を記載します。

パラメーター	説明
VLAN	スイッチが各パケットヘッダーの VLAN 部分を確認し、これを転送用の基準、または、基準の一部として使用します。
IPv4 DSCP	スイッチが各パケットヘッダーの DiffServ コード部分を確認し、これを転送用の基準、または、基準の一部として使用します。
IPv4 Address	[Source IP Mask]または[Destination IP Mask]のどちらかにチェックを入れてそれぞれの IPv4 送信元アドレスマスクまたは IPv4 送信先アドレスマスクを入力します。
ICMP	[ICMP] にチェックを入れて、スイッチが各パケット内の ICMP フィールドを確認するように指定します。 [ICMP Type]にチェックを入れて、アクセスプロファイルをこの ICMP タイプ値に適用するように指定します。 [ICMP Code]にチェックを入れて、アクセスプロファイルをこの ICMP コード値に適用するように指定します。
IGMP	[IGMP] にチェックを入れて、スイッチが各フレームのヘッダー内の IGMP フィールドを確認します。 [IGMP Type]にチェックを入れて、アクセスプロファイルが IGMP タイプ値を適用するように指定します。
TCP	[TCP] にチェックを入れて、受信パケットに含まれる TCP ポート番号を転送基準として使用します。[TCP]にチェックを入れる場合は、送信元ポートマスクまたは送信先ポートマスクを指定する必要があります。フィルターするフラグビットを識別することもできます。フラグビットはパケットの一部です。これでパケットの処理を決めます。[TCP] フィールドのフラグビットに相応するボックスにチックを入れて、指定のフラグビットをフィルターして、パケットをフィルターできます。 Source Port Mask (0-FFFF) - フィルターする送信元ポートの TCP ポートマスクにチェックを入れて、16 進数(16 進法 0x0-0xffff)で指定します。 Destination Port Mask (0-FFFF) - フィルターする送信先ポートの TCP ポートマスクにチェックを入れて、16 進数(16 進法 0x0-0xffff)で指定します。 TCP Flag Bits - [URG]、[ACK]、[PSH]、[RST]、[SYN]、[FIN]、[Check All] にチェックをいれて、パケット内の指定のフラグビットをフィルターします。
UDP	[UDP] にチェックを入れて、受信パケットに含まれる UDP ポート番号を転送基準として使用します。[UDP]にチェックを入れる場合は、送信元ポートマスクまたは送信先ポートマスクを指定する必要があります。 Source Port Mask - フィルターする送信元ポートの TCP ポートマスクにチェックを入れて、16 進数(16 進法 0x0-0xffff)で指定します。 Destination Port Mask - フィルターする送信先ポートの TCP ポートマスクにチェックを入れて、16 進数(16 進法 0x0-0xffff)で指定します。
Protocol ID	[Protocol ID Mask]にチェックを入れて、非表示にするパケットヘッダー内のプロトコル ID を定義する値を入力します。 Protocol ID Mask (0-FF) - にチェックを入れて、IP ヘッダーの後のマスクオプションを定義する値を入力します。

各設定を入力して[Create]をクリックすると、[Access Profile List]ウィンドウに新しいACL プロファイルエントリーが挿入されます。

ACL プロファイルエントリーにルールを追加するには、[Access Profile List]から相対する [Add/View Rules]をクリックし、[Access Rules List]から[Add Rule]をクリックします。次のウィンドウが表示されます：

下記に IPv4 ACL タイプのルール設定のパラメーターの説明を記載します。

パラメーター	説明
Access ID (1-65535)	このアクセス用の固有識別子番号を入力します。この値は 1 ~ 65535 の範囲で設定します。
VLAN Name	VLAN 名を指定します。
VLAN ID (1-4094)	Mask ____ (0-FFF) - VLAN ID を指定します。
Source IP Address	送信元 IP アドレスを指定します。
Source IP Mask	送信元 IP アドレスの IP アドレスマスクを指定します。
Destination IP Address	送信先 IP アドレスを指定します。
Destination IP Mask	送信先 IP アドレスの送信先 IP アドレスマスクを指定します。
DSCP	スイッチが各パケットヘッダーの DiffServ コード部分を確認し、これを転送用の基準、または、基準の一部として使用します。

パラメーター	説明
ICMP	ICMP を選択して、各フレームのヘッダー内の ICMP フィールドを確認します。 ICMP Type - ICMP タイプフィールドを確認するように指定します。 ICMP Code - ICMP コードフィールドを確認するように指定します。
IGMP	Type ____ e.g. (0-255) - スイッチが各フレームの IGMP タイプフィールドを確認するように指定します。
TCP	Source Port - 送信元ポートの TCP ポートを指定します。 Mask(0-FFFF) - 送信元ポートの TCP ポートマスクを指定します。 Destination Port - 送信先ポートの TCP ポートを指定します。 Mask(0-FFFF) - 送信先ポートの TCP ポートマスクを指定します。 Flag Bits - 正しいフラグマスクパラメーターを入力します。すべての受信パケットには TCP ポート番号が転送基準として含まれています。これらの番号にはフラグビットが関連付けられています。フラグビットはパケットの一部です。これでパケットの処理を決めます。パケット内の指定のフラグビットを拒否して、パケットを拒否することができます。 URG/ACK/PSH/RST/SYN/FIN - [URG]、[ACK]、[PSH]、[RST]、[SYN]、[FIN]から選択します。
UDP	Source Port - スイッチが送信元ポートの各フレームの UDP フィールドを確認するように指定します。 Mask(0-FFFF) - 送信先ポートの UDP ポートマスクを指定します。 Destination Port - 送信先ポートの UDP ポートを指定します。 Mask(0-FFFF) - 送信先ポートの UDP ポートマスクを指定します。
Protocol ID	Protocol ID ____ e.g. (0-255) - スイッチが各パケットのプロトコルフィールドにここで入力した値が含まれているかどうかを確認するように指定します。
Action	プルダウンメニューから、[Permit][Deny][Mirror]を選択します。 [Permit]を選択すると、合致するパケットを転送するルールを構成します。 [Deny]を選択すると、合致するパケットをドロップするルールを構成します。 [Mirror]を選択すると、合致するパケットを、ミラーポートの設定で指定したポートにミラーすることを指定します。この場合、ポートミラーリングを有効にして、ターゲットポートを設定する必要があります。
Priority (0-7)	パケットの 802.1p ユーザー優先度を、優先度フィールドに入力した値(このコマンドで事前に指定した基準を満たす値)に書き直す場合は、指定した CoS キューに転送する前に優先度値を入力します。
Replace Priority	指定した CoS キューに転送する前に、ボックスをクリックしてこのオプションを有効にし、Priority フィールドに入力した 802.1p ユーザー優先度値(このコマンドで前に指定した基準を満たす値)を書き直す際に使用する値を手動で入力します。この設定を行わない場合、パケットの 802.1p ユーザー優先度は、スイッチで転送される前に元の値に書き直されます。
Replace DSCP (0-63)	スイッチが DSCP 値(選択した基準を満たすパケットにある値)を隣接するフィールドに入力した値で置き換えます。
Counter	プルダウンメニューでカウンター機能の有効(Enabled)または無効(Disabled)を指定します。デフォルト設定は無効(Disabled)です。
Ports	ルールを適用するポートの範囲を入力します。

各設定項目を入力し、[Apply]をクリックすると ACL ルールが追加されます。

(3) IPv6 ACL の設定

[Add ACL Profile]画面から IPv6 ACL を選択すると、IPv6 ACL 設定用の画面になります。

IPv6 ACL ラジオボタンをチェックすると、右にプロトコル ([TCP]、[UDP]) を選択するプルダウンメニューが出現します。プロトコルを選択後、[Select]をクリックすると、次のウィンドウが表示されます(このウィンドウは、[TCP]、[UDP]のどちらを選択したかによって異なります):

下記に IPv6 ACL タイプのプロファイル設定パラメーターの説明を記載します。

パラメーター	説明
IPv6 Class	このボックスにチェックを入れて、スイッチが IPv6 ヘッダーのクラスフィールドを確認します。クラスフィールドはパケットヘッダーの一部です。
IPv6 Flow Label	このボックスにチェックを入れて、スイッチが IPv6 ヘッダーのフローラベルフィールドを確認します。送信元は、フローラベルを使用してパケットのシーケンスにラベルを付けます(デフォルト以外の QoS、UDP など)。
IPv6 Address	このボックスにチェックを入れて、スイッチが IPv6 送信元アドレスを確認します。
TCP	このボックスにチェックを入れて、TCP トラフィックにルールを適用するように指定します。 指定の [TCP Source Port Mask]、または、[TCP Destination Port Mask] にチェックを入れます。
UDP	このボックスにチェックを入れて、UDP トラフィックにルールを適用するように指定します。 指定の [UDP Source Port Mask]、または、[UDP Destination Port Mask] にチェックを入れます。

各設定を入力して[Create]をクリックすると、[Access Profile List]ウィンドウに新しいACL プロファイルエントリーが挿入されます。

ACL プロファイルエントリーにルールを追加するには、[Access Profile List]から相対する [Add/View Rules]をクリックし、[Access Rules List]から[Add Rule]をクリックします。次のウィンドウが表示されます：

下記に IPv6 ACL タイプのルール設定のパラメーターの説明を記載します。

パラメーター	説明
Access ID (1-65535)	アクセス用の固有識別子番号を入力します。この値は 1 ~ 65535 の範囲で設定します。 Auto Assign - このチェックボックスにチェックを入れ、作成しているルールに対し、スイッチが自動的にアクセス ID を割当てます。
Class	クラスを入力して、スイッチが IPv6 ヘッダーのクラスフィールドを確認します。クラスフィールドはパケットヘッダーの一部です。
Flow Label	IPv6 フローラベルを指定します。0-FFFFFF の値を入力します。
IPv6 Source Address	IPv6 送信元アドレスの IPv6 アドレスを指定します。
IPv6 Source Mask	IPv6 送信元サブマスクを指定します。デバイスが対応するのは、送信元 IPv6 アドレスの最後の 44 ビット(LSB)のフィルタリングのみです。
TCP	Source Port - IPv6 L4 TCP 送信元ポートサブマスクを指定します。 Destination Port - IPv6 L4 TCP 送信先ポートサブマスクを指定します。

UDP	Source Port - IPv6 L4 UDP 送信元ポートサブマスクを指定します。 Destination Port - IPv6 L4 UDP 送信先ポートサブマスクを指定します。
Action	プルダウンメニューから、[Permit][Deny][Mirror]を選択します。 [Permit]を選択すると、合致するパケットを転送するルールを構成します。 [Deny]を選択すると、合致するパケットをドロップするルールを構成します。 [Mirror]を選択すると、合致するパケットを、ミラーポートの設定で指定したポートにミラーすることを指定します。この場合、ポートミラーリングを有効にして、ターゲットポートを設定する必要があります。
Priority (0-7)	パケットの 802.1p ユーザー優先度を、優先度フィールドに入力した値(このコマンドで事前に指定した基準を満たす値)に書き直す場合は、指定した CoS キューに転送する前に優先度値を入力します。
Replace Priority	指定した CoS キューに転送する前に、ボックスをクリックしてこのオプションを有効にし、Priority フィールドに入力した 802.1p ユーザー優先度値(このコマンドで前に指定した基準を満たす値)を書き直す際に使用する置換値を手動で入力します。この設定を行わない場合、パケットの受信 802.1p ユーザー優先度は、スイッチで転送される前に元の値に書き直されます。
Replace DSCP (0-63)	スイッチが DSCP 値(選択した基準を満たすパケットにある値)を隣接するフィールドに入力した値で置き換えます。
Counter	プルダウンメニューでカウンター機能の有効(Enabled)または無効(Disabled)を指定します。デフォルト設定は無効(Disabled)です。
Ports	ルールを適用するポートの範囲を入力します。

各設定項目を入力し、[Apply]をクリックすると ACL ルールが追加されます。

(4) Packet Content ACL の設定

[Add ACL Profile]画面から Packet Content ACL を選択すると、Packet Content ACL 設定用の画面になります。Packet Content ACL は、パケットの種類によらず、パケットの特定の箇所の 4 バイト情報を指定して調査を行います。指定箇所は最大 4 個まで設定することができます。

