

# Web Smart **ギガビットイーサスイッチ** **SMCGSxxC-Smart シリーズ** **SMCGSxxP-Smart シリーズ** **取扱説明書**



第 2.2 版

管理番号:TEC-00-MA0124-02.2

## ご注意

- 本スイッチをご使用の際は、本書に従って正しい取り扱いをしてください。
- 本スイッチを分解したり改造したりすることは絶対に行わないでください。
- 本スイッチの故障、誤動作、不具合、あるいは天災、停電等の外部要因によって、通信などの機会を逸したために生じた損害等の純粋経済損害につきましては、Accton社並びに当社は一切その責任を負いかねますので、あらかじめご了承ください。
- 本スイッチは、改良のため予告なしに仕様が変更される可能性があります。あらかじめご了承ください。
- 本書の中に含まれる情報は、当社（ハイテクインター株式会社）、Accton 社及びその他が所有するものであり、該当する著作権者の同意なしに、全体または一部を複製または転載することは禁止されています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期して作成いたしましたが、万一、ご不審な点や誤り、記載漏れなどのお気づきの点がありましたらご連絡ください。

## 電波障害自主規制について

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

## 改版履歴

第 1 版	2012 年 12 月 12 日	新規作成
第 2 版	2013 年 02 月 13 日	各種項目の追加
第 2.1 版	2013 年 08 月 29 日	お問い合わせ先の電話番号を変更
第 2.2 版	2015 年 09 月 16 日	付属品から CD 削除

## 目 次

1.	本書について.....	11
2.	製品概要.....	11
3.	梱包物一覧.....	11
4.	製品外観.....	12
5.	設置について.....	13
5.1.	設置時の注意事項.....	13
5.2.	19 インチラックへの搭載.....	14
5.3.	電源投入について.....	15
5.4.	電源切断について.....	15
6.	スイッチを設定する前に.....	16
6.1.	IP の設定.....	16
6.2.	Web GUI による管理機能について.....	17
6.3.	Web GUI へのログイン.....	17
6.4.	Web GUI のトップページ.....	18
6.5.	Web GUI 使用時の注意.....	19
6.6.	再起動.....	21
6.7.	設定ファイルのダウンロード.....	22
6.8.	設定ファイルのアップロード.....	23
6.9.	工場出荷時設定.....	24
6.10.	リセットボタン.....	25
6.11.	ファームウェアのアップデート.....	26
7.	スイッチの基本設定.....	27
7.1.	システム情報の設定.....	27
7.2.	IP アドレス、デフォルトゲートウェイの設定.....	28
7.3.	NTP サービス.....	32
7.4.	リモートログメッセージ.....	33
8.	省電力モード.....	34
8.1.	LED 省電力モード (SMCGS10 のみ対応).....	34
8.2.	省電力イーサネットの設定.....	35

9.	熱保護設定 (SMCGS10 のみ対応).....	37
10.	各ポートにおける接続モード設定.....	38
11.	セキュリティ.....	41
11.1.	セキュリティの説明.....	41
11.2.	Management Access Security: Switch 項目下のセキュリティ設定.....	41
11.3.	Privilege Level の設定.....	43
11.4.	リモートアクセス認証の設定.....	45
11.5.	SSH の設定 (未サポート).....	47
11.6.	HTTPS の設定.....	48
11.7.	アクセスマネジメント IP アドレスフィルタリングの設定.....	49
11.8.	SNMP の設定.....	50
11.9.	SNMPv3 コミュニティーアクセスストリングの設定.....	56
11.10.	SNMPv3 ユーザーの設定.....	57
11.11.	SNMPv3 Group の設定.....	59
11.12.	SNMPv3 Views の設定.....	60
11.13.	SNMPv3 Group Access Rights の設定.....	61
11.14.	RMON 統計の設定 (SMCGS18/26/50 のみ対応).....	62
11.15.	RMON ヒストリー情報の設定 (SMCGS18/26/50 のみ対応).....	63
11.16.	RMON アラームの設定 (SMCGS18/26/50 のみ対応).....	64
11.17.	RMON イベントの設定 (SMCGS18/26/50 のみ対応).....	65
11.18.	Port Security Limit Controls の設定.....	66
11.19.	Network Access Server 認証の設定.....	69
11.20.	Network Access Server 認証の設定ガイドライン.....	71
11.21.	Access Control List によるトラフィックコントロールの設定.....	78
11.22.	ACL Rate Limiters の設定.....	81
11.23.	Access Control List の設定.....	82
11.24.	DHCP Snooping の設定.....	90
11.25.	DHCP Relay の設定とオプション 82 に関して.....	92
11.26.	IP SOURCE GUARD の設定.....	94
11.27.	IP SOURCE GUARD の STATIC BINDINGS 設定.....	96
11.28.	ARP INSPECTION の設定.....	97
11.29.	STATIC ARP INSPECTION TABLE の設定.....	99
11.30.	認証サーバの指定.....	100
12.	トランクグループ.....	102
12.1.	トランクグループ設定のガイドライン.....	102
12.2.	静的トランク回線の設定.....	103
12.3.	動的トランク回線 (LACP) の設定.....	105

13. Loop Protection (SMCGS18/26/50 のみ対応) .....	107
13.1. Loop Protection の設定 .....	107
14. スパニングツリーアルゴリズムの設定 .....	108
14.1. スパニングツリー設定のガイドライン .....	108
14.2. マルチプルスパニングツリーの設定 .....	111
14.3. スパニングツリーブリッジプライオリティの設定 .....	113
14.4. MSTI インタフェースの設定 .....	116
15. マルチキャスト VLAN レジストレーション (MVR) .....	118
15.1. MVR のヒント .....	118
15.2. MVR のパラメータ .....	118
16. IGMP スヌーピング .....	120
16.1. IGMP スヌーピングのグローバル設定とポート設定 .....	120
16.2. IGMP スヌーピングとクエリに関する LAN 設定 .....	123
16.3. IGMP フィルタリングの設定 .....	126
17. MLD スヌーピング .....	127
17.1. MLD スヌーピングのヒント .....	127
17.2. MLD スヌーピングとクエリの VLAN 設定 .....	130
17.3. MLD フィルタリングのパラメータ .....	132
18. リンクレイヤ ディスカバリ プロトコル (LLDP) .....	133
18.1. LLDP タイミングと TLV .....	133
18.2. LLDP-MED TLV の設定 .....	136
19. Power over Ethernet(SMCGSxxP のみ対応) .....	143
19.1. PoE 優先順位のヒント .....	143
19.2. PoE のパラメータ .....	144
20. MAC Address Table の設定 .....	146
20.1. MAC Address Table のパラメータ .....	146
21. IEEE802.1Q VLANs の設定 .....	148
21.1. VLAN Membership 設定のパラメータ .....	148
22. ポートへの VLAN 属性の設定 .....	149
22.1. VLAN Port Configuration 設定パラメータ .....	149

23.	IEEE 802.1Q VLANs 設定例 .....	151
24.	PrivateVLANs の設定 .....	153
25.	Port Isolation の設定 .....	154
26.	MAC-Based VLANs の設定 .....	155
27.	Protocol VLANs の設定 .....	156
28.	Protocol Group のポートへの割り当て設定 .....	158
28.1.	Group Name to VLAN Mapping Table 設定ヒント .....	158
28.2.	Group Name to VLAN Mapping Table 設定パラメータ .....	158
28.3.	Subnet-based VLAN の設定(SMCGS18/26/50 のみ対応) .....	159
28.4.	Subnet-based VLAN Configuration 設定パラメータ .....	159
29.	VoIP トラフィック管理設定 .....	160
30.	Telephony OUI の設定 .....	163
31.	Quality of Service の設定 .....	164
32.	Ingress Port Policers の設定 .....	167
33.	Egress Port Scheduler の設定 .....	168
34.	Egress Port Shaper の設定 .....	171
35.	Port Remarking Mode の設定 .....	172
36.	Port DSCP Translation と Rewriting の設定 .....	175
37.	DSCP-Based QoS Ingress Classification の設定 .....	176
38.	DSCP Translation の設定 .....	177
39.	DSCP Classification の設定 .....	178
40.	QoS Control List の設定 .....	179

41. Storm Control の設定 .....	184
42. Mirroring の設定 (SMCGS10 のみ対応).....	185
43. Mirroring&RSPAN の設定 (SMCGS18/26/50 のみ対応).....	186
44. UPnP の設定 .....	188
45. ステータスの確認.....	189
45.1. システム情報の確認 .....	189
45.2. CPU 使用率の確認.....	190
45.3. システムログの確認 .....	191
45.4. システムログの詳細の確認.....	192
46. 熱保護状態の確認 (SMCGS10 のみ対応).....	193
47. ポート状態の確認 .....	194
47.1. パネル表示 .....	194
47.2. ポートステータスの確認 .....	195
47.3. QoS 統計情報の確認.....	196
47.4. QoS Control List の確認 .....	197
47.5. 詳細ポートステータスの確認.....	198
48. セキュリティの確認 .....	200
48.1. アクセス統計情報.....	200
48.2. スイッチセキュリティステータスの確認.....	201
48.3. ポートセキュリティステータスの確認 .....	203
48.4. Network Access Server 認証のステータス.....	204
48.5. Network Access Server 統計.....	205
48.6. Access Control List ステータスの確認 .....	209
48.7. DHCP Snooping 統計情報の確認 .....	210
48.8. DHCP Relay 統計情報の確認 .....	211
48.9. ARP Inspection 情報の確認.....	212
48.10. IP Source Guard Table の確認.....	212
48.11. 認証サーバー一覧の確認 .....	213
48.12. 認証サーバ詳細ステータスの確認 .....	214
49. RMON 統計の確認 .....	217
50. LACP ステータスの確認 .....	218



50.1.	LACP ステータス.....	218
50.2.	LACP ポートステータス.....	219
50.3.	LACP ポート統計 .....	220
50.4.	Loop Protection ステータス (SMCGS18/26/50 のみ対応).....	221
51.	スパンニングツリーのステータス.....	222
51.1.	ブリッジステータス.....	222
51.2.	STP ポートステータス.....	224
51.3.	STP ポート統計 .....	225
52.	MVR ステータス .....	226
52.1.	MVR ステータス.....	226
52.2.	MVR グループステータス (SMCGS10 のみ対応).....	227
52.3.	MVR Channels ステータス (SMCGS18/26/50 のみ対応).....	228
52.4.	MVR SFM Information (SMCGS18/26/50 のみ対応).....	229
53.	IGMP スヌーピングステータス.....	230
53.1.	IGMP スヌーピングステータス.....	230
53.2.	IGMP グループステータス .....	231
53.3.	IGMP SSM ステータス.....	232
54.	MLD スヌーピングステータス.....	233
54.1.	MLD スヌーピングステータス.....	233
54.2.	MLD グループステータス.....	234
54.3.	MLD SSM ステータス.....	235
55.	LLDP ステータス.....	236
55.1.	LLDP ステータス .....	236
55.2.	LLDP-MED ステータス.....	237
55.3.	LLDP PoE ステータス.....	239
55.4.	LLDP EEE ステータス.....	240
55.5.	LLDP ポート統計.....	241
56.	PoE ステータス.....	242
57.	MAC Address Table.....	243
58.	VLANs.....	244
58.1.	VLAN メンバーシップ .....	244
58.2.	VLAN ポートステータス.....	245

