



TD61-6746

ApresiaLightGM152GT

Ver. 1.02

SW マニュアル

APRESIA Systems 株式会社

制定・改訂来歴表

No.	年 月 日	内 容
-	2018年4月23日	<ul style="list-style-type: none">・ Ver.1.01 ソフトウェアマニュアル(TD61-6187)から新規作成 <内容変更><ul style="list-style-type: none">・ 1.1 初期 IP アドレス設定を追加 <機能追加>・ 3.9.2 Show Technical Support項を追加・ 3.10.3 Upload Technical Support項を追加

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、各適用機種の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
ApresiaLightGM152GT	ApresiaLightGM152GT	APLGM152GT



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

注意事項



本ファームウェアは APLGM152GT 専用です。既存の ApresiaLightGM シリーズおよび ApresiaLightFM シリーズのファームウェアをインストールすることは出来ません。

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ルーティングソフトウェアを含む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、事業の中止、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。

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
3.2.4.1 IPv6 Route Settings	24
3.2.5 IPv6 Neighbor Settings	25
3.2.6 IPv4 Static/Default Route Settings	26
3.2.7 IPv4 Route Table	26
3.2.8 Port Configuration	27
3.2.8.1 Port Settings	27
3.2.8.2 Port Description Settings	29
3.2.8.3 Port Error Disabled	30
3.2.8.4 Port Media Type	30
3.2.8.5 Port Green Mode Settings	31
3.2.8.6 EEE Settings	32
3.2.9 Static ARP Settings	33
3.2.10 User Accounts	34
3.2.11 System Log Configuration	35
3.2.11.1 System Log Settings	35
3.2.11.2 System Log Server	35
3.2.12 MAC Address Aging Time	37
3.2.13 Web Settings	37
3.2.14 Telnet Settings	38
3.2.15 CLI Paging Settings	38
3.2.16 Configuration File Information	39
3.2.17 Firmware Information	40
3.2.18 SNTP Settings	41

3.2.18.1 Time Settings	41
3.2.18.2 TimeZone Settings	42
3.2.19 SMTP Settings	44
3.2.19.1 SMTP Service Settings	44
3.2.20 SNMP Settings	46
3.2.20.1 SNMP View Table	47
3.2.20.2 SNMP Group Table	48
3.2.20.3 SNMP User Table	49
3.2.20.4 SNMP Community Table	50
3.2.20.5 SNMP Host Table	51
3.2.20.6 SNMP Engine ID	51
3.2.20.7 SNMP Trap Configuration	52
3.2.20.8 SNMP Linkchange Traps Settings	53
3.2.20.9 RMON	54
3.2.20.10 SNMP v6Host Table Setting	54
3.3 Command Logging	55
3.3.1 Command Logging Settings	55
3.4 L2 Features	56
3.4.1 Jumbo Frame	56
3.4.2 VLANs	56
3.4.3 802.1Q Static VLAN	63
3.4.4 QinQ	66
3.4.4.1 QinQ Settings	66
3.4.4.2 VLAN Translation CVID Entry Settings	67
3.4.5 802.1v Protocol VLAN	68
3.4.5.1 802.1v Protocol Group Settings	68
3.4.5.2 802.1v Protocol VLAN Settings	69
3.4.6 GVRP Settings	71
3.4.7 Asymmetric VLAN Settings	72
3.4.8 MAC-based VLAN Settings	72
3.4.9 PVID Auto Assign Settings	73
3.4.10 Link Aggregation(Port Trunking)	74
3.4.11 LACP Port Settings	76
3.4.12 Traffic Segmentation	77
3.4.13 BPDU Guard Settings	78
3.4.14 IGMP Snooping	79
3.4.14.1 IGMP Snooping Settings	79
3.4.15 MLD Snooping Settings	82
3.4.16 Port Mirror	86
3.4.17 Loopback Detection Settings	87
3.4.18 Spanning Tree	89
3.4.18.1 STP Bridge Global Settings	91

3.4.18.2 STP Port Settings	93
3.4.18.3 MST Configuration Identification	95
3.4.18.4 STP Instance Settings	96
3.4.18.5 MSTP Port Information	96
3.4.19 Forwarding & Filtering	97
3.4.19.1 Unicast Forwarding Settings	97
3.4.19.2 Multicast Forwarding Settings	98
3.4.19.3 Multicast Filtering Mode	99
3.4.20 LLDP	100
3.4.20.1 LLDP Global Settings	100
3.4.20.2 LLDP Port Settings	101
3.4.20.3 LLDP Basic TLVs Settings	102
3.4.20.4 LLDP Dot1 TLVs Settings	103
3.4.20.5 LLDP Dot3 TLVs Settings	104
3.4.21 Show VLAN Ports	105
3.5 サービス品質 (QoS)	106
3.5.1 Bandwidth Control	107
3.5.2 Traffic Control	108
3.5.3 802.1p Default Priority	111
3.5.4 802.1p User Priority	111
3.5.5 QoS Scheduling Settings	112
3.5.6 Priority Mapping	113
3.5.7 TOS Mapping	114
3.5.8 DSCP Mapping	114
3.6 Security	115
3.6.1 Trusted Host	115
3.6.2 Port Security	116
3.6.2.1 Port Security Port Settings	116
3.6.2.2 Port Security FDB Entries	117
3.6.3 Authentication Setting	118
3.6.4 802.1X	119
3.6.4.1 802.1X Global Settings	119
3.6.4.2 802.1X Port Settings	120
3.6.4.3 802.1X User	122
3.6.4.4 Authentication RADIUS Server	122
3.6.5 SSL Settings	126
3.6.6 SSH	129
3.6.6.1 SSH Settings	129
3.6.6.2 SSH Authmode and Algorithm Settings	131
3.6.6.3 SSH User Authentication Lists	132
3.6.7 Access Authentication Control	133
3.6.7.1 Enable Admin	134
3.6.7.2 Authentication Policy Settings	135

3.6.7.3 Application Authentication Settings	136
3.6.7.4 Authentication Server Group	137
3.6.7.5 Authentication Server	138
3.6.7.6 Login Method Lists	139
3.6.7.7 Enable Method Lists	140
3.6.7.8 Local Enable Password Settings	141
3.6.8 MAC-based Access Control	142
3.6.8.1 MAC-based Access Control Settings	143
3.6.8.2 MAC-based Access Control Local Settings	145
3.6.9 Web Authentication	146
3.6.9.1 Web Authentication Settings	146
3.6.9.2 Web Authentication User Settings	147
3.6.9.3 Web Authentication Port Settings	148
3.6.9.4 Web Authentication Customize	149
3.7 アクセス制御一覧(ACL)	152
3.7.1 ACL Configuration Wizard	152
3.7.2 Access Profile List	153
3.7.3 Access profile list-IPv4 ACL	157
3.7.4 Access profile list-IPv6 ACL	162
3.7.5 Access profile list-Packet content ACL	166
3.7.6 ACL Finder	170
3.7.7 ACL Flow Meter	170
3.8 Monitoring	172
3.8.1 Cable Diagnostics	172
3.8.2 SFP General Information	172
3.8.3 SFP Diagnostic Monitoring	173
3.8.4 CPU Utilization Notify	174
3.8.5 CPU Utilization	175
3.8.6 DRAM Utilization Notify	176
3.8.7 DRAM & FLASH Utilization	177
3.8.8 Port Utilization	177
3.8.9 Packet Size	178
3.8.10 Packets	180
3.8.10.1 Received (Rx)	180
3.8.10.2 UMB_cast(Rx)	181
3.8.10.3 Transmitted (Tx)	183
3.8.11 Errors	184
3.8.11.1 Received (RX)	184
3.8.11.2 Transmitted (TX)	186
3.8.12 Port Access Control	187
3.8.12.1 RADIUS Authentication	187
3.8.12.2 RADIUS Account Client	189

3.8.12.3 Authenticator State	191
3.8.12.4 Authenticator Statistics	192
3.8.12.5 Authenticator Session Statistics	193
3.8.12.6 Authenticator Diagnostics	194
3.8.13 Browse ARP Table	196
3.8.14 Browse VLAN	196
3.8.15 IGMP Snooping	197
3.8.15.1 Browse IGMP Router Port	197
3.8.15.2 IGMP Snooping Group	197
3.8.15.3 IGMP Snooping Host	198
3.8.16 MLD Snooping	198
3.8.16.1 Browse MLD Router Port	198
3.8.16.2 MLD Snooping Group	199
3.8.17 LLDP	199
3.8.17.1 LLDP Statistics System	199
3.8.17.2 LLDP Local Port Information	200
3.8.17.3 LLDP Remote Port Information	201
3.8.18 MBA Authentication State	201
3.8.19 Web Authentication State	202
3.8.20 Browse Session Table	202
3.8.21 MAC Address Table	203
3.8.22 System Log	204
3.8.23 Self-Test	204
3.8.24 Port LED Testing	205
3.8.25 Temperature Notify	206
3.8.26 Peripheral	207
3.8.26.1 Device Environment	207
3.9 セーブ	208
3.9.1 Save Configuration/Log	208
3.9.2 Show Technical Support	209
3.10 ツール	210
3.10.1 Configuration File Upload & Download	210
3.10.2 Upload Log File	211
3.10.3 Upload Technical Support	211
3.10.4 Reset	212
3.10.5 Ping Test	212
3.10.6 Download Firmware	213
3.10.7 Reboot System	214
4. 使用上の注意事項	215
5. トラブルシューティング	216
5.1 表示 LED に関する現象と対策	216
5.2 コンソール端末に関する現象と対策	216

5.3 HTTP に関する現象と対策	217
5.4 スイッチングハブ機能に関する現象と対策	217
5.5 VLAN に関する現象と対策	217
5.6 SFP に関する現象と対策	217
5.7 内蔵冷却ファンに関する現象と対策	218
6. 準拠規格	219

1. パラメーター設定手順

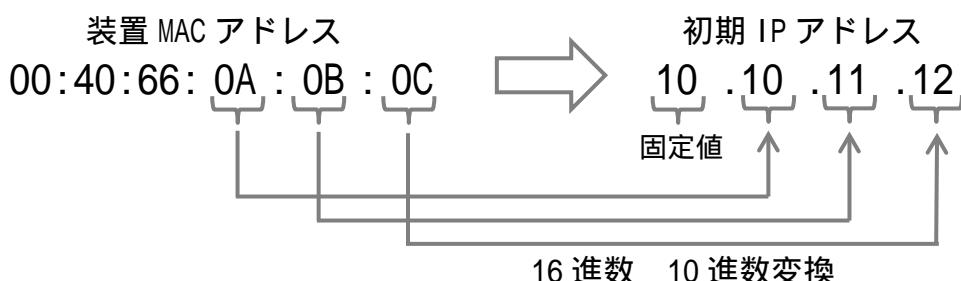
パラメーターの設定は、設定端末の準備、設定端末の接続、パラメーターの設定手順で行います。
Web ベース GUI 方式によるコマンド詳細については 3 章を参照してください。
また、コマンドライン方式については別紙(CLI マニュアル)を参照してください。

1.1 初期 IP アドレス設定

Ver.1.02 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。

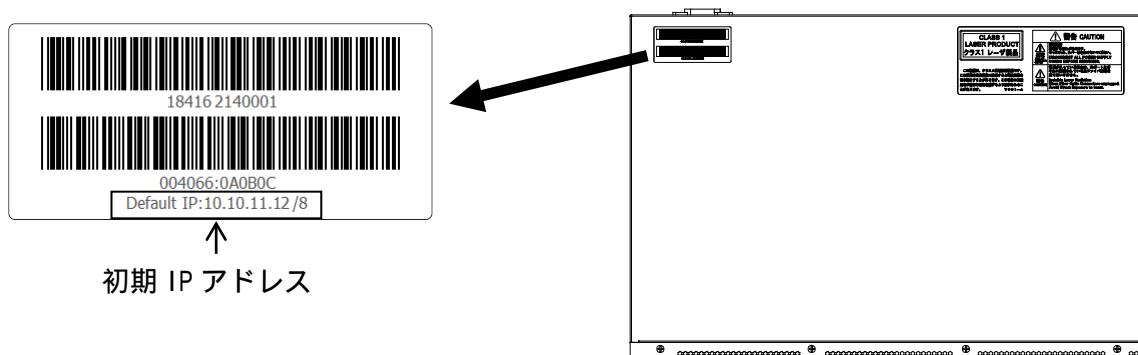


(2) サブネットマスク

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

(4) 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

! デフォルト設定では、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(1.3 節参照)

パラメーター設定端末の接続(1.4 節参照)

パラメーター設定端末の電源 ON

本装置の電源 ON

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

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>

ApresiaLightGM152GT Gigabit Ethernet Switch
Command Line Interface

Firmware: 1.02.00

Copyright (C) 2018 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

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	8bit/キャラクタ
2	ストップビット	1bit
3	parity	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。

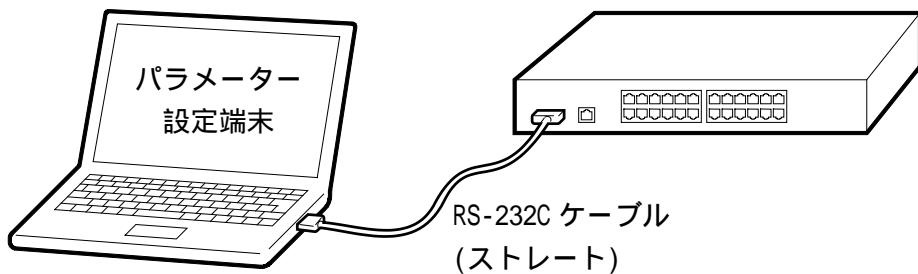


図 1-1 RS-232C ケーブルの接続

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	パラメーター設定用端末 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 > メニュー名オプション	メニュー名 > メニュー名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。

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://10.0.0.1` を入力します。

10.0.0.1 は、スイッチに事前に設定した IP アドレスを示します。IP アドレスが事前に設定されていない場合は、「パラメーター設定手順」に従いコマンドラインインターフェースから IP アドレスの設定を行ってください。

次の図にあるような管理モジュールのユーザー認証ウィンドウが開きます。

下記の図にあるような認証画面が開きます。

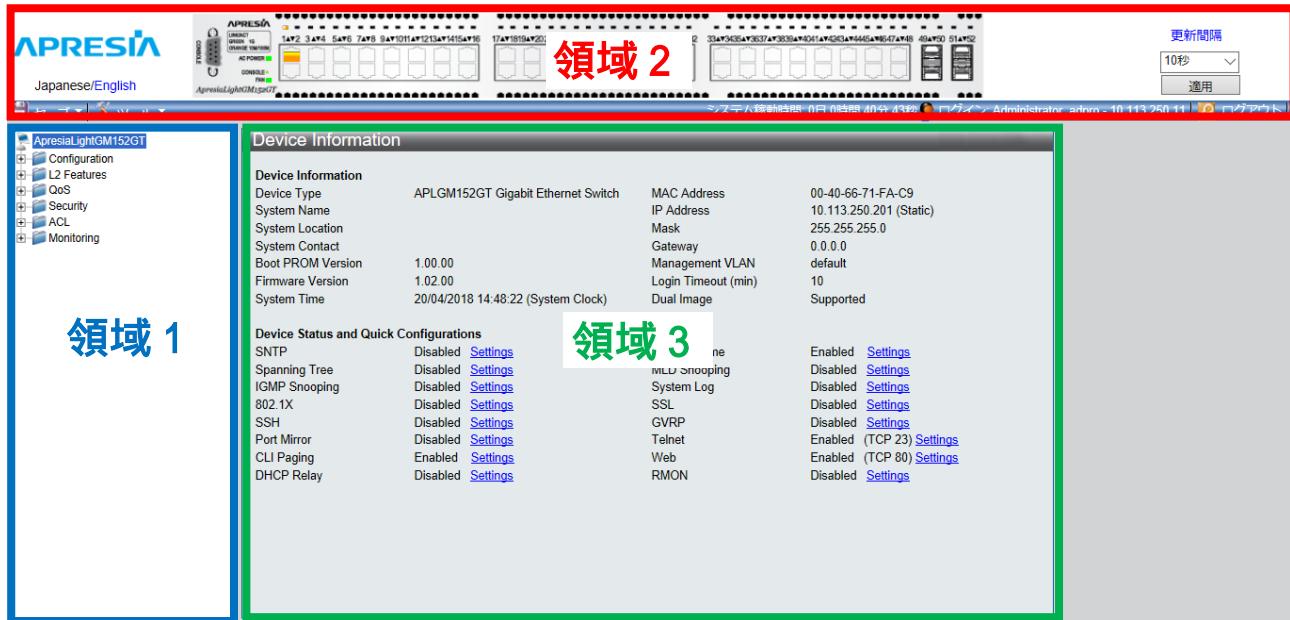


ユーザー名とパスワードを入力し(デフォルトのユーザー名:adpro、パスワード:なし)、OK をクリックします。GUI 画面が開きます。

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	表示するフォルダまたはウィンドウを選択します。フォルダアイコンを開いて、ハイパークリンクウィンドウボタンとそれに含まれるサブフォルダを表示します。
領域 2	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 APREISA ロゴをクリックすると APREISA 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](セーブ > 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. 1.02)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 Type	APLGM152GT Gigabit Ethernet Switch	MAC Address	00-40-66-71-FA-C9
System Name		IP Address	10.113.250.201 (Static)
System Location		Mask	255.255.255.0
System Contact		Gateway	0.0.0.0
Boot PROM Version	1.00.00	Management VLAN	default
Firmware Version	1.02.00	Login Timeout (min)	10
System Time	20/04/2018 14:48:22 (System Clock)	Dual Image	Supported
Device Status and Quick Configurations			
SNTP	Disabled Settings	Jumbo Frame	Enabled Settings
Spanning Tree	Disabled Settings	MLD Snooping	Disabled Settings
IGMP Snooping	Disabled Settings	System Log	Disabled Settings
802.1X	Disabled Settings	SSL	Disabled Settings
SSH	Disabled Settings	GVRP	Disabled Settings
Port Mirror	Disabled Settings	Telnet	Enabled (TCP 23) Settings
CLI Paging	Enabled Settings	Web	Enabled (TCP 80) Settings
DHCP Relay	Disabled Settings	RMON	Disabled Settings

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含まれます。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。

MAC Address	00-40-66-71-FA-C9
Firmware Version	1.02.00
System Name	[Input Field]
System Location	[Input Field]
System Contact	[Input Field]
<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
System Name	スイッチのシステム名を入力します。
System Location	スイッチの場所を入力します。
System Contact	スイッチの連絡先名を入力します。

[Apply]をクリックして変更を適用します。

3.2.2 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:

Baud Rate	9600
Auto Logout	Never
Data Bits	8
Parity Bits	None
Stop Bits	1
<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
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' window with the 'Static' tab selected. The configuration details are as follows:

Setting	Value
IP Interface	System
Management VLAN Name	default
Interface Admin State	Enabled
IPv4 Address	10.90.90.90
Subnet Mask	255.0.0.0
Gateway	0.0.0.0

An 'Apply' button is located at the bottom right of the window.

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。

ポートを有効にする場合は、Interface Admin State プルダウンメニューから [Enabled] を選択します。

BOOTP プロトコルまたは、DHCP 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	有効と無効を切り替えます。IP アドレスを設定する場合は、有効に設定します。
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：

IPv6 Interface Settings

IPv6 Interface Settings	System
Interface Name	Enabled
Interface Admin State	Disabled
DHCPv6 Client	
NS Retransmit Time Settings	IPv6 Network Address (e.g.: 3710::1/64)
NS Retransmit Time (0-4294967295)	0 ms
Automatic Link Local State Settings	Disabled
Automatic Link Local Address	
View All IPv6 Address	
<<Back	

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。
Interface Admin State	現在の管理者状態を表示します。
IPv6 Network Address	IPv6 アドレス/サブネットマスクの形式で入力します。
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ーションの再送タイマーです。デフォルトは 0 です。
Automatic Link Local Address	有効と無効を切り替えます。有効にすると、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。

[Apply]をクリックして変更を適用します。

IPv6 Interface Settings

<<Back	Total Entries: 2
Address Type	IPv6 Address
Link-Local Address	FE80::240:66FF:FE71:F6B2/128
Global Unicast Address	3710::1/64 (Manual)
	Delete
	Delete

3.2.4.1 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：

Total Entries: 1					
IPv6 Prefix	Protocol	Metric	Next Hop	Interface Name	Status
::/0	Static	2	3710::2	System	Inactive

IPv6 ルートテーブルを設定するには、各項目を入力して、[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を 12 文字以内で入力します。
Nexthop Address	ネクストホップとなる 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。

[Apply]をクリックして変更を適用します。

[Delete All]をクリックすると全てのエントリーを削除します。

[Delete]をクリックすると該当するエントリーのみ削除します。

3.2.5 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	Add
Neighbor IPv6 Address		
Link Layer MAC Address		
Interface Name	System	
State	All	Find Clear

Total Entries: 1

Neighbor	Link Layer Address	Interface Name	State	Port	VID
3FFE::1	00-11-22-33-44-55	System	T	NA	1

1/1 1 Go

State: (I) means Incomplete state. (R) means Reachable state. (S) means Stale state.
(D) means Delay state. (P) means Probe state. (T) means Static 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ーを検索するには、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ーを削除するには、[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 インターフェー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。

3.2.6 IPv4 Static/Default Route Settings

スイッチは、IPv4 スタティックルーティングをサポートし、16 個の IPv4 ルートエントリーを作成することができます。IPv4 スタティックルートがセットされると、スイッチは、ネクストホップルーターに ARP リクエストパケットを送信します。スイッチが、ネクストホップからの ARP 応答を取得するとルートが有効となります。しかし、ARP エントリーが既に有効の場合は ARP 応答は送信されません。スイッチはフローティングスタティックルートをサポートします。これは、ユーザが異なるネクストホップのどちらかを選択することができる示します。このセカンダリネクストホップはプライマリのスタティックルートのバックアップとして設定されます。

次のウィンドウを表示するには、Configuration > IPv4 Static/Default Route Settings をクリックします：

IPv4 Static/Default Route Settings

IP Address	<input type="text"/> <input checked="" type="checkbox"/> Default						
Netmask	<input type="text"/> (e.g.: 255.255.255.254 or 0-32)						
Gateway	<input type="text"/> (e.g.: 172.18.211.10)						
Metric (1-65535)	<input type="text"/>						
Backup State	Primary <input type="button" value="▼"/>						
<input type="button" value="Apply"/>							
Total Entries: 0							
<table border="1"><thead><tr><th>IP Address/Netmask</th><th>Gateway</th><th>Cost</th><th>Protocol</th><th>Backup</th><th>Status</th></tr></thead></table>		IP Address/Netmask	Gateway	Cost	Protocol	Backup	Status
IP Address/Netmask	Gateway	Cost	Protocol	Backup	Status		

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	スタティックルートの IPv4 アドレスを入力します。Default チェックボックスをクリックするとデフォルトルートがアサインされます。
Netmask	IP アドレスに対応するサブネットマスクを入力します。
Gateway	IP アドレスに対応するゲードウェイアドレスを入力します。
Metric(1-65535)	メトリックエントリーを 1~65535 の値で入力します。
Backup State	設定したスタティックルートのプライマリ/セカンダリを選択します。

[Apply]をクリックして変更を適用します。

3.2.7 IPv4 Route Table

IP ルートテーブルは全ての外部ルート情報をスイッチによって保存します。このウィンドウではスイッチが保存している外部ルート情報を表示します。

次のウィンドウを表示するには、Configuration > IPv4 Route Table をクリックします：

IPv4 Route Table

<input checked="" type="radio"/> Network Address	<input type="text"/> (e.g.: 172.18.208.11/24)																		
<input type="radio"/> IP Address	<input type="text"/> (e.g.: 172.18.208.11)																		
<input type="button" value="Find"/>																			
Total Entries: 1																			
<table border="1"><thead><tr><th>IP Address</th><th>Netmask</th><th>Gateway</th><th>Interface Name</th><th>Cost</th><th>Protocol</th></tr><tr><th>System</th><th></th><th></th><th></th><th>Local</th><th></th></tr></thead><tbody><tr><td>10.0.0.0</td><td>255.0.0.0</td><td>0.0.0.0</td><td></td><td>1</td><td></td></tr></tbody></table>		IP Address	Netmask	Gateway	Interface Name	Cost	Protocol	System				Local		10.0.0.0	255.0.0.0	0.0.0.0		1	
IP Address	Netmask	Gateway	Interface Name	Cost	Protocol														
System				Local															
10.0.0.0	255.0.0.0	0.0.0.0		1															
1 / 1 <input type="button" value="Go"/>																			

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
Network Address	ルート情報を表示させる宛先ネットワークのアドレスを入力します。
IP Address	ルート情報を表示させる IP アドレスを入力します。

[Find]をクリックして指定したエントリーを表示させます。

[Go]をクリックして表示ページを切り替えます。

3.2.8 Port Configuration

3.2.8.1 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 Settings

From Port	To Port	State	Speed/Duplex	Flow Control	Address Learning	MDIX	Medium Type		
01	01	Enabled	Auto	Disabled	Enabled	Auto	Copper	Apply	Refresh
02									
03									
04									
05									
06									
07									
08									
09									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									
27									
28									
29									
30									
31									
32									
33									
..

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下さい。
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または無効にします。
Speed/Duplex	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、Auto、10M half、10M full、100M half、100M full、1000M full master、1000M full slave および 1000M full があります。 ポート設定を自動調整するには Auto を使用します。 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。 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ドバタ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。
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。
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。
Medium Type	設定するポートのメディアタイプを指定します。 APLGM152GT は、ポート 1 ~ 48(copper)、ポート 49 ~ 52(fiber)を指定します。

[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。

3.2.8.2 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：

Port Description Settings

From Port	To Port	Medium Type	Description	Apply
01	01	Copper		
02				
03				
04				
05				
06				
07				
08				
09				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
..				

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て、ポートのメディアタイプを指定します。 各ポートに記載したコメントが表示されます。

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
From Port/To Port	ポート範囲を選択します。
Medium Type	設定するポートのメディアタイプを指定します。 APLGM152GT は、ポート 1 ~ 48(copper)、ポート 49 ~ 52(fiber)を指定します。
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。

3.2.8.3 Port Error Disabled

次のウィンドウには、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 Error Disabled			
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)。

3.2.8.4 Port Media Type

各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 Media Type	
Port	Type
01	1000BASE-T
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

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。

3.2.8.5 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：

Port Green Mode Settings			
From Port	To Port	State	
01	01	Enabled	<input type="button" value="Apply"/>
			<input type="button" value="Refresh"/>
Port		State	Operation State
01		Disable	Normal
02		Disable	Normal
03		Disable	Normal
04		Disable	Normal
05		Disable	Normal
06		Disable	Normal
07		Disable	Normal
08		Disable	Normal
09		Disable	Normal
10		Disable	Normal
11		Disable	Normal
12		Disable	Normal
13		Disable	Normal
14		Disable	Normal
15		Disable	Normal
16		Disable	Normal
17		Disable	Normal
18		Disable	Normal
19		Disable	Normal
20		Disable	Normal
21		Disable	Normal
22		Disable	Normal
23		Disable	Normal
24		Disable	Normal
25		Disable	Normal
26		Disable	Normal
27		Disable	Normal
28		Disable	Normal
29		Disable	Normal
30		Disable	Normal
31		Disable	Normal
32		Disable	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
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。 デフォルト設定は無効です。

[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。

3.2.8.6 EEE Settings

EEE(Energy Efficient Ethernet)は、IEEE802.3azで標準化された省電力イーサネットの規格です。ポートに設定することでトラフィックの状態に応じて消費電力を低減する効果が得られます。

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

EEE Settings

From Port	To Port	State
01	01	Disabled
1		Disabled
2		Disabled
3		Disabled
4		Disabled
5		Disabled
6		Disabled
7		Disabled
8		Disabled
9		Disabled
10		Disabled
11		Disabled
12		Disabled
13		Disabled
14		Disabled
15		Disabled
16		Disabled
17		Disabled
18		Disabled
19		Disabled
20		Disabled
21		Disabled
22		Disabled
23		Disabled
24		Disabled
25		Disabled
26		Disabled
27		Disabled
28		Disabled
29		Disabled
30		Disabled
31		Disabled
32		Disabled
33		Disabled

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
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。 デフォルト設定は無効です。

[Apply]をクリックして変更を適用します。

注意事項



コマンド入力時、EEEを設定する対象ポートでリンクアップしているポートは一度リンクダウンが発生します。



EEE機能は、ポートのAutoNegotiation設定が「Enable」(有効)の場合に使用することができます。なお、10BASE-Tには対応しておりません。



接続する機器同士がEEE機能に対応している必要があります。

3.2.9 Static ARP Settings

ARP は、IP アドレスを物理アドレスに変換する TCP/IP 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。

Static ARP Settings

Global Settings

ARP Aging Time (0-65535) min

Add Static ARP Entry

IP Address MAC Address

Total Entries: 3

Interface Name	IP Address	MAC Address	Type	Edit	Delete
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
System	10.90.90.90	00-40-66-71-F6-B2	Local	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast	<input type="button" value="Edit"/>	<input type="button" value="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)	ARP エントリーをテーブルから削除する前に、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タリーを適用します。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[Apply]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。

3.2.10 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：

The screenshot shows the 'User Accounts' configuration window. At the top, there's a form for 'Add User Accounts' with fields for 'User Name' (a text input), 'Access Right' (a dropdown menu set to 'Admin'), 'Password' (a text input), and 'Confirm Password' (a text input). Below this is a note: 'Note: Password/User Name should be less than 15 characters.' A table below shows one entry: 'adpro' with 'Admin' access right, and all password fields are masked with asterisks. There are 'Edit' and 'Delete' buttons at the bottom of the table row.