Packet Content ACL ラジオボタンをチェックして[Select]をクリックすると、次のウィンドウが表示されます：

下記に Packet Content ACL タイプのプロファイル設定パラメーターの説明を記載します。

パラメーター	説明
Packet Content	<p>Offset1～4 は、パケットの調査箇所を示すプロファイルで、オフセット値(パケットの先頭から何バイト目を起点とするか)により定められます。指定できるオフセット値は、2 から始まる 4 離れた離散値のみで、2、6、10、14、18、22、・・・、126 となります。オフセット値 126 を指定すると、先頭から 126、127、0、1 バイトが調査対象になります。各 Offset プロファイルを指定することで、最大 4 箇所の 4 バイト情報を調査することができます。</p> <p>オフセット 1 (2-126) ____ マスク____、 オフセット 2 (2-126) ____ マスク____、 オフセット 3 (2-126) ____ マスク____、 オフセット 4 (2-126) ____ マスク____、</p> <p>Packet Content ACL を使用することで、ARP アドレス偽装攻撃などに代表されるネットワーク攻撃の一部を効果的に軽減することができます。</p>

各設定を入力して[Create]をクリックすると、[Access Profile List]ウィンドウに新しい ACL プロファイルエントリーが挿入されます。

ACL プロファイルエントリーにルールを追加するには、[Access Profile List]から相対する [Add/View Rules]をクリックし、[Access Rules List]から [Add Rule]をクリックします。次のウィンドウが表示されます：

Add Access Rule

Profile Information

Profile ID	4	Profile Type	Packet Content
Owner Type	ACL	Offset 1	Byte 2 Value: 0xFFFFFFFF

Rule Detail
(Keep an input field as blank to treat the corresponding option as do not care)

Access ID (1-65535) Auto Assign

Offset 1 e.g.(FFFFFFFF) Mask e.g.(FFFFFFFF)

Rule Action

Action

Priority (0-7)

Replace Priority

Replace DSCP (0-63)

Counter

Ports e.g.(1,4-6,9)

下記に Packet Content ACL タイプのルール設定のパラメーターの説明を記載します。

パラメーター	説明
Access ID (1-65535)	アクセス用の固有識別子番号を入力します。この値は 1 ~ 65535 の範囲で設定します。
Offset(1-4)	ACL プロファイルで指定した各 Offset プロファイルに対して、対象箇所の 4 バイト情報のマッチング条件を 16 進数で指定します。Mask で、マスク条件を指定することもできます。
Action	プルダウンメニューから、[Permit][Deny][Mirror]を選択します。 [Permit]を選択すると、合致するパケットを転送するルールを構成します。 [Deny]を選択すると、合致するパケットをドロップするルールを構成します。 [Mirror]を選択すると、合致するパケットを、ミラーポートの設定で指定したポートにミラーすることを指定します。この場合、ポートミラーリングを有効にして、ターゲットポートを設定する必要があります。
Priority(0-7)	パケットの 802.1p ユーザー優先度を、優先度フィールドに入力した値(このコマンドで事前に指定した基準を満たす値)に書き直す場合は、指定した CoS キューに転送する前に優先度値を入力します。
Replace DSCP	このオプションを選択して、スイッチが DSCP 値(選択した基準を満たすパケットにある値)を隣接するフィールドに入力した値で置き換えます。

パラメーター	説明
Counter	プルダウンメニューでカウンター機能の有効(Enabled)または無効(Disabled)を指定します。デフォルト設定は無効(Disabled)です。
Ports	ルールを適用するポートの範囲を入力します。

各設定項目を入力し、[Apply]をクリックすると ACL ルールが追加されます。

3.6.3 ACL Finder

このウィンドウを使用して、事前に設定した ACL エントリーを検索します。エントリーを検索するには、プルダウンメニューからプロファイル ID を選択して、表示するポートを入力し、状態(標準または CPU)を定義して、次に、[Find]をクリックします。ウィンドウの下半分にあるテーブルにエントリーが表示されます。エントリーを削除するには、相応する[Delete]をクリックします。

次のウィンドウを開くには、ACL > ACL Finder をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
Profile ID	検索対象のプロファイル ID を選択します。
Port	ACL を検索する対象のポート番号を入力します。

3.6.4 ACL Flow Meter

このウィンドウには、イングレストラフィックの帯域幅を制限する際に使用するフロー帯域幅制御を設定します。パケットをフィルターする ACL ルールを作成して、メータリングルールを作成し、この ACL ルールを関連付けてトラフィックを制限できます。帯域幅のステップは 64 kbps です。制限付きメータリングルールのために、メータリングルールに関連付けることのできない ACL ルールもあります。

次のウィンドウを開くには、ACL > ACL Flow Meter をクリックします。

下記にパラメーターの説明を記載します。

パラメーター	説明
Profile ID	フローメータリングパラメーターを構成する事前構成したプロファイル ID です。
Access ID (1-65535)	フローメータリングパラメーターを構成する事前構成したアクセス ID です。

正しい情報を入力して、[Find]をクリックします。 エントリーがテーブルの下半分に表示されま
す。 エントリーを編集するには、 相応する[Modify]をクリックします。 エントリーを削除するには、
相応する[Delete]をクリックします。 新しいエントリーを追加するには、 [Add]をクリックします。
次のウィンドウが表示されます：

ACL Flow Meter Configuration

Profile ID	1		
Access ID (1-65535)			
Mode	Rate	Rate (Kbps)	(64-1024000)
		Burst Size (Kbyte)	(4-16384)
		Rate Exceed	<input type="radio"/> Drop Packet <input checked="" type="radio"/> Remark DSCP (0-63)
		<<Back	Apply

下記にパラメーターの説明を記載します。

パラメーター	説明
Profile ID	フローメータリングパラメーターを設定する際に使用したプロファイル ID を 選択します。
Access ID (1-65535)	フローメータリングパラメーターを構成する際に使用する事前構成したアク セス ID を入力します。 1 ~ 65535 の値を入力します。
Mode	シングルレート 2 色マーカーは、 レートとバーストサイズに基づいて、パケ ットに緑色または赤色の印を付けます。 これはバーストサイズだけが重要な 場合に役に立ちます。 Rate (64-1024000) Kbps - フローの専用帯域幅 Kbps 単位で指定します。 範 囲は 64 ~ 1,024,000 です。 単位は Kbps です。 Burst Size (4-16384) Kbyte - このフローのバーストサイズを指定します。 範囲は 0 ~ 16,384 です。 単位は Kbyte です。
Rate Exceed	Drop - パケットをドロップ(削除)します。 Replace DSCP (0-63) - パケットの DSCP を変更します。

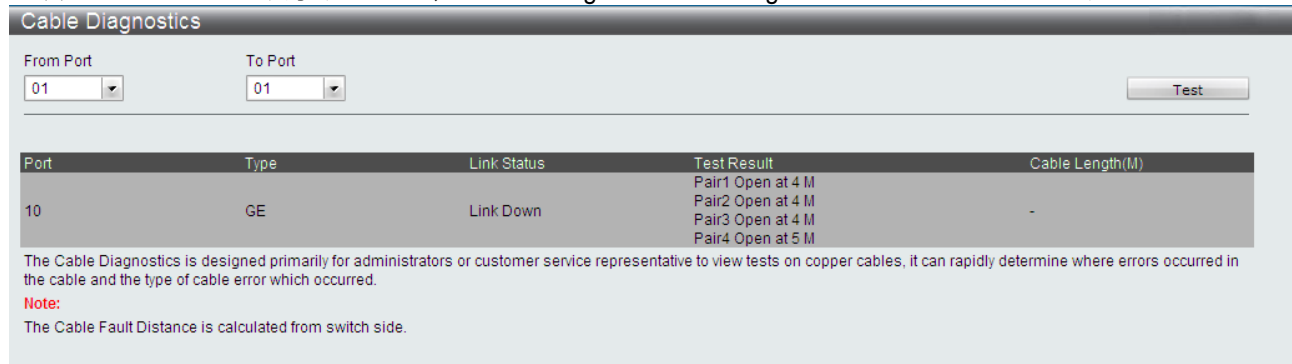
[Apply]をクリックして変更を適用し、 [<<Back]をクリックして[ACL Flow Mete]ウィンドウに戻り
ます。

3.7 Monitoring

3.7.1 Cable Diagnostics

このウィンドウには、スイッチ上の指定のポートに接続されているツイストペアケーブルの詳細が表示されます。ツイストペアケーブルにエラーがある場合に、この機能でエラーの種類、および、エラーが発生した箇所を判断できます。本テストの実行時には、ポートのリンク遷移が発生します。

次のウィンドウを表示するには、Monitoring > Cable Diagnostics をクリックします：



Port	Type	Link Status	Test Result	Cable Length(M)
10	GE	Link Down	Pair1 Open at 4 M Pair2 Open at 4 M Pair3 Open at 4 M Pair4 Open at 5 M	-

The Cable Diagnostics is designed primarily for administrators or customer service representative to view tests on copper cables, it can rapidly determine where errors occurred in the cable and the type of cable error which occurred.

Note:
The Cable Fault Distance is calculated from switch side.

テストするポートの範囲を入力して、[Test]をクリックします。このウィンドウの下半分にあるテーブルに、結果が表示されます。なお、ケーブル長については参考値としてください。

注意事項



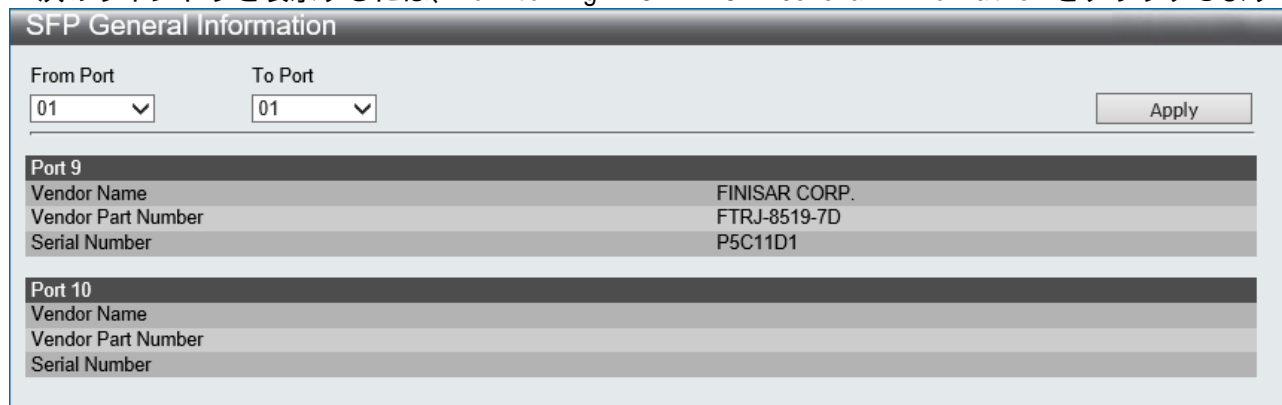
ApresiaLightGM124GT-SS 及び ApresiaLightGM124GT-PoE/PoE2 では、ポート 22 のケーブル診断は 1Gbps でリンクアップしている場合に限り、使用可能です。

3.7.2 SFP

3.7.2.1 SFP General Information

このウィンドウには、SFPポートに実装されたSFPトランシーバーに関する一般情報が表示されます。

次のウィンドウを表示するには、Monitoring > SFP > SFP General Information をクリックします：



The screenshot shows the 'SFP General Information' window. At the top, there are two dropdown menus for 'From Port' and 'To Port', both set to '01', and an 'Apply' button. Below this, there are two sections for SFP transceivers. The first section is for 'Port 9' and lists the following information: Vendor Name: FINISAR CORP., Vendor Part Number: FTRJ-8519-7D, and Serial Number: P5C11D1. The second section is for 'Port 10' and lists the same fields but they are currently empty.