<b>59. MAC ベース VLAN ステータス</b>	<b>246</b>
59.1. MAC ベース VLAN ステータス	246
<b>60. Diagnostics</b>	<b>247</b>
60.1. Ping/Ping6	247
60.2. ケーブル診断	248
<b>61. 製品仕様</b>	<b>249</b>
60.1. SMCGS10P-Smart/SMCGS10C-Smart	249
60.2. SMCGS18P-Smart/SMCGS18C-Smart	251
60.3. SMCGS26P-Smart/SMCGS26C-Smart	253
60.4. SMCGS50P-Smart/SMCGS50C-Smart	255
<b>62. 製品保証</b>	<b>257</b>
付録 1: デフォルト設定一覧	259
62.1. 付録 2: 位置情報 (Location Configuration Information: LCI)フォーマット の内容 261	
62.1.1. 引用・参考文献、及び商標表示	262

## 1. 本書について

本書は、SMC® EZ Switch™ シリーズの SMCGSxxC-Smart 及び SMCGSxxP-Smart の取り扱い方法について記載したものです。

なお、本文中ではこれらを指して「本スイッチ」、または「スイッチ」と呼称しています。

## 2. 製品概要

本スイッチは L2 スイッチングハブに求められる機能を幅広くサポートしております。これらに加えて、PoE(SMCGxxP-Smart のみ PoE 対応)と Web GUI を搭載し、エッジスイッチとして最適な構成を提供します。

本スイッチは工場出荷時の状態においても殆どの機能を利用できますが、各々のネットワーク環境においてパフォーマンスを最大限に発揮させるためには、多くのオプションを設定する必要があります。

## 3. 梱包物一覧

ご使用いただく前に本体と付属品を確認してください。万一、不足の品がありましたら、お手数ですがお買い上げの販売店までご連絡ください。

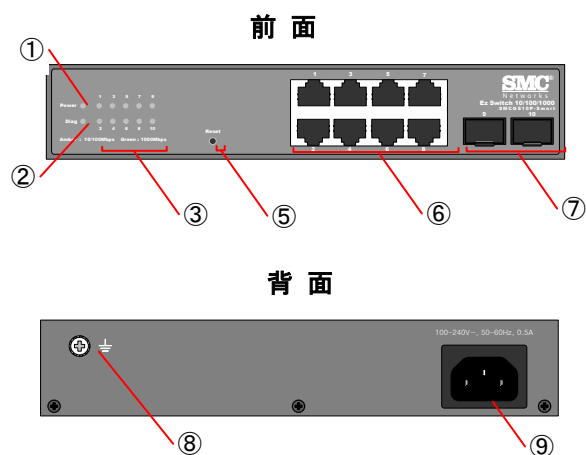
梱包物の名称	数 量
スイッチ本体	1
AC 電源ケーブル	1
19 インチラックマウントキット ( マウントアングル×2, φ3 ネジ×8、ゴム足×4 )	1

## 4. 製品外観

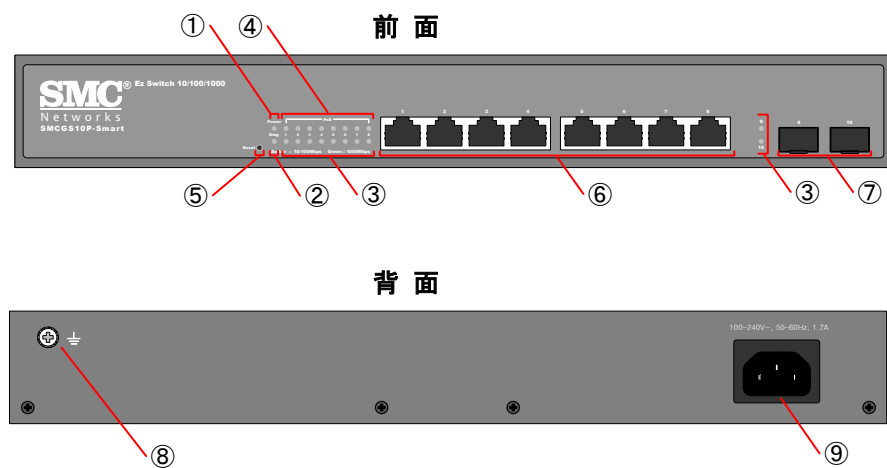
### 4.1. 各種 前面パネル

各部名称は以下をご覧ください。

#### SMCGS10C-Smart



#### SMCGS10P-Smart



No.	名 称	No.	名 称
1	Power LED	6	RJ-45 ポート
2	Diag LED	7	SFP ポート
3	LINK LED	8※	接地端子 (フレームアース)
4	PoE LED	9	AC インレット
5	リセットボタン		

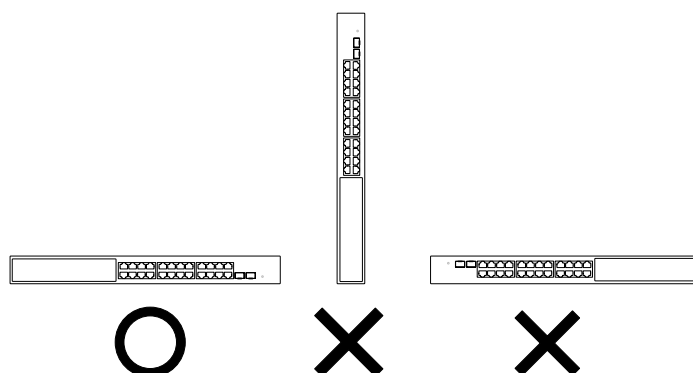
※ 接地端子は SMCGS10C-Smart/SMCGS10P-Smart にだけあります。

## 5. 設置について

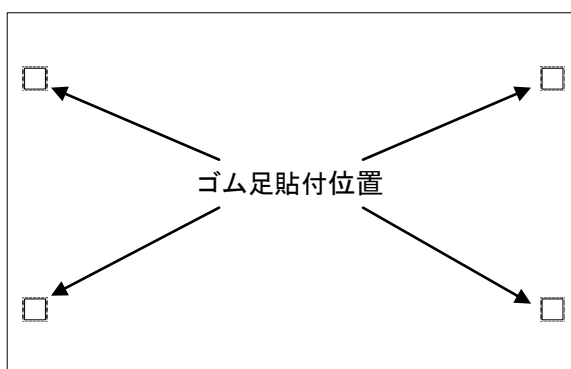
### 5.1. 設置時の注意事項

本スイッチの設置にあたって、以下の点に御注意ください。

- 設置の際は、なるべく水平な場所に、天板を上に向けて設置してください。
- スイッチを立てる、横倒しにする、あるいは天地を逆に設置すると、故障の原因になりますので、お止め下さい。



- 直射日光で暖められるような屋外や、空気の対流が乏しい密閉された箱内での運用は、寿命が短くなるなど故障の原因となる場合があります。
- 卓上や棚に設置する場合のために、ゴム足が付属しています。スイッチの底面に貼付位置を示す窪みが用意されていますので、必要に応じてお使いください。



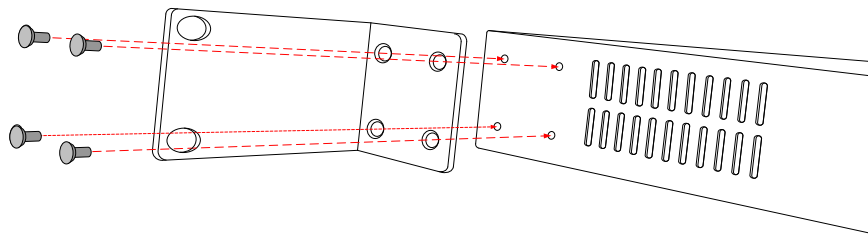
**注意：** 19 インチラックに本スイッチにゴム足をつけたままで設置した場合、稀にゴム足が下段の機材の天板と干渉することがあります。この場合は、ゴム足を取り外すか、あるいは本機の下に機材が何も設置されていない状態を保つことをお勧めします。

## 5.2. 19 インチラックへの搭載

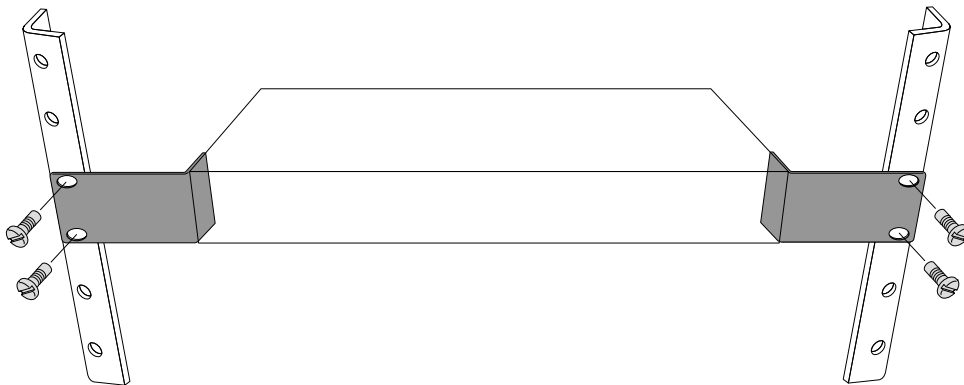
本スイッチには、19 インチラックに搭載するためのアングルが1組と、φ3mm のネジ 8 本が同梱されています。

設置の手順については、以下をご覧ください。

- 1) 本スイッチの両側面に、ラックマウントアングルを取り付けます。φ3mm のネジで、各々4箇所、計8箇所を留めます。取り付ける際は、アングルの向きに御注意ください。



- 2) 19 インチラックに搭載します。下に支えるものがない場合は、取り付け中の落下に十分御注意ください。



**注意：** 19 インチラックに固定するために必要な φ5mm のネジ 4 本およびケージナットは付属していません。恐れ入りますが、お客様にてご用意ください。

### 5.3. 電源投入について

本スイッチは電源スイッチを備えておりませんので、AC 電源に接続されるとただちに起動します。電源ケーブルを繋いだまま電源の On/Off を行いたい場合は、電源スイッチを持つ OA タップなどをご利用ください。

### 5.4. 電源切断について

本スイッチは電源のシャットダウン機能を備えておりません。お手数ですが、電源の切断は電源ケーブルを抜くか、あるいは電源スイッチを持つ OA タップなどをご利用ください。

ただし、ファームのアップデート時、Save ボタンの押下時、あるいは設定ファイルを Load する際には、電源を切らないよう御注意ください。このような動作の際に発生する電源断は、故障の原因となる場合があります。

## 6. スイッチを設定する前に

### 6.1. IP の設定

この章では、本スイッチを管理・設定するために手順を説明します。本スイッチは IP 接続による Telnet, SSH, HTTP 及び HTTPS 経由での管理をサポートしており、本書では IPv4 かつ HTTP 経由の操作について説明します。

ただし、HTTPS は、第三者による証明がない以外は HTTP と同様にお使いいただけます。

- 1) 本スイッチの工場出荷時の IP アドレスは 192.168.1.10、サブネットマスク: 255.255.255.0 に設定されていますので、まず接続したい管理用 PC のネットワークアドレスをこれに合わせます。