Total Entries: 1				
User Name	Access Right	Old Password	New Password	Confirm Password
adpro	Admin	*****	*****	*****

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。
Password	新しいユーザーのパスワードを入力します。
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	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

3.2.11 System Log Configuration

3.2.11.1 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または無効にします。
Save Mode	ブ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)	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。

3.2.11.2 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	プ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。																																																				
Server IP Address	システムログサーバーの IP アドレスです。																																																				
Facility	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、ファシリティー値が割り当てられていることがあります。ファシリティー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” ファシリティーのいずれか、または、”ユーザーレベル” ファシリティーを使用します。割り当てられたファシリティー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ー値は、16~23 です。																																																				
	<table> <thead> <tr> <th>数値</th> <th>ファシリティーコード</th> <th>数値</th> <th>ファシリティーコード</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>カーネルメッセージ</td> <td>12</td> <td>NTP サブシステム</td> </tr> <tr> <td>1</td> <td>ユーザーレベルメッセージ</td> <td>13</td> <td>ログ監査</td> </tr> <tr> <td>2</td> <td>メールシステム</td> <td>14</td> <td>ログアラート</td> </tr> <tr> <td>3</td> <td>システムデーモン</td> <td>15</td> <td>クロックデーモン</td> </tr> <tr> <td>4</td> <td>セキュリティー/認証メッセージ</td> <td>16</td> <td>ローカル使用 0 (local0)</td> </tr> <tr> <td>5</td> <td>システムログラインプリンタサブシステム によって生成されたメッセージ</td> <td>17</td> <td>ローカル使用 1 (local1)</td> </tr> <tr> <td>7</td> <td>ネットワークニュースサブシステム</td> <td>18</td> <td>ローカル使用 2 (local2)</td> </tr> <tr> <td>8</td> <td>UUCP サブシステム</td> <td>19</td> <td>ローカル使用 3 (local3)</td> </tr> <tr> <td>9</td> <td>クロックデーモン</td> <td>20</td> <td>ローカル使用 4 (local4)</td> </tr> <tr> <td>10</td> <td>セキュリティー/認証メッセージ</td> <td>21</td> <td>ローカル使用 5 (local5)</td> </tr> <tr> <td>11</td> <td>FTP デーモン</td> <td>22</td> <td>ローカル使用 6 (local6)</td> </tr> <tr> <td></td> <td></td> <td>23</td> <td>ローカル使用 7 (local7)</td> </tr> </tbody> </table>	数値	ファシリティーコード	数値	ファシリティーコード	0	カーネルメッセージ	12	NTP サブシステム	1	ユーザーレベルメッセージ	13	ログ監査	2	メールシステム	14	ログアラート	3	システムデーモン	15	クロックデーモン	4	セキュリティー/認証メッセージ	16	ローカル使用 0 (local0)	5	システムログラインプリンタサブシステム によって生成されたメッセージ	17	ローカル使用 1 (local1)	7	ネットワークニュースサブシステム	18	ローカル使用 2 (local2)	8	UUCP サブシステム	19	ローカル使用 3 (local3)	9	クロックデーモン	20	ローカル使用 4 (local4)	10	セキュリティー/認証メッセージ	21	ローカル使用 5 (local5)	11	FTP デーモン	22	ローカル使用 6 (local6)			23	ローカル使用 7 (local7)
数値	ファシリティーコード	数値	ファシリティーコード																																																		
0	カーネルメッセージ	12	NTP サブシステム																																																		
1	ユーザーレベルメッセージ	13	ログ監査																																																		
2	メールシステム	14	ログアラート																																																		
3	システムデーモン	15	クロックデーモン																																																		
4	セキュリティー/認証メッセージ	16	ローカル使用 0 (local0)																																																		
5	システムログラインプリンタサブシステム によって生成されたメッセージ	17	ローカル使用 1 (local1)																																																		
7	ネットワークニュースサブシステム	18	ローカル使用 2 (local2)																																																		
8	UUCP サブシステム	19	ローカル使用 3 (local3)																																																		
9	クロックデーモン	20	ローカル使用 4 (local4)																																																		
10	セキュリティー/認証メッセージ	21	ローカル使用 5 (local5)																																																		
11	FTP デーモン	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または無効にします。																																																				

[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。

3.2.12 MAC Address Aging Time

このテーブルで、学習した MAC アドレスをフォ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：

MAC Address Aging Time		
MAC Address Aging Time (10-1000000)	300	sec
<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
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、 $<\text{入力値}> \div 2 \sim <\text{入力値}> - 1$ 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：

Web Settings		
Web State	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Port (1-65535)	80	
<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
WEB State	Web ベース GUI の有効/無効を設定します。
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：

Telnet State	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Port (1-65535)	23
<input type="button" value="Save"/>	

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/無効を設定します。
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：

CLI Paging State	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
<input type="button" value="Save"/>	

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/無効を設定します。

[Apply]をクリックして変更を適用します。

3.2.16 Configuration File Information

スイッチに保存されたコンフィグレーションファイル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 > Configuration File Information をクリックします：

Configuration File Information							
ID	Version	Size (Bytes)	Update Time	User	Set Boot	Active	Delete
*1	1.02.00	32597	2018/04/19 13:04:44	adpro(CONS...)	Set Boot	Active	Delete
2	(Empty)				Set Boot	Active	Delete
<p>** : Boot up configuration (SSH) : Configuration update through SSH (WEB) : Configuration update through WEB (TELNET) : Configuration update through TELNET (CONSOLE) : Configuration update through CONSOLE</p>							

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コンフィグレーション ID 番号を表示します。スイッチには 2 つのコンフィグレーションファイルを保存できます。ID 番号に*印あるコンフィグレーションファイルが起動時に使用されます。
Version	コンフィグレーションのファイル保存時のファームバージョンを表示します。
Size (Bytes)	コンフィグレーションのファイルサイズを表示します。
Update Time	コンフィグレーションのファイル保存時のスイッチ時間を表示します。
User	コンフィグレーションのファイル保存時のユーザーを表示します。

[Set Boot]をクリックして起動時のコンフィグレーションファイルを選択します。

[Active]をクリックして現在のコンフィグレーションファイルに反映します。

[Delete]をクリックして選択したコンフィグレーションファイルを削除します。

注意事項



Active を選択した場合、選択したコンフィグレーションファイルを現在の設定に置き換えるため、リンクアップしているポートは一度リンクダウンが発生します。

3.2.17 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 (Bytes)	Update Time	User	
*1	1.02.00	4689172	2018/04/11 10:46:03	adpro(CONS...)	<button>Boot UP</button> <button>Delete</button>
2	1.01.00	4683304	2018/04/06 16:25:57	adpro(CONS...)	<button>Boot UP</button> <button>Delete</button>
<p>** : 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</p>					

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	ファームウェアバージョンを表示します。
Size (Bytes)	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。

3.2.18 SNTP Settings

3.2.18.1 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：

The screenshot shows the 'Time Settings' configuration window. It has three main sections:

- Status:** SNTP State (radio buttons for Disabled and Enabled, currently Disabled), Current Time (15/01/2014 11:29:38), Time Source (System Clock), and an 'Apply' button.
- SNTP Settings:** SNTP First Server (0.0.0.0), SNTP Second Server (0.0.0.0), SNTP Poll Interval In Seconds (30-99999) (720), and an 'Apply' button.
- Set Current Time:** Date (DD/MM/YYYY) (00/00/0000) and Time (HH:MM:SS) (00:00:00), and an 'Apply' 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
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/無効にします。
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)
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。

3.2.18.2 TimeZone Settings

このウィンドウで SNTP のタイムゾーンと夏時間設定します。

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：

The screenshot shows the 'Time Zone Settings' configuration window. It includes three main sections: 'Daylight Saving Time State' (set to 'Disabled'), 'DST Repeating Settings' (with fields for 'From' and 'To' times and days), and 'DST Annual Settings' (with fields for 'From' and 'To' times and days). At the bottom right is an 'Apply' 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
Daylight Saving Time State	夏時間設定を有効または無効にします。
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週の土曜日に開始し、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。

3.2.19 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。

3.2.19.1 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 Settings' configuration window. It includes the following sections:

- SMTP Global Settings:** Includes fields for 'SMTP State' (radio buttons for Enabled and Disabled), 'SMTP Server Address' (text input: 0.0.0.0), 'SMTP Server Port (1-65535)' (text input: 0), and 'Self Mail Address' (text input).
- SMTP Mail Receiver Address:** Includes a 'Add A Mail Receiver' button and a list of entries.
- Send a Test Mail to All:** Includes 'Subject' and 'Content' fields, each with a text input area and an 'Apply' button.
- Mail Receiver Address Table:** A table showing a list of mail receiver addresses with an index column and a 'Delete' button for each entry.

Index	Mail Receiver Address	Delete
1		Delete
2		Delete
3		Delete
4		Delete
5		Delete
6		Delete
7		Delete
8		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
SMTP State	ラジオボタンで、このデバイス上の SMTP サービスを有効または無効にします。
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だけです。この文字列は 64 文字内の英数字になります。
Add A Mail Receiver	電子メールアドレスの送信先を指定します。 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。
Subject	テスト e-mail の題名を入力します。
Content	テスト e-mail の内容を入力します。

[Apply]をクリックして変更を適用します。

[Add]をクリックしてエントリーしたメール受信アドレスを追加します。

[Delete]をクリックしてエントリーしたメール受信アドレスを削除します。

3.2.20 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)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、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 2c 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ー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。

3.2.20.1 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：

SNMP View Table

View Name	Subtree	View Type	
		Included	Apply
Total Entries: 8			
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	<code>Included</code> 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。 <code>Excluded</code> 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、相応する[Delete]をクリックします。

3.2.20.2 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、コミュニティー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:

SNMP Group Table																																									
Add Group Group Name <input type="text"/> Read View Name <input type="text"/> Write View Name <input type="text"/> Notify View Name <input type="text"/> User-based Security Model <input type="button" value="SNMPv1"/> <input type="button" value="SNMPv2"/> <input type="button" value="SNMPv3"/> Security Level <input type="button" value="NoAuthNoPriv"/> <input type="button" value="AuthNoPriv"/> <input type="button" value="AuthPriv"/>																																									
<input type="button" value="Apply"/>																																									
Total Entries: 5 <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Group Name</th> <th>Read View Name</th> <th>Write View Name</th> <th>Notify View Name</th> <th>User-based Security Model</th> <th>Security Level</th> </tr> </thead> <tbody> <tr> <td>public</td> <td>CommunityV...</td> <td></td> <td>CommunityV...</td> <td>SNMPv1</td> <td>NoAuthNoPriv</td> </tr> <tr> <td>public</td> <td>CommunityV...</td> <td></td> <td>CommunityV...</td> <td>SNMPv2</td> <td>NoAuthNoPriv</td> </tr> <tr> <td>initial</td> <td>restricted</td> <td></td> <td>restricted</td> <td>SNMPv3</td> <td>NoAuthNoPriv</td> </tr> <tr> <td>private</td> <td>CommunityV...</td> <td>CommunityV...</td> <td>CommunityV...</td> <td>SNMPv1</td> <td>NoAuthNoPriv</td> </tr> <tr> <td>private</td> <td>CommunityV...</td> <td>CommunityV...</td> <td>CommunityV...</td> <td>SNMPv2</td> <td>NoAuthNoPriv</td> </tr> </tbody> </table>						Group Name	Read View Name	Write View Name	Notify View Name	User-based Security Model	Security Level	public	CommunityV...		CommunityV...	SNMPv1	NoAuthNoPriv	public	CommunityV...		CommunityV...	SNMPv2	NoAuthNoPriv	initial	restricted		restricted	SNMPv3	NoAuthNoPriv	private	CommunityV...	CommunityV...	CommunityV...	SNMPv1	NoAuthNoPriv	private	CommunityV...	CommunityV...	CommunityV...	SNMPv2	NoAuthNoPriv
Group Name	Read View Name	Write View Name	Notify View Name	User-based Security Model	Security Level																																				
public	CommunityV...		CommunityV...	SNMPv1	NoAuthNoPriv																																				
public	CommunityV...		CommunityV...	SNMPv2	NoAuthNoPriv																																				
initial	restricted		restricted	SNMPv3	NoAuthNoPriv																																				
private	CommunityV...	CommunityV...	CommunityV...	SNMPv1	NoAuthNoPriv																																				
private	CommunityV...	CommunityV...	CommunityV...	SNMPv2	NoAuthNoPriv																																				

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	セキュリティー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triesを削除するには [Delete]をクリックします。

3.2.20.3 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：

SNMP User Table						
Add User						
User Name	<input type="text"/>					
Group Name	<input type="text"/>					
SNMP Version	<input type="button" value="V3"/>					
SNMP V3 Encryption	<input type="button" value="None"/>					
Auth-Protocol by Password	<input type="button" value="MD5"/>					
Priv-Protocol by Password	<input type="button" value="None"/>					
Auth-Protocol by Key	<input type="button" value="MD5"/>					
Priv-Protocol by Key	<input type="button" value="None"/>					
<input type="button" value="Apply"/>						
Total Entries: 1						
User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol		
initial	initial	V3	None	None	<input type="button" value="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
User Name	32 文字までの英数字文字列を入力します。User Name を使用して SNMP ユーザーを識別します。
Group Name	Group Name を使用して、作成した SNMP グループが SNMP メッセージを要求できるように指定します。
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 2c 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	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	None - 認証プロトコルを使用していないことを示します。 DES - CBC-DES(DES-56) 規格に基づいて DES 56-bit 暗号化を使用していることを示します。
Auth-Protocol by Key	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	None - 認証プロトコルを使用していないことを示します。 DES - CBC-DES(DES-56) 規格に基づいて DES 56-bit 暗号化を使用していることを示します。
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。

3.2.20.4 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。コミュニティー名は、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。コミュニティー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：

SNMP Community Table

Add Community			
Community Name	View Name	Access Right	Apply
<input type="text"/>	<input type="text"/>	Read Only	<input type="button" value="Apply"/>

Total Entries: 2

Community Name	View Name	Access Right	
private	CommunityView	read_write	<input type="button" value="Delete"/>
public	CommunityView	read_only	<input type="button" value="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ー名を使用する SNMP コミュニティ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ー名を使用する SNMP コミュニティ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。

3.2.20.5 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。

The screenshot shows the 'SNMP Host Table' configuration window. It includes fields for 'Host IP Address', 'User-based Security Model' (set to 'SNMPv1'), 'Security Level' (set to 'NoAuthNoPriv'), and 'Community String / SNMPv3 User Name'. A summary bar at the bottom displays 'Total Entries: 0' and lists the columns: Host IP Address, User-based Security Model, Security Level, and Community Name/SNMPv3 User Name. An 'Apply' button is located on the right side of the window.

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 を指定します。 SNMPv2 - SNMP バージョン 2 を指定します。 SNMPv3 - SNMP バージョン 3 を指定します。
Security Level	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。

3.2.20.6 SNMP Engine ID

エンジン ID は SNMPv3 適用の際に使用する固有の識別子です。この英数字文字列を使用して、スイッチ上の SNMP エンジンを識別します。

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:

The screenshot shows the 'SNMP Engine ID' configuration window. It features a single input field for 'Engine ID' containing the value '800001160300406671f6b2'. Below the input field is a note: 'Note: Engine ID length is 10-64. The accepted characters are from 0 to F.' An 'Apply' button is located on the right side of the window.

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。

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。

3.2.20.7 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：

SNMP Trap Configuration	
SNMP Trap	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SNMP Authentication Traps	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SNMP Linkchange Traps	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SNMP Login Trap	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SNMP Logout Trap	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SNMP Login Fail Trap	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Apply

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/無効を設定します。
SNMP Authentication Traps	SNMP 認証 トラップの有効/無効を設定します。
SNMP Link Change Traps	SNMP リンク変更 トラップの有効/無効を設定します。
SNMP Login Trap	SNMP ログイントラップの有効/無効を設定します。
SNMP Logout Trap	SNMP ログアウトトラップの有効/無効を設定します。
SNMP Login Fail Trap	SNMP ログインフェイルトラップの有効/無効を設定します。

[Apply]をクリックして変更を適用します。

3.2.20.8 SNMP Linkchange Traps Settings

次のウィンドウを使用して、各ポートの SNMP リンク変更トラップを有効/無効に設定します。

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

SNMP Linkchange Traps Settings

From Port	To Port	State
01	01	Enabled

Linkchange Traps: Enabled

Port	State
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Enabled
7	Enabled
8	Enabled
9	Enabled
10	Enabled
11	Enabled
12	Enabled
13	Enabled
14	Enabled
15	Enabled
16	Enabled
17	Enabled
18	Enabled
19	Enabled
20	Enabled
21	Enabled
22	Enabled
23	Enabled
24	Enabled
25	Enabled
26	Enabled
27	Enabled
28	Enabled
29	Enabled
30	Enabled
31	Enabled
32	Enabled
--	- - -

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	SNMP リンク変更トラップのポート範囲を設定します。
State	SNMP リンク変更トラップの有効/無効を設定します。

[Apply]をクリックして変更を適用します。

3.2.20.9 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：

RMON	
RMON	<input type="radio"/> Enabled <input checked="" type="radio"/> 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
RMON Status	RMON の有効/無効を設定します。

[Apply]をクリックして変更を適用します。

3.2.20.10 SNMP v6Host Table Setting

SNMP トラップの IPv6 ホストを設定します。

次のウィンドウを表示するには、Configuration > SNMP Settings > SNMPv6Host Table Settings をクリックします：

SNMP v6Host Table Settings				
Add Host Table				
Host IPv6 Address	<input type="text"/>			
User-based Security Model	SNMPv1			
Security Level	NoAuthNoPriv			
Community String / SNMPv3 User Name	<input type="text"/>			
<input type="button" value="Apply"/>				
Total Entries: 1				
Host IPv6 Address	User-based Security Model	Security Level	Community Name/SNMPv3 User Name	<input type="button" value="Delete"/>
3::F1	SNMPv1	private		

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 IPv6 Address	SNMP トラップを受信するホストの IPv6 アドレスを入力します。
User-based Security Model	SNMPv1 - SNMP バージョン 1 を指定します。 SNMPv2 - SNMP バージョン 2 を指定します。 SNMPv3 - SNMP バージョン 3 を指定します。
Security Level	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 / SNMP v3 User Name	コミュニティー名または 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。

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。

3.3 Command Logging

3.3.1 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：

The screenshot shows a software interface for 'Command Logging Settings'. At the top, it says 'Command Logging Settings'. Below that, there's a section for 'Command Logging State' with two radio buttons: one labeled 'Enabled' (which is selected) and another labeled 'Disabled'. At the bottom right of the window is a button labeled '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
Command Logging State	コマンドログ機能の有効または無効を設定します。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



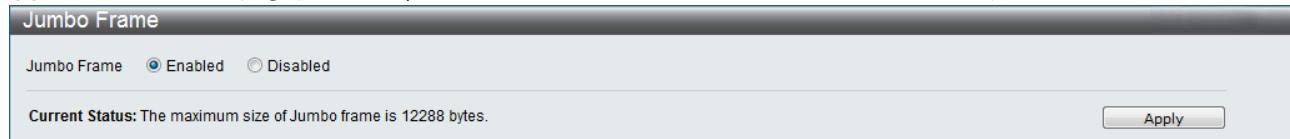
コマンドログ機能はコマンドラインインターフェース上でのコマンド実行結果をシステムログに出力する機能です。Web ユーザーインターフェース上でのコマンド実行結果については、システムログに出力されません。

3.4 L2 Features

3.4.1 Jumbo Frame

このウィンドウで、スイッチ上のジャンボフレーム機能を有効または無効にします。デフォルトは有効です。有効にすると、最大サイズ 12288 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。

3.4.2 VLANs

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、時間に纖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、時間に纖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みの場合です。

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 のデータパケット専用にします。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、セキュリティー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込み、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。

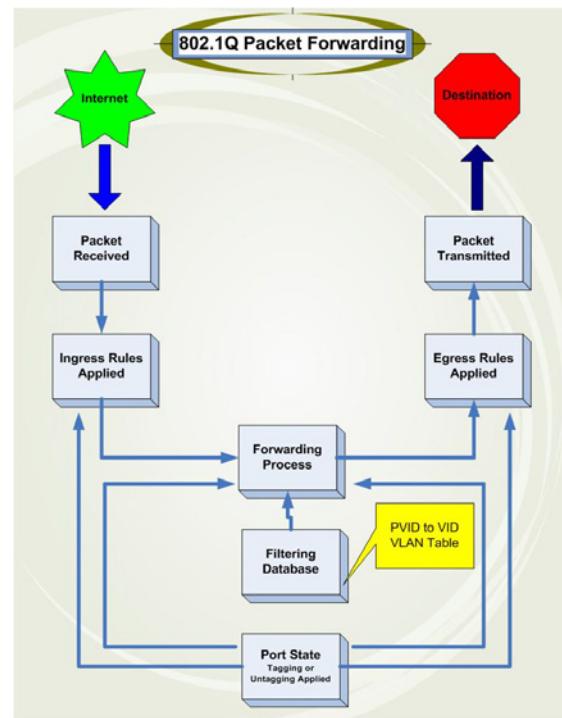
VLAN はネットワークのセキュリティーレベルも提供できます。IEEE 802.1Q VLAN は、VLAN のメンバーであるステーション間だけでパケットを配信します。

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あります。

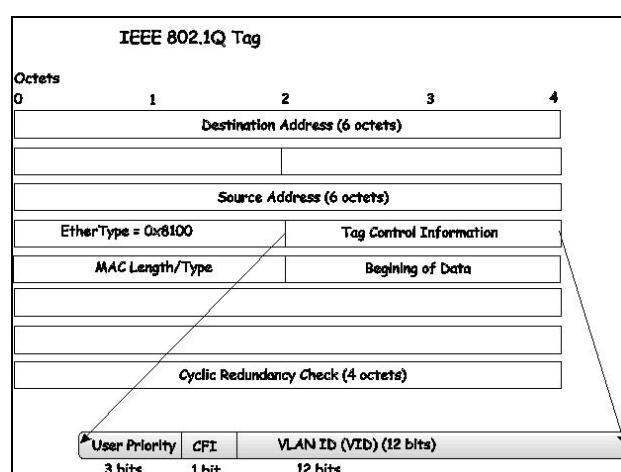
- (1) フィルタリングによってパケットを VLAN に割り当てます。
- (2) 単一のグローバルスパンニングツリーがあることを仮定します。
- (3) 1 レベルタギングの明示的タギングスキームを使用します。
- (4) 802.1Q VLAN パケットフォワーディング
- (5) パケットフォワーディングは、次の 3 種類の規則に基づいて決定します：
 - (a) イングレス規則 - 1 つの VLAN に属する受信フレームの分類に関する規則です。
 - (b) ポート間のフォワーディング規則 - パケットをフィルタするか、転送するかを決定します。
 - (a) イーグレス規則 - パ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



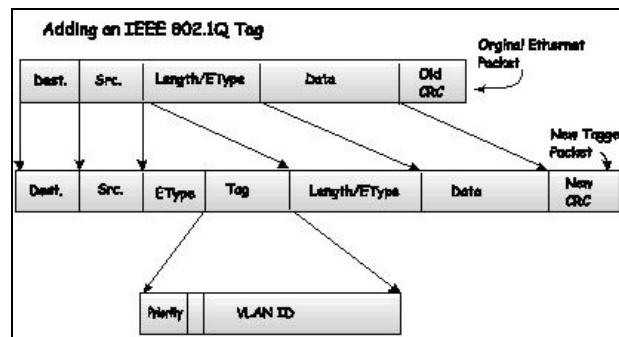
802.1Q VLAN タグ

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 - トーカ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す。

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、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(ポートがタギングポートの場合)。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れ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ラン 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 VLAN タグ)	802.1Q CEVLAN タグ (TPID + カスタマ VLAN タグ)	イーサタイプ	ペイロード

Q-in-Q VLAN の規則

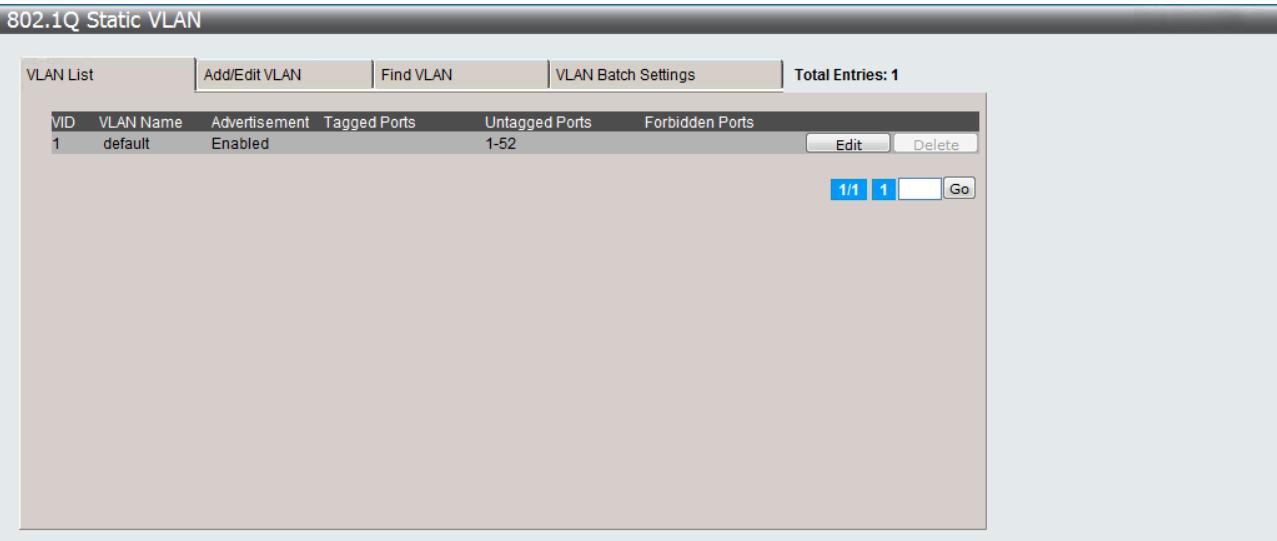
Q-in-Q VLAN をご使用になる際には、以下の規則や規制がございます。

- (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、ジャンボ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。

3.4.3 802.1Q 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：



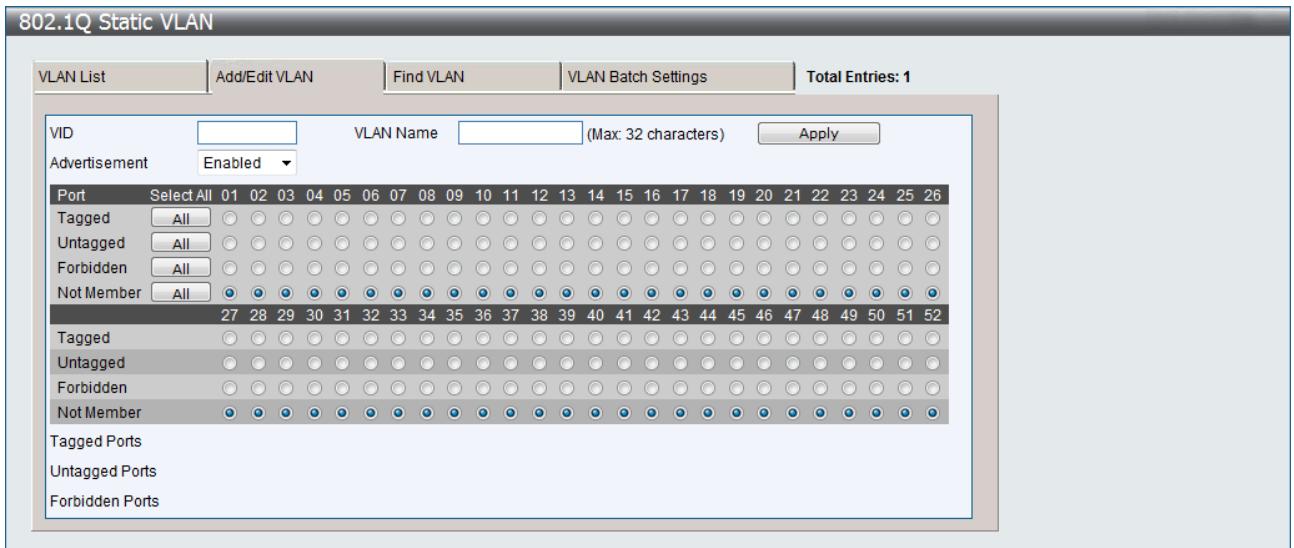
The screenshot shows a software interface titled "802.1Q Static VLAN". At the top, there are four tabs: "VLAN List" (selected), "Add/Edit VLAN", "Find VLAN", and "VLAN Batch Settings". To the right of these tabs, it says "Total Entries: 1". Below the tabs is a table with the following data:

VID	VLAN Name	Advertisement	Tagged Ports	Untagged Ports	Forbidden Ports	Actions
1	default	Enabled		1-52		Edit Delete

At the bottom of the window, there are navigation buttons: "1/1" (highlighted in blue), "1", and "Go".