下記にパラメーターの説明を記載します。

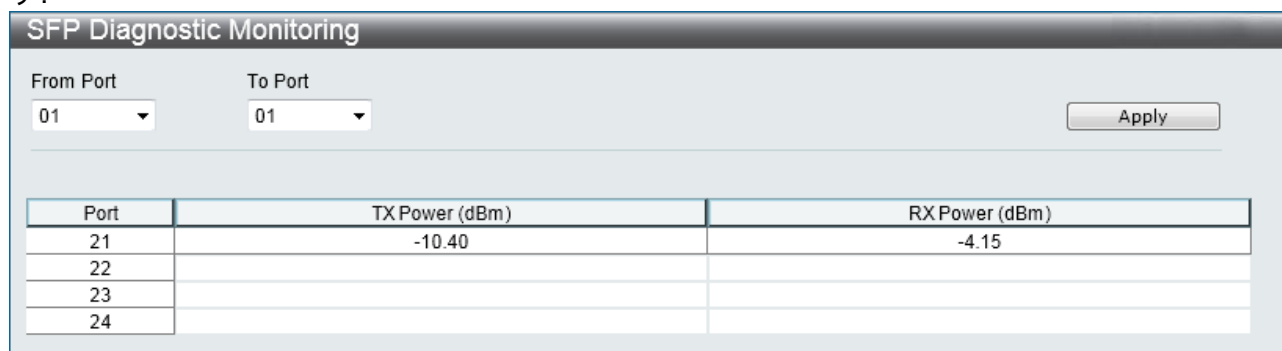
パラメーター	説明
From Port/To Port	表示させたいポートを選択します。

[Apply]をクリックしてSFP情報を表示させます。

3.7.2.2 SFP Diagnostic Monitoring

このウィンドウでは、SFPポートに実装されているSFPトランシーバーの入力と出力が光パワー単位 (dBm) で表示されます。

次のウィンドウを表示するには、Monitoring > SFP > SFP Diagnostic Monitoring をクリックします：



The screenshot shows the 'SFP Diagnostic Monitoring' window. It has the same 'From Port' and 'To Port' dropdowns (both set to '01') and an 'Apply' button as the previous window. Below, there is a table showing power levels for ports 21, 22, 23, and 24.

Port	TX Power (dBm)	RX Power (dBm)
21	-10.40	-4.15
22		
23		
24		

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	光入出力レベルを表示させたいポートを選択します。

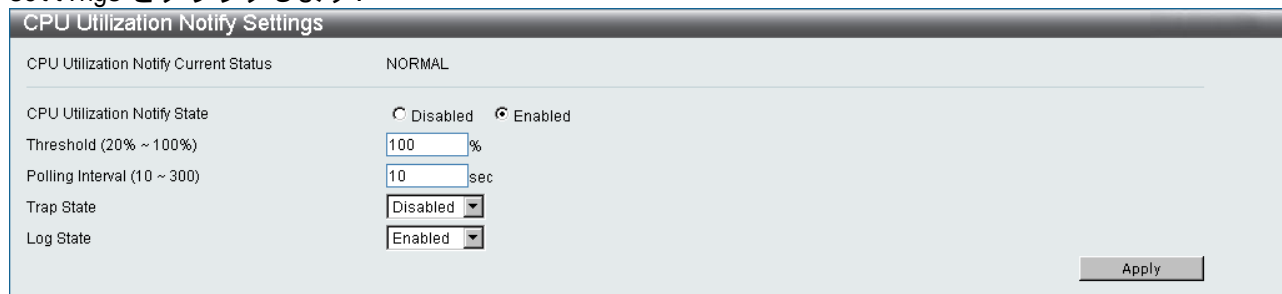
[Apply]をクリックしてSFPの光入出力レベルを表示させます。

3.7.3 Utilization Notify

3.7.3.1 CPU Utilization Notify

このウィンドウでは、CPUの使用率の状態を定期的に監視し、ユーザーが設定する閾値を超えた場合にログやトラップによりユーザーへ通知する機能を設定します。

次のウィンドウを表示するには、Monitoring > Utilization Notify > CPU Utilization Notify settings をクリックします：



[Apply]をクリックして変更を適用します。

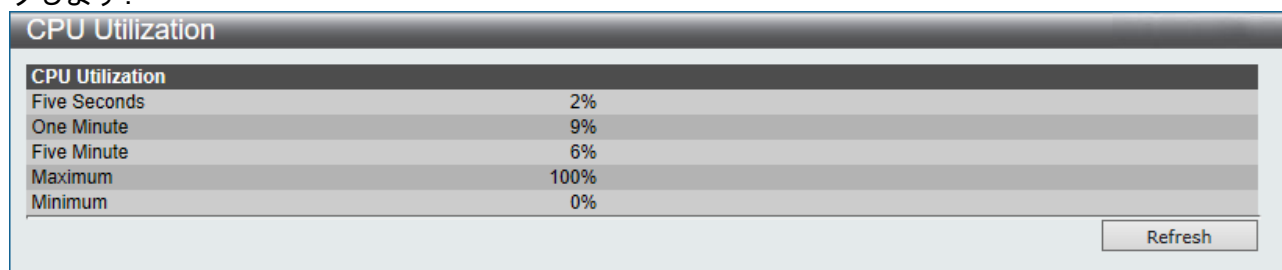
下記にパラメーターの説明を記載します。

パラメーター	説明
CPU Utilization Notify State	ラジオボタンで、CPU 使用率通知機能の有効(Enabled)または無効(Disabled)を指定します。
Threshold (20-100)	CPU 使用率通知の動作閾値を指定します。閾値を超えた場合は overloading 状態を、下回った場合は normal 状態を通知します。デフォルト値は 100%です。
Polling Interval (10-300)	CPU 使用率を監視する間隔時間を指定します。CPU 使用率は 5 秒間の平均値です。デフォルト値は 60 秒です。
Trap State	プルダウンメニューで CPU 使用率の状態遷移による SNMP トラップ出力を有効(Enabled)または無効(Disabled)に指定します。デフォルトは無効(Disabled)です。
Log State	プルダウンメニューから、Enabled あるいは Disabled を選択し、CPU 使用率の状態遷移によるログ出力を有効(Enabled)または無効(Disabled)に指定します。デフォルトは有効(Enabled)です。

3.7.3.2 CPU Utilization

このウィンドウには、CPU 使用率がパーセントで表示されます。これは、時間間隔で単純平均として計算しています。

次のウィンドウを表示するには、Monitoring > Utilization Notify > CPU Utilization をクリックします：



[Refresh]をクリックして画面に表示されるリストを更新します。

3.7.3.3 DRAM Utilization Notify

このウィンドウでは、DRAM の使用率の状態を定期的に監視し、ユーザーが設定する閾値を超えた場合にログやトラップによりユーザーへ通知する機能を設定します

次のウィンドウを表示するには、Monitoring > Utilization Notify > DRAM Utilization Notify settings をクリックします：

[Apply]をクリックして変更を適用します。

下記にパラメーターの説明を記載します。

パラメーター	説明
DRAM Utilization Notify State	ラジオボタンで、Enabled または Disabled を選択して、DRAM 使用率通知機能の有効(Enabled)または無効(Disabled)にします。
Threshold (20-100)	DRAM 使用率通知を動作させる閾値を指定します。閾値を超えた場合に overloading 状態の通知、下回った場合に normal 状態の通知をします。デフォルト値は 100% です。
Polling Interval (10-300)	DRAM 使用率を監視する間隔時間を指定します。デフォルト値は 60 秒です。
Trap State	プルダウンメニューから、Enabled あるいは Disabled を選択し、DRAM 使用率の状態遷移による SNMP トラップ出力を有効(Enabled)または無効(Disabled)に指定します。デフォルトは無効(Disabled)です。
Log State	プルダウンメニューから、Enabled あるいは Disabled を選択し、DRAM 使用率の状態遷移によるログ出力を有効(Enabled)または無効(Disabled)に指定します。デフォルトは有効(Enabled)です。

3.7.3.4 DRAM & FLASH Utilization

このウィンドウは、DRAM およびフラッシュのメモリー使用率情報を表示します。

次のウィンドウを表示するには、Monitoring > Utilization Notify > DRAM & FLASH Utilization をクリックします：

DRAM Utilization

Total DRAM :	131072 KB
Used DRAM :	66317 KB
Utilization :	50%
Utilization(Max) :	50%
Utilization(Min) :	50%

FLASH Utilization

Total FLASH :	16384 KB
Used FLASH :	6965 KB
Utilization :	42%

[Refresh]をクリックして画面に表示されるリストを更新します。

[Clear]をクリックして DRAM の使用率統計情報を初期化します。

3.7.3.5 Port Utilization

このウィンドウには、ポート上で使用できる合計帯域幅のパーセントが表示されます。

次のウィンドウを表示するには、Monitoring > Port Utilization をクリックします：

Port	TX/sec	RX/sec	Util
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0

[Refresh]をクリックして画面に表示されるリストを更新します。

3.7.4 Packet Size

スイッチで受信するパケットを6つのグループに分けてサイズ別にクラス分類し、折れ線グラフまたはテーブルで表示します。ポートプルダウンメニューから、統計を表示するポートを選択します。ポートをクリックして、GUI画面の一番上にあるスイッチのリアルタイムグラフィックを使用することもできます。

次のウィンドウを表示するには、Monitoring > Packet Size をクリックします：

Packet Size						
Port	01				Refresh	Clear
Frame Size	Frame Counts	Frames/sec	Frame Type	Total	Total/sec	
64	25335	0	RX Bytes	9754321	0	
65-127	736	0	RX Frames	27491	0	
128-255	502	0				
256-511	3469	0	TX Bytes	12808703	0	
512-1023	16593	0	TX Frames	25907	0	
1024-1518	6763	0				
Unicast RX	26937	0				
Multicast RX	439	0				
Broadcast RX	115	0				

[Refresh]をクリックして画面に表示されるリストを更新します。

[Clear]をクリックしてデータを初期化します。

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	プルダウンメニューから、統計を表示するポートを選択します。
Frame Size	受信したフレームをサイズ別に区分します。 Unicast RX / Multicast RX / Broadcast RX は、それぞれユニキャスト、マルチキャスト、ブロードキャストに区分して表示します。
Frame Counts	該当するフレームサイズやフレーム種別の総受信フレーム数を表示します。
Frames/sec	単位時間あたりの受信フレーム数を表示します。
Frame Type	統計情報の種類を示します。送信及び受信フレームに対するバイト数、フレーム数に区分されます。
Total	該当する統計情報に関する総数を表示します。RX Bytes の場合、総受信バイト数を示します。
Total/sec	該当する統計情報に関する単位時間の情報を表示します。RX Bytes の場合、単位時間あたりの受信バイト数を示します。

3.7.5 Packets

これらのウィンドウには、スイッチ上の送受信パケットの情報が表示されます。ポートプルダウンメニューから、統計を表示するポートを選択します。ポートをクリックして、GUI画面の一番上にあるスイッチのリアルタイムグラフィックを使用することもできます。

次のウィンドウを表示するには、Monitoring > Packets をクリックします：

Received(Rx)		
Port	01	Refresh Clear
RX Packets	Total	Total/sec
Bytes	10197053	64
Packets	30741	1
RX Packets	Total	Total/sec
Unicast	30143	1
Multicast	466	0
Broadcast	132	0
TX Packets	Total	Total/sec
Bytes	15360371	68
Packets	28614	1

[Refresh]をクリックして画面に表示されるリストを更新します。

[Clear]をクリックしてデータを初期化します。

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	プルダウンメニューから、統計を表示するポートを選択します。
Total	該当する統計情報に関する総数を表示します。RX Packets の Unicast の場合、受信したユニキャストパケットの総数を示します。
Total/sec	該当する統計情報に関する単位時間の情報を表示します。TX Packets の場合、送信したすべての種類のパケットの単位時間あたりの数量を表示します。

3.7.6 Errors

3.7.6.1 Received (RX)

ポートプルダウンメニューから、統計を表示するポートを選択します。ポートをクリックして、GUI 画面の一番上にあるスイッチのリアルタイムグラフィックを使用することもできます。

次のウィンドウを表示するには、Monitoring > Errors > Received (RX)をクリックします：

The screenshot shows a window titled "Received(Rx)". At the top, there is a "Port" dropdown menu set to "01", and two buttons: "Refresh" and "Clear". Below this is a table with two columns: "Rx Error" and "RX Frames".