万一、IP アドレスが不明な場合でもリセットによって工場出荷時の設定に戻すことができますが、この場合、各設定は失われますのでご了承ください。

なお、リセットの手順につきましては章「6.10. リセットボタン」をご覧ください。

- 2) PC と本スイッチのイーサネットポートを LAN ケーブルで接続します。電源ケーブルをスイッチに接続して電源を入れたら、フロントパネルの LED をチェックしてリンクが確立されたことを確かめます。
- 3) ウェブブラウザを開いて、URL として http://192.168.1.10 を入力します。管理用 PC の IP アドレスが正しく設定されていれば、ユーザー名とパスワードの入力を要求するダイアログが表示されます。もしログインページが見られない場合は、手順 1 を繰り返してください。
- 4) 管理者のユーザー名とパスワードを入力し、「Login」ボタンを押します。本スイッチの工場出荷時の管理者ユーザー名は「admin」、パスワードは「admin」です。
- 5) ブラウザ画面の左側のメニューから、「System」をクリックし、次に IP をクリックします。
- 6) ローカルの DHCP サーバにアドレスを要求する場合は、「DHCP Client」チェックボックスをマークします。  
静的なアドレスを設定するには、新しい IP アドレスと IP マスクそしてスイッチの他のオプションパラメータを入力し、「Save」ボタンを押します。  
もし、IPv6 アドレスの設定が必要ならば、System メニューから IPv6 を選択し、「Auto Configuration」チェックボックスをマークして、ローカルの DHCPv6 サーバにアドレスを要求するか、アドレス、ネットワークプリフィックス長、ゲートウェイルータのパラメータを埋めて静的なアドレスを設定するかのどちらかを実行します。
- 7) ログアウトする前に管理者パスワードを変更することをお勧めします。  
パスワードを変更するには、「Security」をクリックし、次に「Users」をクリックします。ユーザーコンフィグレーションリストから「admin」を選択して、パスワードフィールドに記入し、「Save」ボタンをクリックして設定を保存します。



## 6.2. Web GUI による管理機能について

本スイッチは、Webサーバを搭載しており、Webブラウザを利用したGUIからスイッチの設定や、トラフィックの統計を見たりすることができます。

Web GUIへは標準的なWebブラウザ（Internet Explorer 5.0、Netscape 6.2、Mozilla Firefox 2.0.0.0、あるいは、より最近のバージョン）を用いることによって、ネットワーク上のどのコンピュータからもアクセスすることができます。

なお、モニタリング機能を使用する場合、グラフの描写にSVGフォーマットを使用するため、IE8以前ではプラグインの追加が必要となります

## 6.3. Web GUI へのログイン

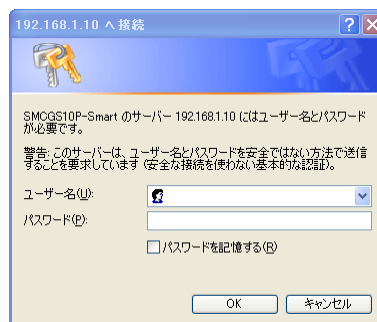
Web GUIにアクセスするには、管理者としてのユーザー名とパスワードが必要です。管理者は全ての設定パラメータと統計を読み書きする権限を持っているため、ユーザー名とパスワードの扱いには十分御注意ください。

なお、Web GUIへのアクセスには、HTTPと、セキュリティを強化したHTTPSの両方が使用できますので、状況に合わせてお使い下さい。

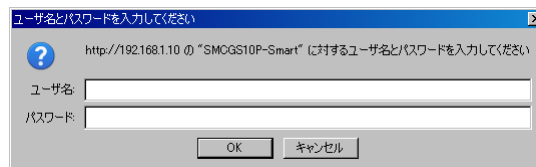
以下、HTTPにて Web GUIにアクセスする場合について説明します。

- 1) Web GUI「<http://192.168.1.10/>」にアクセスすると、以下のようなログインダイアログが表示されます。ここにユーザー名「**admin**」とパスワード「**admin**」を入力します。

Internet Explorer 8.0の場合



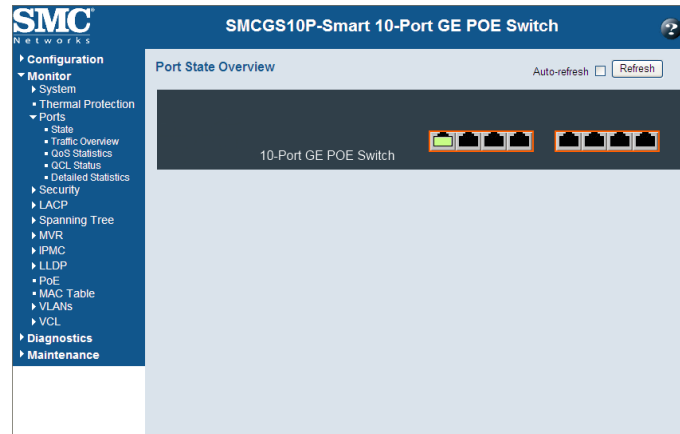
Fire fox 13.0.1の場合



(次ページに続く)

(前ページの続き)

- 2) ログインに成功すると、以下の Web GUIのトップページが表示されます。



#### 6.4. Web GUI のトップページ

Web GUI のトップページは、メインメニューをスクリーンの左側に、フロントパネルの画像をスクリーンの右側に表示します。(画像は SMCG10P-Smart スイッチの画像です。)

メインメニューのリンクは、他のメニューを操作したり、設定パラメータや統計を表示したりするために用います。




## 6.5. Web GUI 使用時の注意

### 6.5.1. 設定オプション

Web GUI での設定に使用する各種パラメータは、手動で入力する場合と、ダイアログボックス、或いはドロップダウンリストから選択する場合の 2 種類があります。

次の表は Web ページにおける設定ボタンの要約です。

ボタン	動 作
Save	指定した値をシステムに設定する。
Reset	指定した値をキャンセルし、“Save”ボタンを押す前に、変更前の値に回復させる。
	選択したページのヘルプを表示する。

#### 注意:

- i. 一旦ページ上の設定を変更した後、設定を確定するには、Save ボタンを押さなければなりません。
- ii. 画面の更新を適切に行うために、Internet Explorer の設定:「保存しているページの新しいバージョンの確認」で、「ページを表示するごとに確認する」(Web サイトを表示するたびに確認する)が選択されていることを確認してください。

Internet Explorer 6.x とそれ以前:

「ツール」→「インターネットオプション」→「全般」タブ→「インターネット一時ファイル」の設定ボタンを押し、「設定」ダイアログで「ページを表示するごとに確認する」のラジオボタンを押します。

Internet Explorer 7.x1:

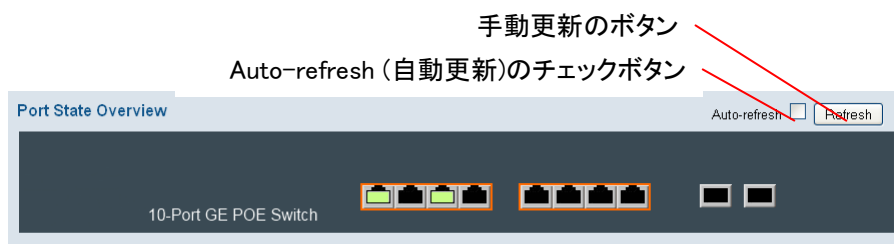
「ツール」→「インターネットオプション」→「全般」→「閲覧の履歴」の設定ボタンを押すと、設定のダイアログが表示されるので、「自動的に確認する」のラジオボタンを押します。

### 6.5.2. パネル表示

Web GUIにアクセスすると、スイッチの前面を模した画像が表示されます。これにはポートの状態画面を自動更新するモードはデフォルトで禁止(Disabled)になっています。

Auto-refreshをクリックすると、表示されたデータをおよそ5秒間隔で再表示します。

Refreshボタンをクリックすると、直ちに画面を最新情報に更新します。



### 6.5.3. LED の状態について

LED の状態を以下の表で説明します。

LED 名称	説明	状態	表示内容
Power	スイッチ電源	緑点灯	内部電源が正常に動作しています。
		消灯	電源が入っていません
Diag	システムの診断	緑点灯	システム診断の結果異常なし
		緑点滅	システムのブート中
		アンバー点灯/点滅	システム診断テストを実施しています
		消灯	システム診断了
PoE	PoE の状態	アンバー点灯	Powered Device が接続されています。
		消灯	Powered Device が接続されていません。
1-8	RJ-45 Gigabit Ethernet Ports (Port 1-8)	アンバー点灯/点滅	ポートは10または100Mbpsでリンクアップしています。点滅はポートでデータの送受信が行われていることを示しています。
		緑点灯/点滅	ポートは 1Gbps でリンクアップしています。点滅はポートでデータの送受信が行われていることを示しています。
		消灯	ポートがリンクアップしていません。
9-10	SFP Gigabit Ethernet Ports(Port 9-10)	アンバー点灯/点滅	ポートは10または100Mbpsでリンクアップしています。点滅はポートでデータの送受信が行われていることを示しています。
		緑点灯/点滅	ポートは 1Gbps でリンクアップしています。点滅はポートでデータの送受信が行われていることを示しています。
		消灯	ポートがリンクアップしていません。

**注意:** PoE LED は SMCGSxxP-Smart シリーズにのみ実装されています。

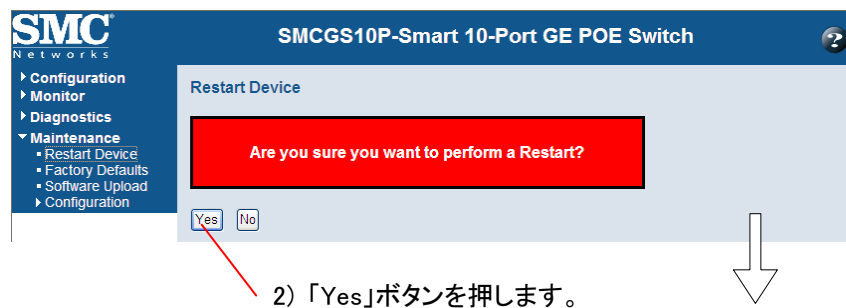
## 6.6. 再起動

スイッチの再起動を行います。

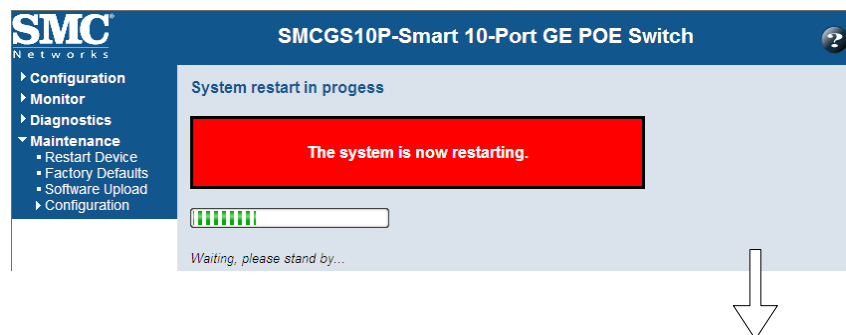
### 再起動の手順

- 1) メニューから「Maintenance」→「Restart Device」を順にクリックします。
- 2) 「Are you sure you want to perform a Restart?」(本当に再起動しますか?) と聞いてきますので、「Yes」ボタンを押して再起動させます。
- 3) 再起動が完了すると、トップページが表示されます。

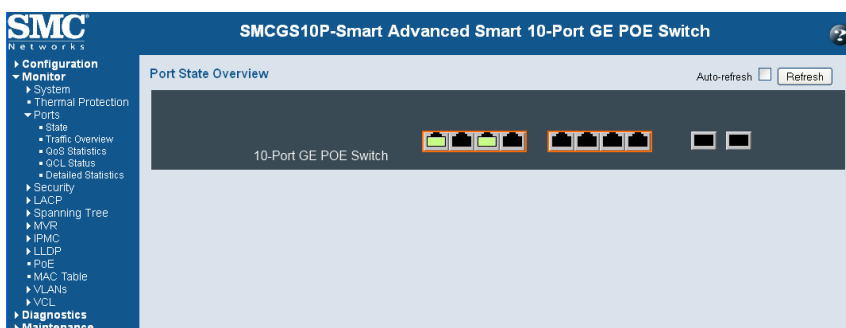
### 再起動の状態 1(開始前)