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、上の相応する 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 を表示できます。VLAN は VLAN ID 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。

The screenshot shows the '802.1Q Static VLAN' configuration window. At the top, there are four tabs: 'VLAN List', 'Add/Edit VLAN', 'Find VLAN' (which is currently selected), and 'VLAN Batch Settings'. Below the tabs, there is a search bar with 'VID' and a text input field containing '1', followed by a 'Find' button. A message 'Total Entries: 1' is displayed above the main content area.

VLAN バッチエントリーを作成するには、ウィンドウの一番上にある [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：

The screenshot shows the '802.1Q Static VLAN' configuration window with the 'VLAN Batch Settings' tab selected. The interface includes fields for 'VID List (e.g.:2-5)', 'Advertisement' (set to 'Disabled'), 'Port List (e.g.:1-5)', and options for 'Add', 'Delete', and 'Config'. There are also dropdown menus for 'Add' and 'Tagged'. An 'Apply' button is located at the bottom right of the form.

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。

3.4.4 QinQ

3.4.4.1 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：

The screenshot shows the 'QinQ Settings' configuration interface. At the top, there's a 'QinQ Global Settings' section with two radio buttons: 'Enabled' (unchecked) and 'Disabled' (checked). Below this are dropdown menus for 'From Port' (01), 'To Port' (01), 'Role' (NNI), and 'Outer TPID (hex: 0x1-0xffff)' (set to 0x88A8). To the right of these is a 'VLAN Translation' dropdown set to 'Disabled'. There are two 'Apply' buttons: one for the global settings and one for the port-specific table below.

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
25	NNI	0x88A8	Disabled
26	NNI	0x88A8	Disabled
27	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	ラジオボタンをクリックして、QinQ グローバル設定を有効または無効にします。
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 変換を有効または無効にします。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。デフォルトは無効です。

[Apply]をクリックして変更を適用します。

3.4.4.2 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

From Port 01	To Port 01	CVID List (1, 5-7)	Action Add	SVID (1-4094)	Priority None	Apply
						Delete All
Total Entries: 1						
Port	CVID	SVID	Action	Priority		
2	1	2	Add	-	Edit	Delete
1/1		1		Go		

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。
CVID List(1-4094)	タグ付きパケットが追加されるカスタマービルトイン VLAN ID 一覧です。
Action	サービスプロバイダーVLAN ID(SVID)の追加または置換を指定します。
SVID (1-4094)	サービスプロバイダの 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。
Priority	サービスタグ(s-tag)の優先度を設定します。

[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。

[Edit]をクリックして対象のポートを再設定します。

[Delete]をクリックして対象のポートの設定を削除します。

3.4.5 802.1v 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。

3.4.5.1 802.1v 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：

Total Entries: 1			
Group ID	Group Name	Frame Type	Protocol Value
1	group	-	0xFFFF

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 LLC には対応しておりません)
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作成します。

[Delete All]をクリックして全てのエントリーを削除します。

[Edit]をクリックして対象のグループを再設定します。

[Delete Setting]をクリックして指定したエントリーのプロトコル VLAN グループ情報を削除します。

[Delete Group]をクリックして指定したエントリーのプロトコル VLAN グループを削除します。

3.4.5.2 802.1v 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：

802.1v Protocol VLAN Settings

Add New Protocol VLAN

Group ID VID (1-4094) 802.1p Priority

Group Name VLAN Name

Port List (e.g.: 1-6)

Protocol VLAN Table

Search Port List

Total Entries: 52

Port	VID	VLAN Name	Group ID	802.1p Priority	Edit	Delete
1	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
2	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
3	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
4	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
5	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
6	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
7	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
8	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
9	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
10	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
11	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
12	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
13	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
14	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
15	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
16	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
17	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
18	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
19	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
20	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
21	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
22	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
...	1	default	1	0	<input type="button" value="Edit"/>	<input type="button" value="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 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。

[Edit]をクリックして対象のポートを再設定します。

[Delete]をクリックして対象のポートの設定を削除します。

3.4.6 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
25	1	-	Disabled	Enabled	All
26	1	-	Disabled	Enabled	All
27	1	-	Disabled	Enabled	All
28	1	-	Disabled	Enabled	All
29	1	-	Disabled	Enabled	All
30	1	-	Disabled	Enabled	All
31	1	-	Disabled	Enabled	All
32	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	ラジオボタンをクリックし、GVRP グローバル設定を有効または無効にします。
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 チェックを有効に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「enable」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。

3.4.7 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:

The screenshot shows a configuration window titled "Asymmetric VLAN Settings". It contains a single row with two columns: "Asymmetric VLAN State" and "Enabled". There is also an "Apply" button at the bottom right.

Asymmetric VLAN State	Enabled
-----------------------	---------

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
Asymmetric VLAN State	asymmetric VLAN の設定の有効/無効を設定します。

[Apply]をクリックして変更を適用します。

3.4.8 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:

The screenshot shows a configuration window titled "MAC-based VLAN Settings". It has a search bar at the top with fields for "MAC Address", "VID (1-4094)", and "VLAN Name", along with "Find" and "Add" buttons. Below is a table with one entry:

Total Entries: 1
MAC Address: 00-11-22-33-44-55, VID: 1, Status: Active, Type: Static

At the bottom are buttons for "View All", "Delete All", "Delete", and page navigation "1/1" and "Go".

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。
VID(1-4094)	VLAN ID を入力します。
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。

[View All]をクリックして現在のエントリーを全て表示します。

[Delete All]をクリックして全てのエントリーを削除します。

[Delete]をクリックして対象のエントリーを削除します。

3.4.9 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:

The screenshot shows a software interface for configuring PVID auto assignment. At the top, a title bar reads "PVID Auto Assign Settings". Below it, there is a section labeled "PVID Auto Assign State" with two radio buttons: one selected (blue outline) labeled "Enabled" and another unselected (grey outline) labeled "Disabled". At the bottom right of the window is a grey rectangular button labeled "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
PVID Auto Assign State	PVID auto assign の有効/無効を設定します。

[Apply]をクリックして変更を適用します。

3.4.10 Link Aggregation(Port Trunking)

リンクアグリゲーション(ポートトランкиング)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 26 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

- !** APLGM152GT のリンクアグリゲーショングループ数の最大は、製品搭載ポート数 ÷ 2 となります。
- !** メンバーポートは、UTP ポートと Fiber ポートを組み合わせることは出来ません。
- !** 認証機能 (802.1X 認証、MAC 認証、Web 認証) とのポート併用はできません。

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、单一リンクとして動作するようにできます。これによって、单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 26 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ー、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单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。

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：

Link Aggregation Settings

Algorithm	MAC Source	System Priority (1-65535)	32768	Apply				
Total Entries: 0								
Group ID	Type	Master Port	Member Ports	Active Ports	Status	Flooding Port		
Edit Link Aggregation Information								
Group ID (1-26)	Type	Static	Master Port	01	State	Disabled		
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 25 26						Clear All	Add
Ports	27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52							

Note: Maximum 8 ports in a static trunk or LACP group.

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	スイッチがポートトランクグループを構成するポート間で負荷を分散する際に使用するアルゴリズムを定義します。 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	グループの ID 番号を選択します。1 から 26 の範囲で入力します。
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から、トランクグループのマスターポートを選択します。
State	トランクグループを有効または無効に設定します。
Member 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。

[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。

[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。

[Add]をクリックして新しいエントリーを追加します。

3.4.11 LACP Port 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)																																																																													
01	01	Passive	Short		<input type="button" value="Apply"/>																																																																												
<table border="1"> <thead> <tr> <th>Port</th> <th>Activity</th> <th>LACP Timeout</th> <th>Port Priority</th> </tr> </thead> <tbody> <tr><td>1</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>2</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>3</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>4</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>5</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>6</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>7</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>8</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>9</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>10</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>11</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>12</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>13</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>14</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>15</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>16</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>17</td><td>Passive</td><td>Short</td><td>32768</td></tr> <tr><td>18</td><td>Passive</td><td>Short</td><td>32768</td></tr> </tbody> </table>						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
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。

3.4.12 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配向する方法です。このウィンドウで、スイッチ上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。指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:

Port	Forward Port List
1	1-52
2	1-52
3	1-52
4	1-52
5	1-52
6	1-52
7	1-52
8	1-52
9	1-52
10	1-52
11	1-52
12	1-52
13	1-52
14	1-52
15	1-52
16	1-52
17	1-52
18	1-52
19	1-52
20	1-52
21	1-52
22	1-52
23	1-52
24	1-52
25	1-52
26	1-52
27	1-52
28	1-52
29	1-52
30	1-52
...	...

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	トラフィックを制限する対象のポートを入力します。All Ports をチェックするとすべてのポートが設定対象となります。
Forward Port List	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、Port List で指定したポートからパケットを受信します。All Ports をチェックするとすべてのポートからのパケットを受信します。

[Apply]をクリックして変更を適用します。

3.4.13 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：

The screenshot shows the 'BPDU Guard Settings' window. At the top, there's a radio button for 'Enabled' (unchecked) and 'Disabled' (checked). Below it are 'Log Status' (set to 'Both') and 'Recovery Time (60-1000000)' (set to '60 sec'). A large table below lists port configurations:

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
11	Disabled	Shutdown	Normal
12	Disabled	Shutdown	Normal
13	Disabled	Shutdown	Normal
14	Disabled	Shutdown	Normal
15	Disabled	Shutdown	Normal
16	Disabled	Shutdown	Normal
17	Disabled	Shutdown	Normal
18	Disabled	Shutdown	Normal
19	Disabled	Shutdown	Normal
20	Disabled	Shutdown	Normal
21	Disabled	Shutdown	Normal
22	Disabled	Shutdown	Normal
23	Disabled	Shutdown	Normal
24	Disabled	Shutdown	Normal
25	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	BPDU ガード機能のグローバル設定を有効または無効に設定します。
Log Status	BPDU ガードログ出力を設定します。このオプションは None、Attack Detected、Attack Cleared、Both から選択します。Attack Detected 選択時は BPDU フレームを検知の際にログ出力します。Attack Cleared 選択時は BPDU フレームを検知しない際にログ出力します。Both 選択時はその両方でログ出力します。
Recovery Time (60-1000000)	自動復帰に関する BPDU ガードリカバリータイムを指定します。この値は 60 ~ 1,000,000 秒の範囲で指定が必要です。デフォルト値は 60 秒です。Infinite を指定すると自動復帰しなくなります。
From Port/To Port	設定をするポートの範囲指定をします。
State	指定したポートに BPDU ガード機能の状態を有効または無効に設定します。
Mode	このオプションで BPDU ガードの Shutdown mode を設定します。

[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。

3.4.14 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、指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。

3.4.14.1 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：

The screenshot shows the 'IGMP Snooping Settings' window. At the top, it says 'IGMP Snooping Global Settings'. There are two radio buttons: 'Enabled' (selected) and 'Disabled'. Below that is a table with one entry:

Total Entries: 1			
VID	VLAN Name	State	
1	default	Disabled	Modify Router Port Edit

At the bottom right are buttons for '1/1' and 'Go'.

[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：

The screenshot shows the 'IGMP Snooping Parameters Settings' window for VLAN 1. It contains the following parameters:

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

At the bottom are buttons for '<< Back' and '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
VID	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 IP	ネットワークの IGMP クエリーランサムとして動作するデバイスの IP アドレスです。
Querier Expiry Time	クエリー有効時間を表示します。
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。

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。
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。
Last Member 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も含みます。デフォルトは 1 です。
Querier State	有効を選択して、IGMP クエリーパケットの送信を有効にします。または、無効を選択して、IGMP クエリーパケットの送信を無効にします。デフォルトは無効です。
Fast Leave	このパラメーターで、高速脱退機能を有効にします。この機能を有効にして、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します(最終メンバークエリータイマは必要ありません)。デフォルトは無効です。
State	有効を選択して、IGMP スヌーピングを有効にします。デフォルトでは、無効です。
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] ハイパーオンクをクリックします。

IGMP Snooping Router Port Settings

VID: 1 VLAN Name: default

Static Router 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	25	26
<input type="checkbox"/>																									
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
<input type="checkbox"/>																									

Forbidden Router 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	25	26
<input type="checkbox"/>																									
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
<input type="checkbox"/>																									

Dynamic Router 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	25	26
<input type="checkbox"/>																									
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
<input type="checkbox"/>																									

Select All Clear All <<Back Apply

Router IP Table NO. Router IP

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]をクリックして新しいエントリーを追加します。

[<<Back]をクリックして以前のウィンドウに戻ります。

3.4.15 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 上のポートを探査します。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トナークエリー、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、準備が完了した指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ト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トナーレポート、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。ICMP 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ト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、指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、指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トナークエリー、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ト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指定のマルチキャストアドレスのリスト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:

The screenshot shows the 'MLD Snooping Settings' configuration window. It includes a 'MLD Snooping Global Settings' section with a radio button for 'Enabled' (selected) and 'Disabled'. Below this is a table titled 'Total Entries: 1' with one entry for VID 1, VLAN Name 'default', and State 'Disabled'. There are 'Modify Router Port' and 'Edit' buttons, along with navigation buttons '1/1' and 'Go'.

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	MLD Snooping Global Settings でグローバル設定を有効または無効に設定します。

[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。

The screenshot shows the 'MLD Snooping Parameters Settings' configuration window. It contains fields for VID (1), Querier IP (0), Query Interval (1-65535, set to 125 sec), Robustness Value (1-255, set to 2), Querier State (Disabled), State (Disabled), Querier Role (Non-Querier), VLAN Name (default), Querier Expiry Time (0 sec), Max Response Time (1-25, set to 10 sec), Last Listener Query Interval (1-25, set to 1 sec), Fast Done (Disabled), and Version (2). At the bottom are '<< Back' and 'Apply' buttons.

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	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も含みます。デフォルトは 1 です。
Fast Done	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します(最終リスナークエリーゲートは必要ありません)。デフォルトは無効です。
State	MLD スヌーピングを有効または無効にします。デフォルトは無効です。
Version	MLD バージョンが表示されます。
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。

MLD Snooping Router Port Settings

VID: 1		VLAN Name: default																									
Static Router Port:		<input type="checkbox"/> Select All <input type="checkbox"/> Clear All																									
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26		
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Forbidden Router Port:		<input type="checkbox"/> Select All <input type="checkbox"/> Clear All																									
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26		
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Dynamic Router Port:		<input type="checkbox"/> Select All <input type="checkbox"/> Clear All																									
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26		
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
<input type="button" value="<<Back"/> <input type="button" value="Apply"/>																											
Router IP Table <table border="1"> <tr> <td>NO.</td> <td>Router IP</td> </tr> </table>																										NO.	Router IP
NO.	Router IP																										

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。

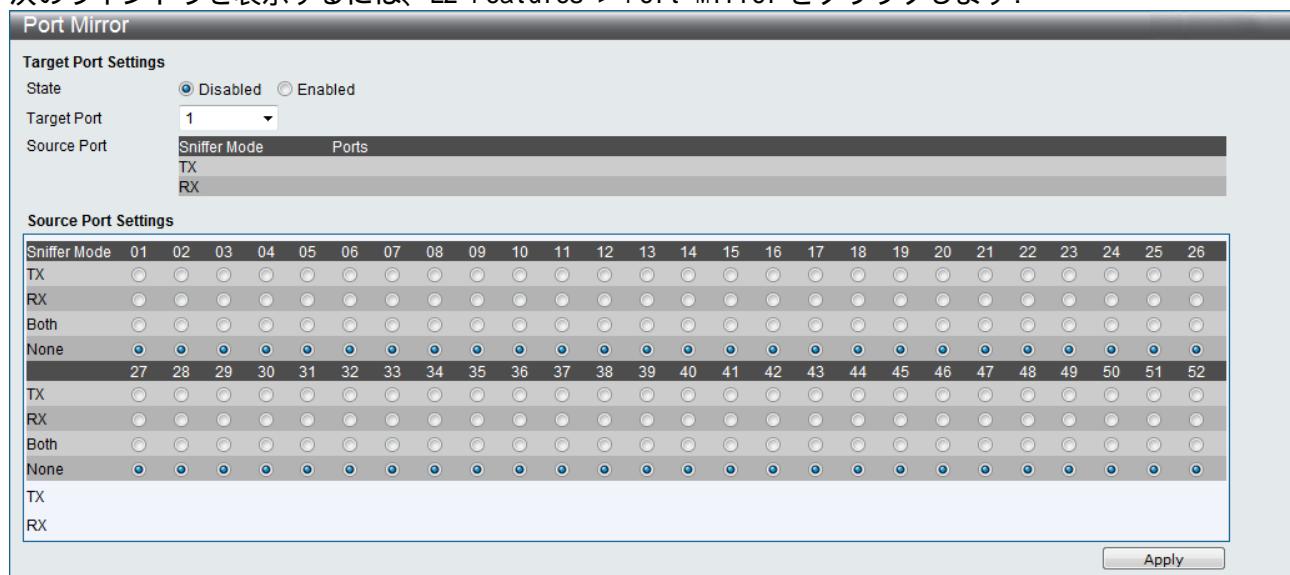
選択したすべてのルーターポートを消去する場合は、相応する[Clear All]をクリックします。

[<<Back]をクリックして、[MLD Snooping Settings]ウィンドウに戻ります。

3.4.16 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できます。スニファーや RMON プローブ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：



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。

3.4.17 Loopback Detection Settings

ループ防止機能設定を設定します。

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：

Port	Loopback Detection State	Method	Loop 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
State(Global)	スイッチのループ防止機能を有効または無効にします。 デフォルト設定は無効です。 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(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)	指定されたポートのループ防止機能を有効または無効に設定します。デフォルト設定は無効です。
Method	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。
- !** 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）
- !** 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)を設定して、手動復旧に設定されることを推奨します。

3.4.18 Spanning Tree

スイッチは、STP、RSTP、MSTP に対応しています。

802.1Q-2005 MSTP

MSTP は、IEEE コミュニティーが定義する規格です。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ア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、インターネットブリッジ経由で、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、スパニングツリーアンサンス、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、マルチプラ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 Revision番号(ここでは、リ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 エレメントテーブル(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 設定に設定します(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 VLAN ID 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ー内のポートの役割(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)を組み合わせて、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ー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ーを計算します。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、トポロジー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、トポロジー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、直ちに通常のスパン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ー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、ポート基盤のユーザー定義グループ毎に適用されます。

3.4.18.1 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：

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	STP を有効または無効に設定します。
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	このフィールドは、BPDU パケットの転送を有効または無効にします。デフォルトは有効です。
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、スイッチのスパン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 Sec)	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。
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。
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ン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、最大エイジより長くすることはできません。最大エイ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。

$$\text{最大エイジ} \leq 2 \times (\text{送信遅延} - 1 \text{秒})$$

$$\text{最大エイジ} \geq 2 \times (\text{Hello 時間} + 1 \text{秒})$$

3.4.18.2 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 BPDU	Enabled		

Port	External Cost	Edge	P2P	Port STP	Restricted Role	Restricted TCN	Forward BPDU	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
9	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
10M	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
11T	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
12T	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
13T	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
14	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
15	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 BPDU	Enabled	Hello Time (1-2)	2 sec

Port	External Cost	Edge	P2P	Port STP	Restricted Role	Restricted TCN	Forward BPDU	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
9	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
10M	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
11T	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
12T	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
13T	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
14	Auto/200000	Auto/No	Auto/Yes	Enabled	False	False	Enabled	2/2
15	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ロックします。STP グループは、VLAN グループに対応するよう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	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。
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	True 選択では、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 選択では、エッジポートとして指定されていないことを示します。Auto 選択では、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	True を選択すると、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に似ていますが、P2P ポートは全二重で動作しなければなりません。エッジポートと同様に、P2P ポートはフォワーディング状態へ高速遷移するので、RSTP の利点を活用できます。False は、ポートを P2P 状態にできません。Auto にすると、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 状態は P2P 値が False であるのと同様に動作するように変更されます。このパラメーターのデフォルト設定は Auto です。
Port STP	STP をポート単位で有効または無効にします。
Restricted Role	パケットの制限付き役割状態を設定します。デフォルト値は False です。
Restricted TCN	パケットの制限付き TCN を設定します。デフォルト値は False です。
Forward BPDU	有効な場合は、その他のネットワークデバイスからの BPDU パケットを転送します。デフォルトは有効です。
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。

[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。

3.4.18.3 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ラ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：

MST Configuration Identification Settings	
Configuration Name	00:40:66:71:F6:B2
Revision Level (0-65535)	0
Instance ID Settings	
MSTI ID (1-4)	<input type="text"/>
Type	Add VID
VID List (e.g.: 2-5, 10)	<input type="text"/>
Total Entries: 1	
MSTI ID	VID List
CIST	1-4094

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。

3.4.18.4 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:

STP Instance Settings

STP Priority Settings		
MSTI ID	Priority	Apply
0	0	[Apply]
Total Entries: 1		
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	--
Time Since Topology Change	Topology Change 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	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。

3.4.18.5 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:

MSTP Port Information

Port	01	Find			
MSTP Port Settings					
Instance ID	Internal Path Cost (1-200000000)	Priority	0	Apply	
Port 1 Settings					
MSTI	Designated Bridge	Internal Path Cost	Priority	Status	Role
0	N/A	200000	128	Forwarding	NonStp

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	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。

3.4.19 Forwarding & Filtering

3.4.19.1 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:

Unicast Forwarding Settings			
Unicast Forwarding Settings			
<input checked="" type="radio"/> VLAN Name	<input type="text"/>	MAC Address	<input type="text" value="00-00-00-00-00-00"/>
<input type="radio"/> VLAN List	<input type="text"/>	Port	<input type="text"/>
<input type="button" value="Apply"/>			
Total Entries: 1			
VID	VLAN Name	MAC Address	Port
1	default	00-11-22-33-44-55	3
<input type="button" value="Delete"/>			
1/1 1 <input type="button" value="Go"/>			

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 Name	ラジオボタンをクリックしてユニキャスト MAC アドレスが属する VLAN 名を入力します。
VLAN List	ラジオボタンをクリックしてユニキャスト MAC アドレスが属する VLAN リストを入力します。
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	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。指定したエントリーを削除するには[Delete]をクリックします。

3.4.19.2 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：

Multicast Forwarding Settings																													
VID	<input type="text"/>																												
Multicast MAC Address	<input type="text"/>																												
Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26		
None	<input checked="" 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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Egress	<input checked="" 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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52		
None	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress Ports																													
Total Entries: 1																													
VID	MAC Address	Mode	Egress Ports																										
1	01-80-C2-01-02-55	Static	<input type="button" value="Edit"/> <input type="button" value="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
VID (1-4094)	MAC アドレスに割り当てる VLAN ID を指定します。
Multicast 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	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します。

[All]をクリックして全てのポートを選択します。

3.4.19.3 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：

Multicast Filtering Mode			
From Port	To Port	Filtering Mode	
01	01	Forward Unregistered Groups	<input type="button" value="Apply"/>
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	
25		Forward Unregistered Groups	
26		Forward Unregistered Groups	
27		Forward Unregistered Groups	
28		Forward Unregistered Groups	
29		Forward Unregistered Groups	
30		Forward Unregistered Groups	
31		Forward Unregistered Groups	
32		Forward Unregistered Groups	
33		Forward Unregistered Groups	
34		Forward Unregistered Groups	
35		Forward Unregistered Groups	
36		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。

3.4.20 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。

3.4.20.1 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：

The screenshot shows the 'LLDP Global Settings' configuration window. It includes sections for 'LLDP State' (Enabled), 'LLDP Forward Message' (Enabled), and various timing parameters: 'Message TX Interval' (30 sec), 'Message TX Hold Multiplier' (4), 'LLDP Reinit Delay' (2 sec), 'LLDP TX Delay' (2 sec), and 'LLDP Notification Interval' (5 sec). Below these are 'LLDP System Information' fields for Chassis ID Subtype, Chassis ID, System Name, System Description, and System Capabilities, along with a MAC Address field (00-40-66-71-F6-B2). There are also 'Apply' buttons for each section.

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	スイッチ上の LLDP を有効または無効にします。
LLDP Forward Message	LLDP が無効な場合に、この機能で、LLDP パケット転送メッセージを個別ポートに基づいて制御します。ポート上で LLDP が有効な場合は、LLDP パケットを、ポート VLAN が同じすべてのポートにフラッシュし、同じ 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します。
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)。
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。
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)。
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)。
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。

[Apply]をクリックして変更を適用します。

3.4.20.2 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	
Apply			

Note: The IPv4 address should be the switch's address.