Rx Error	RX Frames
CRC Error	0
UnderSize	0
OverSize	0
Fragment	0
Jabber	0
Drop Pkts	652

[Refresh]をクリックして画面に表示されるリストを更新します。

[Clear]をクリックしてデータを初期化します。

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	プルダウンメニューから、統計を表示するポートを選択します。
Rx Error	受信したエラーフレームをエラーの種別で区分します。 CRC Error: CRC エラーが発生したパケット UnderSize: 64 バイトの最小許容パケットサイズよりも小さく、CRC が正常であることが検出されたパケット OverSize: 1518 オクテットよりも長く、1536 オクテット未満の有効な受信パケット Fragment: 不良フレーミングまたは無効な CRC のある 64 バイト未満のパケット Jabber: 1518 オクテットよりも長く、1536 オクテット未満の無効な受信パケット Drop pkts: 破棄したパケット
RX Frames	該当するエラーが発生した受信フレーム数を表示します。

3.7.6.2 Transmitted (TX)

ポートプルダウンメニューから、統計を表示するポートを選択します。ポートをクリックして、GUI 画面の一番上にあるスイッチのリアルタイムグラフィックを使用することもできます。

次のウィンドウを表示するには、Monitoring > Errors > Transmitted (Tx)をクリックします：

Tx Error	TX Frames
Excessive Deferral	0
CRC Error	0
Late Collision	0
Excessive Collision	0
Single Collision	0
Collision	0

[Refresh]をクリックして画面に表示されるリストを更新します。

[Clear]をクリックしてデータを初期化します。

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	プルダウンメニューから、統計を表示するポートを選択します。
Tx Error	送信したエラーフレームをエラーの種別で区分します。 Excessive Deferral: メディアが使用中だったために、特定のインターフェース上での最初の転送の試みが遅れたパケット CRC Error: CRC エラーが発生したパケット Late Collision: パケットの送信中、512 ビット時間以降にコリジョンが検出された回数 Excessive Collision: 過度のコリジョンのために送信に失敗したパケット Single Collision: シングルコリジョンフレーム。1つ以上のコリジョンにより送信が禁止されたパケットで、送信に成功した数 Collision: このネットワークセグメント上のコリジョンの推定合計数
TX Frames	該当する送信エラーが発生した回数を表示します。

3.7.7 Port Access Control

3.7.7.1 RADIUS Authentication

このテーブルには、RADIUS 認証プロトコルのクライアント側の RADIUS 認証クライアントのアクティビティに関する情報が含まれます。

次のウィンドウを表示するには、Monitoring > Port Access Control > RADIUS Authentication をクリックします：

ServerIndex	InvalidServerAddr	Identifier	AuthServerAddr	ServerPortNumber	RoundTripTime	AccessRequests	AccessRetrans	AccessAcc
1	0	APRESIA Systems	0.0.0.0	0	0	0	0	0
2	0	APRESIA Systems	0.0.0.0	0	0	0	0	0
3	0	APRESIA Systems	0.0.0.0	0	0	0	0	0

[Clear]をクリックしてデータを初期化します。

[Refresh]をクリックして画面に表示されるリストを更新します。

下記にパラメーターの説明を記載します。

パラメーター	説明
InvalidServerAddr	不明なアドレスから受信した RADIUS アクセス応答パケットの数です。
Identifier	RADIUS 認証クライアントの NAS 識別子です。
ServerIndex	各 RADIUS 認証サーバーに割り当てられた識別番号です。
AuthServerAddr	RADIUS 認証サーバーの IP アドレス一覧表です。
ServerPortNumber	クライアントがこのサーバーに要求する際に使用する UDP ポート番号です。
RoundTripTime	直近のアクセス応答/アクセスチャレンジと、この RADIUS 認証サーバーからのアクセス要求と一致したアクセス要求との間の時間間隔です(単位は 100 分の 1 秒です)。
AccessRequests	RADIUS 認証サーバーに送信された RADIUS アクセス要求パケットの数です。再送は含みません。
AccessRetrans	RADIUS 認証サーバーに再送信された RADIUS アクセス要求パケットの数です。
AccessAccepts	RADIUS 認証サーバーから受信した RADIUS アクセス承認パケット(有効または無効)の数です。
AccessRejects	RADIUS 認証サーバーから受信した RADIUS アクセス拒否パケット(有効または無効)の数です。
AccessChallenges	RADIUS 認証サーバーから受信した RADIUS アクセスチャレンジパケット(有効または無効)の数です。
AccessResponses	RADIUS 認証サーバーから受信した不正な形式の RADIUS アクセス応答パケットの数です。不正な形式のパケットには、長さが無効なパケットも含まれません。不良なオーセンティケーターまたは署名属性、あるいは、既知のタイプは、不正な形式のアクセス応答には含まれません。

BadAuthenticators	RADIUS 認証サーバーから受信した、無効なオーセンティケーターまたは署名属性を含む RADIUS アクセス応答パケットの数です。
PendingRequests	RADIUS 認証サーバー宛の期限切れになっていない RADIUS アクセス要求パケット、または、応答を受信した RADIUS アクセス要求パケットの数です。アクセス要求が送信されると、この変数は大きくなります。アクセス承認、アクセス拒否、または、アクセスチャレンジを受信したり、あるいは、タイムアウトになったり再送すると、この変数は小さくなります。
Timeouts	RADIUS 認証サーバーの認証タイムアウトの数です。タイムアウトの後で、クライアントは同じサーバーに再試行したり、異なるサーバーへ送信したり、または、放棄することができます。同じサーバーに再試行すると、再送およびタイムアウトとしてカウントされます。異なるサーバーへ送信すると、要求およびタイムアウトとしてカウントされます。
UnknownTypes	認証ポート上の RADIUS 認証サーバーから受信した不明なタイプの RADIUS パケットの数です。
PacketsDropped	認証ポート上で RADIUS 認証サーバーから受信して、何らかの理由でドロップ (破棄)された RADIUS パケットの数です。

3.7.7.2 RADIUS Account Client

このウィンドウには、RADIUS アカウンティングクライアントを管理する際に使用する管理オブジェクトと、それに関連する現在の統計が表示されます。

次のウィンドウを表示するには、Monitoring > Port Access Control > RADIUS Account Client をクリックします：

RADIUS Authentication								
Clear		Refresh						
ServerIndex	InvalidServerAddr	Identifier	AuthServerAddr	ServerPortNumber	RoundTripTime	AccessRequests	AccessRetrans	AccessAcc
1	0	APRESIA Systems	0.0.0.0	0	0	0	0	0
2	0	APRESIA Systems	0.0.0.0	0	0	0	0	0
3	0	APRESIA Systems	0.0.0.0	0	0	0	0	0

[Clear]をクリックしてデータを初期化します。

[Refresh]をクリックして画面に表示されるリストを更新します。

下記にパラメーターの説明を記載します。

パラメーター	説明
InvalidServerAddr	不明アドレスから受信した RADIUS アカウンティング応答パケットの数です。
Identifier	RADIUS アカウントの NAS 識別子です。
ServerIndex	各 RADIUS 認証サーバーに割り当てられた識別番号です。
ServerAddr	RADIUS 認証サーバーの IP アドレス一覧表です。
ServerPortNumber	要求を RADIUS 認証サーバーに送信する際に使用する UDP ポートです。

パラメーター	説明
RoundTripTime	直近のアカウントティング応答と、この RADIUS アカウントティングサーバーからのアカウントティング要求と一致したアカウントティング要求との間の時間間隔です。
Requests	RADIUS アカウントティング要求パケットの数です。再送は含みません。
Retransmissions	この RADIUS アカウントティングサーバーに送信された RADIUS アカウントティング要求パケットの数です。識別子とアカウント遅延が更新された再試行、および、識別子とアカウント遅延が同じままの再試行は、再送に含まれます。
Responses	アカウントティングポート上で RADIUS 認証サーバーから受信した RADIUS パケットの数です。
MalformedResponses	RADIUS 認証サーバーから受信した不正な形式の RADIUS アカウントティング応答パケットの数です。不正な形式のパケットには、長さが無効なパケットも含まれます。不良なオーセンティケーターおよび既知のタイプは、不正な形式のアカウントティング応答には含まれません。
BadAuthenticators	RADIUS 認証サーバーから受信した、無効なオーセンティケーターを含む RADIUS アカウントティング応答パケットの数です。
PendingRequests	RADIUS 認証サーバーに送信された期限切れになっていない RADIUS アカウントティング要求パケット、または、応答を受信していない RADIUS アカウントティング要求パケットの数です。アカウントティング要求が送信されると、この変数は大きくなります。アカウントティング応答を受信したり、あるいは、タイムアウトになったり再送すると、この変数は小さくなります。
Timeouts	RADIUS 認証サーバーのアカウントティングタイムアウトの数です。タイムアウトの後で、同じサーバーに再試行したり、異なるサーバーへ送信したり、または、放棄することができます。同じサーバーに再試行すると、再送およびタイムアウトとしてカウントされます。異なるサーバーへ送信すると、アカウントティング要求およびタイムアウトとしてカウントされます。
UnknownTypes	アカウントティングポート上で RADIUS 認証サーバーから受信した不明なタイプの RADIUS パケットの数です。
PacketsDropped	アカウントティングポート上で RADIUS 認証サーバーから受信して、何らかの理由でドロップ(削除)された RADIUS パケットの数です。

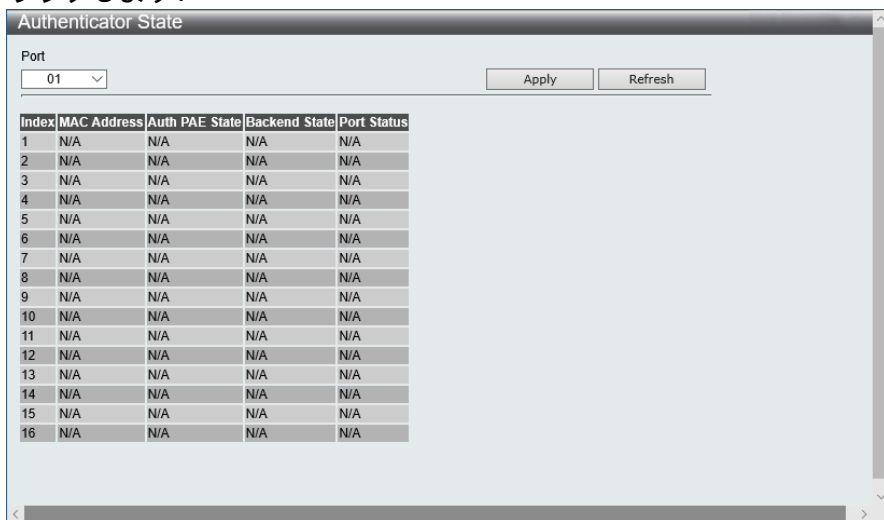
3.7.7.3 Authenticator State

このセクションではスイッチ上の 802.1X 状態について説明します。

注意事項

! 本操作画面は、802.1X 認証が有効の場合に表示されます。

次のウィンドウを表示するには、Monitoring > Port Access Control > Authenticator State をクリックします：



[Apply] をクリックして変更を適用します。

[Refresh] をクリックして画面に表示されるリストを更新します。

下記にパラメーターの説明を記載します。

パラメーター	説明
MAC Address	相応するインデックス番号のデバイスの MAC アドレスです。
Auth PAE State	認証状態 (PAE State) 表示は以下のいずれかで表示されます： [Initialize] 初期化 [Disconnected] 切断済み [Connecting] 接続中 [Authenticating] 認証中 [Authenticated] 認証済み [Aborting] 中断中 [Held] 保留 [Force_Auth] 強制認証 [Force_Unauth] 強制非認証 [N/A] 該当なし [N/A] 該当なしは、ポートの認証機能が無効になっていることを示します。
Backend State	バックエンド認証状態は次のいずれかで表示されます。 [Request] 要求 [Response] 応答 [Success] 成功

	[Fail]失敗 [Timeout]タイムアウト [Idle]アイドル [Initialize]初期化 [N/A]該当なし [N/A]該当なしは、ポートの認証機能が無効になっていることを示します。
Port Status	制御ポートの状態は、[Authorized]認証済み、[Unauthorized]、非認証 [N/A]該当なしとなります。

3.7.7.4 Authenticator Statistics

このウィンドウには、各ポートに関連付けられたオーセンティケータPAEの統計オブジェクトが含まれます。このテーブルに、オーセンティケータ機能に対応する各ポートのエントリが表示されます。

注意事項

! 本操作画面は、802.1X 認証が有効の場合に表示されます。

次のウィンドウを表示するには、Monitoring > Port Access Control > Authenticator Statistics をクリックします：

Index	Frames Rx	Frames Tx	Rx Start	Tx ReqId	Rx LogOff	Tx Req	Rx RespId	Rx Resp	Rx Invalid	Rx Error	Last Version	Last Source
1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
13	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
14	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
15	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
16	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

[Apply]をクリックして変更を適用します。

[Refresh]をクリックして画面に表示されるリストを更新します。

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	ポートのあるシステムでポートに割り当てられた識別番号です。
Frames Rx	オーセンティケータで受信した有効な EAPOL フレームの数です。
Frames Tx	オーセンティケータで送信した EAPOL フレームの数です。
Rx Start	オーセンティケータで受信した EAPOL 開始フレームの数です。
TxReqId	オーセンティケータで送信した EAPOL 要求/Id フレームの数です。