### 再起動の状態 2(途中)



### 再起動の状態 3(完了時)



注意: LAN ポートの点等状態は一例です。

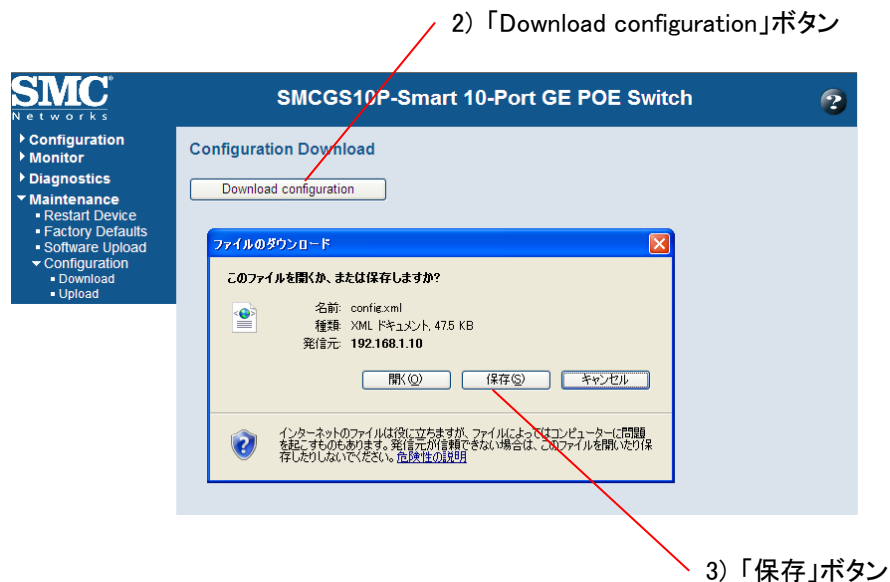
## 6.7. 設定ファイルのダウンロード

現在の設定をファイルとしてダウンロードすることが可能です。

また、後にアップロードすることが可能です。アップロードについては、6.8 章の「設定ファイルのアップロード」をご参照ください。

### 設定ファイルのダウンロード手順

- 1) メニューから「Maintenance」→「Configuration」→「Download」を順にクリックします。
- 2) 「Download configuration」ボタンを押します。
- 3) 「ファイルのダウンロード」ダイアログが出ますので、「保存(S)」ボタンを押して、ファイルのダウンロード場所を指定します。



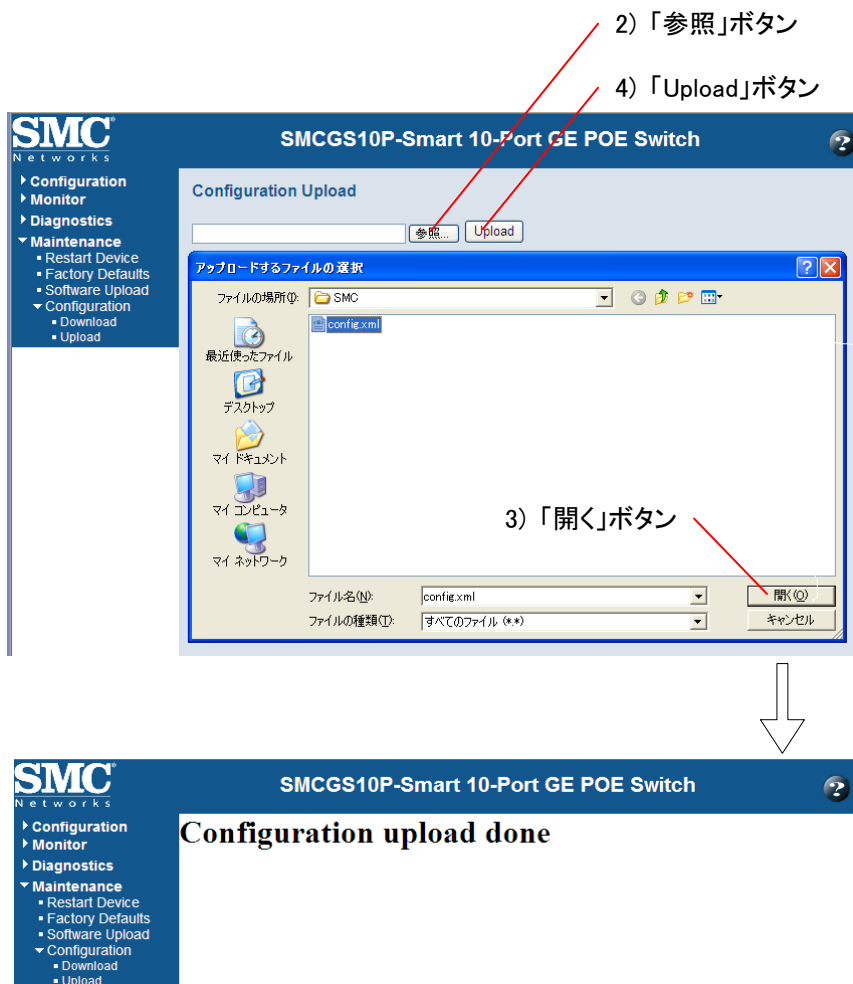
## 6.8. 設定ファイルのアップロード

以前にダウンロードした設定ファイルを読み込ませることが可能です。

ただし、お客様が手書きで作成した設定ファイルを読み込ませようとした場合は、動作を保証しかねますので御注意ください。

### 設定ファイルのアップロード手順

- 1) メニューから「Maintenance」→「Configuration」→「Upload」を順にクリックします。
- 2) 「参照」ボタンを押して、ファイルダイアログから設定ファイルを開きます。
- 3) 設定ファイルを選択し、「開く(O)」ボタンを押します。
- 4) 続いて「Upload」ボタンを押すと、設定が読み込まれます。
- 5) 「Configuration upload done」が表示されたら読み込み完了です。
- 6) 読み込みが完了したら、スイッチを再起動させることを推奨します。詳細は「6.6. 再起動」をご覧ください。



## 6.9. 工場出荷時設定

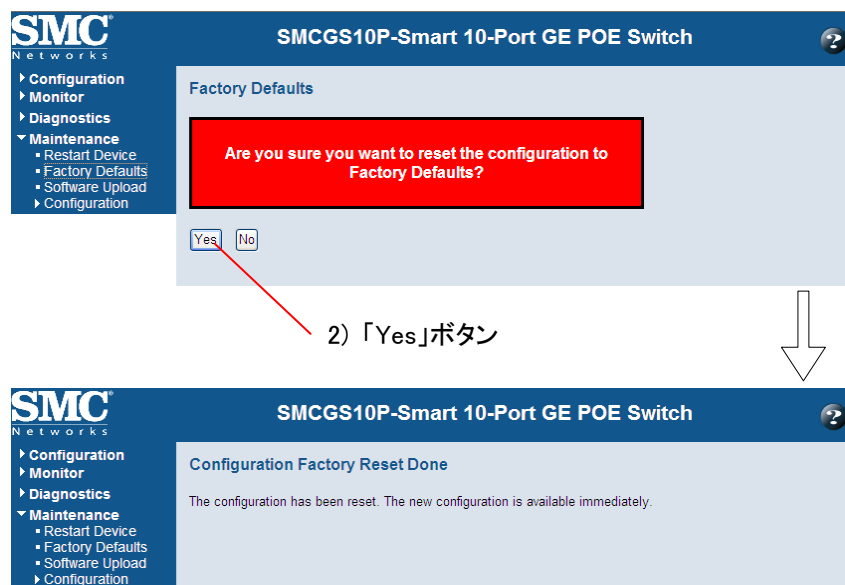
Web GUI から、本スイッチを工場出荷時の状態(ファクトリーデフォルト)に戻すことが可能です。

ただし、以下の IP Configuration 設定は初期化されませんので御注意ください。IP Configuration の設定を初期化する場合、リセットボタンを使用してください。

- 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
- VLAN ID
- DNS Server

### 工場出荷時設定の手順

- 1) メニューから「Maintenance」→「Factory Defaults」を順にクリックします。
- 2) 「Yes」ボタンをクリックすると、数秒で「Configuration Factory Reset Done」の表示がなされ、初期化が完了します。





## 6.10. リセットボタン

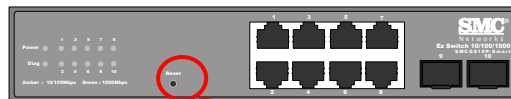
本スイッチが応答しなくなった、あるいは回復できない状態に陥ったとき、リセットボタンを押すことによって、設定を工場出荷時の状態に戻すことができます。

なお、本スイッチのリセットボタンは何れもフロントパネルにあります。

### リセットの手順

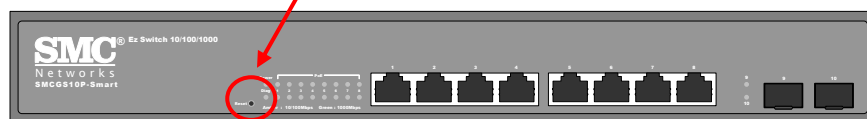
- 1) 導通性がなく、先端が尖っていない、直径 1.5mm 程度の棒等を用意します。
- 2) スwitchに電源が入っていることを確認します。
- 3) 項 1) で用意した棒でリセットボタンを 10 秒以上押し続けます。

#### SMCGS10C-Smart



リセットボタン

#### SMCGS10P-Smart



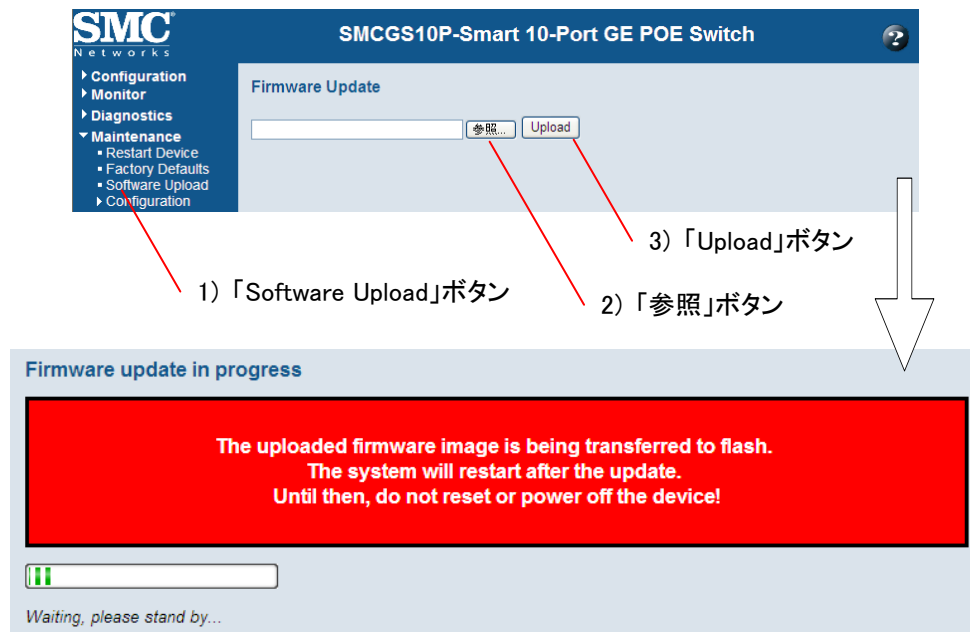
## 6.11. ファームウェアのアップデート

本スイッチには、ソフトウェアの修正や機能の向上のために、新しいファームウェアを導入する機能があります。

### ファームウェアのアップデートの手順

- 1) メニューから「Maintenance」→「Software Upload」を順にクリックします。
- 2) 「参照」ボタンを押して、ファームウェアのファイルを選択します。
- 3) 「Upload」ボタンを押して、ファームウェアを更新します。ファームウェアのアップデート中は、フロントパネルの LED が緑色に点滅します。