Port ID	Notification	Admin Status	IPv4 Address
1	Disabled	TX and RX	
2	Disabled	TX and RX	
3	Disabled	TX and RX	
4	Disabled	TX and RX	
5	Disabled	TX and RX	
6	Disabled	TX and RX	
7	Disabled	TX and RX	
8	Disabled	TX and RX	
9	Disabled	TX and RX	
10	Disabled	TX and RX	
11	Disabled	TX and RX	
12	Disabled	TX and RX	
13	Disabled	TX and RX	
14	Disabled	TX and RX	
15	Disabled	TX and RX	
16	Disabled	TX and RX	
17	Disabled	TX and RX	
18	Disabled	TX and RX	
19	Disabled	TX and RX	
20	Disabled	TX and RX	
21	Disabled	TX and RX	
22	Disabled	TX and RX	
23	Disabled	TX and RX	
24	Disabled	TX and RX	
25	Disabled	TX and RX	
26	Disabled	TX and RX	
27	Disabled	TX and RX	
28	Disabled	TX and RX	
29	Disabled	TX and RX	
30	Disabled	TX and RX	

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	LLDP 通知を有効または無効にします。この機能で SNMP トランプルを制御します。ただし、通知が無効な場合は、SNMP トランプルを送信しません。
Admin Status	ローカル LLDP エージェントを制御して、ローカル LLDP エージェントがポート上で LLDP フレームを送受信できるようにします。送信、受信、送受信、無効のオプションがあります。 Tx: LLDP フレームの送信しかできません。 Rx: LLDP フレームの受信しかできません。 Tx and Rx: LLDP フレームの送受信ができます。 Disabled: LLDP フレームの送受信ができません。 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	アドバタイズ管理アドレス機能ベースポートを有効または無効にします。
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。

3.4.20.3 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：

LLDP Basic TLVs Settings

From Port	01	To Port	01	
Port Description	Disabled	System Name	Disabled	
System Description	Disabled	System Capabilities	Disabled	
<input type="button" value="Apply"/>				
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
25	Disabled	Disabled	Disabled	Disabled
26	Disabled	Disabled	Disabled	Disabled
27	Disabled	Disabled	Disabled	Disabled
28	Disabled	Disabled	Disabled	Disabled
29	Disabled	Disabled	Disabled	Disabled
30	Disabled	Disabled	Disabled	Disabled
31	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	ポートの種別を有効または無効にします。
System Name	システム名を有効または無効にします。
System Description	システムの種別を有効または無効にします。
System Capabilities	システム性能を有効または無効にします。

[Apply]をクリックして変更を適用します。

3.4.20.4 LLDP Dot1 TLVs Settings

LLDP Dot1 TLV は、IEEE 802.1 で定義された組織上の特殊 TLV です。LLDP Dot1 TLV を使用して、個別のポートまたはポートのグループが、1つまたは複数の IEEE 802.1 の組織上ポートの VLAN ID TLV データ型をアウトバウンド LLDP アドバタイズメントから除くように設定します。

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：

LLDP Dot1 TLVs Settings

From Port	01	To Port	01
Dot1 TLV PVID	Disabled	Dot1 TLV Protocol VLAN	VLAN Name
Dot1 TLV VLAN	Disabled	VLAN Name	
Dot1 TLV Protocol Identity	Disabled	EAPOL	<input type="button" value="Apply"/>

Port	PVID State	Port and Protocol VID State	VID	VLAN Name State	VID	Protocol Identity State	Protocol Identity
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	
25	Disabled	Disabled		Disabled		Disabled	
26	Disabled	Disabled		Disabled		Disabled	
27	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。
Dot1 TLV PVID	アドバタイズ PVID を有効または無効にします。
Dot1 TLV Protocol VLAN ID	プロトコル VLAN ID を有効または無効にします。
Dot1 TLV VLAN	アドバタイズ VLAN 名を有効または無効にします。
Dot1 TLV Protocol Identity	プロトコル識別を有効または無効にします。

[Apply]をクリックして変更を適用します。

3.4.20.5 LLDP Dot3 TLVs Settings

このウィンドウを使用して、個別のポートまたはポートのグループが、1つまたは複数の IEEE 802.3 の組織上の特殊 TLV データ型をアウトバウンド LLDP アドバタイズメントから除くように設定します。

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：

LLDP Dot3 TLVs Settings

From Port	01	To Port	01	
MAC / PHY Configuration Status	Disabled	Link Aggregation	Disabled	
Maximum Frame Size	Disabled	Power Via MDI	Disabled	
<input type="button" value="Apply"/>				
Port	MAC / PHY Configuration Status	Link Aggregation	Maximum Frame Size	Power Via MDI
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
25	Disabled	Disabled	Disabled	Disabled
26	Disabled	Disabled	Disabled	Disabled
27	Disabled	Disabled	Disabled	Disabled
28	Disabled	Disabled	Disabled	Disabled
29	Disabled	Disabled	Disabled	Disabled
30	Disabled	Disabled	Disabled	Disabled
31	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	LLDP エージェントが「MAC/PHY 設定状態 TLV」を送信します。これは IEEE 802.3 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 タイプについての情報が含まれます。デフォルトは無効です。
Link Aggregation	LLDP エージェントが「Link Aggregation TLV」を送信します。ポートがリンクアグリゲーションができるか、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 についての情報が含まれます。デフォルトは無効です。
Maximum Frame Size	LLDP エージェントが「最大フレームサイズ TLV」を送信します。デフォルトは無効です。

[Apply]をクリックして変更を適用します。

3.4.21 Show VLAN Ports

このウィンドウでは、VLAN のポートアサイン状態を表示します。ポートリストを指定し、Find ボタンを押すことで指定のポートのみ表示させることができます。

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

Show VLAN Ports					
Port List (e.g.: 1, 5-10)					
Total Entries: 52					
Ports	VID	Untagged	Tagged	Dynamic	Forbidden
1	1	X	-	-	-
2	1	X	-	-	-
3	1	X	-	-	-
4	1	X	-	-	-
5	1	X	-	-	-
6	1	X	-	-	-
7	1	X	-	-	-
8	1	X	-	-	-
9	1	X	-	-	-
10	1	X	-	-	-

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 (e.g.: 1,5-10)	VLAN アサイン状態を表示するポート番号を入力します。

[Find]をクリックすると Port List で入力した対象のポートの VLAN アサイン状態を表示します。

[View All]をクリックすると全てのポートの VLAN アサイン状態を表示します。

[Go]ボタンで次のページを表示します。

3.5 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 7 の優先度は、スイッチ上の 8 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 8 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 0~7 のラベルが付いています。7 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 Q2 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 Q1 キューに割り当てられています。
優先度 3 はスイッチの Q3 キューに割り当てられています。
優先度 4 はスイッチの Q4 キューに割り当てられています。
優先度 5 はスイッチの Q5 キューに割り当てられています。
優先度 6 はスイッチの Q6 キューに割り当てられています。
優先度 7 はスイッチの Q7 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てから、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 8 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。

3.5.1 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	To Port	Type	No Limit	Rate (64-1024000)
01	01	RX	Disabled	Kbit/sec
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
11	No Limit	No Limit	No Limit	No Limit
12	No Limit	No Limit	No Limit	No Limit
13	No Limit	No Limit	No Limit	No Limit
14	No Limit	No Limit	No Limit	No Limit
15	No Limit	No Limit	No Limit	No Limit
16	No Limit	No Limit	No Limit	No Limit
17	No Limit	No Limit	No Limit	No Limit
18	No Limit	No Limit	No Limit	No Limit
19	No Limit	No Limit	No Limit	No Limit
20	No Limit	No Limit	No Limit	No Limit
21	No Limit	No Limit	No Limit	No Limit
22	No Limit	No Limit	No Limit	No Limit
23	No Limit	No Limit	No Limit	No Limit
24	No Limit	No Limit	No Limit	No Limit
25	No Limit	No Limit	No Limit	No Limit
26	No Limit	No Limit	No Limit	No Limit
27	No Limit	No Limit	No Limit	No Limit
28	No Limit	No Limit	No Limit	No Limit
29	No Limit	No Limit	No Limit	No Limit
30	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	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	選択したポートの帯域幅を制限するか、無制限にするかを指定します。
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。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。

3.5.2 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あふれています。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できます。

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：

The screenshot shows the 'Traffic Control' configuration window. At the top, there are fields for 'From Port' (01), 'To Port' (01), 'Action' (Drop), 'Count Down (0-1800)' (0 sec), 'Threshold (64-1000000)' (64 kbit/s), 'Time Interval (5-30)' (5 sec), 'Recover Time (10-300)' (300 sec), and 'Storm Control Type' (None). An 'Apply' button is also visible. Below this is a table listing port configurations:

Port	Storm Control Type	Action	Threshold	Count Down	Interval	Recover Time
1	None	Drop	64	0	5	300
2	None	Drop	64	0	5	300
3	None	Drop	64	0	5	300
4	None	Drop	64	0	5	300
5	None	Drop	64	0	5	300
6	None	Drop	64	0	5	300
7	None	Drop	64	0	5	300
8	None	Drop	64	0	5	300
9	None	Drop	64	0	5	300
10	None	Drop	64	0	5	300
11	None	Drop	64	0	5	300
12	None	Drop	64	0	5	300
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
19	None	Drop	64	0	5	300
20	None	Drop	64	0	5	300
21	None	Drop	64	0	5	300
22	None	Drop	64	0	5	300
23	None	Drop	64	0	5	300
24	None	Drop	64	0	5	300
25	None	Drop	64	0	5	300
26	None	Drop	64	0	5	300
27	None	Drop	64	0	5	300
28	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
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	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、「drop」または「shutdown」を指定することが出来ます。 Drop - スイッチ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。 Shutdown - スイッチ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。
Count Down (0 to 1800)	カウントダウンタイマを設定して、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。0 に設定すると、ポートはシャットダウンされません。
Time Interval (5-30)	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。
Threshold (64- 1000000)	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。
Recover Time (10-300)	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。
Storm Control Type	検出するストームの種類を次から選択します: 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。

[Apply]をクリックして設定を適用します。

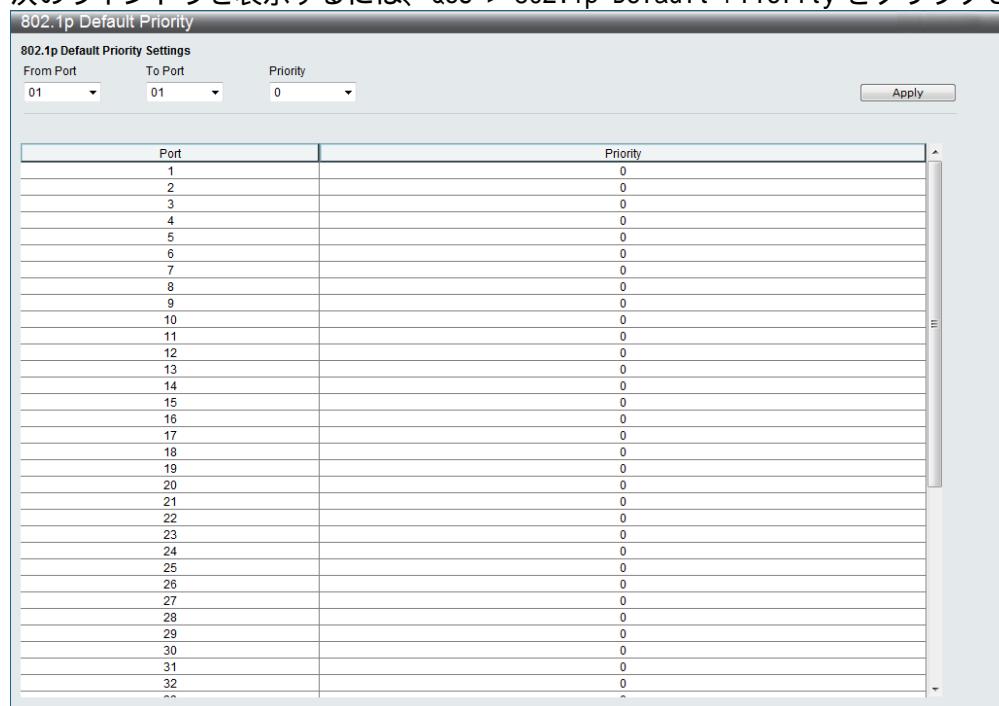
注意事項

- !** 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。

3.5.3 802.1p 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 Default Priority をクリックします：



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。

3.5.4 802.1p 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：



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
Priority	802.1p の優先度を選択します。
Class ID	Class-0 ~ 7 のクラス ID を選択します。

[Apply]をクリックして変更を適用します。

3.5.5 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ことがあります。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：

The screenshot shows the 'QoS Scheduling Settings' window. At the top, there's a dropdown menu labeled 'Scheduling Mechanism' set to 'Strict'. Below it is a large table titled 'QoS Scheduling Weight Settings' with 8 rows, each representing a priority class from 0 to 7. The columns are 'Class ID', 'Mechanism', and 'Weight (1-127)'. The 'Mechanism' column for all rows is 'Strict'. The 'Weight' column contains values 1 through 8 respectively. There are two 'Apply' buttons at the bottom of the table.

Class ID	Mechanism	Weight (1-127)
0	Strict	1
1	Strict	2
2	Strict	3
3	Strict	4
4	Strict	5
5	Strict	6
6	Strict	7
7	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	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 (1-127)	1 ~ 127 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。

3.5.6 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	To Port	Priority	Ethernet Priority	IP Priority	
01	01	<input type="checkbox"/> None	<input checked="" type="checkbox"/> 802.1p	<input type="checkbox"/> TOS	<input type="button" value="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
25			802.1p		Off
26			802.1p		Off
27			802.1p		Off
28			802.1p		Off
29			802.1p		Off
30			802.1p		Off
31			802.1p		Off
32			802.1p		Off
33			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。

3.5.7 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 ▾

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	Class-0~7 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。

3.5.8 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 Mapping	
DSCP Value	Class ID
0	Class-0 ▾
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
29	0
30	0
31	0
32	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	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	Class-0~7 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。

3.6 Security

3.6.1 Trusted Host

セキュリティーIP管理を使用して、装置へのIPアクセスを許可するトラストホストを作成します。最大10個までのIPアドレスまたはIPネットワークアドレスを指定できます。また、IPアクセスを許可するインターフェース（サービス）を指定することで、さらに信頼されたトラストホストを作成できます。トラストホストが作成されると、指定しないIPアドレスまたはインターフェースからの装置IPアクセスはできなくなります。

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：

Trusted Host

<input checked="" type="radio"/> IPv4 Address	<input type="text"/>	Net Mask	<input type="text"/> (e.g.: 255.255.255.254 or 1-32)
<input type="radio"/> IPv6 Address	<input type="text"/>	Net Mask	<input type="text"/> (1-128)
Access Interface	<input type="checkbox"/> SNMP <input type="checkbox"/> Telnet <input type="checkbox"/> SSH <input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS <input type="checkbox"/> Ping <input type="checkbox"/> All	<input type="button" value="Add"/> <input type="button" value="Delete All"/>	
Total Entries: 1			
IP Address	Access Interface		
172.0.0.8	SNMP Telnet SSH HTTP HTTPS Ping	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Note: Create a list of IPv4 / IPv6 addresses that can access the switch. Your local host IPv4 / IPv6 address must be one of the IPv4 / IPv6 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
IPv4 Address / Net Mask	IPv4 アドレス/ネットマスクを入力します。
IPv6 Address / NetMask	IPv6 アドレス/ネットマスク(Prefix)を入力します。
Access Interface	許可する IP アクセスのインターフェース（サービス）を選択します。

[Add]をクリックして新しいエントリを追加します。

[Delete All]をクリックして全てのエントリを削除します。

[Edit]をクリックして指定エントリを再設定します。

[Delete]をクリックして指定エントリを削除します。

3.6.2 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。

3.6.2.1 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 Settings

From Port	To Port	Admin State	Max Learning Address (0-64)	Lock Address Mode	
01	01	Disabled	0	Delete on Reset	<input type="button" value="Apply"/>

Port Security Port Table

Port	Admin State	Max Learning Address	Lock Address Mode	
1	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
2	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
3	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
4	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
5	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
6	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
7	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
8	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
9	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
10	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
11	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
12	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
13	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
14	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
15	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
16	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
17	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
18	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
19	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
20	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
21	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
22	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
23	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
24	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>
25	Disabled	1	DeleteOnTimeout	<input type="button" value="Edit"/>

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ーを設定するポート範囲を選択します。
Admin State	ポートセキュリティー(選択したポート用のロックした MAC アドレステーブル)を有効または無効にします。
Max. Learning Address (0-64)	ポートセキュリティーで 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ー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。

3.6.2.2 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:

The screenshot shows the 'Port Security Entries' window. At the top, there are two radio button options: 'VLAN Name' (selected) and 'VID List (e.g.: 1, 4-6)'. Below each option are input fields. Under 'VLAN Name', there is a 'Port List (e.g.: 1, 4-6)' field and a 'All' checkbox. To the right of these fields are 'Find' and 'Clear' buttons. At the bottom of the window, there are 'Show All' and 'Clear All' buttons. A status bar at the bottom left indicates '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	FDB の VLAN 名を入力します。
VID List	FDB の VLAN ID を入力します。
Port List	削除対象のポート番号を入力します。

[Find]をクリックして対象のエントリーを表示します。

[Clear]をクリックして指定のエントリーを削除します。

[Show All]をクリックしてエントリーリストを表示します。

[Clear All]をクリックして全てのエントリーを削除します。

3.6.3 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：

Authentication Port Settings		
From Port	To Port	Authorized Mode
01	52	Host-based
1		Host-based
2		Host-based
3		Host-based
4		Host-based
5		Host-based
6		Host-based
7		Host-based
8		Host-based
9		Host-based
10		Host-based
11		Host-based
12		Host-based
13		Host-based
14		Host-based
15		Host-based
16		Host-based
17		Host-based
18		Host-based
19		Host-based
20		Host-based
21		Host-based
22		Host-based
23		Host-based
24		Host-based
25		Host-based
26		Host-based
27		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
Authorization Network State	認証属性を割り当てるグローバル設定を有効または無効にします。
Authentication Server Failover	認証サーバーの failover 機能を有効または無効にします。
From Port/To Port	ポート範囲を選択します。
Authorized Mode	使用される認証モードを指定します Host-based - 各ユーザーは個々に認証可能です。 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。もし那个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 になります。

[Apply]をクリックして変更を適用します。

3.6.4 802.1X

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。

3.6.4.1 802.1X Global Settings

このウィンドウでは、802.1Xのグローバル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、Security > 802.1X > 802.1X Global Settings をクリックします：

802.1X Global Settings			
Authentication State	Disabled	Authentication Protocol	RADIUS EAP
Forward EAPOL PDU	Enabled	Max User (1-1000)	1000
RADIUS Authorization	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
Authentication State	802.1X を有効または無効に設定します。
Authentication Protocol	認証プロトコルを Local または RADIUS EAP から選択します。
Forward EAPOL PDU	EAPOL PDU 転送設定をグローバルに有効または無効に設定します。
Max User (1-1000)	認証時の最大収容端末数を設定します。装置の最大収容端末数は、1000 です。
RADIUS Authorization	RADIUS 認証が有効の場合、RADIUS サーバーによりアサインされた認証データが受け付けられます。

[Apply]をクリックして変更を適用します。

注意事項

- !** 認証属性を有効とするためには、認証属性のグローバル設定を有効にする必要があります。この設定は「Authentication Settings」ウィンドウで行います。
- !** 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。
- !** 802.1X のローカル認証は、MD5 のみサポートします。

3.6.4.2 802.1X Port Settings

このウィンドウで 802.1X 認証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、Security > 802.1X > 802.1X Port Settings をクリックします：

802.1X Port Settings

802.1X Port Access Control											
From Port	01	To Port	01	Port Control	Auto	Direction	Both	Max User (1-1000)	16	Refresh	Apply
QuietPeriod (0-65535)	60	SuppTimeout (1-65535)	30	MaxReq (1-10)	2	ReAuthPeriod (1-65535)	3600	sec	sec		
ServerTimeout (1-65535)	30							times			
TX Period (1-65535)	30								sec		
ReAuthentication	Disabled										
Capability	None										
Forward EAPOL PDU	Enabled										

Port	AdmDir	OpenCrlDir	Port Control	TX Period	Quiet Period	Supp-TIMEOUT	Server-TIMEOUT	MaxReq	ReAuth Period	ReAuth	Capability	Forward EAPOL PDU	Max User
1	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
2	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
3	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
4	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
5	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
6	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
7	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
8	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
9	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
10	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
11	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
12	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
13	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16
14	Both	Both	Auto	30	60	30	30	2	3600	Disabled	None	Enabled	16

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。
QuietPeriod (0-65535)	サプ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プ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)	サプ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、サプ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)	サプ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	定期的に再認証するかどうかを決めます。デフォルト設定は無効です。
Port Control	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。 [ForceUnauthorized]を選択すると、ポートは 802.1X の認証プロセスを行わ

パラメーター	説明
	<p>必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。</p> <p>[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、サプリカントからの 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。</p> <p>デフォルト設定は Auto です。</p>
Capability	<p>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。</p> <p>[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。</p>
Direction	<p>管理制御方向を受信または双方向に設定します。</p> <p>[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。</p> <p>[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。</p>
Forward EAPOL PDU	EAPOL PDU 転送設定をグローバルに有効または無効にします。
Max User	認証時の最大収容端末数を設定します。1 ポート当りの最大収容端末数は、1000 です。

[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。

3.6.4.3 802.1X 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、相応する[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
<small>Note: 802.1X User and Password should be less than 16 characters.</small>		
802.1X User Table Total Entries: 1		
User Name	Password	
1xUser	*****	<input type="button" value="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
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。

[Delete]をクリックして対象のエントリーを削除します。

3.6.4.4 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:

Authentication RADIUS Server Settings						
Index	1	IP Address	(e.g.: 10.90.90.90)	Auth-Port	Acct-Port	Timeout
Authentication Port (1-65535)				<input checked="" type="checkbox"/> Default		
Accounting Port (1-65535)				<input checked="" type="checkbox"/> Default		
Timeout (1-255)			sec	<input checked="" type="checkbox"/> Default		
Retransmit (1-255)			times	<input checked="" type="checkbox"/> Default		
Key (Max: 32 characters)						
Confirm Key						<input type="button" value="Apply"/>
RADIUS Server List						
Index	IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Key
1						
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。
Authentication 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じキーを入力します。

[Apply]をクリックして変更を適用します。

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-based Port(s)をクリックします：



The screenshot shows the 'Initialize Port-based Port(s)' configuration window. It has two dropdown menus for 'From Port' and 'To Port', and an 'Apply' button. Below these are two input fields: 'MAC Address' and 'VID'. A large table below lists ports with columns for Port, MAC Address, PAE State, Backend State, Status, VID, and Priority.

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 Host-based Port(s)をクリックします：



The screenshot shows the 'Initialize Host-based Port(s)' configuration window. It features three dropdown menus for 'From Port', 'To Port', and 'MAC Address', and an 'Apply' button.

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。
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]切断済み、[Connecting]接続中、 [Authenticating]認証中、[Authenticated]認証済み、[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。
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。

[Apply]をクリックして変更を適用します。

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 Host-based Port(s)をクリックします：

Port	MAC Address	Authenticated VID	PAE State	Backend State	Status	VID	Priority
------	-------------	-------------------	-----------	---------------	--------	-----	----------

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。
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。
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]切断済み、[Connecting]接続中、 [Authenticating]認証中、[Authenticated]認証済み、[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。
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。

[Apply]をクリックして変更を適用します。

3.6.5 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ー機能です。これらのセキュリティー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ー文字列です。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ー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 RC4 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。

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、セキュリティー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 と TLSv1 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に、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。サイバースイートは、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3つのサイバ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バースイートは有効です。特定のサイバースイートを使用するには、認証の際に使用するサイバースイート以外の不要なサイバ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 window. It includes sections for 'SSL Global Settings' (with 'SSL State' set to 'Disabled'), 'SSL Ciphersuite Settings' (with three cipher suites listed, all enabled), 'SSL Certificate Download' (with fields for 'Server IP Address', 'Certificate File Name', and 'Key File Name', and a 'Download' button), and a status message 'Loaded with RSA Certificate!'.

SSL Settings

SSL Global Settings

SSL State Enabled Disabled

Cache Timeout (60-86400) sec

Note: Web will be disabled if SSL is enabled.

SSL Ciphersuite Settings

RSA with RC4_128_MD5	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
RSA with 3DES EDE CBC SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DHE DSS with 3DES EDE CBC SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

SSL Certificate Download

Server IP Address

Certificate File Name

Key File Name

Current Certificate **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	SSL を有効または無効に設定します。デフォルトは無効です。
Cache Timeout (60-86400)	SSL 機能を使用してクライアントとホストの間で新しいキーを交換する時間を設定します。クライアントとホストがキー交換する度に、新しい SSL セッションが確立されます。デフォルト設定は 600 秒です。
SSL Ciphersuite Settings	
RSA with RC4_128_MD5	このサイファースイートは、RSA キー交換とストリームサイファー RC4 暗号化を、128 ビットキーおよび MD5 ハッシュアルゴリズムと組み合わせます。プルダウンメニューから有効または無効に設定します。デフォルトは有効です。
RSA with 3DES EDE CBC SHA	このサイファースイートは、RSA キー交換、CBC ブロックサイファー 3DES_EDE 暗号化、および、SHA ハッシュアルゴリズムを組み合わせます。プルダウンメニューから有効または無効に設定します。デフォルトは有効です。
DHE DSS with 3DES EDE CBC SHA	このサイファースイートは、DSA Diffie Hellman キー交換、CBC ブロックサイファー 3DES_EDE 暗号化、SHA ハッシュアルゴリズムを組み合わせます。プルダウンメニューから有効または無効に設定します。デフォルトは有効です。
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。このファイルには .der 拡張子が必要です(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。このファイルには .der 拡張子が必要です(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 のエンターは「https://」で始まる必要があります。



ダウ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

3.6.6 SSH

SSH は、リモートホストコンピュータ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ー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。

3.6.6.1 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：

The screenshot shows the 'SSH Settings' window with the following configuration:

- SSH Server State:** Enabled (radio button selected)
- SSH Global Settings:**
 - Max Session (1-8): 8
 - Connection Timeout (120-600): 120 sec
 - Authfail Attempts (2-20): 2 times
 - Rekey Timeout: Never
 - TCP Port Number (1-65535): 22
- Buttons:** Apply (top right), Apply (bottom right)

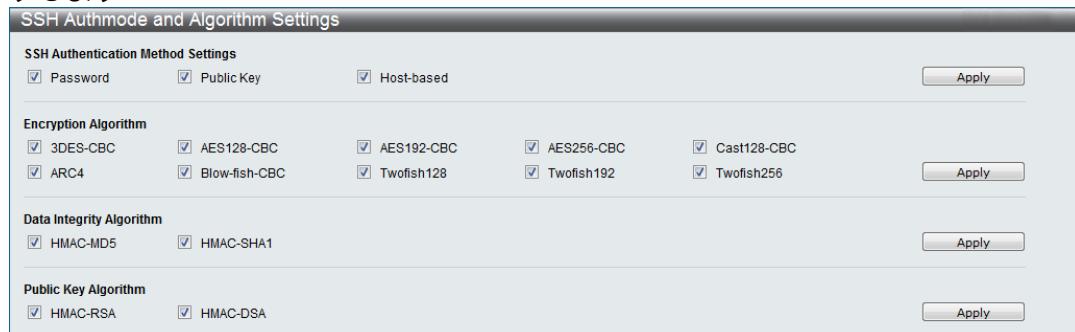
下記にパラメーターの説明を記載します。

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。
TCP Port Number(1-65535)	SSH で使用する TCP ポート番号を入力します。デフォルト設定は 22 です。

[Apply]をクリックして変更を適用します。

3.6.6.2 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。

3.6.6.3 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：

The screenshot shows a table with the following columns: User Name, Authentication Method, Host Name, and Host IP. There is one entry for 'adpro' with 'Password' selected as the authentication method. A note at the bottom states: 'Note: Maximum 8 entries and Host Name should be less than 33 characters.'

SSH User Authentication Lists			
Total Entries: 1			
User Name	Authentication Method	Host Name	Host IP
adpro	Password		

Note: Maximum 8 entries and Host Name should be less than 33 characters.