RxLogOff	オーセンティケーターで受信した EAPOL ログオフフレームの数です。
Tx Req	オーセンティケーターで送信した EAPOL 要求フレーム(要求/Id フレーム以外)の数です。
Rx Respld	オーセンティケーターで受信した EAPOL 応答/Id フレームの数です。
Rx Resp	オーセンティケーターで受信した有効な EAPOL 応答フレーム(応答/Id フレーム以外)の数です。
Rx Invalid	オーセンティケーターで受信した、フレームタイプが認識されない EAPOL フレームの数です。
Rx Error	オーセンティケーターで受信した、パケットボディー長フィールドが無効な EAPOL フレームの数です。
Last Version	最近受信した EAPOL フレームにあるプロトコルバージョン番号です。
Last Source	最近受信した EAPOL フレームにある送信元 MAC アドレスです。

3.7.7.5 Authenticator Session Statistics

このウィンドウには、各ポートに関連付けられたオーセンティケーターPAE のセッション統計オブジェクトが含まれます。このテーブルに、オーセンティケーター機能に対応する各ポートのエントリが表示されます。

注意事項



本操作画面は、802.1X 認証が有効の場合に表示されます。

次のウィンドウを表示するには、Monitoring > Port Access Control > Authenticator Session Statistics をクリックします：

Index	Octets Rx	Octets Tx	Frames Rx	Frames Tx	ID	AuthenticMethod	Time	TerminateCause	UserName
1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
13	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
14	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
15	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
16	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

[Apply] をクリックして変更を適用します。

[Refresh] をクリックして画面に表示されるリストを更新します。

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	ポートのあるシステムでポートに割り当てられた識別番号です。
Octets Rx	セッション中にこのポート上のユーザーデータフレームで受信したオクテットの数です。
Octets Tx	セッション中にこのポート上のユーザーデータフレームで送信したオクテットの数です。
Frames Rx	セッション中にこのポート上で受信したユーザーデータフレームの数です。
Frames Tx	セッション中にこのポート上で送信したユーザーデータフレームの数です。
ID	セッションの固有識別子です。3文字以上の印刷可能な ASCII 文字列です。
Authentic Method	セッションを確立する際に使用する認証方法です。有効な認証方法は次のとおりです。 (1) Remote Authentic Server - 外部認証サーバーです。 (2) Local Authentic Server - ローカル認証サーバーです。
Time	セッションの長さです(秒単位)。
Terminate Cause	セッション切断の理由です。次の8つの切断理由があります。 (1) サプリカントのログオフ (2) ポートエラー (3) サプリカントの再起動 (4) 再認証エラー (5) 認証制御型ポート制御が強制非認証に設定されている (6) ポートの再初期化 (7) ポートが管理上無効になっている (8) まだ切断されていない
UserName	サプリカント PAE を識別するユーザー名です。

3.7.7.6 Authenticator Diagnostics

このウィンドウには、各ポートに関連付けられているオーセンティケーターの動作に関する診断情報が含まれています。このテーブルに、オーセンティケーター機能に対応する各ポートのエントリが表示されます。

注意事項

! 本操作画面は、802.1X 認証が有効の場合に表示されます。

次のウィンドウを表示するには、Monitoring > Port Access Control > Authenticator Diagnostics をクリックします：

Index	Connect Enter	Connect LogOff	Auth Enter	Auth Success	Auth Timeout	Auth Fail	Auth Reauth	Auth Start	Auth LogOff	Authed Reauth	Authed Start	Authed LogOff	Responses	AccessChallenges	Other
1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
13	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
14	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
15	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
16	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

[Apply]をクリックして変更を適用します。

[Refresh]をクリックして画面に表示されるリストを更新します。

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	ポートのあるシステムでポートに割り当てられた識別番号です。
Connect Enter	認証状態が他の状態から接続中状態に遷移する回数をカウントします。
Connect LogOff	EAPOL ログオフメッセージの受信により、認証状態が接続中状態から切断済み状態に遷移する回数をカウントします。
Auth Enter	サブリカントから EAPOL 応答/識別メッセージの受信により、認証状態が接続中状態から認証中状態に遷移する回数をカウントします。
Auth Success	バックエンド認証状態がサブリカントの認証により、認証中状態から認証済み状態に遷移する回数をカウントします。
Auth Timeout	バックエンド認証状態が認証タイムアウトにより、認証中状態から中断中状態に遷移する回数をカウントします。
Auth Fail	バックエンド認証状態が認証失敗により、認証中状態から保留状態に遷移する回数をカウントします。
Auth Reauth	再認証要求の受信により、認証状態が認証中状態から中断中状態に遷移する

パラメーター	説明
	回数をカウントします。
Auth Start	サブリカントから EAPOL 開始メッセージの受信により、認証状態が認証中状態から中断中状態に遷移する回数をカウントします。
Auth LogOff	サブリカントから EAPOL ログオフメッセージの受信により、認証状態が認証中状態から中断中状態に遷移する回数をカウントします。
Authed Reauth	再認証要求の受信により、認証状態が認証済み状態から接続中状態に遷移する回数をカウントします。
Authed Start	サブリカントから EAPOL 開始メッセージの受信により、認証状態が認証済み状態から接続中状態に遷移する回数をカウントします。
Authed LogOff	サブリカントから EAPOL ログオフメッセージの受信により、認証状態が認証済み状態から切断済み状態に遷移する回数をカウントします。
Responses	アクセス要求パケットを認証サーバーに送信した回数をカウントします(応答をサーバーへ送信して、応答状態に入る場合)。オーセンティケーターが認証サーバーとの通信を試みたことを示します。
AccessChallenges	アクセスチャレンジパケットを認証サーバーから受信した回数をカウントします。認証サーバーがオーセンティケーターと通信したことを示します。
OtherReqToSupp	EAP 要求パケット(識別、通知、失敗、成功メッセージ以外)をサブリカントへ送信をカウントします(要求を送信して要求状態に入る場合)。オーセンティケーターが EAP 方法を選択したことを示します。
NonNakRespFromSup	サブリカントから初期 EAP 要求への応答を受信し、その応答が EAP-NAK 以外の場合にカウントします。サブリカントがオーセンティケーターが選択した EAP 方法に応答できることを示します。
Bac Auth Success	認証サーバーから承認メッセージを受信する回数をカウントします。サブリカントが認証サーバーに正常に認証されたことを示します。
Bac Auth Fail	認証サーバーから拒否メッセージを受信する回数をカウントします。サブリカントが認証サーバーに認証されなかったことを示します。

3.7.8 Peripheral

3.7.8.1 Device Environment

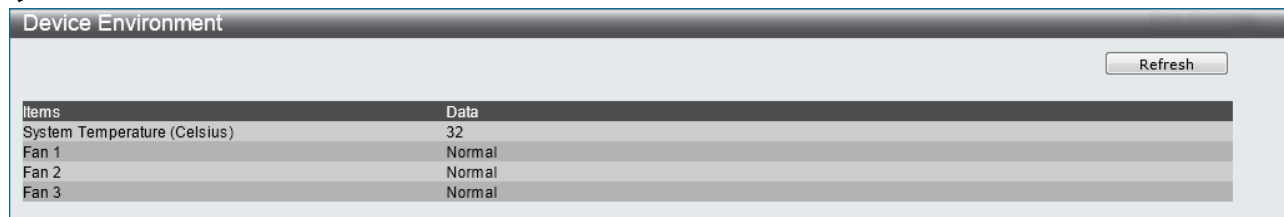
Device Environment 機能は、APLGM110GTPOE/POE2、APLGM118GTPOE/POE2、APLGM124GTPOE/POE2 のみ対応しています。

このウィンドウには、スイッチの内部温度と FAN 動作状態が表示されます。

スイッチの内部温度は外部温度より約 5 ほど高くなります。

実装する FAN 番号は、APLGM110GTPOE/POE2 (FAN1)、APLGM118GTPOE/POE2 および APLGM124GTPOE/POE2 (FAN1/FAN2/FAN3) です。

次のウィンドウを表示するには、Monitoring > Peripheral > Device Environment をクリックします：



Items	Data
System Temperature (Celsius)	32
Fan 1	Normal
Fan 2	Normal
Fan 3	Normal

[Refresh]をクリックして画面に表示されるリストを更新します。

注意事項



スイッチは温度異常(65 超過)の検知により PoE 給電を停止します。
また、APLGM118GTPOE/POE2 および APLGM124GTPOE/POE2 のみ、FAN 異常の検知により PoE 給電を停止します。

3.7.9 Browse ARP Table

このウィンドウにはスイッチ上の現在の ARP エントリーが表示されます。指定の ARP エントリーを検索するには、ウィンドウの一番上に IP アドレスを入力して、[Find]をクリックします。[Show Static]をクリックして、静的 ARP テーブルエントリーを表示します。ARP テーブルを消去するには、[Clear All]をクリックします。

次のウィンドウを表示するには、Monitoring > Browse ARP Table をクリックします：

Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
System	10.90.90.90	00-40-66-49-EA-72	Local
System	10.90.90.99	00-50-BA-DA-01-23	Dynamic
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast

- [Find]をクリックして入力パラメーターに基づく指定エントリーを検索します。
- [Show Static]をクリックして全てのスタティックエントリーを表示します。
- [Clear All]をクリックしてフィールドからの全ての入力データをクリアします。

3.7.10 Browse VLAN

このウィンドウを使用して、スイッチの各ポートの VLAN 状態を VLAN 別に表示します。ウィンドウの一番上にあるフィールドに VID(VLAN ID)を入力して、[Find]をクリックします。

次のウィンドウを表示するには、Monitoring > Browse VLAN をクリックします：

Port																							
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

Note: T: Tagged Port, U: Untagged Port, F: Forbidden Port.

3.7.11 IGMP Snooping

3.7.11.1 Browse IGMP Router Port

現在ルーターポートとして構成されているスイッチのポートが表示されます。 コンソールまたは Web ベース GUI を使用してユーザーが設定したルーターポートは、静的ルーターポートとして S で示されます。スイッチが動的に設定したルーターポートは D で示されます。禁止ポートは F で示されま
す。ウィンドウの一番上にあるフィールドに VID(VLAN ID)を入力して、[Find]をクリックすると、指
定した VLAN に属する様々なタイプの IGMP ルーターポートが表示されます。

次のウィンドウを表示するには、Monitoring > IGMP Snooping > Browse IGMP Router Port をクリ
ックします：

Browse Router Port

VID Find

VLAN ID: 1
VLAN Name: default

Total Entries: 1

Port																							
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

<<Back Next>>

Note: S:Static Router Port, D:Dynamic Router Port, F:Forbidden Router Port

3.7.11.2 IGMP Snooping Group

スイッチの IGMP スヌーピンググループを検索します。IGMP スヌープしたレポートの数はレポート
フィールドに表示されます。

次のウィンドウを表示するには、Monitoring > IGMP Snooping > IGMP Snooping Group をクリッ
クします：

IGMP Snooping Group

VLAN Name

VID List (e.g.: 1,4-6)

Group IP Address Find

View All

IGMP Snooping Group Table Total Entries: 0

VID	VLAN Name	Source	Group	Member Ports	Router Ports	Reports	Up time	Expire Time(sec)	Filter Mode
-----	-----------	--------	-------	--------------	--------------	---------	---------	------------------	-------------

<<Back Next>>

下記にパラメーターの説明を記載します。

パラメーター	説明
VLAN Name	マルチキャストグループの VLAN 名を入力します。
VID List	マルチキャストグループの VLAN ポートを入力します。
Group IP Address	マルチキャストグループの IP アドレスを入力します。

正しい情報を入力して、[Find]をクリックします。検索したエントリーが IGMP スヌーピンググル
ープテーブルに表示されます。[View All]をクリックして、すべてのエントリーを表示します。

3.7.11.3 IGMP Snooping Host

スイッチ上の現在の IGMP スヌーピングホスト情報が表示されます。

次のウィンドウを表示するには、Monitoring > IGMP Snooping > IGMP Snooping Host をクリックします：

IGMP Snooping Host

VLAN Name

VLAN List (e.g.: 1,4-6)

Port List (e.g.: 1,4-6)

Group

Find

IGMP Snooping Host Table Total Entries: 0

VLAN ID	Group	Port No	IGMP Host
---------	-------	---------	-----------

相応するラジオボタンをクリックし、IGMP スヌーピングホスト情報を表示する VLAN 名、VLAN 一覧、ポート一覧、または、グループを入力して、[Find]をクリックします。検索したエントリーがウィンドウの下半分に表示されます。