**注意：** ファームウェアの更新が完了するまで、電源を切ったり、リセットボタンを押したりすると、ファームウェアが壊れて故障に至る場合があります。



## 7. スイッチの基本設定

この章では、スイッチの基本的な設定について説明します。

### 7.1. システム情報の設定

本スイッチに、連絡先、システム名、スイッチの設置場所、及びタイムゾーンオフセットを設定する手順を説明します。

#### 各種パラメータ

- 1) **System Contact** : システムに責任を持つ管理者。(最大長: 255文字)
- 2) **System Name**: スイッチシステムに割り当てた名前。(最大長: 255文字)
- 3) **System Location** : システムの設置場所を指定する。(最大長: 255文字)
- 4) **System Timezone Offset**: タイムゾーンの設定 (単位: 分): タイムゾーンを、グリニッジ標準時 (GMT) からのオフセット時間として設定します。負の値はGMTよりも前の地域(東)、正の値はGMTよりも後の地域(西)を表します。

#### システム情報の設定手順

- 1) メニューから「Configuration」→「System」→「Information」の順にクリックします。
- 2) スイッチの名前や位置と同様に、システム管理者への連絡先を指定します。適切なオフセットを与えて、ローカル・タイムゾーンを指定してください。日本では540(9時間)を設定します。
- 3) 「Save」をクリックして設定を保存します。

System Information Configuration	
System Contact	<input type="text"/>
System Name	<input type="text"/>
System Location	<input type="text"/>
System Timezone Offset (minutes)	<input type="text" value="0"/>
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

- 2) 各情報を記入する。  
System Timezone Offset には  
日本の場合、540 を指定する。
- 3) 「Save」ボタンを押して保存する。

## 7.2. IP アドレス、デフォルトゲートウェイの設定

この章では、ネットワーク越しでスイッチへ管理アクセスを行うための IP アドレス、デフォルトゲートウェイの設定方法について説明します。

本スイッチは IPv4 と IPv6 の両方をサポートしており、それらのアドレスタイプのいずれかを通じて管理することができます。指定の IPv4 か IPv6 のアドレスを手動で設定したり、あるいはスイッチが起動時に直接 DHCP サーバから IPv4 アドレスを獲得したりすることもできます。

なお、IPv6 アドレスは手動での設定や、動的な生成が可能です。

管理者は手動で IP アドレスを設定するか、あるいはスイッチが自ら DHCP サーバからアドレスを取得するように指定することができます。

### 各種パラメータ

- 1) **DHCP クライアント:** IPをDHCP経由で取得するかどうかを指定します。DHCPによるIP取得を許可した場合、IPはサーバから返信を受け取るまで機能しません。この間、IPアドレスのリクエストがスイッチから定期的にブロードキャストされます。DHCPで取得される値は、IPアドレス、サブネットマスク、デフォルトゲートウェイが含まれます。
  - デフォルト値: チェックなし(DHCPは使用せず)
- 2) **IP Address:** IPアドレスを設定します。
  - デフォルト値: 192.168.1.10
- 3) **IP Mask:** 特定のサブネットへのルーティングに用いるホストアドレスビットを識別します。
  - デフォルト値: 255.255.255.0
- 4) **IP Router:** 本スイッチと管理端末が異なるセグメントに接続されている場合に指定するゲートウェイのアドレスです。
- 5) **VLAN ID:** 全てのポートの初期値はVLAN1です。VLANにIPアドレスが割り当てられている限り、ポートがどのVLANに属していても、管理端末を参加させることができます。
  - 設定値の範囲: 1~4095
  - デフォルト値: 1
- 6) **DNS Server:** ドメインネームサーバのIPアドレスを指定します。
  - デフォルト値: 0.0.0.0
- 7) **DNS Proxy:** チェックボックスにチェックを入れると、スイッチはDNSサーバの代理(プロキシ)として動作します。スイッチの配下にあるクライアントがDNSクエリを発行すると、スイッチはそれに対するレスポンスがデータベース上にあれば、クライアントへその情報を返します。一方、情報がデータベースになければ、DNSクエリはそのままDNSサーバに転送され、そのレスポンスはクライアントに返されます。レスポンスはさらにスイッチのデータベースにも蓄積されていて、将来クライアントから問合せがあった際に利用されます。

## IP アドレスの設定手順

- 1) メニューから「Configuration」→「System」→「IP」の順にクリックします。
- 2) IPv4 設定を指定し、必要であれば DNS proxy service を Enabled にします。
- 3) 「Save」ボタンをクリックして設定を保存します。

IP Configuration

	Configured	Current
DHCP Client	<input type="checkbox"/>	<input type="button" value="Renew"/>
IP Address	<input type="text" value="192.168.1.10"/>	192.168.1.10
IP Mask	<input type="text" value="255.255.255.0"/>	255.255.255.0
IP Router	<input type="text" value="0.0.0.0"/>	0.0.0.0
VLAN ID	<input type="text" value="1"/>	1
DNS Server	<input type="text" value="0.0.0.0"/>	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy ☐

### 7.2.1. IPv6 アドレス

この章では、IPv6 を用いて、スイッチの管理アクセスを行う方法について説明します。

IPv6 は、リンクローカルユニキャストとグローバルユニキャストの2つの異なるアドレスタイプを含みます。

リンクローカルアドレスは、同じローカルサブネットに接続された全てのデバイスをIPv6で利用できるようにします。このアドレスの種類を用いる管理トラフィックは、サブネットの外側にあるどのルータも通過することができません。

リンクローカルアドレスはセットアップが容易で、単純なネットワークや、基本的なトラブルシューティング作業に役立ちます。

いずれにせよ、複数のセグメントを持つ大きなネットワークに接続するには、スイッチはグローバルユニキャストアドレスを持つように設定されなければなりません。

リンクローカルアドレスは手動で設定されなければなりませんが、グローバルユニキャストアドレスは手動と動的の何れの方法でも割り当てることができます。

#### 7.2.1.1. IPv6 使用時のガイドライン

- 1) 全てのIPv6アドレスは、RFC 2373 “IPv6 アドレス構造”に基づいた表記が必要です。8個のコロンセパレータ、16ビット16進値、連続する2つのコロンは、定義されていない桁を適切な数の0で埋めることを示すために使われます。
- 2) リンクローカルアドレスを設定する場合、プレフィックス長は64ビットに固定されていることに注意してください。デフォルトアドレスのホスト部は、インタフェース識別子の修正EUI-64(拡張ユニバーサル識別子)形式に基づいています(例えば、物理MACアドレス)。ネットワークプレフィックス FE80と共にフルアドレスで入力することで、リンクローカルアドレスを手動で設定できます。
- 3) 複数のサブネットを持つ広いネットワークに接続するには、グローバルユニキャストアドレスを設定しなければなりません。このアドレスタイプを設定する幾つかの代替手段があります。
  - i) グローバルユニキャストアドレスは、ローカルインタフェースで観測されるルータ通知からプリフィックスを取り除くことで設定でき、修正EUI-64形式のインタフェース識別子を用いれば、アドレスのホスト部を自動的に生成します。このオプションはAuto Configurationオプションを可能にすることによって選択できます。
  - ii) フルアドレスとプレフィックス長を入力することによって、手動でグローバルユニキャストアドレスを設定することもできます。
- 4) IPv6アドレスが割り当てられた管理VLAN は、IP設定ページで指定する必要があります。詳細は、章「7.2.2. IPv4アドレス」をご覧ください。

### 7.2.1.2. IPv6 の設定パラメータ

インタフェースのIPv6アドレスを自動設定するには、当該ポートのIPv6アドレスステートレス自動設定を有効にし、インタフェースのIPv6機能を有効にします。

アドレスのネットワーク部は、IPv6ルータ通知メッセージで受取ったプレフィックスを元にし、ホスト部はインタフェース識別子の修正EUI-64形式を用いて自動的に生成されます。即ち、スイッチのMACアドレスです。

- 1) **Auto Configuration:** チェックボックスにチェックを入れると、IPv6 アドレスを自動的に生成するようになります。ただし、まずチェックボックスにチェックを入れた後、Save を行ってください。
  - デフォルト値: チェックあり (自動設定)
- 2) **Address:** フルアドレスとネットワークプレフィックス長 (プレフィックスフィールド内)を使って、グローバルユニキャストアドレスを手動で設定します。
  - デフォルト値: ::192.168.1.10
- 3) **Prefix:** プレフィックス長を、プレフィックスを含むアドレスのうち、(左から始まる)連続したビットが幾つかを示す 10 進値として定義します。即ち、アドレスのネットワーク部です。96bit のデフォルトプレフィックス長は、アドレスのネットワーク部を含む最初の 6 つのコロンで区切られた値を指定します。
  - デフォルト値: 96 (bit)
- 4) **Router:** デフォルトのネクストホップルータの IPv6 アドレスをセットします。管理端末が異なる IPv6 セグメントにある場合には、IPv6 デフォルトゲートウェイを定義しなければなりません。IPv6 デフォルトゲートウェイは、直接ゲートウェイに接続するネットワークインタフェースをスイッチに設定した場合に正しく設定されます。

### IPv6 手動設定の手順

- 1) メニューから「Configuration」→「System」→「IPv6」の順にクリックします。
- 2) IPv6 を指定します。
- 3) 「Save」ボタンをクリックして、設定を保存します。

IPv6 Configuration		
	Configured	Current
Auto Configuration	<input type="checkbox"/>	<input type="button" value="Renew"/>
Address	<input type="text" value="2001:db8:2222:7272::72"/>	2001:db8:2222:7272::72 Link-Local Address: fe80::201:c1ff:fe01:203
Prefix	<input type="text" value="96"/>	96
Router	<input type="text" value="::"/>	::

### 7.3. NTP サービス

本章では、NTP (Network Time Protocol)を用いて、他のネットワーク機器との時刻を合わせる方法を説明します

スイッチの時刻を正確に維持することで、システムログに記録されるイベント発生日時が有意義なものとなります。時計をセットしない場合は、スイッチは最後に起動したときに行われたファクトリーデフォルトからの時間を記録します。

NTPクライアントがEnabledになっている場合、スイッチは定期的に時刻更新のリクエストを、指定のタイムサーバに送ります。最大5つのタイムサーバのIPを設定可能で、スイッチは、設定された順に各々のサーバへ問合せを試みます。

**注意：** NTP サーバの NTP Version が 4 よりも古い場合には同期することができません。御注意下さい。(Windows XP や Windows 7 に搭載されている NTP サーバは NTP Version3 のため、同期することができません)