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、相応する [Edit] をクリックして、次のウィンドウを表示します。

The screenshot shows a table with the same four columns. The 'Host Name' field is empty. An 'Apply' button is visible on the right. A note at the bottom states: 'Note: Maximum 8 entries and Host Name should be less than 33 characters.'

SSH User Authentication Lists			
Total Entries: 1			
User Name	Authentication Method	Host Name	Host IP
adpro	Password		

Note: Maximum 8 entries and Host Name should be less than 33 characters.

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。
Authentication Method	管理者は、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、次の情報を入力して SSH ユーザーを識別します。 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。 Host IP - 相応する SSH ユーザーの IP アドレスを入力します。 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 ユーザーの相応する 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。

3.6.7 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、セキュリティー目的のために、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イ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) サーバーは認証エラーに応答しません。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、同様に続けます。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hoszt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。

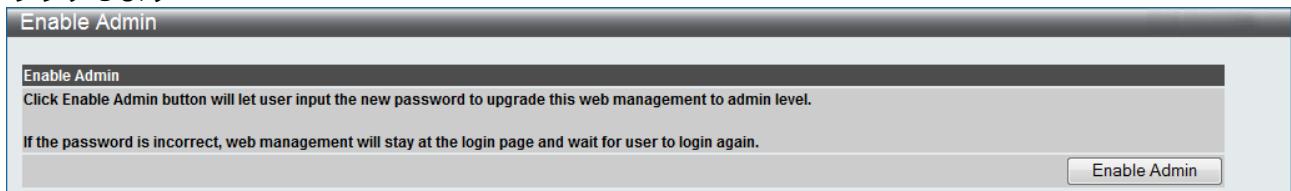
3.6.7.1 Enable Admin

このウィンドウで、スイッチにログインした一般レベルのユーザーが、その権限を管理者レベルに変更することができます。

スイッチにログインした後にユーザーは一般レベルの特権を持っています。

管理者レベルの特権に変更するために、ユーザーはこの画面から認証パスワードを入力します。

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



一般レベルのユーザーが管理者レベルでログインするためには、Enable Admin ボタンをクリックします。次に以下のウィンドウが表示されますので認証のためのユーザー名、パスワードを入力します。認証が成功すると管理者特権でスイッチにログインすることができます。



3.6.7.2 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：

Authentication Policy Settings	
Authentication Policy	Disabled
Response Timeout (0-255)	30 sec
User Attempts (1-255)	3 times
<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
Authentication Policy	スイッチ上の認証ポリシーを有効または無効にします。
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す。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。

3.6.7.3 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 Authentication Settings			
Application	Login Method List	Enable Method List	
Console	default	default	
Telnet	default	default	
SSH	default	default	
HTTP	default	default	

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。

3.6.7.4 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：

Authentication Sever Group

Server Group List		Edit Sever Group	
Group Name (Max: 15 characters) <input type="text"/> <input type="button" value="Add"/>			
Total Entries: 4			
Group Name			
radius	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	
tacacs	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	
tacacs+	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	
xtacacs	<input type="button" value="Edit"/>	<input type="button" value="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。

指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 Server Group]タブをクリックします。次のタブが表示されます：

Authentication Sever Group

Server Group List		Edit Sever Group	
Group Name (Max: 15 characters) <input type="text"/> <input type="button" value="Add"/>			
Server Host			
IP Address	<input type="text"/>	Protocol	TACACS <input type="button" value="▼"/> <input type="button" value="Add"/>
Host List			
IP Address	<input type="text"/>	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。

3.6.7.5 Authentication Server

このウィンドウで、スイッチ上のTACACS/XTACACS/TACACS+/RADIUSセキュリティープロトコル用に、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：

Authentication Server					
IP Address	Port (1-65535)	Protocol	Timeout (1-255)	Key (Max: 254 characters)	Retransmit (1-255)
	49	TACACS	5 sec		2 times

Total Entries: 0

IP Address	Protocol	Port	Timeout	Key	Retransmit

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。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、エンティーが表示されます。

3.6.7.6 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：

The screenshot shows the 'Login Method Lists' configuration window. At the top, there is a field for 'Method List Name (Max: 15 characters)' with a placeholder 'default'. Below it are four priority dropdown menus labeled 'Priority 1' through 'Priority 4'. To the right of these dropdowns is an 'Apply' button. Below these controls is a table titled 'Total Entries: 1'. The table has columns for 'Method List Name', 'Priority 1', 'Priority 2', 'Priority 3', and 'Priority 4'. The first row contains the value 'default' under 'Method List Name' and 'local' under 'Priority 1'. At the bottom right of the table are 'Edit' and 'Delete' buttons.

Total Entries: 1				
Method List Name	Priority 1	Priority 2	Priority 3	Priority 4
default	local	----	----	----

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、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。

3.6.7.7 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:

Total Entries: 1	Method List Name	Priority 1	Priority 2	Priority 3	Priority 4	Edit	Delete
	default	local_enable	----	----	----		

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	この Method List には、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。

3.6.7.8 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：

The screenshot shows a dialog box titled "Local Enable Password Settings". It contains three input fields: "Old Local Enable Password (Max: 15 characters)", "New Local Enable Password", and "Confirm Local Enable Password". At the bottom right is a "Apply" button.

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。
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。

3.6.8 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のアクセスを認証する方法です。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



APLGM152GT では、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属性が引き継がれます。

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、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。

3.6.8.1 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：

MAC-based Access Control Global Settings

MAC-based Access Control State	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled	Apply
Method	Local	Password	default
RADIUS Authorization	Disabled	Local Authorization	Disabled
Trap State	Enabled	Log State	Enabled
Max User (1-1000)	1000		
MAC Format	Uppercase, None	Password Type	Manual String
Apply			

Port Settings

From Port	To Port	State	Aging Time (1-1440)	Hold Time (0-300)	Max User (1-1000)
01	01	Disabled	1440 min	300 sec	128
Apply					

Port	State	Mode	Aging Time (min)	Hold Time (sec)	Max User
1	Disabled	Host-based	1440	300	128
2	Disabled	Host-based	1440	300	128
3	Disabled	Host-based	1440	300	128
4	Disabled	Host-based	1440	300	128
5	Disabled	Host-based	1440	300	128
6	Disabled	Host-based	1440	300	128
7	Disabled	Host-based	1440	300	128
8	Disabled	Host-based	1440	300	128
9	Disabled	Host-based	1440	300	128
10	Disabled	Host-based	1440	300	128

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	
MAC-based Access Control State	スイッチ上の MAC ベースアクセス制御機能をグローバルに有効または無効にします。
Method	指定したポートで MAC 認証する際の認証の種類を以下から選択します。 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。 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。

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。
RADIUS Authorization	プルダウンメニューから RADIUS 認証属性を有効または無効にします。
Local Authorization	プルダウンメニューからローカル認証属性を有効または無効にします。
Trap State	プルダウンメニューからトラップを有効または無効にします。
Log State	プルダウンメニューからログを有効または無効にします。
Max User (1-1000)	装置全体の収容可能な端末数を 1 ~ 1000 で入力します。デフォルトは 1000 です。
MAC Format	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。
Password Type	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。
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入力します。
State	各ポート上の MAC ベースアクセス制御機能を有効または無効にします。
Aging Time (1-1440)	1 ~ 1440 分のエージング値を入力します。デフォルトは 1440 です。エー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 (1-1000)	ポート毎の収容可能な端末数を 1 ~ 1000 で入力します。デフォルト設定は 128 です。

[Apply]をクリックして変更を適用します。

注意事項

- !** 認証属性を有効とするためには、認証属性のグローバル設定を有効にする必要があります。この設定は「Authentication Settings」ウィンドウで行います。
- !** 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。

3.6.8.2 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-based Access Control Local Settings

MAC Address	VLAN Name	VID (1-4094)			
<input type="text"/>	<input checked="" type="radio"/>	<input type="text"/>			
<input type="button" value="Add"/>	<input type="button" value="Delete by MAC"/>	<input type="button" value="Delete by VLAN"/>	<input type="button" value="Find by MAC"/>	<input type="button" value="Find by VLAN"/>	<input type="button" value="View All"/>

Total Entries: 1

MAC Address	VLAN Name	VID	Edit by Name	Edit by ID
00-11-22-33-44-55	default	1	<input type="button" value="Edit by Name"/>	<input type="button" value="Edit by ID"/>

1/1 1 Go

[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。

3.6.9 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サーバー認証に対応します。IPv6のWeb認証は未サポートです。

注意事項

- !** APLGM152GT では、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属性が引き継がれます。
- !** 認証属性を有効とするためには、認証属性のグローバル設定を有効にする必要があります。この設定は「Authentication Settings」ウィンドウで行います。
- !** 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 認証ポートの最大同時セッション数は 128 です。

3.6.9.1 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。

The screenshot shows the 'Web Authentication Settings' configuration window. It includes sections for 'Web Authentication Global Settings' (with 'Global State' set to 'Disabled') and 'Web Authentication Settings' (with 'Virtual IP' set to '0.0.0.0', 'Method' set to 'Local', 'Redirection Path' cleared, 'Local Authorization' enabled, and 'HTTP(S) Port' set to '80'). Buttons for 'Apply' are visible at the bottom right of each section.

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 Authentication Global State	Web 認証機能を有効または無効に設定します。
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。

Method	Web 認証方法を設定します。RADIUS を選択した場合は RADIUS プロトコルによる 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。
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。
Clear Redirection Path	Web 認証のリダイレクト URL を消去するか維持するか選択します。
RADIUS Authorization	RADIUS 認証が有効の場合、RADIUS サーバーによりアサインされた認証データが受け付けられます。
Local Authorization	ローカル認証が有効になると、ローカルデータベースにより割り当てられた認証データが受け付けられます
HTTP(S) Port	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。

[Apply]をクリックして変更を適用します。

3.6.9.2 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 認証ユーザー設定を行うには、Security > Web Authentication > Web Authentication User Settings をクリックします

Web Authentication User Settings

Create User			
User Name	<input checked="" type="radio"/> VLAN Name	<input type="radio"/> VID (1-4094)	Password
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="password"/>
<input type="button" value="Apply"/>		<input type="button" value="Delete All"/>	
Note: Web Authentication User and Password should be less than 16 characters.			
Total Entries: 1			
User Name	VLAN Name	VID	Password
WAC	default	1	*****
		<input type="button" value="Edit VLAN Name"/>	<input type="button" value="Edit VID"/>
		<input type="button" value="Clear VLAN"/>	<input type="button" value="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
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。
VID	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。
Confirm Password	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。

3.6.9.3 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 認証ポート設定を行う時に用います。

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

Web Authentication Port Settings

From Port	01	To Port	01
Aging Time (1-1440)	1440	min	<input type="checkbox"/> Infinite
Block Time (0-300)	60	sec	
<input type="button" value="Apply"/>			
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
14	Disabled	1440	60
15	Disabled	1440	60
16	Disabled	1440	60
17	Disabled	1440	60
18	Disabled	1440	60
19	Disabled	1440	60
20	Disabled	1440	60
21	Disabled	1440	60
22	Disabled	1440	60
23	Disabled	1440	60
24	Disabled	1440	60
25	Disabled	1440	60
26	Disabled	1440	60
27	Disabled	1440	60
28	Disabled	1440	60
29	Discard	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	ポートに対する Web 認証を有効または無効に設定します。
Aging Time	認証されたホストが認証状態を保持する時間を指定します。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。

3.6.9.4 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できます。 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	
パスワード	
[] 入力 [] 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。
ログアウト 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

Clear Apply Preview

下記にパラメーターの説明を記載します。

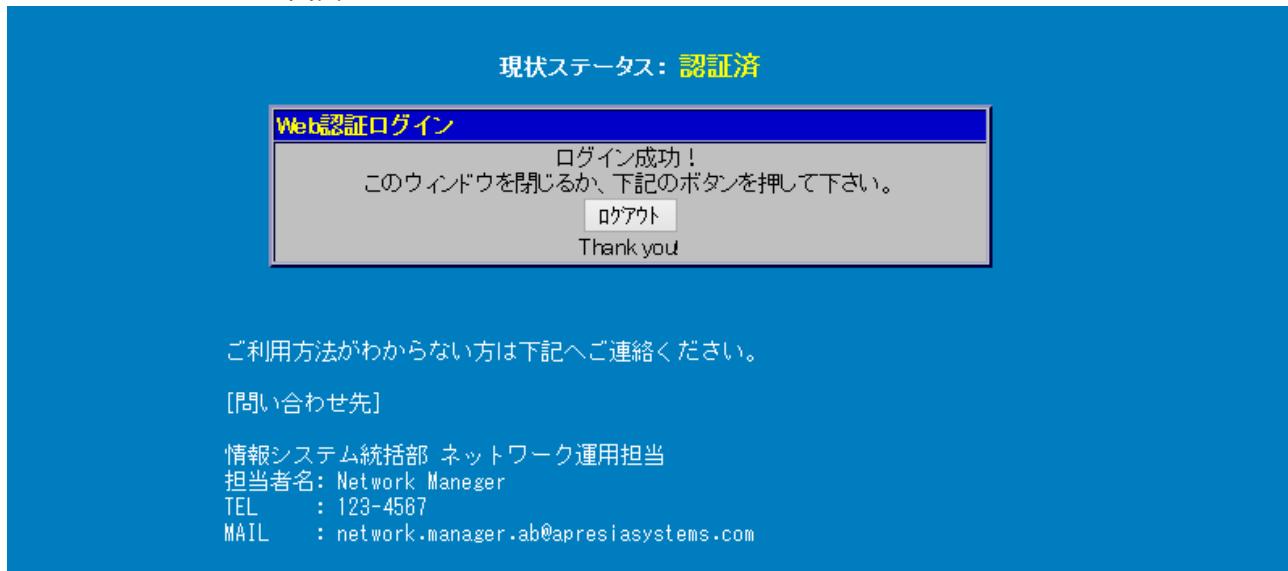
パラメーター	説明
English/Japanese	カスタマイズ画面に表示する言語を英語または日本語から選択します。
Login/Logout	ログイン画面またはログアウト画面のどちらをカスタマイズするか指定します。
Customize Textbox(1-8)	ログアウト画面下にある1番から8番のユーザーテキストボックスに文字を登録できます。 登録可能な任意の文字列は最大で半角70文字です。全角の場合は最大35文字となります。

[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



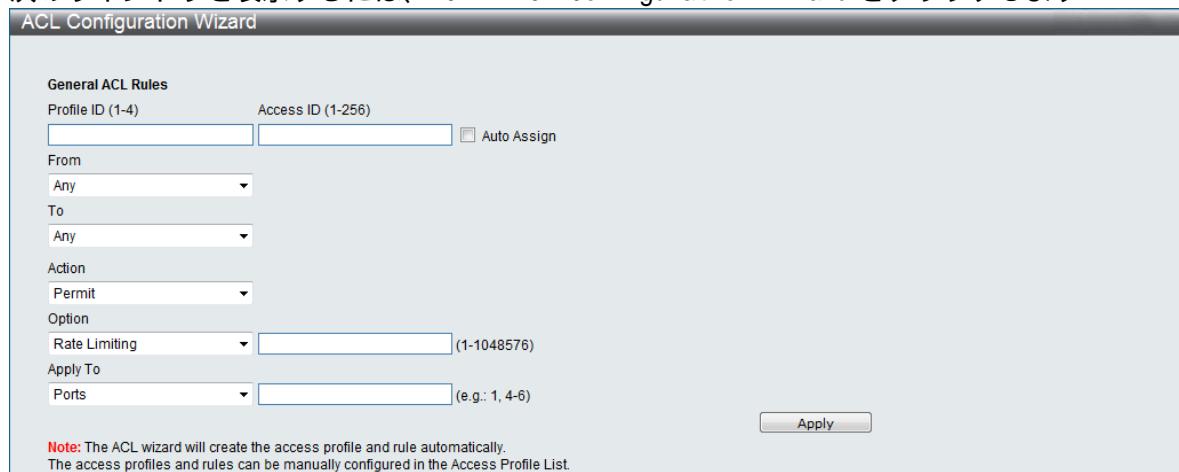
3.7 アクセス制御一覧(ACL)

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。

3.7.1 ACL Configuration Wizard

このウィンドウで、アクセスプロファイルと ACL ルールを作成します。

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 (1-4)	このプロファイルセット用の固有識別子番号を入力します。この値は 1~4 の範囲で設定します。
Access ID (1-256)	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 1~256 の範囲で設定します。
From/To	プルダウンメニューで、From(送信元)および To(送信先)の対象プロトコルを [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。
Action	[Permit]を選択して、追加した規則に従って、アクセスプロファイルと一致するパケットをスイッチで転送することを指定します。 [Deny]を選択して、アクセスプロファイルと一致するパケットをスイッチで転送せずに、ドロップすることを指定します。 [Mirror]を選択して、アクセスプロファイルと一致するパケットを、ミラーポートの構成コマンドで定義したポートにミラーすることを指定します。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	[Rate Limiting]、[Change IP Priority]、[Replace DSCP] から選択します。
Apply To	プルダウンメニューから追加する設定を選択します。 Ports - 追加するポート範囲を設定します。 VLAN Name - VLAN 名を入力します。 VLAN ID - VLAN ID を入力します。

[Apply]をクリックして変更を適用します。

3.7.2 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:

Access Profile List				
Add ACL Profile		Delete All		
Total User Set Rule Entries / Total Used HW Entries / Total Available HW Entries: 3 / 127 / 897				
Profile ID	Profile Type			
1	Ethernet	Show Details	Add/View Rules	Delete
2	IP	Show Details	Add/View Rules	Delete
3	IPv6	Show Details	Add/View Rules	Delete
4	Packet Content	Show Details	Add/View Rules	Delete

1/1 1

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。

Add ACL Profile				
Profile ID (1-4)	1			
Select ACL Type	<input checked="" type="radio"/> Ethernet ACL <input type="radio"/> IPv4 ACL <input type="radio"/> IPv6 ACL <input type="radio"/> Packet Content ACL <small>You can select the field in the packet to create filtering mask</small>			
	MAC Address	VLAN	802.1p	Ethernet Type
MAC Address	<input type="checkbox"/> Source MAC Mask <input type="text"/> <input type="checkbox"/> Destination MAC Mask <input type="text"/>			
802.1Q VLAN	<input type="checkbox"/> VLAN <input type="text"/> <input type="checkbox"/> VLAN Mask (0-FFF) <input type="text"/>			
802.1p	<input type="checkbox"/> 802.1p			
Ethernet Type	<input type="checkbox"/> Ethernet Type			
	<input type="button" value="<<Back"/> <input type="button" value="Create"/>			

アクセスプロファイル構成ウィンドウには4つのセットがあります。Ethernet ACL/IPv4 ACL/IPv6 ACL/Packet Content ACLです。プロファイルを追加する場合、プロファイルIDを1~4で選択し(例では1が選択)、ACLタイプを選択(例では、Ethernet ACLが選択)して、[Select]をクリックします。ACL設定の対象となるボックスをクリックすると、ボックスの色が赤に変わり設定用のパラメーターが表示されます(例では、MAC Address、802.1Q VLAN、802.1P、Ethernet Typeが選択可能)。[Create]をクリックする前に、最低1つのマスクを選択します。[Access Profile List]ウィンドウに戻るには、[<<Back]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
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するように指示します。

注意事項



APLGM152 で設定可能な ACL ルール数は装置最大 900 です。
また、1 つのプロファイルに設定可能な最大ルール数は 256 です。

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 Detail Information

ACL Profile Details	
Profile ID	1
Profile Type	Ethernet
VLAN	0xFFFF
Show All Profiles	

[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規則を追加するには、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:

Access Rule List

Consumed HW Entries: 193				
Profile ID	Access ID	Profile Type	Action	
1	1	Ethernet	Permit	Show Details Delete Rules
1/1 1 <input type="button" value="Go"/> <input type="button" value="Search"/>				

[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	1	Profile Type	Ethernet
VLAN	0xFFFF		

Rule Detail
 (Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-256)	1	<input type="checkbox"/> Auto Assign	
VLAN Name	<input type="text"/>		
VLAN ID	<input type="text"/>		
VLAN Mask (0-FFF)	<input type="text"/>		
Rule Action			
Action	Permit	<input type="checkbox"/>	
Priority (0-7)	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Replace Priority	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Replace DSCP (0-63)	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
Counter	Disabled	<input type="text"/> (e.g.: 1, 4-6, 9)	
Ports	<input type="text"/>		

[<< 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
Access ID (1-256)	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1~256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、作成している規則に対し、スイッチが自動的にアクセス ID を割当てるよう指示します。
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	事前に設定した VLAN の VLAN ID を入力できます。
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。
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	[Permit]を選択して、追加した規則に従って、アクセスプロファイルと一致するパケットをスイッチで転送することを指定します。 [Deny]を選択して、アクセスプロファイルと一致するパケットをスイッチで転

パラメーター	説明
	送せずに、ドロップすることを指定します。 [Mirror]を選択して、アクセスプロファイルと一致するパケットを、ミラーポートの構成コマンドで定義したポートにミラーすることを指定します。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	カウンター機能の有効または無効を指定します。 デフォルトは無効です。
Ports	設定するポート範囲を入力します。

[Apply]をクリックすると、次の[Access Rule List]ウィンドウが表示されます:

The screenshot shows the 'Access Rule List' window with the following details:

Profile ID	Access ID	Profile Type	Action
1	1	Ethernet	Permit

Buttons at the top: << Back, Add Rule, Show Details, Delete Rules.

Buttons at the bottom: << Back, Next >>.

事前に構成した規則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[Access Rule Detail Information]ウィンドウが表示されます:

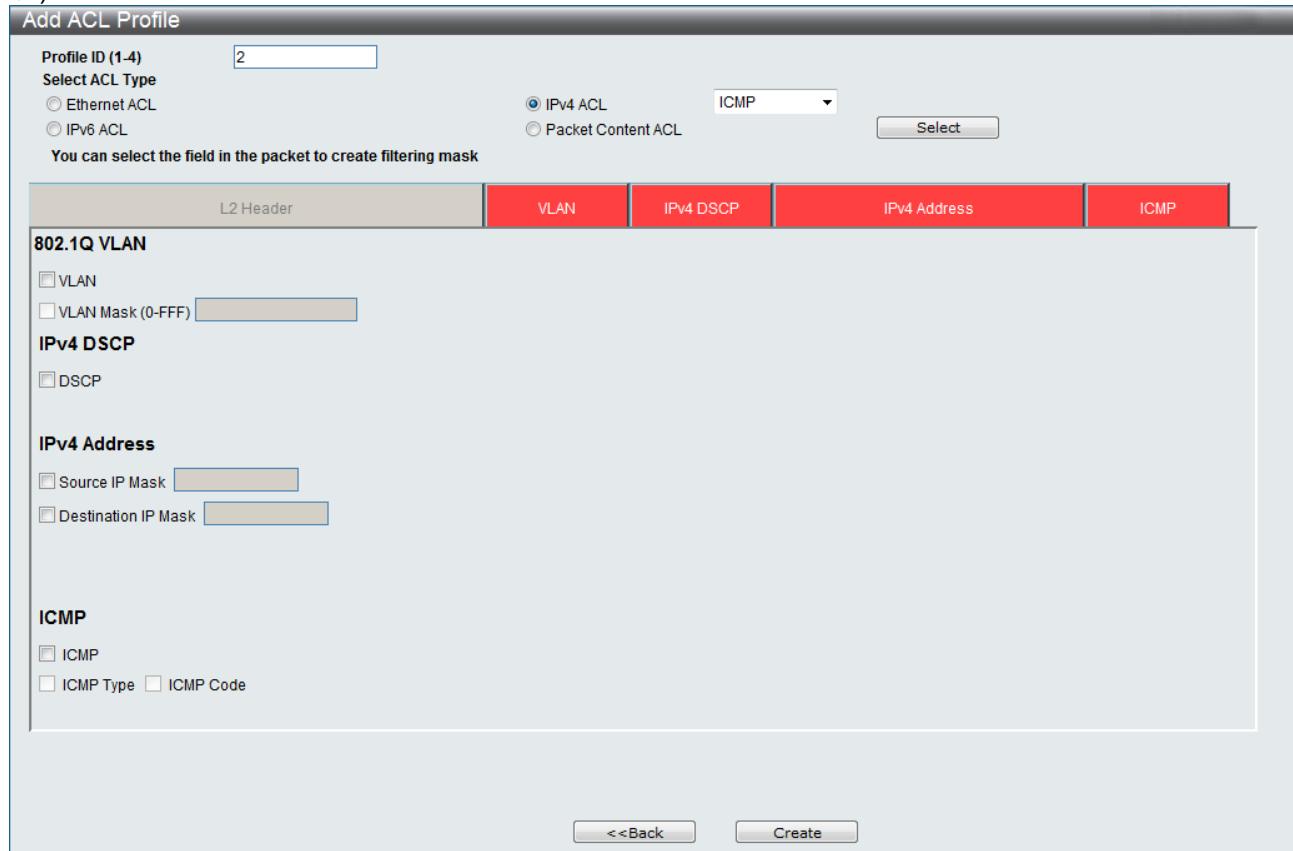
The screenshot shows the 'Access Rule Detail Information' window with the following details:

ACL Rule Details	
Profile ID	1
Access ID	1
Profile Type	Ethernet
VLAN ID	1
Action	Permit
Ports	2

Buttons at the bottom: Show All Rules.

3.7.3 Access profile list - IPv4 ACL

IPv4 ACLを作成するには、[Access Profile List]ウィンドウにある[Add ACL Profile]をクリックし、次に、プルダウンメニューから1~256のプロファイルIDを選択した後、[IPv4 ACL]ラジオボタンをクリックします。次に、プルダウンメニューからプロトコル([ICMP]、[IGMP]、[TCP]、[UDP]、[Protocol ID])を選択します。[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)：



ウィンドウの一番上近くにあるボックスをクリックします。ボックスの色が赤に変わり、構成用のパラメーターが表示されます。新しいエントリーを追加するには、正しい情報を入力して、[Create]をクリックします。[Access Profile List]ウィンドウに戻るには、[<<Back]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	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ェックを入れて、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できます。 Source Port Mask (0-FFFF) - フィルタ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。

[Apply]をクリックして変更を適用します。

[Create]をクリックすると、下の[Access Profile List]ウィンドウに、新しいアクセスプロファイル一覧エントリーが表示されます。その他のアクセスプロファイルを追加するには、[Add ACL Profile]をクリックします。プロファイルを削除するには、相応する[Delete]ボタンをクリックします。エントリーの指定の設定を表示するには、[Show Details]をクリックします。

アクセスプロファイルエントリーに規則を追加するには、[Add/View Rules]をクリックします。

The screenshot shows the 'Access Rule List' window. At the top, there are buttons for '<< Back' and 'Add Rule', and a message 'Consumed HW Entries: 193'. Below is a table with the following data:

Profile ID	Access ID	Profile Type	Action
2	1	IP	Permit

At the bottom right are buttons for 'Show Details', 'Delete Rules', and page navigation '1/1 1 Go'.

事前に設定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：

The screenshot shows the 'Access Profile Detail Information' window. It displays the following details for Profile ID 2:

- Profile ID: 2
- Profile Type: IP
- DSCP: Yes
- ICMP: Yes

At the bottom left is a 'Show All Profiles' button.

[Access Profile List]ウィンドウに戻るには、[Show All Profiles]をクリックします。事前に設定したエントリーに規則を追加するには、対応する[Add/View Rules]をクリックして、[Access Rule List]ウィンドウにある[Add Rule]をクリックします。次のウィンドウが表示されます：

The screenshot shows the 'Add Access Rule' window. It has two main sections: 'Profile Information' and 'Rule Detail'.

Profile Information:

- Profile ID: 2
- Profile Type: IP
- DSCP: Yes
- ICMP: Yes

Rule Detail: (Keep the input field blank to specify that the corresponding option does not matter).