3.7.12 MLD Snooping

3.7.12.1 Browse MLD Router Port

現在 IPv6 内のルーターポートとして設定されているスイッチのポートが表示されます。コンソールまたは Web ベース GUI を使用してユーザーが設定したルーターポートは、静的ルーターポートとして S で示されます。スイッチが動的に設定したルーターポートは D で示されます。禁止ポートは F で示されます。ウィンドウの一番上にあるフィールドに VID(VLAN ID)を入力して、[Find]をクリックすると、指定した VLAN に属する様々なタイプの MLD ルーターポートが表示されます。

次のウィンドウを表示するには、Monitoring > MLD Snooping > Browse MLD Router Port をクリックします：

Browse MLD Router Port

VID Find

VLAN ID: 1

VLAN Name: default

Total Entries: 1

Port																							
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

<<Back Next>>

Note: S:Static Router Port, D:Dynamic Router Port, F:Forbidden Router Port

3.7.12.2 MLD Snooping Group

スイッチ上にある MLD スヌーピンググループを表示します。MLD スヌーピングは、IPv4 の IGMP スヌーピングと同様の IPv6 機能です。下の空いているフィールドに VLAN 名を入力し、[Find]をクリックして、スイッチ内の VLAN 別に閲覧します。

次のウィンドウを表示するには、Monitoring > MLD Snooping > MLD Snooping Group をクリックします：

VID	VLAN Name	Source	Group	Member Port	Filter Mode
Total Entries: 0					

下記にパラメーターの説明を記載します。

パラメーター	説明
VLAN Name	マルチキャストグループの VLAN 名を入力します。
VID List	マルチキャストグループの VLAN ID を入力します。
Group IP Address	マルチキャストグループの IP アドレスを入力します。

[Find]をクリックして、検索したエントリーが MLD スヌーピンググループテーブルに表示されま
す。[View All]をクリックして、すべてのエントリーを表示します。

3.7.13 LLDP

3.7.13.1 LLDP Statistics System

次のウィンドウを表示するには、Monitoring > LLDP > LLDP Statistics System をクリックします：

LLDP Statistics	
Last Change Time	1344
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Ageout	0

Port: 01 [Find]

LLDP Statistics Ports	
Total Tx Frames	0
Total Discarded Rx Frames	0
Rx Errors Frames	0
Total Rx Frames	0
Total Discarded Rx TLVs	0
Total Unrecognized Rx TLVs	0
Total Aged out Neighbor Information	0

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	この設定に使用されているポートを指定します。

[Find]をクリックして、入力パラメーターに基づく指定エントリーを検索します。

3.7.13.2 LLDP Local Port Information

次のウィンドウを表示するには、Monitoring > LLDP > LLDP Local Port Information をクリックします：

LLDP Local Port Information			
LLDP Local Port Brief Table			
Port	Port ID Subtype	Port ID	Port Description
1	Local	1/1	APRESIA Systems APLGM110GTSS R1.14 Port 1
2	Local	1/2	APRESIA Systems APLGM110GTSS R1.14 Port 2
3	Local	1/3	APRESIA Systems APLGM110GTSS R1.14 Port 3
4	Local	1/4	APRESIA Systems APLGM110GTSS R1.14 Port 4
5	Local	1/5	APRESIA Systems APLGM110GTSS R1.14 Port 5
6	Local	1/6	APRESIA Systems APLGM110GTSS R1.14 Port 6
7	Local	1/7	APRESIA Systems APLGM110GTSS R1.14 Port 7
8	Local	1/8	APRESIA Systems APLGM110GTSS R1.14 Port 8
9	Local	1/9	APRESIA Systems APLGM110GTSS R1.14 Port 9
10	Local	1/10	APRESIA Systems APLGM110GTSS R1.14 Port 10

[Show Normal] をクリックした後、以下のウィンドウが現れます：

LLDP Local Port Information	
LLDP Local Port Normal Table	
Port	01
Find Show Brief	
LLDP Normal Ports	
Port ID Subtype	Local
Port ID	1/1
Port Description	APRESIA Systems APLGM110GTSS R1.14 Port 1
Port PVID	1
Management Address Count	Show Detail
PPVID Entries	Show Detail
VLAN Entries	Show Detail
Protocol Identity Entries Count	Show Detail
MAC/PHY Configuration/Status	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	1536

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	この設定に使用されているポートを指定します

入力された指定エントリーを探すために[Find]をクリックします。

選択されたポートの短縮表示一覧を見るために[Show Brief]をクリックします。

このウィンドウでユーザーは隣の[Show Detail リンク]をクリックすることにより個別カテゴリーの詳細情報を見ることが出来ます。

3.7.13.3 LLDP Remote Port Information

次のウィンドウを表示するには、Monitoring > LLDP > LLDP Remote Port Information をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	この設定に使用されているポートを指定します

入力された指定エントリーを探すために[Find]をクリックします

選択されたポートの標準表示一覧を見るために[Show Normal]をクリックします

[Show Normal]をクリックした後、以下のウィンドウが現れます

3.7.14 MBA Authentication State

MBA 認証状態ウィンドウを表示するには Monitoring > MBA Authentication State をクリックします：

下記にパラメーターの説明を記載します。

パラメーター	説明
Port List	この設定に使用されているポートリストを指定します。

入力された指定エントリーを探すために[Find]をクリックします。

ポート単位でクリアするために[Clear By Port]をクリックします。

全ての MBA 認証ホスト一覧を見るために[View All Hosts]をクリックします。

全ての MBA 認証ホストをクリアするために[Clear All Hosts]をクリックします。

3.7.15 Web Authentication State

このウィンドウで Web 認証の設定情報を表示します。

次のウィンドウを表示するには、Monitoring > Web Authentication State をクリックします：

Web Authentication State

Port List (e.g.:1,5-10)

Port List (e.g.:1,5-10) Authenticated Authenticating Blocked

Total Authenticating Hosts: 0
Total Authenticated Hosts: 0
Total Blocked Hosts: 0

Port	MAC Address	RX VLAN ID	State	Assign VLAN ID	Aging Time/Block Time
------	-------------	------------	-------	----------------	-----------------------

Note: H: Host-Based, P:Port-Based

下記にパラメーターの説明を記載します。

パラメーター	説明
Port List	この設定で使用されるポートリストを指定します
Authenticated	表示ポートに認証された全てのユーザーを含むために指定します
Authenticating	表示ポートに認証中の全てのユーザーを含むために指定します
Blocked	表示ポートにブロックされた全てのユーザーを含むために指定します

入力された指定エントリーを探すために[Find]をクリックします。

ポート単位でクリアするために[Clear By Port]をクリックします。

全てのホスト一覧を見るために[View All Hosts]をクリックします。

全てのホストをクリアするために[Clear All Hosts]をクリックします。

3.7.16 Browse Session Table

最後にスイッチを再起動してからの管理セッションが表示されます。

次のウィンドウを表示するには、Monitoring > Browse Session Table をクリックします：

Browse Session Table

ID	Live Time	From	Level	Name
8	03:31:57.0	Serial Port	1	Anonymous

3.7.17 MAC Address Table

スイッチの動的 MAC アドレスを表示します。スイッチが MAC アドレスとポート番号の対応を学習すると、フォワーディングテーブルにエントリが作成されます。これらのエントリを使用してスイッチ経由でパケットを転送します。

次のウィンドウを表示するには、Monitoring > MAC Address Table をクリックします。

MAC Address Table

Port:

VLAN Name:

MAC Address:

Total Entries :0

VID	VLAN Name	MAC Address	Port	Type
1	default	00-40-66-45-5E-78	CPU	Self

下記にパラメーターの説明を記載します。

パラメーター	説明
Port	フォワーディングテーブルを参照するポート番号を指定します。
VLAN Name	フォワーディングテーブルを参照する VLAN 名を入力します。
MAC Address	フォワーディングテーブルを参照する MAC アドレスを入力します。
Find	Port/VLAN Name/MAC Address の各項目に対応するデータベースを表示します。
Clear Dynamic Entries	アドレステーブルのすべての動的エントリを削除します。
View All Entry	アドレステーブルのすべてのエントリを表示します。
Clear All Entry	アドレステーブルのすべてのエントリを削除します。

[Find]をクリックして入力パラメーターに基づく指定エントリを検索します。

[Clear Dynamic Entries]をクリックして全てのダイナミックエントリをクリアーします。

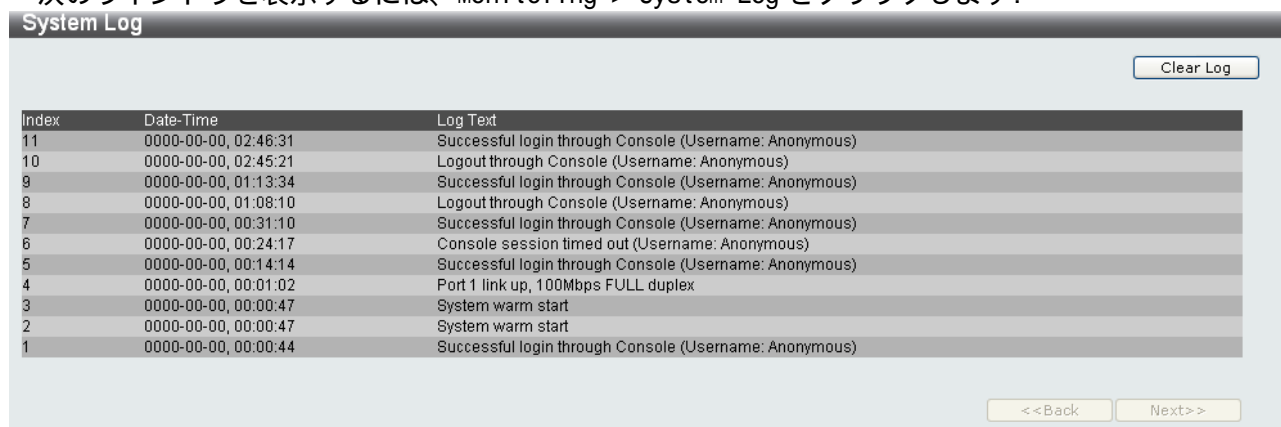
[View All Entry]をクリックして使用可能な全てのエントリ一覧を表示します。

[Clear All Entry]をクリックして表示されている全てのエントリをクリアーします。

3.7.18 System Log

スイッチの履歴ログを表示します。

次のウィンドウを表示するには、Monitoring > System Log をクリックします：



スイッチのイベントログ情報を表示します。[Next]をクリックして次ページのログ情報を表示します。[Clear log]をクリックして、全てのログ情報を消去します。

下記にパラメーターの説明を記載します。

パラメーター	説明
Index	イベントログ情報の発生した順番を示します。Index 値が大きいほど新しく発生したログ情報となります。
Date-Time	イベントログ情報の発生した時刻を示します。表示される時刻は、起動からの経過時間または現在の時刻が表示されます。
Log Text	イベントログ情報の内容が表示されます。

3.7.19 Self-Test

スイッチの起動時に実施された Self-Test の結果を表示します。

POE Test の結果は、APLGM110GTPOE/POE2、APLGM118GTPOE/POE2、APLGM124GTPOE/POE2 のみ表示されます。

次のウィンドウを表示するには、Monitoring > Self-Test をクリックします：



3.7.20 PD Monitoring

PD モニタリング機能は、PoE 電源供給ポートに接続されている受電デバイス(PD: Powered Device)の死活を定期的に監視し、応答がない場合に対象ポートでの PoE の再起動などの指定したアクションを実行する機能です。この機能を使用すると、なんらかの理由で受電デバイスが応答しなくなった場合に、自動的にデバイスを再起動させることができます。

受電デバイスの死活監視は、対象ポートから ICMP パケットを送信して行われます。そのため、監視対象は装置本体の管理 IP アドレスと同じネットワークに属する IP アドレスのノードに限定されます。また、対象ポートには管理 IP アドレスを割り当てた VLAN と同一の PVID を設定する必要があります。

この機能は APLGM110GTPOE/POE2、APLGM118GTPOE/POE2 および APLGM124GTPOE/POE2 の計 6 機種のみで対応しています。

3.7.20.1 PD Monitoring Global Settings

このウィンドウを使用して、PD モニタリング機能のグローバル設定を行います。

次のウィンドウを表示するには、Monitoring > PD Monitoring > PD Monitoring Global Settings をクリックします：