#### 7.3.1. NTP 設定のパラメータ

- 1) **Mode:** NTP クライアントの可否
  - デフォルト値: Disabled
- 2) **Server:** タイムサーバの IPv4 あるいは IPv6 アドレスを 5 つまで設定できます。スイッチは最初のサーバから時刻の更新を試み、失敗すると、順に次のサーバで更新を試みようとします。

#### NTP設定の手順

- 1) メニューから「Configuration」→「System」→「NTP」の順にクリックします。
- 2) Mode を選択し、NTP サーバを指定します。
- 3) 「Save」ボタンをクリックして、設定を保存します。

NTP Configuration	
Mode	Disabled
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	
<input type="button" value="Save"/> <input type="button" value="Reset"/>	



## 7.4. リモートログメッセージ

この設定では、System Log Configurationで、ログメッセージをsyslogサーバか、あるいは他の管理ステーションに送る設定を行います。

また、イベントメッセージを特定の種別へ送ることを制限することもできます。

### 7.4.1. リモートログメッセージのヒント

リモートロギングが有効な場合、システムログメッセージは目的のサーバに送られます。

Syslogプロトコルは、UDPを利用して、UDPポート514で受取ります。

ただし、UDPはコネクションレスのプロトコルなので、SyslogパケットはSyslogサーバが存在しなくても常に送り出されます。

### 7.4.2. リモートログメッセージのパラメータ

- 1) **Server Mode:** Enabled / Disabled で、リモートロギングプロセスをデバッグログ、あるいはエラーメッセージのどちらにするかを選択します。
  - デフォルト値: Disabled
- 2) **Server Address:** シスログメッセージを送るべき IPv4 アドレス或いはリモートサーバのエイリアスを指定します。
- 3) **Syslog Level:** リモート Syslog サーバに送られるログメッセージの種類を指定の内容に制限します。
  - 設定値の範囲:
    - Info- 情報、警告及びエラー情報を送ります。
    - Warning - 警告とエラー情報を送ります。
    - Error - エラー情報を送ります。
  - デフォルト値: Info

### リモートログメッセージの設定手順

- 1) メニューから「Configuration」→「System」→「Log」の順にクリックします。
- 2) リモートロギングを Enabled にし、リモートサーバの IP と、送信するシスログメッセージの種類を入力します。
- 3) 「Save」ボタンをクリックして設定保存します。

System Log Configuration	
Server Mode	Disabled
Server Address	
Syslog Level	Info
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

## 8. 省電力モード

本スイッチには、LED と、LAN の回路において省電力の機能追を搭載しています。  
本章ではこれらの省電力の設定について説明します。

### 8.1. LED 省電力モード (SMCGS10 のみ対応)

本スイッチでは、1時間単位でLEDの輝度を指定することができます。

#### 8.1.1. LED 省電力モードのヒント

LED省電力モードでは、LEDの輝度を低くすることによって省電力を実現しますが、これには次の動作が指定可能です。

- 1 時間単位で、LED の輝度を指定できます。23 回指定を追加することができますので 24 時間分の指定が可能です。
- LED が省電力モードで消灯になっている場合、通常、リンク状態の変化はスイッチの外観からは判断できません。このような場合のために、リンクに変化が起きたときだけ一定時間輝度を100%にする設定が可能です。つまり、確認のために逐一、省電力設定を解除しなくてもよくなります。

#### 8.1.2. LED 省電力モードのパラメータ

- 1) **Time:** LED の輝度を指定する時間です。
  - 設定値の範囲: 00:00~23:00
  - デフォルト値: 00.00
- 2) **Intensity:** LED の輝度です。
  - 設定値の範囲: 0~100% (10% 刻み。0% は消灯で、100% は最大輝度)
  - デフォルト値: 100%
- 3) **On-time at link change:** リンクが変化したとき、指定した時間だけ LED が最大輝度となります。
  - デフォルト値: 10 (秒)
- 4) **On at errors:** リンクエラーが発生したとき、LED を最大輝度にします。
  - デフォルト: チェックなし。

#### LED輝度の設定手順:

- 1) メニューから「Configuration」→「Power Reduction」→「LED」と順にクリックします。
- 2) LED の輝度を指定する時刻をプルダウンメニューから選択します。
- 3) 項 2) に指定したい LED の輝度をプルダウンメニューから選択します。
- 4) 必要があれば、「Add Time」ボタンをクリックして、時刻を追加します。

(次ページに続く)

(前ページの続き)

- 5) 追加した時刻を削除する場合は、該当する行の「Delete」のチェックボックスを ON にして、「Save」ボタンを押します。
- 6) リンクが変化したときに最大輝度にする秒数を指定します。
- 7) リンクエラー時に輝度を最大にするかどうかを指定します。
- 8) 「Save」ボタンをクリックして設定を保存します。

The screenshot shows the 'LED Power Reduction Configuration' page. It includes a table for 'LED Intensity Timers' with columns 'Delete', 'Time', and 'Intensity'. Below the table is an 'Add Time' button. The 'Maintenance' section has two checkboxes: 'On time at link change' and 'On at errors', each with a time input field. At the bottom are 'Save' and 'Reset' buttons. Red lines with numbers point to specific elements: 2 points to the 'Time' dropdown, 3 points to the 'Intensity' dropdown, 4 points to the 'Add Time' button, 5 points to the 'Delete' checkbox, 6 points to the 'On time at link change' time field, and 7 points to the 'On at errors' checkbox.

2) 時刻のプルダウンメニュー。  
24 時間制です。

3) 輝度のプルダウンメニュー。

4) 時刻の項目を増やします。

5) 追加した時刻を削除したい場合にチェックを入れて、「Save」ボタンを押します。

6) リンクが変化した際の最大輝度を維持する時間を指定します。

7) チェックを入れると、エラー時に最大輝度になります。

## 8.2. 省電力イーサネットの設定

EEE Configurationページを使用して、指定したキューにEnergy Efficient Ethernet(EEE: 省電力型イーサネット)の設定をします。データの転送を急ぐキューを指定すると、最大の待ち時間の後、キューに溜まっているデータ量を考慮せずにデータを廃棄します。

### 8.2.1. 省電力イーサネット設定のヒント

- 1) トラフィックがない場合、省電力回路によって EEE が動作します。ポートが転送すべきデータを得ると、全ての関連する回路が起動しますが、回路の起動に掛かる時間を、ウェイクアップタイムと呼びます。  
トラフィックがない場合、省電力回路によって EEE が動作します。ポートが転送すべきデータを得ると、全ての関連する回路が起動しますが、回路の起動に掛かる時間を、ウェイクアップタイムと呼びます。デフォルトのウェイクアップタイムは、1Gbps リンクでは 1.7μs、他のリンクスピードでは 30μs です。

(次ページに続く)

(前ページの続き)

受信と送信の両方を行うデバイスは、トラフィックが発生したときに全ての回路を確実に起動する必要があるため、各 EEE デバイスはウェイクアップタイムの値を一致させなければなりません。

デバイスは LLDP プロトコルを用いて、デバイスのウェイクアップタイムの情報を交換します。省電力を最大にするために、データがポートから転送可能になっても直ぐには開始せず、代わりに 3000 バイトのデータがポートのキューに溜まるまで待ちます。

溜まったデータが 3000 バイトよりも少ない場合に大きな遅延が発生することを避けるため、データは常に 48μs 後に転送され、ウェイクアップタイムに加えて最大 48μs の最大遅延を与えます。

- もし必要であれば、フレームと指定のキューを関連させることにより、指定したフレームの遅延を最小にすることが可能です(EEE Urgent Queue)。急ぎのキューが転送すべきデータを得たとき、回路は直ちに起動し、遅延はウェイクアップタイムまで低減します。

## 8.2.2. 省電力イーサネットのパラメータ

- 1) Port: 設定の対象となるポートの番号。
- 2) EEE Enabled: 指定したポートの EEE を、有効あるいは無効にします。
- 3) EEE Urgent Queues: 指定されたキューは、最大遅延時間の経過後にデータを廃棄します。

### 省電力イーサネットの設定手順

- 1) メニューから「Configuration」→「Power reduction」→「EEE」を順にクリックします。
- 2) EEE を使用する回路を選択します。
- 3) 必要ならば EEE Urgent Queues も指定します。(urgent queue: データが溜まると、デフォルトのウェイクアップタイムの経過後、起動するキュー)
- 4) 「Save」ボタンをクリックして設定を保存します。

EEE Configuration

Port	EEE Enabled	EEE Urgent Queues							
		1	2	3	4	5	6	7	8
1	<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"/>
2	<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"/>
3	<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"/>
4	<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"/>
5	<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"/>
6	<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"/>
7	<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"/>
8	<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"/>

Save Reset

## 9. 熱保護設定 (SMCGS10 のみ対応)

本スイッチは、過負荷時等の異常な温度上昇から本体を守る保護機能を有しています。ポート毎に優先度と許容温度を指定することができます。

本章では、これらの設定について説明します。

### 9.1. 熱保護設定のヒント

熱保護は、スイッチのASICチップをオーバーヒートから保護するために使用します。スイッチの内部温度が指定した保護レベルを超えたとき、消費電力を減らすためにポートをオフにすることができます。ポートのシャットダウンは割り当てられた温度を元に優先順位をつけることができます。

### 9.2. 熱保護設定のパラメータ

- 1) **Priority:** 温度に対して関連付ける優先度。0～3 の 4 段階に分かれます。
- 2) **Temperature:** 優先度に対応した、ポートをオフにする温度
  - 設定値の範囲: 00:00～23:00
  - 設定値の範囲: 0～255 (°C)
  - デフォルト値: 255
- 3) **Port:** ポート番号です。
- 4) **Priority:** ポートをシャットダウンする優先度を割り当てます。
  - 設定値の範囲: 0～3
  - デフォルト値: 0

#### 熱保護設定の手順

- 1) メニューから「Configuration」→「Thermal Protection」を順にクリックします。
- 2) EEE を使用する回路を指定します。
- 3) 各優先度の温度の閾値を設定し、次いで優先度を各ポートに割り当てます。
- 4) 「Save」をクリックして設定を保存します。

**Thermal Protection Configuration**  
Temperature settings for priority groups

Priority	Temperature
0	255 °C
1	255 °C
2	255 °C
3	255 °C

2) ポートをシャットダウンする温度。  
優先度と組み合わせます。

**Port priorities**

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

4) ポートをシャットダウンする優先度

Save Reset

## 10. 各ポートにおける接続モード設定

ここでは、各ポートの接続パラメータを設定します。このページはオートネゴシエーションや手動による速度と二重化モードの設定、フロー制御、最大フレーム長、過度のコリジョンに対する応答あるいは、省電力モードの設定オプションを含んでいます。

### 10.1. ポートの接続モードのパラメータ

- 1) **Port:** ポート番号です。
- 2) **Link:** リンクの Up あるいは Down を示します。
- 3) **Speed(Configured):** ポートの速度と二重化モードを、オートネゴシエーションあるいは手動で行うかどうかを設定します。
  - 設定値の範囲は以下の7通りです。
 

i) <b>Disabled</b>	- インタフェースを無効にします。 セキュリティの理由により、インタフェースを無効にすることもできます。
ii) <b>Auto</b>	- オートネゴシエーションを許可します。オートネゴシエーションを使用すると、リンクパートナーとの間でそれぞれの機能が通知され、最適な設定が選定されます。
iii) <b>1Gbps FDX</b>	- 1Gbps、全二重通信 (RJ-45/SFP)
iv) <b>100Mbps FDX</b>	- 100Mbps、全二重通信 (RJ-45 のみ)
v) <b>100Mbps HDX</b>	- 100Mbps、半二重通信 (RJ-45 のみ)
vi) <b>10Mbps FDX</b>	- 10Mbps、全二重通信 (RJ-45 のみ)
vii) <b>10Mbps HDX</b>	- 10Mbps、半二重通信 (RJ-45 のみ)
  - デフォルト値: Auto (オートネゴシエーション許可)