- Access ID (1-256): 1 (with 'Auto Assign' checked)
- DSCP: (empty input field)
- ICMP: (checkbox checked)
- Rule Action:
 - Action: Permit (selected)
 - Priority (0-7): (empty input field)
 - Replace Priority: (checkbox checked)
 - Replace DSCP (0-63): (empty input field)
 - Counter: (empty input field)
 - Ports: (empty input field)

At the bottom right are '<< Back' and 'Apply' buttons.

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
Access ID (1-256)	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1~256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アドレスの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アドレスの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。
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 - 各フレームのICMPタイプフィールドを確認するように指定します。 ICMP Code - 各フレームの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(0xFFFF) - 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(0xFFFF) - 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(0xFFFF) - 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(0xFFFF) - 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	[Permit]を選択して、追加した規則に従って、アクセスプロファイルと一致するパケットをスイッチで転送することを指定します。 [Deny]を選択して、アクセスプロファイルと一致するパケットをスイッチで転送せずに、ドロップすることを指定します。 [Mirror]を選択して、アクセスプロファイルと一致するパケットを、ミラーポートに転送します。

パラメーター	説明
	ポートの構成コマンドで定義したポートにミラーすることを指定します。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	カウンター設定を有効または無効にします。
Ports	設定するポートの範囲を入力します。

[Apply]をクリックすると、次の[Access Rule List]ウィンドウが表示されます:

The screenshot shows the 'Access Rule List' window with the following details:

- Buttons: << Back, Add Rule.
- Table Headers: Profile ID, Access ID, Profile Type, Action.
- Table Data: 1 row with values 2, 1, IP, Permit.
- Buttons: Show Details, Delete Rules.
- Navigation: << Back, Next >>.

事前に構成した規則の設定を表示するには、相応する[Show Details]をクリックします。次の[Access Rule Detail Information]ウィンドウが表示されます:

The screenshot shows the 'Access Rule Detail Information' window with the following details:

ACL Rule Details

Profile ID	2
Access ID	1
Profile Type	IP
Action	Permit
Ports	3
DSCP	3
ICMP	Yes

Show All Rules

3.7.4 Access profile list - IPv6 ACL

IPv6 ACLを作成するには、[Access Profile List]ウィンドウにある[Add ACL Profile]をクリックし、次に、プルダウンメニューから1~4のプロファイルIDを選択して、[IPv6 ACL]ラジオボタンをクリックします。次に、プルダウンメニューからプロトコル(TCPまたはUDP)を選択します。

[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またはUDPのどちらを選択したかによって異なります)：

Add ACL Profile

Profile ID (1-4) 3

Select ACL Type

Ethernet ACL IPv4 ACL
 IPv6 ACL Packet Content ACL

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

IPv6 Class

IPv6 Class

IPv6 Flow Label

IPv6 Flow Label

TCP

TCP
 Source Port Mask (0-FFFF)
 Destination Port Mask (0-FFFF)

IPv6 Address

IPv6 Source Mask
 IPv6 Destination Mask

<< Back Create

ウィンドウの一番上にあるボックスをクリックします。ボックスの色が赤に変わり、設定用のパラメーターが表示されます。新しいエントリーを追加するには、正しい情報を入力して、[Create]をクリックします。[Access Profile List]ウィンドウに戻るには、[<<Back]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
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。
IPv6 TCP	このボックスにチェックを入れて、TCP トラフィックに規則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]にチェックを入れて入力できます。
IPv6 UDP	このボックスにチェックを入れて、UDP トラフィックに規則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]にチェックを入れて入力できます。
ICMP	このボックスにチェックを入れて、ICMP プロトコルフィールドを確認します。 ICMP Type をチェックすると、ICMP タイプ値を ACL ルールに適用します。 ICMP Code をチェックすると、ICMP コード値を ACL ルールに適用します。

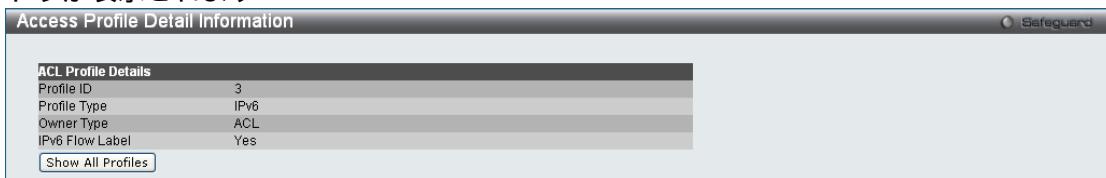
[Select]をクリックして ACL タイプを指定します。

[Create]をクリックしてプロファイルを作成します。

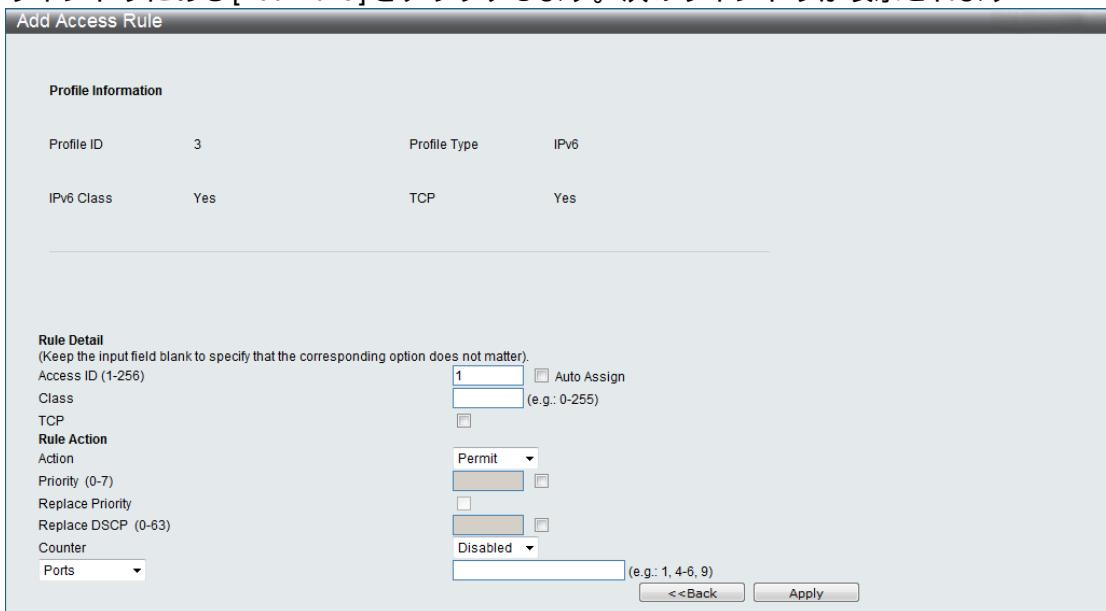
[<<Back]をクリックして前のページに戻ります。

[Create]をクリックすると、下の[Access Profile List]ウィンドウに、新しいアクセスプロファイル一覧エントリーが表示されます。 さらにアクセスプロファイルを追加するには、[Add ACL Profile]をクリックします。 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。 すべてのエントリーを削除するには、[Delete All]をクリックします。 エントリーした設定を表示するには、[Show Details]をクリックします。

事前に設定したエントリーを表示するには、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。事前に設定したエントリーに規則を追加するには、相応する[Add/View Rules]をクリックして、[Access Rule List] ウィンドウにある[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 (1-256)	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 に設定します。 Auto Assign - このチェックボックスにチェックを入れ、作成している規則に対し、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-FFFFF 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。
IPv6 Destination Address	IPv6宛先アドレスを指定します。
IPv6 Destination Mask	IPv6 宛先サブマスクを指定します。

パラメーター	説明
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。
ICMP	ICMP プロトコルフィールドを確認するように指示します。 ICMP Type - スイッチはフレームの ICMP タイプフィールドをチェックします。 ICMP Code - スイッチはフレームの ICMP コードフィールドをチェックします。
Action	[Permit]を選択して、追加した規則に従って、アクセスプロファイルと一致するパケットをスイッチで転送することを指定します。 [Deny]を選択して、アクセスプロファイルと一致するパケットをスイッチで転送せずに、ドロップすることを指定します。 [Mirror]を選択して、アクセスプロファイルと一致するパケットを、ミラーポートの構成コマンドで定義したポートにミラーすることを指定します。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	カウンター設定を有効または無効にします。
Ports	構成するポートの範囲を入力します。

[Apply]をクリックすると、次の[Access Rule List]ウィンドウが表示されます:

The screenshot shows the 'Access Rule List' window with the following details:

- Buttons: << Back, Add Rule.
- Table Headers: Profile ID, Access ID, Profile Type, Action.
- Table Data: Profile ID: 3, Access ID: 1, Profile Type: IPv6, Action: Permit.
- Buttons: Show Details, Delete Rules.
- Navigation: << Back, Next >>.

事前に構成した規則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[Access Rule Detail Information]ウィンドウが表示されます:

The screenshot shows the 'Access Rule Detail Information' window with the following details:

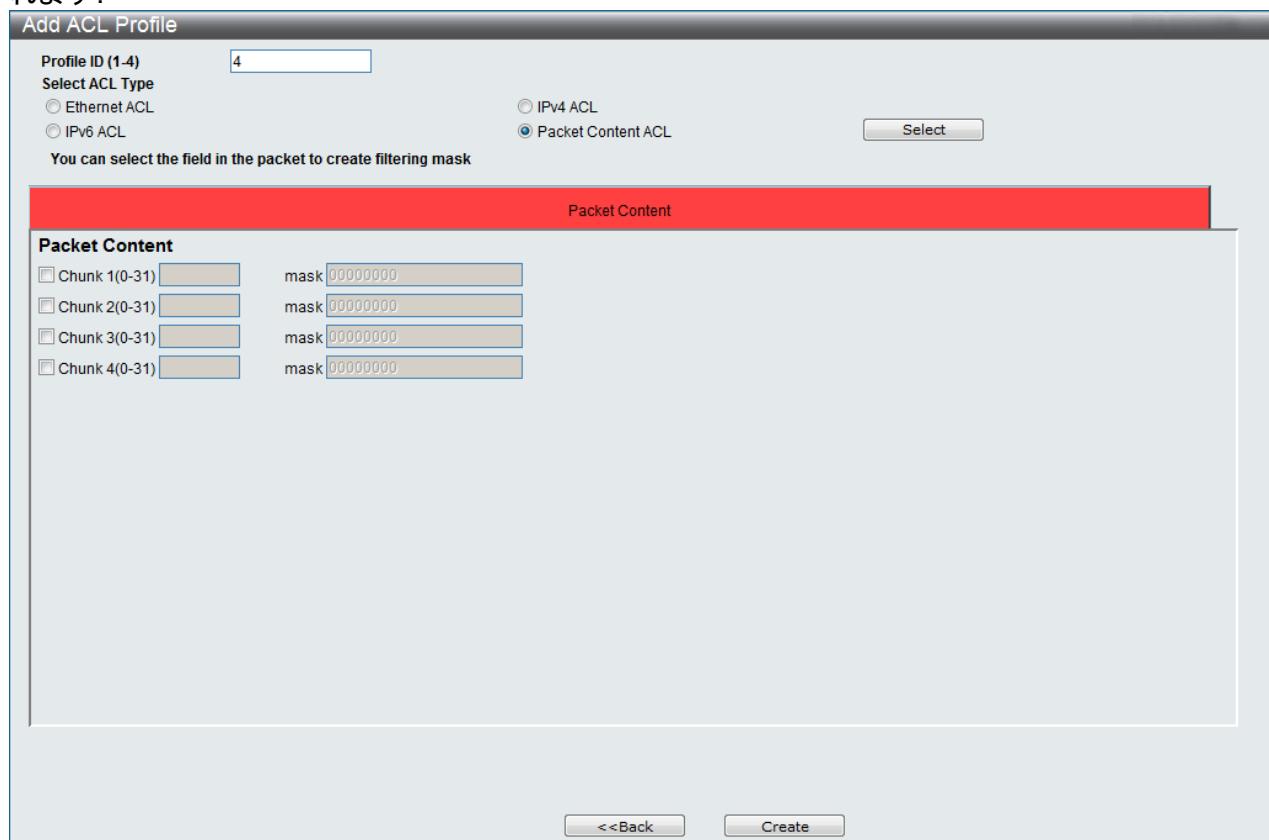
ACL Rule Details

Profile ID	3
Access ID	1
Profile Type	IPv6
Action	Permit
Ports	4
IPv6 Class	30
TCP	Yes

Buttons: Show All Rules.

3.7.5 Access profile list-Packet content ACL

パケット内容を確認する ACL を作成するには、[Access Profile List] ウィンドウにある [Add ACL Profile] をクリックし、プルダウンメニューからプロファイル ID を 1~4 から選択して、[Packet Content ACL] ラジオボタンをクリックします。[Select] をクリックすると、次のウィンドウが表示されます：



ウィンドウの一番上にあるボックスをクリックします。ボックスの色が赤に変わり、設定用のパラメーターが表示されます。新しいエントリーを追加するには、正しい情報を入力して、[Create]をクリックします。[Access Profile List] ウィンドウに戻るには、[<<Back]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
Packet Content	<p>最大 4 までのオフセットを指定することができます。</p> <p>Chunk 1 (0-31) _____マスク_____、 Chunk 2 (0-31) _____マスク_____、 Chunk 3 (0-31) _____マスク_____、 Chunk 4 (0-31) _____マスク_____、</p> <p>この高度かつ独自の Packet Content ACL を使用することで、スイッチは、今日急増している一般 ARP アドレス偽装攻撃などのネットワーク攻撃を効果的に軽減します。Packet Content ACL は、異なるプロトコルレイヤー内のパケットの指定した内容を確認することができます</p>

[Select]をクリックして ACL タイプを選択します。

[Create]をクリックしてプロファイルを作成します。

[<< Back]をクリックして前のページに戻ります。

[Create]をクリックすると、下の[Access Profile List]ウィンドウに、新しいアクセスプロファイル一覧エントリーが表示されます。さらにアクセスプロファイルを追加するには、[Add ACL Profile]をクリックします。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。すべてのエントリーを削除するには、[Delete All]をクリックします。エントリーした構成を表示するには、[Show Details]をクリックします。アクセスプロファイルエントリーに規則を追加するには、[Add/View Rules]をクリックします。

Access Profile List

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

事前に設定したエントリーを表示するには、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 Detail Information

ACL Profile Details	
Profile ID	4
Profile Type	Packet Content
Chunk 1	2, Value: 0x00000000

Show All Profiles

[Access Profile List] ウィンドウに戻るには、[Show All Profiles] をクリックします。事前に設定したエントリーに規則を追加するには、相応する [Add/View Rules] をクリックして、[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
Chunk 1	1, Value: 0x00000000	Chunk 2	2, Value: 0x00000000
Chunk 3	3, Value: 0x00000000	Chunk 4	4, Value: 0x00000000

Rule Detail
(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-256)
Chunk 1
Chunk 2
Chunk 3
Chunk 4

Mask
Mask
Mask
Mask

Auto Assign
□

Rule Action

Action
Priority (0-7)
Replace Priority
Replace DSCP (0-63)
Counter
Ports ▾

Permit
Disabled
□
□

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

<< 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
Access ID (1-256)	アクセス用の固有識別子番号を入力します。この値は1~256の範囲で設定します。
Offset(1-4)	それぞれのUDFフィールドは4バイトデータであり、オフセットリファレンスからnバイト離れています。ここでnはオフセット値のことです。 合計で4つのパケットコンテンツフィールドはパケットの最初の128バイトから選択可能です。最初のオフセットは2で始まります。パケットコンテンツフィールドは重複できません。そして、それぞれのフィールドは4バイトであるのでとれるオフセット値は2、6、10、14、18、22、26、30、34、…、126となります。
Action	[Permit]を選択して、追加した規則に従って、アクセスプロファイルと一致するパケットをスイッチで転送します。 [Deny]を選択して、アクセスプロファイルと一致するパケットをスイッチで転送せずに、ドロップします。 [Mirror]を選択して、アクセスプロファイルと一致するパケットを、ミラーポートを定義したポートにミラーします。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。
Counter	このACL規則のカウンターを有効または無効にします。
Ports	設定するポートの範囲を入力します。

[Apply]をクリックすると、次の[Access Rule List]ウィンドウが表示されます:

The screenshot shows the 'Access Rule List' window with the following details:

- Buttons: << Back, Add Rule.
- Table Headers: Profile ID, Access ID, Profile Type, Action.
- Table Data: A single row with values 4, 1, Packet Content, Permit.
- Buttons: Show Details, Delete Rules.
- Navigation: << Back, Next >>.

事前に設定した規則を表示するには、相応する[Show Details]をクリックします。次のアクセス規則詳細情報ウィンドウが表示されます:

The screenshot shows the 'Access Rule Detail Information' window with the following details:

ACL Rule Details

Profile ID	4
Access ID	1
Profile Type	Packet Content
Action	Permit
Ports	5
Chunk 1	2, Value: 0x00000000, Mask: 0x00000000

Buttons: Show All Rules.

3.7.6 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。

The screenshot shows the 'ACL Finder' window. At the top, there is a message: 'The ACL rule finder helps you to identify any rules that have been assigned to a specific port.' Below this are three dropdown menus: 'Profile ID' set to 'Any', 'Port' with an empty input field, and 'State' set to 'Normal'. To the right of these is a 'Find' button. The main area is a table with the following columns: Profile ID, Access ID, Profile Type, Summary, and Action. There are four rows of data:

Profile ID	Access ID	Profile Type	Summary	Action
1	1	Ethernet	VLAN,802.1p	Permit
2	1	IP	DSCP,ICMP	Permit
3	1	IPv6	IPv6 Class,TCP	Permit
4	1	Packet Content	Chunk 1	Permit

At the bottom left is a 'Delete' button, and at the bottom right are pagination controls '1/1' and '1' with a 'Go' 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
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。
State	プルダウンメニューで状態を選択します。 Normal - 閲覧が許可されている通常の ACL ルール

3.7.7 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する ACL 規則を作成して、メータリング規則を作成し、この ACL 規則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規則のために、メータリング規則に関連付けることのできない ACL 規則もあります。

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

The screenshot shows the 'ACL Flow Meter' window. At the top, there are two input fields for 'Profile ID' and 'Access ID (1-256)', and a 'Find' button. Below these are three buttons: 'Add', 'View All', and 'Delete All'. The main area is a table with columns: Profile ID, Access ID, and Mode. There is one row of data:

Profile ID	Access ID	Mode
1	1	Meter

At the bottom right are pagination controls '1/1' and '1' with a 'Go' 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
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 (1-256)	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。ユーザーはここで構成できます：

ACL Flow Meter Configuration			
<input checked="" type="radio"/> Profile ID (1-4)			
Access ID (1-256)			
Mode	Rate	Rate (Kbps)	(1-1048576)
		Burst Size (Kbyte)	(1-262144)
		Rate Exceeded	<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	フローメーター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 (1-256)	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。1~256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 4 ~ 16,384 です。単位は Kbyte です。
Rate Exceed	Drop Packet - 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 Meter]ウィンドウに戻ります。

[View]をクリックすると、次の[ACL Flow Meter Display]ウィンドウが表示されます：

ACL Flow Meter Display			
Profile ID	1		
Access ID	1		
Mode	Rate	Rate (Kbps)	120
		Burst Size (Kbyte)	120
		Rate Exceeded	Remark DSCP
<<Back			

[<< Back]をクリックして前のページに戻ります。

3.8 Monitoring

3.8.1 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ーケーブルの詳細が表示されます。ツイストペアー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：

The screenshot shows the 'Cable Diagnostics' window. At the top, there are dropdown menus for 'From Port' (set to 01) and 'To Port' (set to 01), and a 'Test' button. Below this is a table with columns: Port, Type, Link Status, Test Result, and Cable Length(M). A single row is shown for port 1, which is a 1000BASE-T type, Link Up, Test Result OK, and Cable Length 3 meters. Below the table, a note states: '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.' A note also says: 'The Cable Fault Distance is calculated from switch side.'

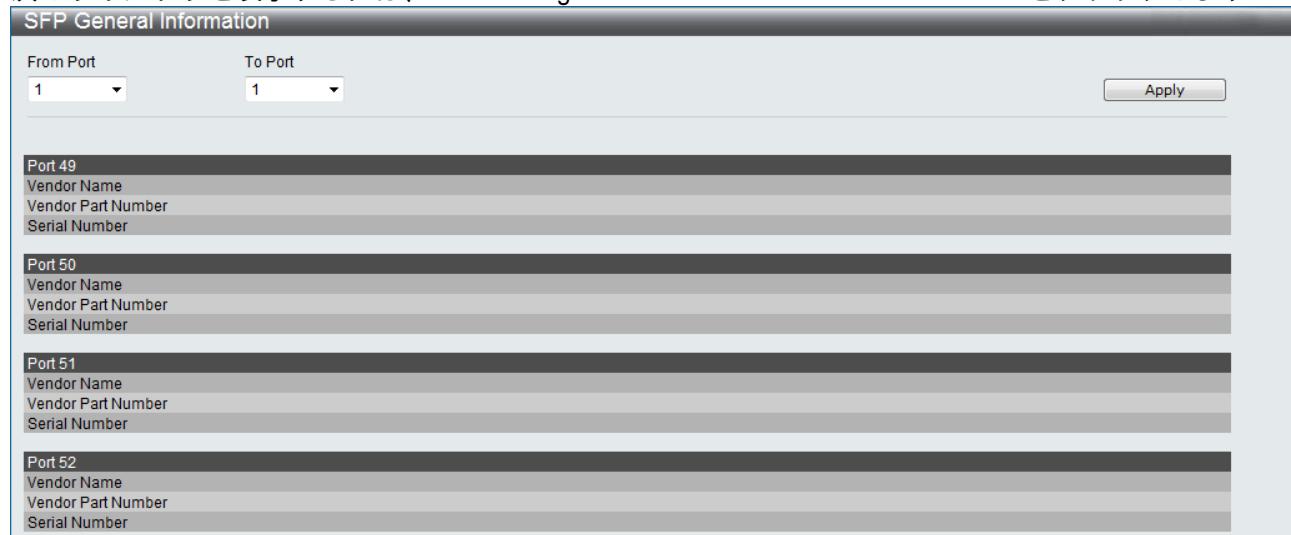
Port	Type	Link Status	Test Result	Cable Length(M)
1	1000BASE-T	Link Up	OK	3

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。

3.8.2 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. It has dropdown menus for 'From Port' (1) and 'To Port' (1), and an 'Apply' button. Below these are four sections, each corresponding to a different SFP port: Port 49, Port 50, Port 51, and Port 52. Each section contains fields for Vendor Name, Vendor Part Number, and Serial Number.

Port	Vendor Name	Vendor Part Number	Serial Number
Port 49			
Port 50			
Port 51			
Port 52			

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。

[Apply]をクリックして SFP 情報を表示させます。

3.8.3 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. At the top, there are dropdown menus for 'From Port' (set to 1) and 'To Port' (set to 1), and an 'Apply' button. Below this is a table with three columns: 'Port', 'TX Power (dBm)', and 'RX Power (dBm)'. The table lists ports 49, 50, 51, and 52, with empty rows for TX and RX power.

Port	TX Power (dBm)	RX Power (dBm)
49		
50		
51		
52		

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。

3.8.4 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：

CPU Utilization Notify Settings

CPU Utilization Notify Current Status	NORMAL
CPU Utilization Notify State	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Threshold (20% ~ 100%)	100 %
Polling Interval (10 ~ 300)	60 sec
Trap State	Disabled
Log State	Enabled

Apply

[Apply]をクリックして変更を適用します。

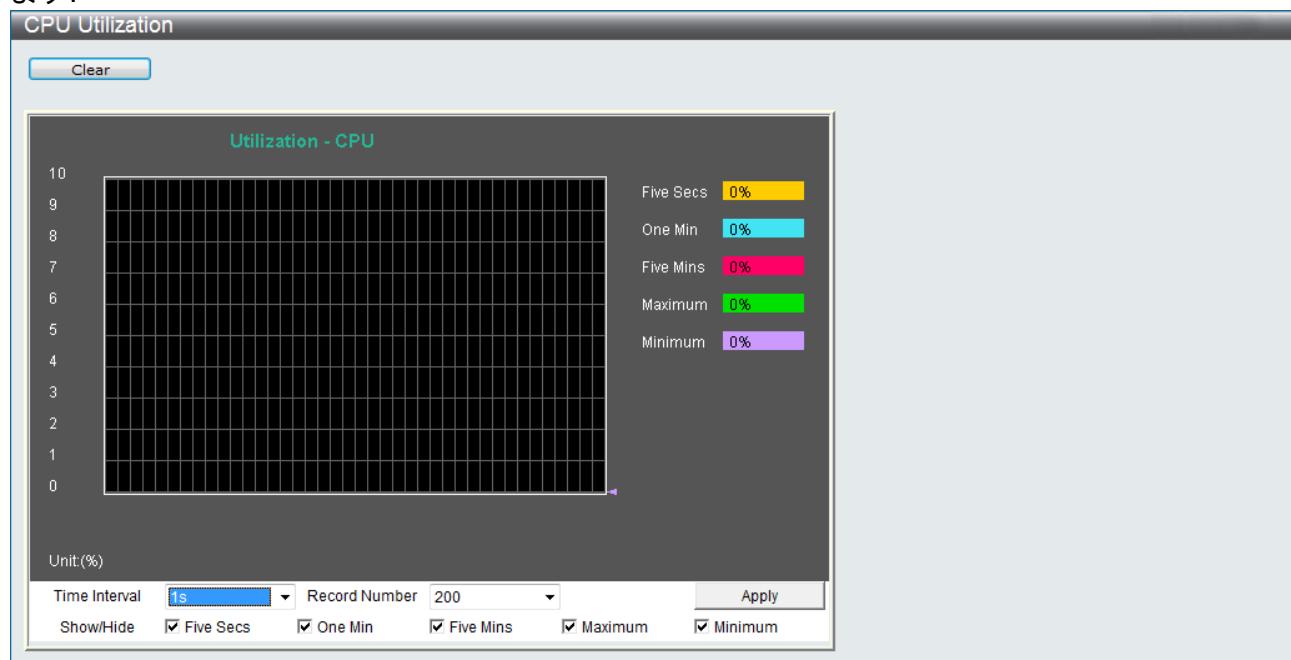
下記にパラメーターの説明を記載します。

パラメーター	説明
CPU Utilization Notify State	CPU 使用率通知機能の有効または無効を指定します。
Threshold (20-100)	CPU 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)	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	CPU 使用率の状態遷移による SNMP トラップ出力を有効または無効に指定します。デフォルトは無効です。
Log State	CPU 使用率の状態遷移によるログ出力を有効または無効に指定します。デフォルト値は有効です。

3.8.5 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：



CPU 使用率をポート別に表示するには、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します。[Apply]をクリックして設定を適用します。 ウィンドウは新しく更新した統計で自動的に更新されます。

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
Time Interval	1 ~ 60 秒から希望する設定を選択します。デフォルト値は 1 秒です。
Record Number	記録する回数を 20 ~ 200 から選択します。デフォルト値は 200 です。
Show/Hide	[Five Secs]、[One Min]、[Five Mins] 表示間隔を指定します。

3.8.6 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：

DRAM Utilization Notify Current Status NORMAL

DRAM Utilization Notify State Disabled Enabled
Threshold (20% ~ 100%) 100 %
Polling Interval (10 ~ 300) 60 sec
Trap State Disabled
Log State Enabled