PD Monitoring Global Settings

global state

period to start (1-10)

restart poe retry (1-3)

Apply

ICMP

interval (1-60)

timeout (500-3000)

count (3-10)

Apply

下記にパラメーターの説明を記載します。

パラメーター	説明
global state	プルダウンメニューで、Enabled または Disabled を選択して、PD モニタリング機能の有効(Enabled)または無効(Disabled)を設定します。
period to start	PD モニタリング機能の監視開始時間を分単位で指定します(1~10 分)。
restart poe retry	PD モニタリング機能での再起動による受電デバイス復旧試行回数を指定します(1~3 回)。指定した回数 PoE 再起動を実行してもデバイスの復旧を確認できない場合、ポートの PoE 給電を停止します。
interval	PD モニタリング機能の ICMP パケット送信間隔を秒単位で指定します(1~60 秒)。
timeout	PD モニタリング機能の ICMP パケットのタイムアウト時間をミリ秒単位で指定します(500~3000 ミリ秒)。
count	PD モニタリング機能の ICMP パケットの再送回数を指定します(3~10 回)。この回数を超えて連続してデバイスからの応答がない場合、指定したアクションを実施します。

[Apply] をクリックして変更を適用します。

3.7.20.2 PD Monitoring Port Settings

このウィンドウを使用して、PD モニタリング機能の自動復旧時間を設定します。自動復旧時間は、デバイスが応答しない場合のアクションで restart-poe が選択されていて、その動作によりポートの PoE 給電設定が無効に切り替わった場合に、自動的に有効に戻すまでの時間です。

次のウィンドウを表示するには、Monitoring > PD Monitoring > PD Monitoring Port Settings をクリックします：

Port	Auto-Recovery Time
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	設定するポートの範囲指定をします。
Auto-Recovery Time	PD モニタリング機能によりポートの PoE 給電が無効になった場合に、自動的に有効に戻るまでの時間を分単位で指定します。0 の場合、自動復旧は行われず、PoE 給電を再開するためには、Configuration > PoE > PoE Port Settings の画面からポートの PoE 設定を有効に変更する必要があります。

[Apply] をクリックして変更を適用します。[Refresh] をクリックすると、情報が更新されます。

3.7.20.3 PD Monitoring Port ICMP Settings

このウィンドウを使用して、PD モニタリング機能の各ポートでの監視対象やアクションを設定します。アクションは監視パケットを送信したデバイスから応答が確認できない場合に実行する処理で、該当するポートで PoE の再起動を実施する restart-poe と、PoE 再起動を実施せず通知のみを行う notify-only の 2 種類から選択することができます。

次のウィンドウを表示するには、Monitoring > PD Monitoring > PD Monitoring Port ICMP Settings をクリックします：

PD Monitoring Port ICMP Settings

From Port: To Port: ICMP State: PD-IP Type: IP address(IPv6 address): Action:

Delete ICMP PD-IP From Port: To Port:

Port	icmp state	IP address(IPv6 address)	action
1	Disabled	0.0.0.0	Restart-PoE
2	Disabled	0.0.0.0	Restart-PoE
3	Disabled	0.0.0.0	Restart-PoE
4	Disabled	0.0.0.0	Restart-PoE
5	Disabled	0.0.0.0	Restart-PoE
6	Disabled	0.0.0.0	Restart-PoE
7	Disabled	0.0.0.0	Restart-PoE
8	Disabled	0.0.0.0	Restart-PoE

下記にパラメーターの説明を記載します。

パラメーター	説明
From Port/To Port	設定するポートの範囲指定をします。
ICMP State	各ポートで PD モニタリングによる監視を行うか(Enabled)、監視しないか(Disabled)を設定します。
PD-IP Type	監視パケットを送信するデバイスのアドレスタイプを IPv4 もしくは IPv6 で指定します。
IP address (IPv6 address)	監視パケットの送信先 IP アドレスもしくは IPv6 アドレスを指定します。
Action	監視パケットに対するデバイスからの応答が確認できない場合のアクションを指定します。restart-poe を指定すると、ポートで PoE の再起動を実施し、デバイスの復旧を試行します。notify-only を指定すると、PoE の再起動は実施せず、通知のみ行われます。
Delete ICMP PD-IP From Port/To Port	監視対象の設定を削除する場合に使用します。この場合、削除するポートを範囲指定し、[Apply]をクリックします。

[Apply]をクリックして変更を適用します。[Refresh]をクリックすると、情報が更新されます。

3.8 セーブ

下記に示す 3 つの保存ウィンドウを使用して設定情報をスイッチのメモリーに保存します。

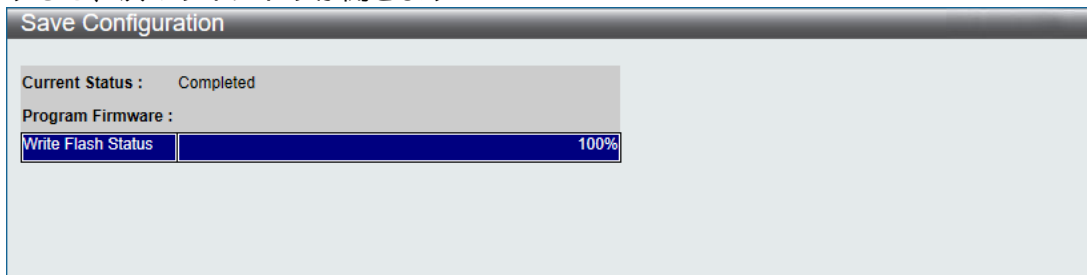
(1)[Save Configuration]で現在の設定情報を保存します。

(2)[Save Log]で現在のログだけを保存します。

(3)[Save All]で現在の設定情報とログを保存します。

3.8.1 Save Configuration

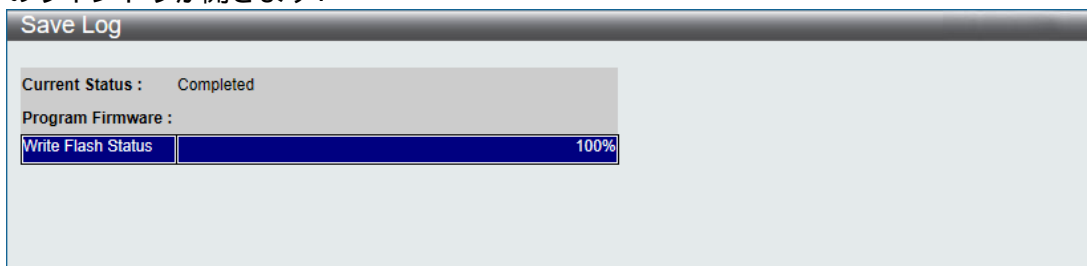
GUI 画面の一番上にある[セーブ]プルダウンメニューを開いて、[Save Configuration]をクリックすると、次のウィンドウが開きます：



Write Flash Status が 100%になると保存完了です。

3.8.2 Save Log

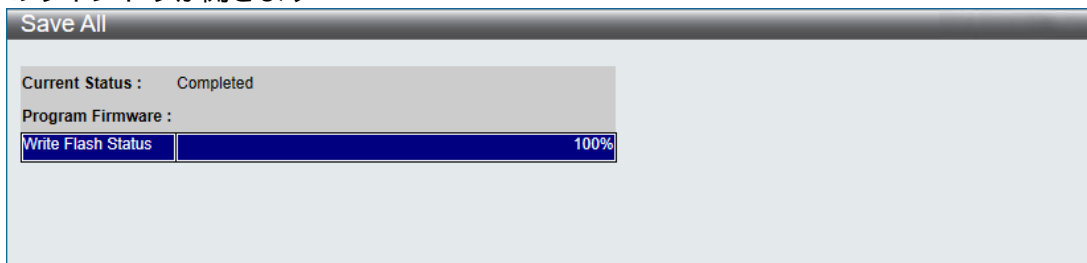
GUI 画面の一番上にある[セーブ]プルダウンメニューを開いて、[Save Log]をクリックすると、次のウィンドウが開きます：



Write Flash Status が 100%になると保存完了です。

3.8.3 Save All

GUI 画面の一番上にある[セーブ]プルダウンメニューを開いて、[Save All]をクリックすると、次のウィンドウが開きます：



Write Flash Status が 100%になると保存完了です。

注意事項

- ❗ save コマンドの実行時、CPU 高負荷状態を示す CPU utilization (OVERLOADING) ログが出力される場合があります。

3.8.4 Show Technical Support

GUI 画面の一番上にある[セーブ]プルダウンメニューを開いて、[Show Technical Support]を選択し、Show ボタンをクリックすると、次のウィンドウが開きます:

```
=====
                        APLGM118GTSS Gigabit Ethernet Switch
                        Technical Information Report
=====
[CPU Utilization 6160870ms]
CPU Utilization :
=====
Five Seconds - 4 %      One Minute - 2 %      Five Minutes - 3 %
=====
[Device Information 6161070ms]
Device Type       : APLGM118GTSS Gigabit Ethernet Switch
MAC Address       : 00-40-86-55-4C-D2
IP Address        : 10.85.76.210 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.01
Firmware Version  : Build 1.14.00
Hardware Version  : A
Serial number     : 170882130003
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
802.1x            : Disabled
TELNET            : Enabled (TCP 23)
WEB               : Enabled (TCP 80)
RMON              : Disabled
SSH               : Disabled
SSL               : Disabled
Syslog Global State: Disabled
Dual Image        : Supported
=====
[Connection Session Status 6161270ms]
To  Local Time  Local Time  From  Local Time  Local Time
=====
```

[Show]をクリックしてテクニカルサポート情報の表示を更新します。
ページ番号をクリックまたは指定して画面情報の表示を変更します。

注意事項

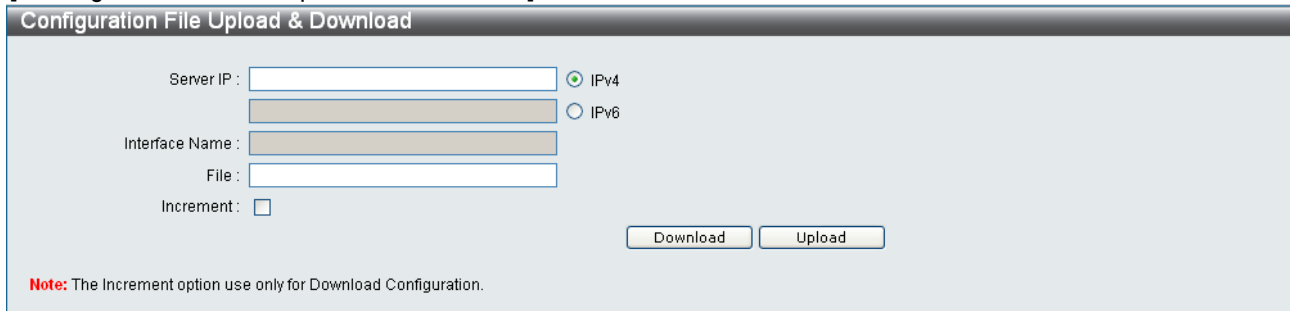
- ❗ テクニカルサポート情報が表示されるまで時間がかかる場合があります。

3.9 ツール

3.9.1 Configuration File Upload & Download

スイッチは設定情報をアップロード、またはダウンロードすることができます。

GUI 画面の一番上にあるメニューバーの左側の[ツール]プルダウンメニューを開いて、[Configuration File Upload & Download]をクリックすると、次のウィンドウが開きます：



Configuration File Upload & Download

Server IP : IPv4
 IPv6

Interface Name :

File :

Increment :

Note: The Increment option use only for Download Configuration.