**注意:** 1000BASE-T 規格は強制モードをサポートしません。オートネゴシエーションをお使い下さい。オートネゴシエーションを使わない場合、他のタイプのスイッチとの接続は保証しかねます。

- 4) **Flow Control(Configured)**: フローコントロールは、スイッチのバッファが満杯になったとき、端末或いは、スイッチに直接接続されたセグメントからのトラフィックをブロックすることによって、フレームロスを削除します。有効にした場合、Half Duplex 時=バックプレッシャー、Full Duplex 時=IEEE 802.3x PAUSE が使用されます。
- デフォルト値: チェックなし
- 5) **Maximum Frame Size**: スイッチを通過する最大のフレーム長を設定します。最大フレーム長を超えるパケットは破棄されます。
- 設定値の範囲: 9600~1518 (単位:byte)
  - デフォルト値: 9600 (単位:byte)
- 6) **Excessive Collision Mode**: ポートが過剰なコリジョンを検知したときの動作を設定します。
- 設定値の範囲:
    - Discard: コリジョンを 16 個受けたらフレームを廃棄する。
    - Restart: コリジョンを 16 個受けたら、バックオフアルゴリズムで再開する。
  - デフォルト値: Discard
- 7) **Power Control**: 他のデバイスと接続されたケーブルの長さによって、ポートに供給する電力を調整します。接続条件を維持するのに十分な電力だけが供給されます。IEEE 802.3 は、イーサネットの規格と、続いて 100m で動作するケーブル接続に基づいた電力の必要条件を定義します。省電力モードを可能にすると、20m あるいはそれ以下のケーブル長で使用する電力を十分低減でき、信号の完全性を保証し続けます。
- 設定値の範囲:
    - Disabled: すべての省電力機能を禁止する。
    - ActiPHY: リンクダウンの省電力を許可する。
    - PerfectReach: リンクアップの省電力を許可する。
    - Enabled: リンクアップとリンクダウンの省電力を許可する。
  - デフォルト値: Disabled

### 接続モードの設定手順

- 1) メニューから「Configuration」→「Ports」をクリックします。
- 2) Speed の「Configured」の設定をプルダウンメニューから選択します。
- 3) Flow Control の「Configured」にチェックを入れます。
- 4) 「Maximum Frame Size」を入力します。
- 5) 「Excessive Collision Mode」の設定をプルダウンメニューから選択します。
- 6) 「Power Control」の設定をプルダウンメニューから選択します。
- 7) 「Save」ボタンをクリックして設定を保存します。

6) Power Control

5) Excessive Collision Mode

3) Flow Control (Configured)

2) Speed (Configured)

4) Maximum Frame Size

The screenshot shows the 'Port Configuration' interface with a table of 10 ports. Annotations with red arrows point to specific settings in the table:

- '6) Power Control' points to the 'Power Control' column.
- '5) Excessive Collision Mode' points to the 'Excessive Collision Mode' column.
- '3) Flow Control (Configured)' points to the 'Configured' checkbox in the 'Flow Control' section.
- '2) Speed (Configured)' points to the 'Configured' dropdown menu in the 'Speed' section.
- '4) Maximum Frame Size' points to the 'Maximum Frame Size' input field.

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode	Power Control
		Current	Configured	Current Rx	Current Tx	Configured			
1	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
2	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
3	100fdx	Auto	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
4	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
5	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
6	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
7	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
8	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600	Discard	Disabled
9	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600		
10	Down	Auto	Auto	X	X	<input type="checkbox"/>	9600		

Save Reset



## 11. セキュリティ

本章ではユーザーからスイッチへのアクセス、データシステムへのアクセスに対しての認証によるアクセスコントロールを説明します。

### 11.1. セキュリティの説明

本スイッチではセキュリティ機能を大別し設定を Management Access Security と General Security Measures 2 項目に分けています。

1) Management Access Security (メインメニューSecurity 下の Switch 項目設定ページ)

管理目的でのアクセスをスイッチに登録されたユーザー名とパスワードをもとにした認証や、ユーザーアクセスを RADIUS や TACACS+ サーバを使用して管理することができます。また他の認証方式として Secure Shell (SSH)、Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL)、IP アドレスでの認証、SNMP をサポートしています。これらの認証設定は Switch 設定ページにて行うことができます。

2) General Security Measures (メインメニューSecurity 下の Network 項目設定ページ)

本スイッチは許可されたユーザーのみがネットワークにアクセスできるよう、さまざまなデータトラフィック分離方法をサポートしています。Private VLAN や IEEE802.1X などが上記目的のために広く使用されています。

上記に上げた方法以外にも本スイッチではポート単位でアクセスできるユーザー数の制限機能、DHCP Snooping 機能、IP Source Guard 機能、ARP Inspection 機能を本スイッチは実装し許可の無いユーザーからのネットワークアクセスを制限することができます。

以下に Management Access Security、General Security Measures にて設定可能なセキュリティ機能の設定方法を説明します。

### 11.2. Management Access Security: Switch 項目下のセキュリティ設定

本章では Management Access Security 機能の設定方法を説明します。

#### 11.2.1. ユーザアカウントの設定

スイッチに作成されたユーザーとそのパスワードをもとにユーザーに権限を付与しスイッチの運用・管理権限を統制することができます。

User Configuration ページにてスイッチに作成されたユーザーのアクセス権限を設定します。

#### 11.2.2. ユーザアカウント設定のガイドライン

本スイッチは管理者ユーザー admin が初期設定時に登録されています。ユーザー admin の初期設定時パスワードは admin です。ユーザー admin には全ての権限が与えられているため、初期パスワードを即座に変更しパスワードは安全な場所に保管してください。

(次ページに続く)

(前ページの続き)

アドミニストレーターは Privilege Level 15 を与えられており、全ての項目を閲覧が可能で、設定の書き換えも行うことができます。

Privilege Level はスイッチ機能のグループ毎に設定が可能となっています。初期設定ではほとんどのグループが Privilege Level 5 (閲覧のみ可能)、か Privilege Level 10、(閲覧及び設定変更可能)な権限を付与されています。しかし、ソフトウェアアップデート、設定の初期化といったシステム管理に必要な作業を行うには Privilege Level 15 が必要になります。

従って、管理者権限を持つユーザーには Privilege Level 15 を、本スイッチの運用権限が必要なユーザーには Privilege Level 10 を、監視目的が主なユーザーには Privilege level 5 を各々付与するのが一般的です。

### 11.2.3. ユーザアカウント設定パラメータ

- 1) **UserName:** ユーザー名(最大長:8 文字;最大ユーザー数:16)
- 2) **Password:** ユーザーパスワード(使用可能文字数:0-8 文字、大文字と小文字は区別されません。)
- 3) **Password(again):** Password で入力した文字列を再入力します。Password で入力した文字列と一致しない場合はパスワードが変更されません。
- 4) **Privilege Level:** ユーザーの権限レベルを設定します(設定可能レベル(1-15)。各 Privilege Level の権限設定は以下の Privilege Level Configuration 項目にて設定できます。なお 4 つの Privilege Level が初期設定で定義されています。
  - 設定値の範囲:
    - 1: ポートステータスと統計情報の閲覧が可
    - 5: Maintenance と Debugging を除いたシステム機能設定の閲覧が可
    - 10: Maintenance と Debugging を除いたシステム機能の閲覧と設定変更が可
    - 15: Maintenance と Debugging を含むすべてのシステム機能の閲覧と設定変更が可

#### 既存ユーザアカウントの参照方法

メニューから「Configuration」→「Security」→「Switch」→「Users」を順にクリックします。



### ユーザアカウント設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「Users」
- 2) 「Add new user」ボタンをクリックします。
- 3) 「User Name」、「Password」、「Password (again)」を入力します。
- 4) 「Privilege Level」でユーザーの権限レベルを選択します。
- 5) 「Save」ボタンをクリックし設定を保存します。

### 11.3. Privilege Level の設定

Privilege Level ページはスイッチの機能をグループ単位に考えて、機能に対し Privilege Level を設定しユーザーの閲覧、設定変更に制限を設けることができます。

#### 11.3.1. Privilege Level 設定パラメータ

- 1) **Group Name:** 権限グループ名。ほとんどのグループ名は単一機能ごと(例 LACP、RSTP、QoS)に分かれていますが、複数機能を含んだグループ名もあります。以下に複数機能を含んだ、もしくは他のシステム設定へのアクセスができるグループ名とその説明を示します。

**System:** Contact、Name、TimeZone、Log

**Security:** Authentication、System Access Management、Port(Dot1x port、MAC Based & MAC Address Limit)、ACL、HTTPS、SSH、ARP Inspection、IP Source Guard

**IP:** Ping を除くすべて。

**Port:** VeriPHY を除くすべて

**Diagnostics:** Ping と VeriPHY

**Maintenance:** CLI-System Reboot、System Restore Default、System Password、Configuration、Save、Configuration Load、Firmware Load、Web-Users、Privilege Levels、Maintenance 全て

**Debug:** CLI でのみ有効なグループ

- 2) **Privilege Levels:** 全ての Privilege Level グループは以下の様に機能やシステム設定へのアクセス権限を設定できます。

Configuration Read-Only

Configuration Execute、Read-Write

Status/Statistics Read-Only

Status/Statistics Read-Write

4 つのアクセス権限レベルがデフォルトで設定されています。

Level1: ポートの状態と統計を閲覧可能

Level5: Maintenance と Debugging 以外のシステム機能を閲覧可能

Level10: Maintenance と Debugging 以外のシステム機能を閲覧, 設定が可能

Level15: Maintenance と Debugging を含むシステム機能の閲覧, 設定が可能

### ユーザアカウント設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「Privilege Level」
- 2) 各機能グループに対して必要な「Privilege Level」を設定します。
- 3) 「Save」ボタンをクリックし設定を保存します。

Privilege Level Configuration					
Group Name	Privilege Levels				
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write	
Aggregation	5	10	5	10	
Debug	15	15	15	15	
Diagnostics	5	10	5	10	
DualCPU	5	10	5	10	
EEE	5	10	5	10	
IP	5	10	5	10	
IPMC_Snooping	5	10	5	10	
LACP	5	10	5	10	
LLDP	5	10	5	10	
LLDP_MED	5	10	5	10	
MAC_Table	5	10	5	10	
MVR	5	10	5	10	
Maintenance	15	15	15	15	
Mirroring	5	10	5	10	
POE	5	10	5	10	
Port_Security	5	10	5	10	
Ports	5	10	1	10	
Private_VLANs	5	10	5	10	
QoS	5	10	5	10	
SNMP	5	10	5	10	
Security	5	10	5	10	
Spanning_Tree	5	10	5	10	
System	5	10	1	10	
UPnP	5	10	5	10	
VCL	5	10	5	10	
VLANs	5	10	5	10	
Voice_VLAN	5	10	5	10	