Apply

[Apply]をクリックして変更を適用します。

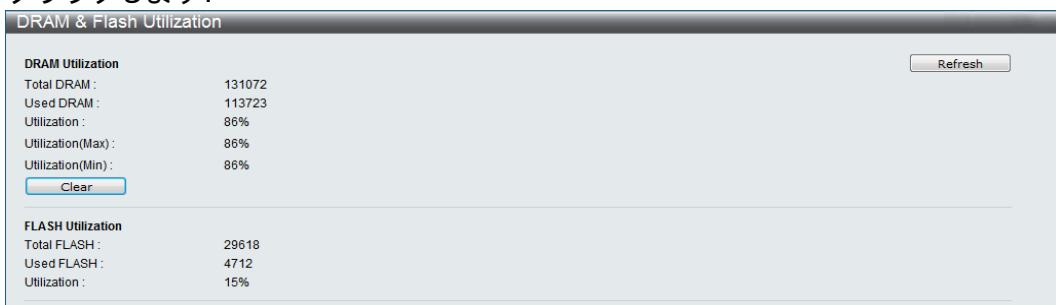
下記にパラメーターの説明を記載します。

パラメーター	説明
DRAM Utilization Notify State	DRAM 使用率通知機能の有効または無効を指定します。
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	DRAM 使用率の状態遷移による SNMP トラップ出力を有効または無効に指定します。デフォルト設定は無効です。
Log State	DRAM 使用率の状態遷移によるログ出力を有効または無効に指定します。 デフォルト設定は有効です。

3.8.7 DRAM & FLASH Utilization

このウィンドウは、DRAM およびフラッシュのメモリ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：



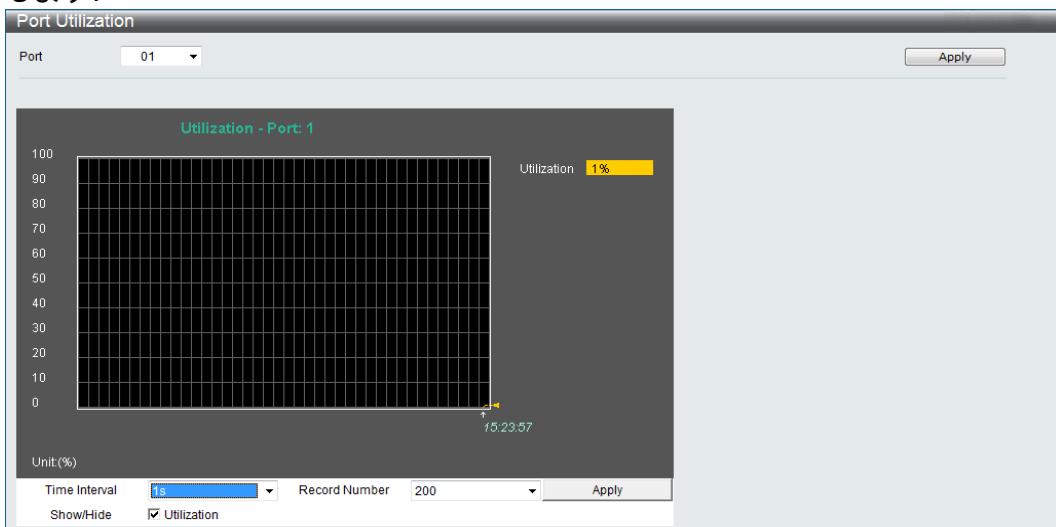
[Refresh]をクリックして画面に表示されるリストを更新します。

[Clear]をクリックして DRAM の使用率統計情報を初期化します。

3.8.8 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 > Utilization Notify > Port Utilization をクリックします：



[Apply]をクリックして変更を適用します。

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。

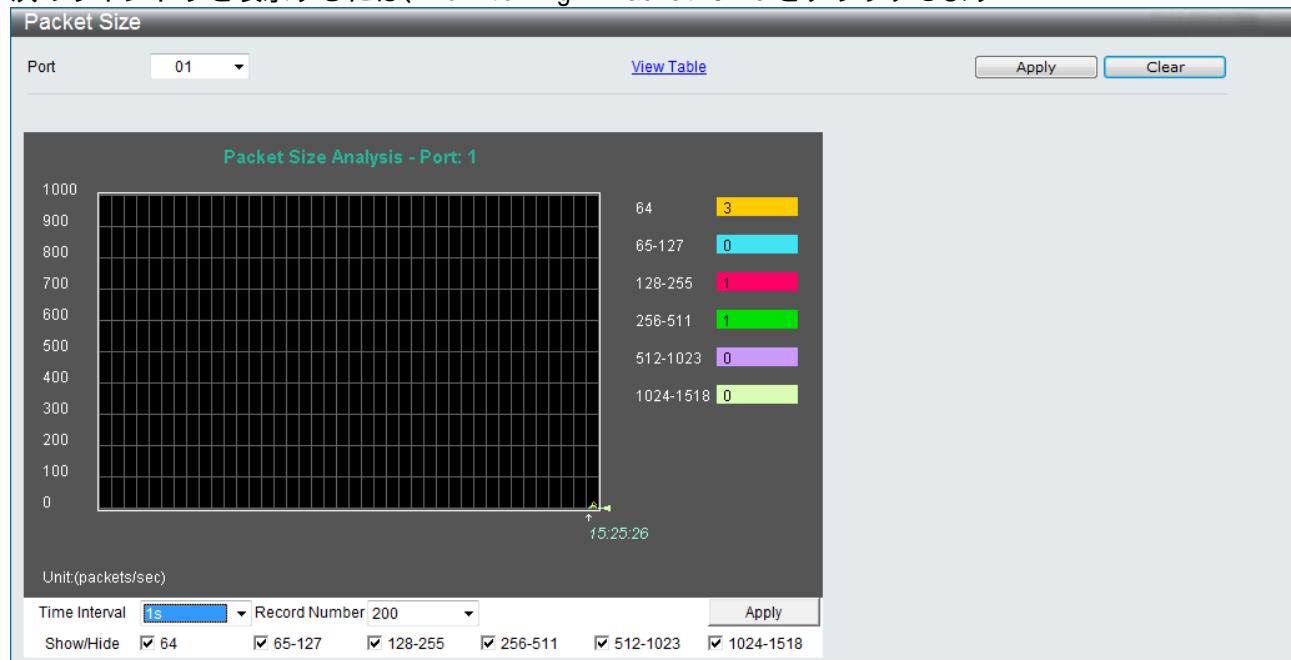
下記にパラメーターの説明を記載します。

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。
Time Interval	1 ~ 60 秒から希望する設定を選択します。デフォルト値は 1 秒です。
Record Number	記録する回数を 20 ~ 200 から選択します。デフォルト値は 200 です。
Show/Hide	使用率を表示する場合にチェックを入れます。

3.8.9 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：



[Apply]をクリックして変更を適用します。

[Packet Size Table]ウィンドウを表示するには、View Tableをクリックします。次のテーブルが表示されます：

The screenshot shows the 'Packet Size Table' interface for Port 1. It has a similar header with 'Port' set to '01', 'View Graphic' button, and 'Apply' and 'Clear' buttons. The main area displays a table of frame sizes and their counts over a 1-second interval. The table has columns for 'Frame Size', 'Frame Counts', and 'Frames/sec'. The data is as follows:

Frame Size	Frame Counts	Frames/sec
64	19240	28
65-127	611	2
128-255	6376	6
256-511	4313	4
512-1023	5688	17
1024-1518	6967	15

[Apply]をクリックして変更を適用します。

[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。
Time Interval	1~60 秒から希望する設定を選択します。デフォルト値は 1 秒です。
Record Number	スイッチを記録する回数を 20~200 から選択します。デフォルト値は 200 です。
64	長さが 64 オクテット(フレーミングビットは含みません。ただし、FCS オクテットは含みます)の受信パケットの合計数です(不良パケットを含みます)。
65-127	長さが 65~127 オクテット(フレーミングビットは含みません。ただし、FCS オクテットは含みます)の受信パケットの合計数です(不良パケットを含みます)。
128-255	長さが 128~255 オクテット(フレーミングビットは含みません。ただし、FCS オクテットは含みます)の受信パケットの合計数です(不良パケットを含みます)。
256-511	長さが 256~511 オクテット(フレーミングビットは含みません。ただし、FCS オクテットは含みます)の受信パケットの合計数です(不良パケットを含みます)。
512-1023	長さが 512~1023 オクテット(フレーミングビットは含みません。ただし、FCS オクテットは含みます)の受信パケットの合計数です(不良パケットを含みます)。
1024-1518	長さが 1024 ~ 1518 オクテット(フレーミングビットは含みません。ただし、FCS オクテットは含みます)の受信パケットの合計数です(不良パケットを含みます)。
Show/Hide	64、65-127、128-255、256-511、512-1023、1024-1518 の受信パケットを表示する場合に選択します。
Clear	このウィンドウ上のすべての統計カウンターを消去します。
View Table	テーブルを表示します。
View Graphic	折れ線グラフを表示します。

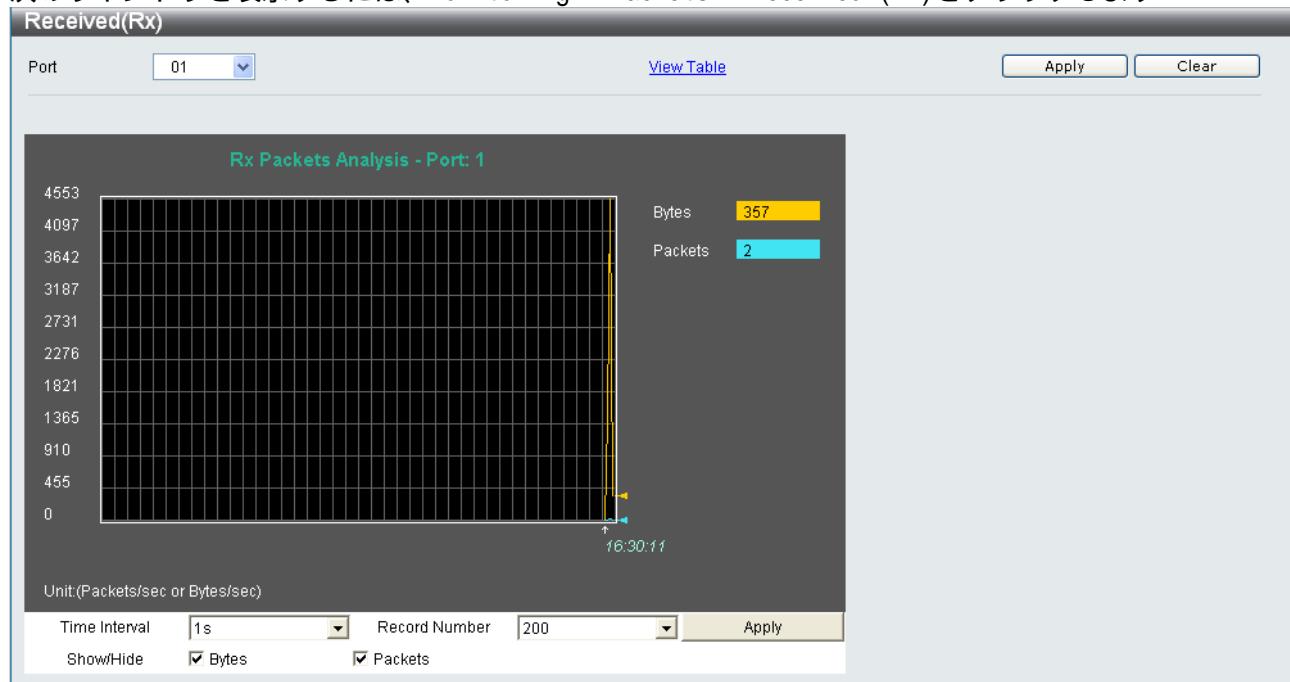
[Apply]をクリックして変更を適用します。

3.8.10 Packets

3.8.10.1 Received (Rx)

これらのウィンドウには、スイッチ上の受信パケットが表示されます。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 > Received (Rx)をクリックします：



[Apply]をクリックして変更を適用します。

[Clear]をクリックしてデータを初期化します。

[Received (Rx) Table]ウィンドウを表示するには、View Tableをクリックします。

The figure shows the 'Received (Rx) Table' window for Port 1. At the top, there is a dropdown menu for 'Port' set to '01'. To the right are 'View Graphic', 'Apply', and 'Clear' buttons. Below this is a table with various statistics. The table has three main sections: RX Packets, TX Packets, and a section for Unicast, Multicast, and Broadcast traffic. The RX Packets section shows a total of 2946410 bytes and 22921 packets per second. The TX Packets section shows a total of 15826054 bytes and 21743 packets per second. The traffic type section shows 18009 unicast packets, 81 multicast packets, and 4831 broadcast packets per second. At the top of the table, there is a 'Time Interval' dropdown set to '1s' and an 'OK' button. The table has alternating row colors (yellow and blue).

RX Packets		
	Total	Total/sec
Bytes	2946410	2913
Packets	22921	21
TX Packets		
	Total	Total/sec
Bytes	15826054	27250
Packets	21743	30
Unicast		
	Total	Total/sec
Bytes	18009	21
Multicast		
	Total	Total/sec
Bytes	81	0
Broadcast		
	Total	Total/sec
Bytes	4831	0

[Apply]をクリックして変更を適用します。

[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。
Time Interval	1~60秒から希望する設定を選択します。デフォルト値は1秒です。
Record Number	記録する回数を20~200から選択します。デフォルト値は200です。
Bytes	ポート上で受信したバイト数をカウントします。
Packets	ポート上で受信したパケット数をカウントします。
Unicast	ユニキャストアドレスで受信したパケットの合計数をカウントします。
Multicast	マルチキャストアドレスで受信したパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスで受信したパケットの合計数をカウントします。
Show/Hide	バイトとパケットを表示するかどうかにチェックを入れます。
View Table	テーブルを表示します。
View Graphic	折れ線グラフを表示します。

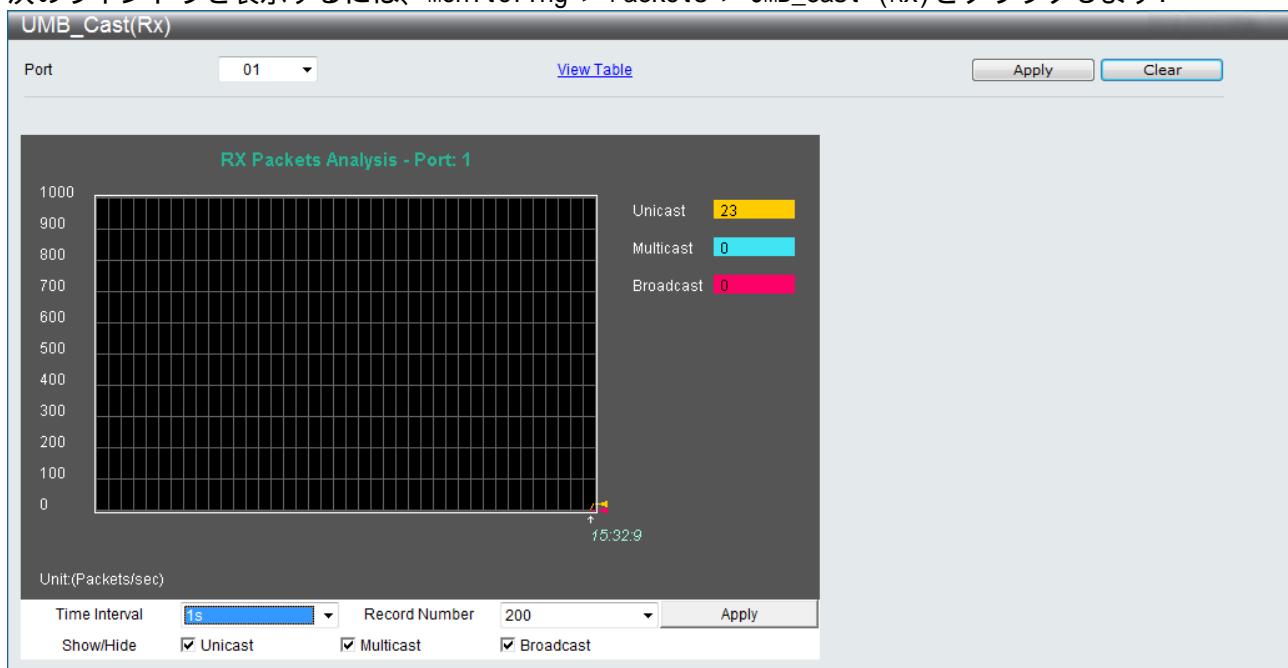
[Apply]をクリックして変更を適用します。

[Clear]をクリックしてデータを初期化します。

3.8.10.2 UMB_cast(Rx)

スイッチ上のUMB_cast Rx パケットが表示されます。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 > UMB_cast (Rx)をクリックします：



[Apply]をクリックして変更を適用します。

[Clear]をクリックしてデータを初期化します。

[UMB_cast (Rx) Table] ウィンドウを表示するには、View Table をクリックします。

UMB_cast(RX) Table		
Port	01	View Graphic
Time Interval <input type="button" value="1s"/> <input type="button" value="OK"/>		
RX Packets	Total	Total/sec
Bytes	3065667	5412
Packets	23755	37
RX Packets	Total	Total/sec
Unicast	18733	37
Multicast	81	0
Broadcast	4941	0
TX Packets	Total	Total/sec
Bytes	16108526	50117
Packets	22371	57

[Apply]をクリックして変更を適用します。

[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。
Time Interval	1~60秒から希望する設定を選択します。デフォルト値は1秒です。
Record Number	記録する回数を20~200から選択します。デフォルト値は200です。
Unicast	ユニキャストアドレスで受信したパケットの合計数をカウントします。
Multicast	マルチキャストアドレスで受信したパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスで受信したパケットの合計数をカウントします。
Show/Hide	マルチキャストパケット、ブロードキャストパケット、および、ユニキャストパケットを表示するかどうかにチェックを入れます。
View Table	テーブルを表示します。
View Graphic	折れ線グラフを表示します。

3.8.10.3 Transmitted (Tx)

これらのウィンドウには、スイッチ上の送信済み(Tx)パケットが表示されます。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 > Transmitted (Tx)をクリックします：



[Apply]をクリックして変更を適用します。

[Clear]をクリックしてデータを初期化します。

[Transmitted (Tx) Table]ウィンドウを表示するには、View Tableをクリックします。

The screenshot shows a table titled "Transmitted (Tx) Table" for Port 01. It displays three sections of statistics:

RX Packets		
	Total	Total/sec
Bytes	3188474	3797
Packets	24619	25

RX Packets		
	Total	Total/sec
Unicast	19480	25
Multicast	81	0
Broadcast	5058	0

TX Packets		
	Total	Total/sec
Bytes	16393587	28997
Packets	23019	36

[Apply]をクリックして変更を適用します。

[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。

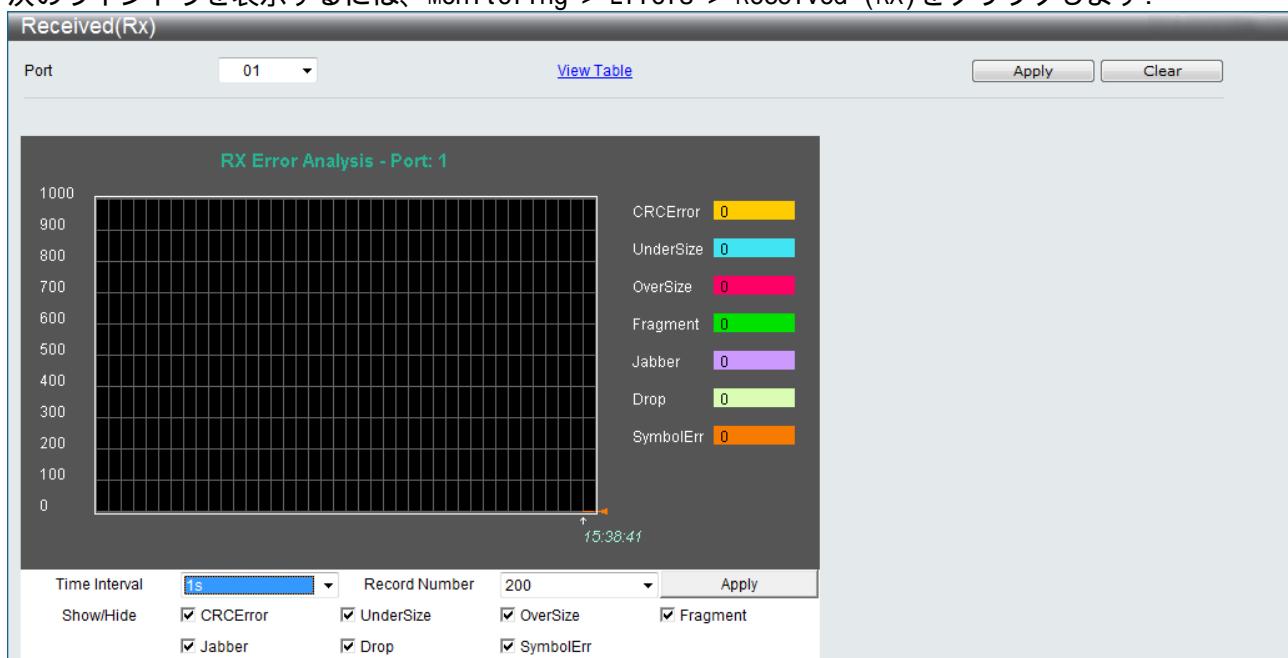
パラメーター	説明
Port	プルダウンメニューから、統計を表示するポートを選択します。
Time Interval	1~60秒から希望する設定を選択します。デフォルト値は1秒です。
Record Number	記録する回数を20~200から選択します。デフォルト値は200です。
Bytes	ポート上で正常に送信したバイト数をカウントします。
Packets	ポート上で正常に送信したパケット数をカウントします。
Unicast	ユニキャストアドレスで送信したパケットの合計数をカウントします。
Multicast	マルチキャストアドレスで送信したパケットの合計数をカウントします。
Broadcast	プロードキャストアドレスで送信したパケットの合計数をカウントします。
Show/Hide	バイトとパケットを表示するかどうかにチェックを入れます。
View Table	テーブルを表示します。
View Graphic	折れ線グラフを表示します。

3.8.11 Errors

3.8.11.1 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：



[Apply]をクリックして変更を適用します。

[Clear]をクリックしてデータを初期化します。

[Received (Rx) Table] ウィンドウでエラーを表示するには、View Table をクリックします。次のテーブルが表示されます：

Received(Rx) Table				
Port	01	View Graphic	Apply	Clear
Time Interval				1s OK
RX Error				RX Frame
CRCError				0
UnderSize				0
OverSize				0
Fragment				0
Jabber				0
Drop				0
Symbol				0

[Apply]をクリックして変更を適用します。

[Clear]をクリックしてデータを初期化します。

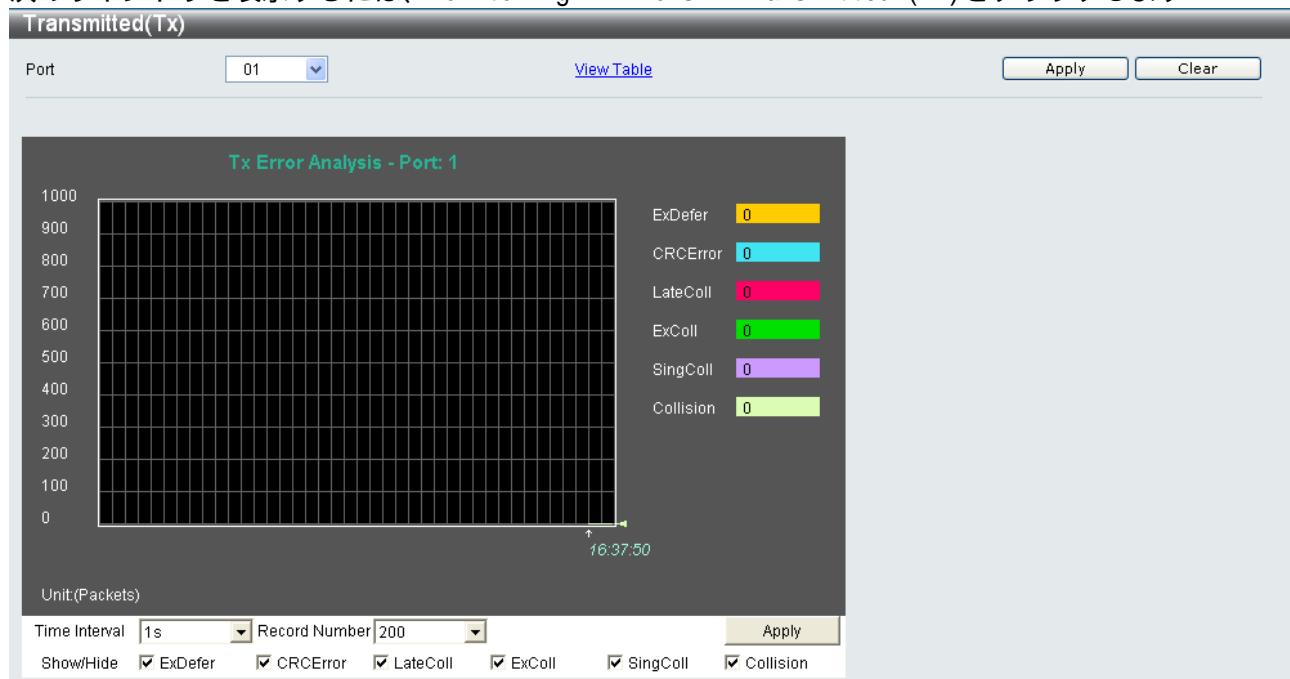
下記にパラメーターの説明を記載します。

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。
Time Interval	1~60 秒から希望する設定を選択します。デフォルト値は 1 秒です。
Record Number	スイッチを記録する回数を 20~200 から選択します。デフォルト値は 200 です。
CRCError	CRC エラーが発生したパケットをカウントします。
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の数です。
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をカウントします。
Fragment	不良な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の数です。
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をカウントします。
Drop	このポートでドロップ(削除)されたパケットの数です。
Show/Hide	CRCError、UnderSize、OverSize、Fragment、Jabber、Drop を表示するかどうかにチェックを入れます。
View Table	テーブルを表示します。
View Graphic	折れ線グラフを表示します。

3.8.11.2 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：



[Apply]をクリックして変更を適用します。

[Clear]をクリックしてデータを初期化します。

[Transmitted (Tx) Table]ウィンドウを表示するには、View Tableをクリックします。次のテーブルが表示されます：

The screenshot shows the 'Transmitted (Tx) Table' window. It has a dropdown for 'Port' set to '01', a 'View Graphic' button, and 'Apply' and 'Clear' buttons. Above the table is a 'Time Interval' dropdown set to '1s' and an 'OK' button. The table itself has columns for 'TX Error' and 'TX Frames', with data rows:

TX Error	TX Frames
ExDefer	0
CRC Error	0
LateColl	0
ExColl	0
SingColl	0
Collision	0

[Apply]をクリックして変更を適用します。

[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。
Time Interval	1~60秒から希望する設定を選択します。デフォルト値は1秒です。
Record Number	スイッチを記録する回数を20~200から選択します。デフォルト値は200です。
ExDefer	メディアが使用中だったために、指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の数をカウントします。
CRC Error	CRCエラーが発生したパケットをカウントします。
LateColl	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をカウントします。
ExColl	過度のコリジョンのために送信に失敗したパケットの数です。
SingColl	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、送信に成功した数です。
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です。
Show/Hide	ExDefer、CRCError、LateColl、ExColl、SingColl、Collisionを表示するかどうかにチェックを入れます。
View Table	テーブルを表示します。
View Graphic	折れ線グラフを表示します。

3.8.12 Port Access Control

3.8.12.1 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：

RADIUS Authentication

Clear

ServerIndex	InvalidServerAddr	Identifier	AuthServerAddr	ServerPortNumber	RoundTripTime	AccessRequests	AccessAccepted
1	0	Hitachi Metals		0	0	0	
2	0	Hitachi Metals		0	0	0	
3	0	Hitachi Metals		0	0	0	

[Clear]をクリックしてデータを初期化します。

統計を更新する時間間隔を1~60秒の範囲から選択します。デフォルト値は1秒です。表示されている現在の統計を消去するには、左上端にある[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
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す。不良なオーセンティケータまたは署名属性、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つてない 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、タイムアウトになつたり再送すると、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。

3.8.12.2 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 Account Client			
<input type="button" value="Clear"/>			
ServerIndex	InvalidServerAddr	Identifier	ServerAddr
1	0	Hitachi Metals	
2	0	Hitachi Metals	
3	0	Hitachi Metals	

[Clear]をクリックしてデータを初期化します。

統計を更新する時間間隔を 1 ~ 60 秒の範囲から選択します。デフォルト値は 1 秒です。表示されている現在の統計を消去するには、左上端にある [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
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。
RoundTripTime	直近のアカウンティング応答と、この RADIUS アカウンティングサーバーからのアカウンティング要求と一致したアカウンティング要求との間の時間間隔です。
Requests	RADIUS アカウン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 アカウンティングサーバーに送信された RADIUS アカウン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および既知のタイプは、不正な形式のアカウン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を含む RADIUS アカウン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 アカウンテ

パラメーター	説明
	イング要求パケットの数です。アカウン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。

3.8.12.3 Authenticator State

このセクションではスイッチ上に設定した 802.1X の状態表示について説明します。

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：

Authenticator State					
Port	01	Find	Refresh		
Total Authenticating Hosts:	0				
Total Authenticated Hosts:	0				
Port	MAC Address	PAE State	Backend State	Status	VID

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	設定を表示する対象ポートを選択します。
MAC Address	Port 番号に対応するデバイスの MAC アドレスです。
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 [Hold]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。
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。
VID	ポートが所属する VLAN ID を表示します。

3.8.12.4 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ー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ー機能に対応する各ポートのエントリーが表示されます。

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

Authenticator Statistics							
Port	01			Apply	Refresh		
Total Entries: 0							
Index	MAC Address	Frames RX	Frames TX	RX Start	TX ReqId	RX LogOff	TX

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。
MAC Address	Index 番号に対応するデバイスの MAC アドレスです。
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 RespId	オーセンティケータで受信した 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で受信した、パケットボディ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。

3.8.12.5 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機能に対応する各ポートのエントリーが表示されます。

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

Authenticator Session Statistics					
Port	01	<input type="button" value="Apply"/>	<input type="button" value="Refresh"/>		
Total Entries: 0					
Index	MAC Address	Octets RX	Octets TX	Frames RX	Frames TX

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。
MAC Address	Index番号に対応するデバイスのMACアドレスです。
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。

3.8.12.6 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ーが表示されます。

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

The screenshot shows a software interface titled "Authenticator Diagnostics". At the top, there is a dropdown menu labeled "Port" with "01" selected, and two buttons: "Apply" and "Refresh". Below this is a table header row with the following columns: "Total Entries: 0", "Index", "MAC Address", "Connect Enter", "Connect LogOff", "Auth Enter", "Auth Success", "Auth Timeout", "Auth Fail", and "A". The table body is currently empty, showing only the header row.