ラジオボタンで[IPv4]または[IPv6]を選択して、サーバーIPアドレス、インターフェース名、ファイル名を入力します。[Download]または[Upload]をクリックして、ファイルの転送を開始します。

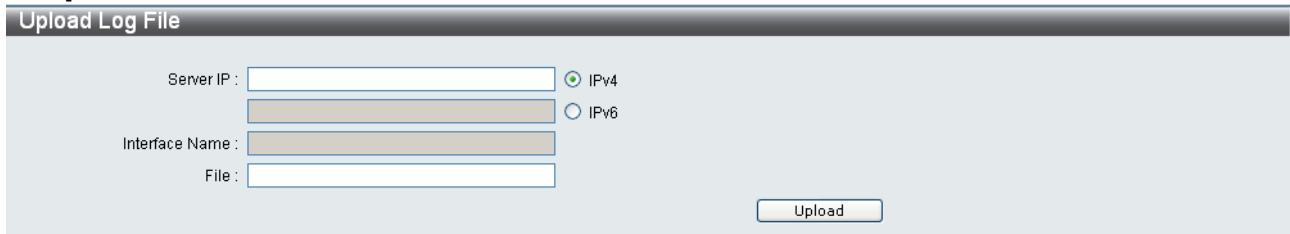
注意事項

- ❗ ダウンロードしたコンフィグファイルを現在の設定に置き換える場合、リンクアップしているポートは一時切断されます。
- ❗ アップロードしたコンフィグファイルに account 情報は含まれません。

3.9.2 Upload Log File

ログファイルのアップロードは、[IPv4]または[IPv6]を選択して、サーバーIPアドレス、ファイル名を入力します。入力後、[Upload]をクリックします。

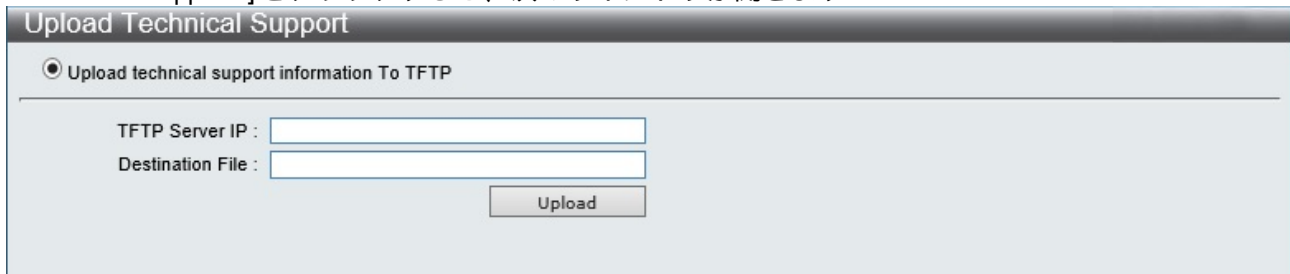
GUI画面の一番上にあるメニューバーの左側の[ツール]プルダウンメニューを開いて、[Upload Log File]をクリックすると、次のウィンドウが開きます：



3.9.3 Upload Technical Support

テクニカルサポート情報のアップロードは、サーバーIPアドレス、ファイル名を入力します。入力後、[Upload]をクリックします。

GUI画面の一番上にあるメニューバーの左側の[ツール]プルダウンメニューを開いて、[Upload Technical Support]をクリックすると、次のウィンドウが開きます：



注意事項

- ❗ upload コマンドの実行中、CPU 高負荷状態を示す CPU utilization (OVERLOADING) ログが出力される場合があります。

3.9.4 Reset


リセット機能にはスイッチをリセットするいくつかのオプションがあります。

GUI 画面の一番上にあるメニューバーの左側の[ツール]プルダウンメニューを開いて、[Reset System]をクリックすると、次のウィンドウが開きます：

パラメーター	説明
Reset	Proceed with system reset except IP address, log, user account and banner.
Reset Config	Switch will be reset to factory defaults.
Reset System	Switch will be reset to factory defaults and reboot.

パラメーター	説明
Reset	スイッチの現在の IP アドレス、アカウント、およびスイッチの履歴ログは変更されません。他のすべてのパラメーターはデフォルト設定にリストアされます。スイッチのコンフィグ設定保存および装置再起動は行われません。
Reset Config	IP アドレス、アカウント、スイッチ履歴ログなどを含むすべての設定がデフォルト設定に戻ります。スイッチは再起動せずに、即時反映されます。
Reset System	スイッチの設定がデフォルト値に変更され、保存および再起動が行われます。

注意事項

 reset system コマンドを選択した場合、コンフィグ設定ファイル(ID1/ID2 とともに)の初期化と再起動が行われます。

3.9.5 Ping Test

GUI 画面の一番上にあるメニューバーの左側の[ツール]プルダウンメニューを開いて、[Ping Test]をクリックすると、次のウィンドウが開きます：

パラメーター	説明
IPv4 Ping Test	Enter the IP address of the device or station you want to ping, then click Start . Target IP Address : 0.0.0.0 Repeat Pinging for: <input checked="" type="radio"/> Infinite times, <input type="radio"/> (1-255 times) Timeout: 1 (1-99 sec)
IPv6 Ping Test	Enter the IP address of the device or station you want to ping, then click Start . Target IP Address : Interface Name: Repeat Pinging for: <input checked="" type="radio"/> Infinite times, <input type="radio"/> (1-255 times) Size: 100 (1-6000) Timeout: 1 (1-10 sec)

[infinite times]選択では、手動停止するまで Ping を送信し続けます。[infinite times]選択では、1 ~ 255 まで Ping 実行回数を指定することができます。[Start]をクリックして Ping を開始します。

下記にパラメーターの説明を記載します。

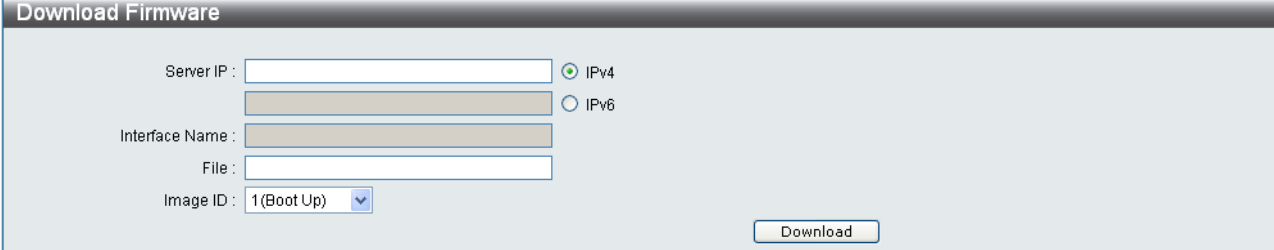
パラメーター	説明
Target IP Address	ping を送信する IP アドレスを入力します。
Interface Name	IPv6 では、インターフェースの名前を入力します。
Repeat Pinging for	ping を実施する回数を入力します。1 ~ 255 の範囲で設定します。
Size	IPv6 では、1 ~ 6000 の値を入力します。デフォルトは 100 です。
Timeout	IPv4 では、この ping メッセージが送信先に届くまでのタイムアウト時間を 1 ~ 99 秒から選択します。IPv6 では、この ping メッセージが送信先に届くまでのタイムアウト時間を 1 ~ 10 秒から選択します。どちらの場合も、パケットが指定した時間内に IP アドレスを見つけないと、ping パケットはドロップ（破棄）されます。

[Start]をクリックして Ping プログラムを開始します。

3.9.6 Download Firmware

スイッチは、バックアップと復旧用として、2つのファームウェアファイルを保持できます。ファームウェアイメージには ID 番号 1 または 2 が付いています。ブートファームウェアイメージを変更するには、イメージ ID プルダウンメニューから、バックアップまたは復旧するファームウェアファイルを選択します。デフォルトのスイッチ設定では、イメージ ID 1 をブートファームウェアファイルとして使用します。

GUI 画面の一番上にあるメニューバーの左側の[ツール]プルダウンメニューを開いて、[Download Firmware]をクリックすると、次のウィンドウが開きます：



ラジオボタンで [IPv4] または [IPv6] を選択します。選択したタイプの TFTP サーバー IP アドレスを入力します。TFTP サーバーのファイルのパス/ファイル名を指定します。イメージ ID を 1 (ブートアップ) または 2 から選択します。[Download] をクリックしてファイルの転送を開始します。

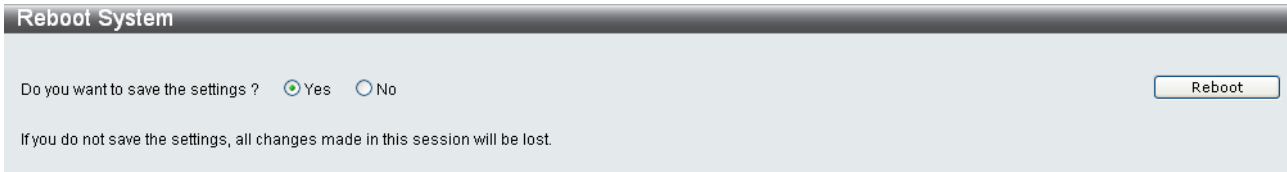
注意事項



ファームウェアのダウンロード時、CPU 高負荷状態を示す CPU utilization (OVERLOADING) ログが出力される場合があります。

3.9.7 Reboot System

次のウィンドウを使用してスイッチを再起動します。



Do you want to save the settings ? Yes No Reboot



If you do not save the settings, all changes made in this session will be lost.

[Yes]のラジオボタンでスイッチを再起動する前に、現在の設定を NV-RAM に保存します。

[No]のラジオボタンでスイッチを再起動する前に、現在の設定を保存しません。最後に設定情報を保存した後に入力したすべての設定情報は失われます。

[Reboot]をクリックしてスイッチを再起動します。

注意事項

-  指定したセクション ID 番号のファームウェア異常により起動できない場合、自動的に別 ID 番号のファームウェアで起動します。
-  電源を再投入する場合、電源切断後 5 秒以上間隔をあ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。
- (2) ポートミラーリング機能は、source ポートとして設定したポートで送受信されたフレーム等を解析するための機能です。従って、Target ポートとして設定したポートには、アナライザー等ネットワークを解析する装置以外は接続しないでください。
- (3) ポート VLAN を設定する場合、ホスト(スイッチングハブ)が属していないグループのポートからホスト宛に通信を行うことはできません。またホストは複数のグループに属することはできません。

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。
	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。	
「CONSOLE」 LED が点滅している。	当該装置またはその接続先ネットワークにてループが生じていないか確認してください。

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 HTTP に関連する現象と対策

現象	対策
端末から HTTP 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。
	HTTP 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 スイッチングハブ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 VLAN に関連する現象と対策

現象	対策
VID を指定するとエラーメッセージが表示される。	指定した VID が、既に他の VLAN グループで使用されているとき、エラーメッセージが表示されます。VID の設定を修正してください。

5.6 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。

5.7 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。また、PD モニタリング機能を使用している場合、定められた動作に基づいて PoE 給電を停止するようにポートの設定を自動的に変更することがありますので、設定内容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。

5.8 内蔵冷却ファンに関連する現象と対策

現象	対策
電源投入しても冷却ファンが回転しない	ファンそのものの異常が考えられます。カバーをあけることなく、お買い求めの販売店もしくは販売元にお問い合わせください。

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 IEEE802.3u : Auto-Negotiation IEEE802.3z : 1000BASE-X IEEE802.3ab : 1000BASE-T
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 SimpleNetwork Management Protocol 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 the Simple Network Management Protocol (SNMP)
4	ネットワーク管理対象	RFC1213 : Internet 標準 MIB RFC1493 : Bridge MIB RFC2819 : RMON MIB 4 グループ RFC2021 : RMON2 MIB のうち Probe config の一部 RFC2863 : ifMIB 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 RFC1769 : SNTP(Simple Network Time Protocol) RFC3164 : SYSLOG RFC5321 : SMTP(Simple Mail Transfer Protocol) RFC951/RFC1541 : BootP/DHCP Client
6	IGMP snooping	RFC1112 : IGMPv1 (snooping only) RFC2236 : IGMPv2 (snooping only) RFC3376 : IGMPv3 (awareness only)

No.	項 目	準 拠 規 格
7	セキュリティープロトコル	RFC2865 : RADIUS (client only) RFC1492 : TACACS+ Authentication For the Management Access RFC2138/RFC2139 : RADIUS Auth. For Management Access RFC2866 : RADIUS Accounting (802.1x only) 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 RFC4254 : The Secure Shell(SSH) Connection Protocol RFC4256 : Generic Message Exchange Authentication for the Secure Shell Protocol(SSH)
8	その他	VCCI Class A 準拠 IEEE802.3ad : リンクアグリゲーション IEEE802.1Q : tag group VLAN, QoS(IEEE802.1Q priority mapping/queuing) IEEE802.1D : STP/RSTP IEEE802.1Q : MSTP IEEE802.3x : フロー制御 IEEE802.1AB : LLDP IEEE802.3at : PoE Plus

ApresiaLightGM シリーズ Ver.1.14 SW マニュアル

Copyright(c) 2020 APRESIA Systems, Ltd.

2020年7月初版

APRESIA Systems 株式会社
東京都中央区築地二丁目3番4号
築地第一長岡ビル

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