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。
MAC Address	Index 番号に対応するデバイスの MAC アドレスです。
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	サプリカントから 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プ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回数をカウントします。
Auth Start	サプリカントから 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	サプリカントから 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	サプリカントから 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	サプリカントから 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

パラメーター	説明
	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)をサプ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	サプリカントから初期 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。サプ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。サプ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。サプ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。

3.8.13 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：

Browse ARP Table			
Interface Name	IP Address	MAC Address	Find
			Show Static Clear All
Total Entries: 4			
Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
System	10.90.90.82	00-03-FF-BE-2E-18	Dynamic
System	10.90.90.90	00-40-66-71-F6-B2	Local
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。

3.8.14 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：

Browse VLAN																													
VID																													
VID:																													
VLAN Name:																													
VLAN Type:																													
Advertisement:																													
Total Entries: 1																													
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26				
U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52				
U	U	U	U	U	U	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

3.8.15 IGMP Snooping

3.8.15.1 Browse IGMP Router Port

現在ルーター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として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ルーターとして表示されます。

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：

The screenshot shows a search interface for router ports. It has fields for VID and VLAN Name, and a 'Find' button. Below is a grid of port numbers (01-52). A note at the bottom explains the symbols: S for Static Router Port, D for Dynamic Router Port, and F for Forbidden Router 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	25	26
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52

Note: S:Static Router Port, D:Dynamic Router Port, F:Forbidden Router Port

3.8.15.2 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：

The screenshot shows a search interface for IGMP snooping groups. It has fields for VLAN Name, VID List, Port List, and Group IPv4 Address, and a 'Find' button. Below is a table header with columns: Total Entries, VID, VLAN Name, Source, Group, Member Port, Router Port, Group Type, Up Time, Expiry Time, and Filter Mode.

Total Entries: 0	VID	VLAN Name	Source	Group	Member Port	Router Port	Group Type	Up Time	Expiry Time	Filter Mode
------------------	-----	-----------	--------	-------	-------------	-------------	------------	---------	-------------	-------------

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。
Port List	マルチキャストグループのポート番号を入力します。
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。

3.8.15.3 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：

The screenshot shows a search interface for IGMP Snooping Host. It has four input fields: 'VLAN Name' (radio button selected), 'VID List' (e.g.: 1, 4-6), 'Port List' (e.g.: 1, 3-5), and 'Group Address' (e.g.: 224.1.1.1). Below the fields are 'Find' and 'View All' buttons. At the bottom, it displays 'Total Entries: 0' and a table header with columns VID, Group, Port, and Host.

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。
Port List	マルチキャストグループのポート番号を入力します。
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。

3.8.16 MLD Snooping

3.8.16.1 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：

The screenshot shows a search interface for MLD Router Port. It has a 'VID' input field and a 'Find' button. Below is a table with columns VID and VLAN Name. A note at the bottom states: 'Note: S:Static Router Port, D:Dynamic Router Port, F:Forbidden Router Port'.

VID	VLAN Name
01	-
02	-
03	-
04	-
05	-
06	-
07	-
08	-
09	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-
25	-
26	-
27	-
28	-
29	-
30	-
31	-
32	-
33	-
34	-
35	-
36	-
37	-
38	-
39	-
40	-
41	-
42	-
43	-
44	-
45	-
46	-
47	-
48	-
49	-
50	-
51	-
52	-

3.8.16.2 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	Router Port	Group Type	Up Time	Expiry Time	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 ポートを入力します。
Port List	マルチキャストグループのポート番号を入力します。
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。

3.8.17 LLDP

3.8.17.1 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	1777
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。

3.8.17.2 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...
2	Local	1/2	APRESIA Systems...
3	Local	1/3	APRESIA Systems...
4	Local	1/4	APRESIA Systems...
5	Local	1/5	APRESIA Systems...
6	Local	1/6	APRESIA Systems...
7	Local	1/7	APRESIA Systems...
8	Local	1/8	APRESIA Systems...
9	Local	1/9	APRESIA Systems...
10	Local	1/10	APRESIA Systems...
11	Local	1/11	APRESIA Systems...
12	Local	1/12	APRESIA Systems...
13	Local	1/13	APRESIA Systems...
14	Local	1/14	APRESIA Systems...
15	Local	1/15	APRESIA Systems...
16	Local	1/16	APRESIA Systems...

[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
	<input type="button" value="Find"/> <input type="button" value="Show Brief"/>
LLDP Normal Ports	
Port ID Subtype	Local
Port ID	1/1
Port Description	Hitachi Metals ApresiaLightGM152GT R1.00 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
Power Via MDI	Show Detail
Link Aggregation	Show Detail
Maximum Frame Size	12284

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できます。

LLDP Local Port Information				
LLDP Local Management Address Detail Table				
Total Entries: 1				
Port	Subtype	Address	IF Type	OID
1	IPv4	10.90.90.90	IfIndex	1.3.6.1.4.1.278.1.35...

3.8.17.3 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：

LLDP Remote Port Information

LLDP Remote Port Brief Table

Port 01 Find Show Normal

Total Entries: 0

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description
--------	--------------------	------------	-----------------	---------	------------------

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

LLDP Remote Port Information

LLDP Remote Entity Information Table

<< Back

Total Entries: 0

Entity	Information
--------	-------------

3.8.18 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：

MAC-based Access Control Host State

Port List (e.g.: 1, 5-10) Find Clear by Port

View All Hosts Clear All Hosts

Total Authenticating Hosts: 0
Total Authenticated Hosts: 0
Total Hold Hosts: 0

Port	MAC Address	State	VID	Aging Time / Hold Time
------	-------------	-------	-----	------------------------

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。

3.8.19 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：

The screenshot shows the 'Web Authentication Host State' window. At the top, there are two input fields for 'Port List (e.g.: 1, 5-10)' with dropdown menus, and three checkboxes: 'Authenticated' (checked), 'Authenticating' (checked), and 'Blocked' (checked). To the right are 'Find' and 'Clear by Port' buttons. Below these are 'View All Hosts' and 'Clear All Hosts' buttons. A summary section displays 'Total Authenticating Hosts: 0', 'Total Authenticated Hosts: 0', and 'Total Blocked Hosts: 0'. The main table has columns: Port, MAC Address, Original RX VID, State, VID, and Aging Time / Block Time.

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。

3.8.20 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：

The screenshot shows the 'Browse Session Table' window. It includes a 'Refresh' button and a table with columns: ID, Live Time, From, Level, and Name. One row is visible with ID 8, Live Time 04:50:58.20, From Serial Port, Level 1, and Name Anonymous.

3.8.21 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ーが作成されます。これらのエントリー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	01	Find	Clear Dynamic Entries		
VLAN Name	<input type="text"/>	Find	Clear Dynamic Entries		
VID List	<input type="text"/>	Find			
MAC Address	00-00-00-00-00-00	Find			
View All Entries Clear All Entries					
Total Entries: 2					
VID	VLAN Name	MAC Address	Port	Type	
1	default	00-03-FF-BE-2E-18	1	Dynamic	Add to Static MAC table
1	default	00-40-66-71-F6-B2	CPU	Self	Add to Static MAC table
				1/1	1 <input type="text"/> Go

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。
VID List	フォワーディングテーブルを参照する VLAN ID 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ーを削除します。
View All Entry	アドレステーブルのすべてのエントリーを表示します。
Clear All Entry	アドレステーブルのすべてのエントリーを削除します。

[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ーを検索します。

[Clear Dynamic Entries]をクリックして全てのダイナミックエントリーをクリアします。

[View All Entry]をクリックして使用可能な全てのエントリー一覧を表示します。

[Clear All Entry]をクリックして表示されている全てのエントリーをクリアします。

3.8.22 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：

System Log																							
Total Entries: 6																							
<table><thead><tr><th>Index</th><th>Date-Time</th><th>Log Text</th></tr></thead><tbody><tr><td>6</td><td>2014-01-20, 10:38:52</td><td>Successful login through Web (Username: adpro, IP: 10.90.90.82)</td></tr><tr><td>5</td><td>2014-01-20, 10:35:09</td><td>Port 1 link up, 1000Mbps FULL duplex</td></tr><tr><td>4</td><td>2014-01-20, 09:23:30</td><td>System cold start</td></tr><tr><td>3</td><td>2014-01-14, 16:40:16</td><td>CPU utilization enters OVERLOADING status.</td></tr><tr><td>2</td><td>2014-01-14, 16:40:11</td><td>Port 1 link up, 1000Mbps FULL duplex</td></tr><tr><td>1</td><td>2014-01-14, 16:40:09</td><td>Port 1 link down</td></tr></tbody></table>			Index	Date-Time	Log Text	6	2014-01-20, 10:38:52	Successful login through Web (Username: adpro, IP: 10.90.90.82)	5	2014-01-20, 10:35:09	Port 1 link up, 1000Mbps FULL duplex	4	2014-01-20, 09:23:30	System cold start	3	2014-01-14, 16:40:16	CPU utilization enters OVERLOADING status.	2	2014-01-14, 16:40:11	Port 1 link up, 1000Mbps FULL duplex	1	2014-01-14, 16:40:09	Port 1 link down
Index	Date-Time	Log Text																					
6	2014-01-20, 10:38:52	Successful login through Web (Username: adpro, IP: 10.90.90.82)																					
5	2014-01-20, 10:35:09	Port 1 link up, 1000Mbps FULL duplex																					
4	2014-01-20, 09:23:30	System cold start																					
3	2014-01-14, 16:40:16	CPU utilization enters OVERLOADING status.																					
2	2014-01-14, 16:40:11	Port 1 link up, 1000Mbps FULL duplex																					
1	2014-01-14, 16:40:09	Port 1 link down																					
Clear Log																							
1/1 1 Go																							

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。

3.8.23 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。

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：

Self-Test	
Self-Test Result	
DRAM Test	No error
FLASH Test	No error
SWLSI Test	No error
PHY Test	No error
POE Test	N/A

3.8.24 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：

The screenshot shows a configuration window titled "Port Led Testing". Inside, there is a dropdown menu currently set to "Off". At the bottom right of the window is a button labeled "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
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。

3.8.25 Temperature Notify

このウィンドウでシステムの温度通知機能の設定を行います。

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

Temperature Notify Settings

Polling Interval (10 ~ 300)	60	sec	Apply
High Temperature Notify Settings			
High Temperature Notify Current Status	Normal		
High Temperature Notify State	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	Apply
Threshold (-50~85)	55	(Celsius)	Apply
Traps State	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	Apply
Log State	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	Apply
Low Temperature Notify Settings			
Low Temperature Notify Current Status	Normal		
Low Temperature Notify State	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	Apply
Threshold (-50~85)	-5	(Celsius)	Apply
Traps State	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	Apply
Log State	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	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
Polling Interval	温度検知のポーリング時間を入力します。
High Temperature Notify State	高温側の通知機能を有効または無効に設定します。
Low Temperature Notify State	低温側の通知機能を有効または無効に設定します。
Threshold (-50~85)	高温側、低温側の温度通知の閾値温度を設定します。
Traps State	温度通知機能の状態遷移によるSNMPトラップ出力を有効または無効に設定します。デフォルト設定は有効です。
Log State	温度通知機能の状態遷移によるログ出力を有効または無効に設定します。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。

3.8.26 Peripheral

3.8.26.1 Device Environment

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。

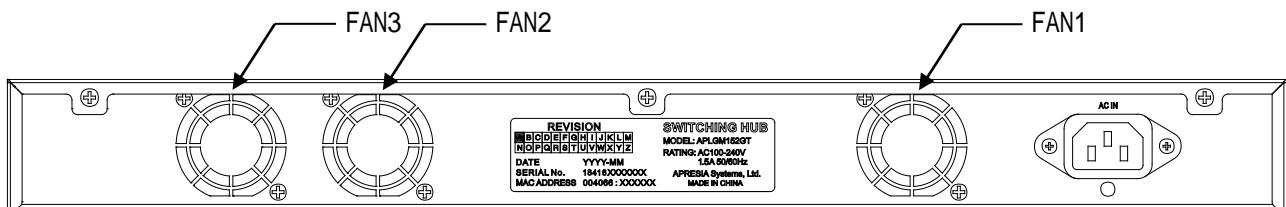
FAN 動作状態の表示では、正常回転時(Normal)・回転数低下時(Abnormal slow)・回転停止時(Stop)と表示されます。

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：

Device Environment		Refresh
Items	Data	
System Temperature(Celsius)	24	
Fan 1	Normal	
Fan 2	Normal	
Fan 3	Normal	
Fan Led Error State	Enable	

[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。

FAN 番号と実装位置の関係を以下の図に示します。



注意事項



装置が起動してから内部温度を検知するまで約1分程度かかります。その間、System Temperature は0表示となりますが異常ではありません。

3.9 セーブ

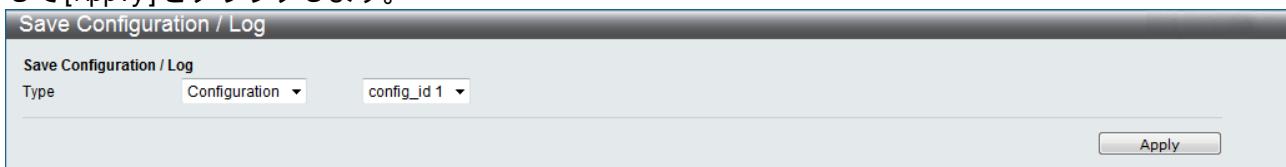
下記に示す3つの保存ウィンドウを使用して設定情報をスイッチのメモリーに保存します。

- (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。

3.9.1 Save Configuration/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 Configuration/Log]をクリックすると、次のウィンドウが開きます：

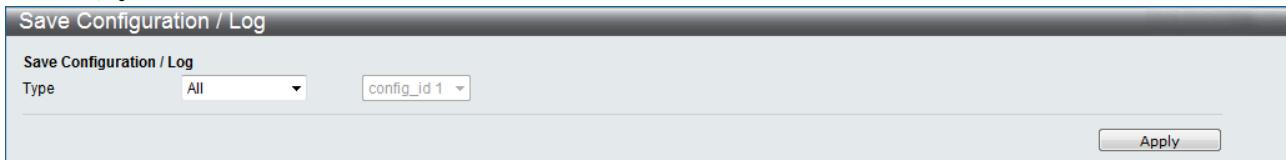
コンフィグレーションを保存する場合は、プルダウンメニューで Configuration と保存する ID を選択して[Apply]をクリックします。



ログを保存する場合は、プルダウンメニューで Log を選択し[Apply]をクリックします。



コンフィグレーションとログを保存する場合は、プルダウンメニューで All を選択し[Apply]をクリックします。



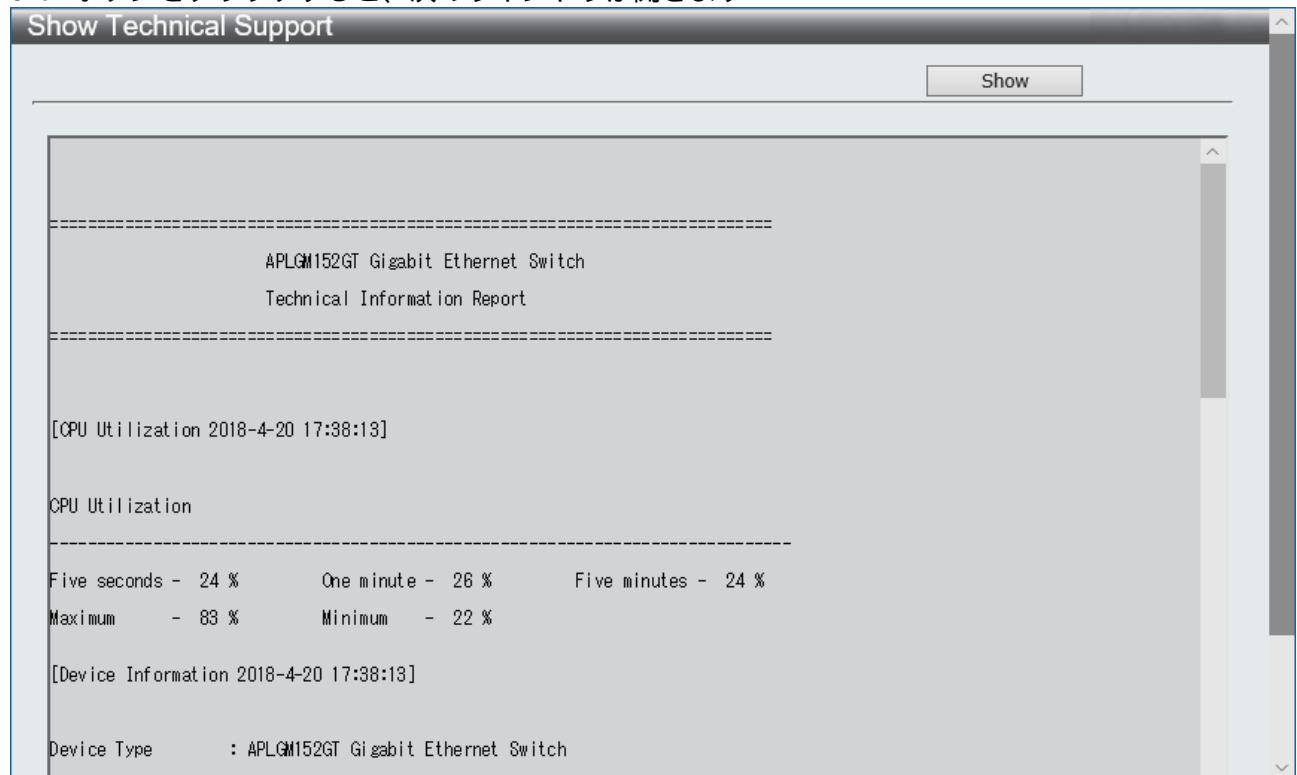
注意事項



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。

3.9.2 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：



[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。

右下にある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

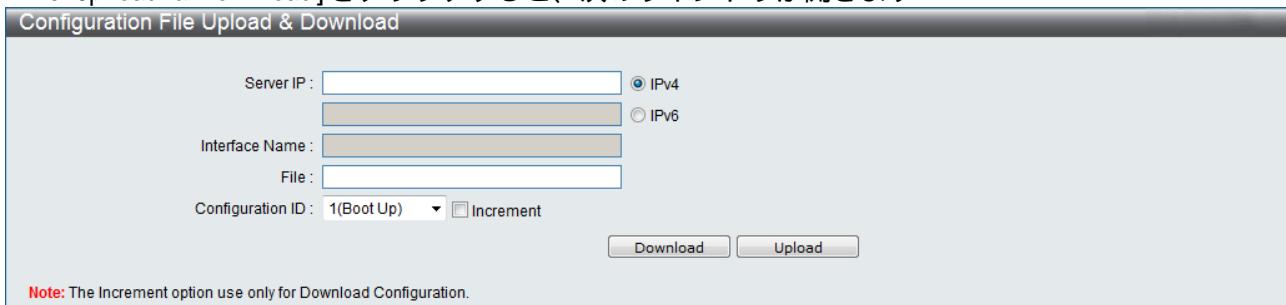
- !** テクニカルサポート情報が表示されるまで時間がかかる場合があります。

3.10 ツール

3.10.1 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：



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。

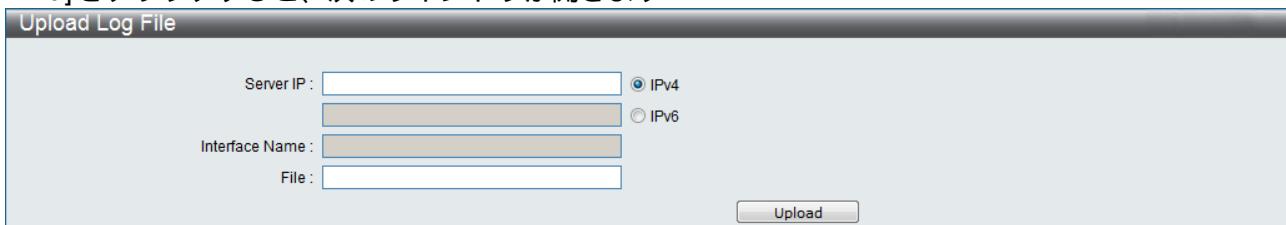
注意事項

- !** ダウンロードしたコンフィグレーション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度リンクダウンが発生します。
- !** アップロードしたコンフィグレーションファイルに account 情報は含まれません。

3.10.2 Upload Log File

ログファイルのアップロードは、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。入力後、[Upload]をクリックします。

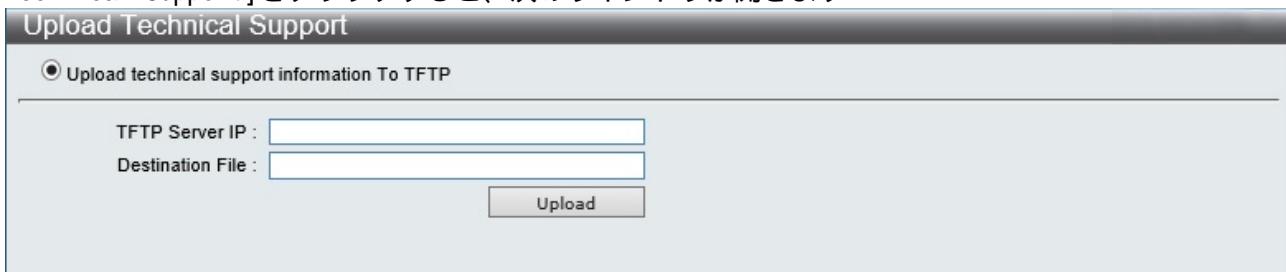
GUI 画面の一番上にあるメニューバーの左側の[ツール]プルダウンメニューを開いて、[Upload Log File]をクリックすると、次のウィンドウが開きます：



3.10.3 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

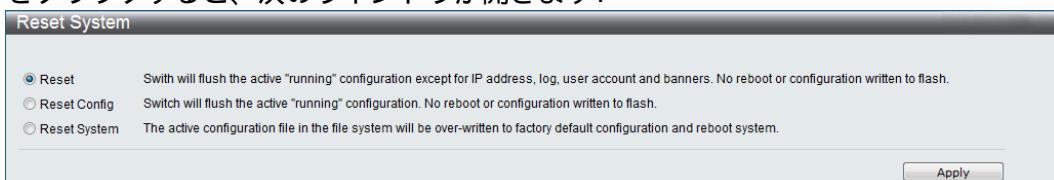


upload コマンドの実行中、CPU 高負荷状態を示す CPU utilization (OVERLOADING) ログが出力される場合があります。

3.10.4 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	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レーション保存および再起動されません。
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、即時設定が反映されます。Reset Config は、実行中の設定ファイルのみ初期化されます。
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 ともに)の初期化と再起動が行われます。

3.10.5 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：



[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までの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。

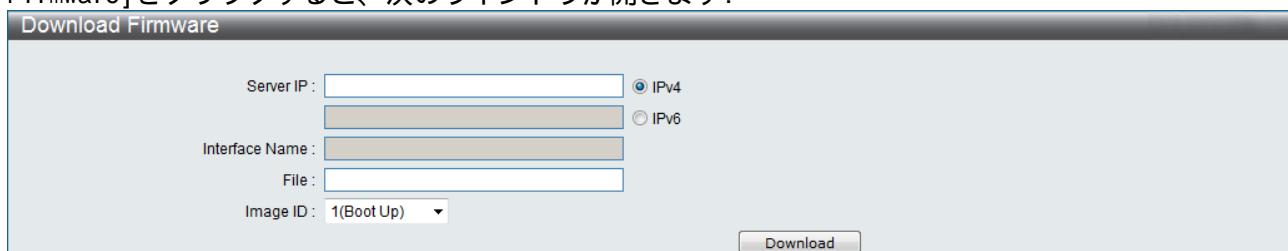
パラメーター	説明
Target IP Address	ping を送信する IP アドレスを入力します。
Interface Name	IPv6 では、インターフェースの名前を入力します。
Repeat Pinging for	ping を実施する回数を入力します。1 ~ 255 の範囲で設定します。
Size	IPv6 では、1 ~ 6000 の値を入力します。デフォルトは 100 です。
Timeout	IPv4 では、この ping メッセージが送信先に届くまでのタイムアウト時間を 1 ~ 99 秒から選択します。IPv6 では、この ping メッセージが送信先に届くまでのタイムアウト時間を 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 アドレスを見つけることができないと、ping パケットはドロップ(削除)されます。

[Start]をクリックして Ping プログラムを開始します。

3.10.6 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。

3.10.7 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。



[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、パラメーター設定時に 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。
ツイストケーブルを接続しても 「LINK/ACT」 LED が点灯しない。	ツイスト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、ツイスト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、ツイスト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。
「FAN LED」 が赤点滅または赤点灯している。	内蔵 FAN が故障している可能性があります。装置の使用を中止して販売元に修理を依頼してください。

5.2 コンソール端末に関する現象と対策

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 内蔵冷却ファンに関する現象と対策

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 Simple Network 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 RFC2233 : 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 IEEE802.1W : RSTP IEEE802.1S : MSTP IEEE802.3x : フロー制御 IEEE802.1AB : LLDP IEEE802.3az : Energy Efficient Ethernet

ApresiaLightGM152GT Ver.1.02 SW マニュアル

Copyright(c) 2018 APRESIA Systems, Ltd.

2018 年 4 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
<http://www.apresiasystems.co.jp/>