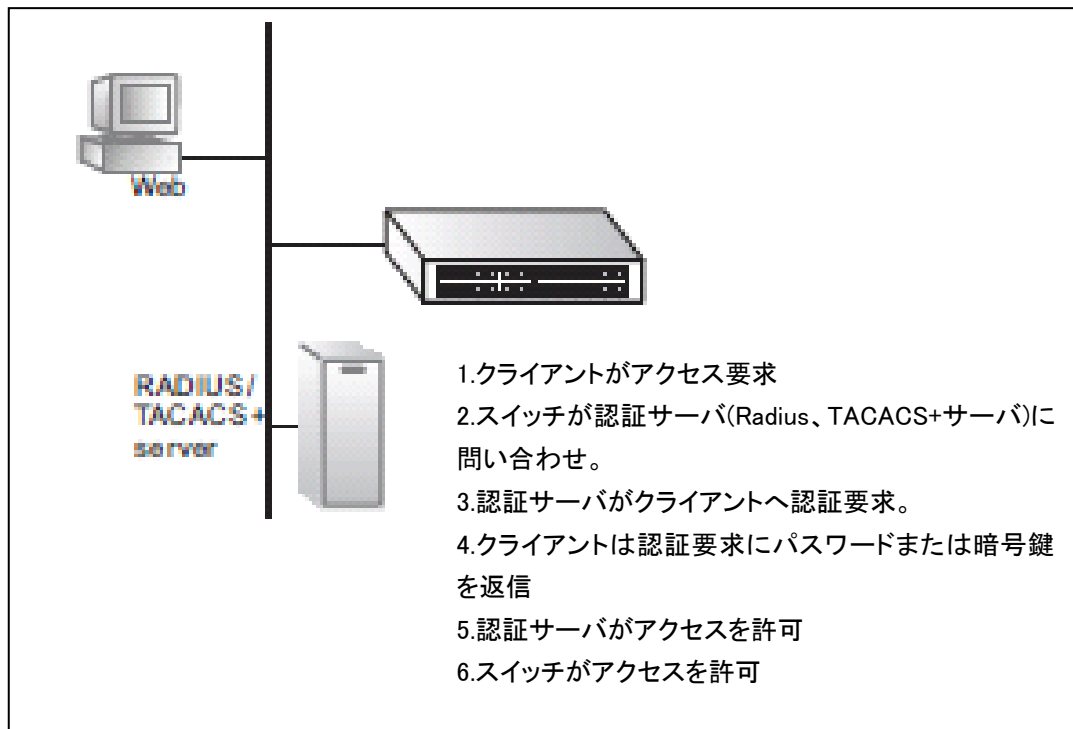
Save Reset

#### 11.4. リモートアクセス認証の設定

ユーザーのリモートアクセスは認証を使用して制限することができます。アクセス制限はスイッチにて設定したユーザー名とパスワードを使用する方法と RADIUS や TACACS+といった認証サーバを使用する方法があります。

**注意：** RADIUS サーバを使用したポート認証 IEEE802.1X の設定は、後述の別章でも説明しています。

Remote Authentication Dial-in User Service(RADIUS)と Terminal Access Controller Access Control System Plus(TACACS+)はサーバ上で稼働するソフトウェアのログオン認証プロトコルです。RASIDUS または TACACS+との連携が可能なネットワーク機器と連動してネットワークへのアクセスを制限します。



##### 11.4.1. リモートアクセス認証設定ガイドライン

本スイッチは以下のアクセス認証サービスをサポートしています。

- 1) Telnet、SSH、WEB によるユーザー認証。
- 2) Telnet、SSH、WEB によるユーザーのアクセス管理
- 3) スイッチを経由しての IEEE802.1X 認証ユーザーのアクセス管理

(次ページに続く)

(前ページの続き)

設定を施さない限りユーザーアクセスはスイッチ内の認証データベースと照合されます。もし外部の認証サーバを使用する場合は、Network Access Server Configuration項目にて認証方法やパラメータを適切に設定する必要があります。

ログイン認証にRADIUSやTACACS+を使用する場合は、ユーザー名、パスワードが認証サーバ上に設定しておく必要があります。また、認証時に使用される暗号方法も設定する必要があります。

本スイッチでは認証サーバとクライアント間のメッセージが暗号化され、暗号化に以下の暗号方法が使用することができます。

MD5: Message-Digest 5

TLS: Transport Layer Security

TTLS: Tunneled Transport Layer Security

**注意:** RADIUS、TACACS+サーバは AAA をサポートしていると仮定しています。RADIUS、TACACS+の設定はこの取扱説明書では説明範囲外になります。RADIUS、TACACS+サーバの設定はご使用になる RADIUS、TACACS+サーバの取扱説明書をご参照ください。

#### 11.4.2. リモートアクセス認証設定パラメータ

- 1) **Client:** 管理者が Telnet、SSH、WEB を通してスイッチにログインする際にどのように認証されるか。
- 2) **Authentication Method:** 認証方法を選択します。これには None、Local、RADIUS、TACACS+。初期設定値は local です。None を選択した場合指定した管理インタフェースからのアクセスは無効になります。
- 3) **Fallback:** 選択した認証方法が利用不可の場合にスイッチ上の認証データベースを使用してアクセスを行います。Fallback は Authentication Method の設定が”none”、”local”以外の時に使用できます。

#### リモートアクセス認証の設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「Auth Method」を順にクリックします。
- 2) 管理ユーザータイプごとに認証方法を設定します。None、local 以外を選択した場合には Fallback 機能を使用するか指定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

Authentication Method Configuration		
Client	Authentication Method	Fallback
console	local	<input type="checkbox"/>
telnet	local	<input type="checkbox"/>
ssh	local	<input type="checkbox"/>
web	local	<input type="checkbox"/>

Save Reset

## 11.5. SSH の設定 (未サポート)

SSH 項目にて Secure Shell(SSH)経由でスイッチへのアクセスを設定します。ユーザーが SSH プロトコルを使用してスイッチへのアクセスを行うとスイッチの管理インタフェースとユーザーとの通信は暗号化され、秘匿性を高めます。SSH は Telnet の代替として安全なリモートアクセス手段を提供します。

### 11.5.1. SSH 設定のガイドライン

SSH でスイッチにアクセスする場合にはユーザーの使用する端末が SSH クライアントをインストールしている必要があります。

本スイッチは SSH ver.1.5 と ver.2.0 のクライアントに対応しています。

スイッチの SSH サービスはパスワード認証のみサポートしています。パスワードはスイッチ上、外部の RADIUS サーバ、TACACUS+サーバでのみ認証されます。

SSH でパスワード認証を使用する際に、公開鍵がクライアントに付与される必要があります。公開鍵はクライアント端末の最初のログイン時に付与されます。クライアント側での暗号鍵の作製は必要ありません。

スイッチ上の SSH サービスは最大 4 セッションまでサポートします。最大セッション数は SSH と Telnet でのセッション両方を合わせたものになります。

例: リモートアクセスが Telnet 2 セッション、SSH 2 セッション同時にあった場合、合計 4 セッションのため Telnet または SSH を使用したリモートアクセスはこれ以上受け付けられません。

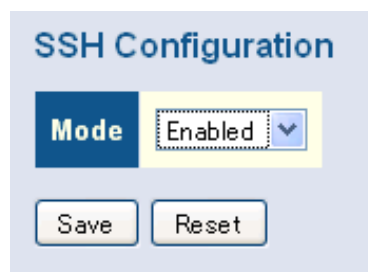
### 11.5.2. SSH 設定パラメータ

- 1) **Mode:** スwitchの SSH を有効または無効に設定します。

➤ デフォルト値: Enabled

#### SSH の設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「SSH」を順にクリックします。
- 2) SSH を有効にするには Mode を Enabled に、無効にするには Disabled を選択します。
- 3) 「Save」ボタンをクリックして設定を保存します。



## 11.6. HTTPS の設定

HTTPS項目にてHypertext Transfer Protocol (HTTPS) over the Secure Socket Layerの設定を行います。  
HTTPSは暗号化による安全なWEBユーザーインタフェースを提供します。

### 11.6.1. HTTPS 設定のガイドライン

HTTPS を使用するに明示的に URL を入力してください。

例: https://device :ポート番号

HTTPS を使用するとスイッチとリモートアクセス端末間では以下の様なやり取りが行われます。

- 1) リモートアクセス端末でスイッチ上の HTTPS サーバが使用するデジタル証明書を認証します。
- 2) リモート端末とスイッチ上のサーバは、コネクションに使用するセキュリティプロトコルの情報交換をします。
- 3) リモート端末とスイッチ上のサーバはデータを暗号化し、複合化するためのセッションキーを生成します。

以下のWEBブラウザとオペレーティングシステム(OS)がHTTPSをサポートしています。

WEBブラウザ	OS
Internet Explorer 5.0またはそれ以降	Windows98、Windows NT(service Pack 6a 適用)、Windows 2000、Windows XP、Windows VISTA、Windows 7
Netscape 6.2またはそれ以降	Windows98、Windows NT(service Pack 6a 適用)、Windows 2000、Windows XP、Windows VISTA、Solaris 2.6
Mozilla Firefox2.0.0.0またはそれ以降	Windows 2000、Windows XP、Windows VISTA、Unix

### 11.6.2. HTTPS 設定パラメータ

- 1) **Mode:** スwitchの HTTP サービスを有効、無効にします。  
     ➤ デフォルト値: Enabled
- 2) **Automatic Redirect:** Automatic Redirect パラメータを有効とするとスイッチへの HTTP でのアクセスを HTTPS へのアクセスに自動的にリダイレクトします。  
     ➤ デフォルト値: Enabled

(次ページに続く)



(前ページの続き)

## HTTPSの設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「HTTPS」を順にクリックします。
- 2) HTTPS を有効にするには Mode を Enabled に、無効にするには Disabled を選択します
- 3) 要に応じて Automatic Redirect を有効:Enabled、無効:Disabled に設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

## 11.7. アクセスマネジメント IP アドレスフィルタリングの設定

アクセスマネジメント設定項目ではWEB、Telnet、SNMPでのスイッチへのアクセスをIPアドレス、IPアドレスグループをもとにフィルタリングすることができます。最大16までIPアドレスまたは、IPアドレスグループリストを作成できアクセスの許可を与えることが可能です。

スイッチは初期状態で全てのIPアドレスに対してアクセスを許可しています。アクセスマネジメントでは特定のIPアドレスに対してのみ許可を与えることで、リストに無いアドレスからのアクセスを拒否します。

### 11.7.1. アクセスマネジメント設定パラメータ

- 1) **Mode:** IP アドレスベースでユーザーアクセスのフィルタリングを行います。Enabled でフィルタリングを有効、Disabled で無効にします。  
 ➤ デフォルト値: Disabled
- 2) **Start IP Address:** フィルタリングする IP アドレス範囲のスタートアドレス。
- 3) **End IP Address:** フィルタリングする IP アドレス範囲のエンドアドレス。
- 4) **HTTP/HTTPS:** HTTP や HTTPS を使用して WEB インタフェースへのアクセスを IP アドレスベースでフィルタリングする場合に選択します。
- 5) **SNMP:** SNMP でのアクセスを IP アドレスベースでフィルタリングする場合に選択します。
- 6) **Telnet/SSH:** Telnet や SSH でのアクセスを IP アドレスベースでフィルタリングする場合に選択します。

### アクセスマネジメントの設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「Access Management」を順にクリックします。
- 2) アクセスマネジメントを有効にするには Mode を Enabled に、無効にするには Disabled を選択します
- 3) 「Add new entry」をクリックします。
- 4) アクセスを許可する IP アドレスの範囲を「Start IP Address」に、アドレス範囲の最初の IP アドレスを、「End IP Address」にアドレス範囲の最後の IP アドレスを入力します。
- 5) HTTP/HTTPS、SNMP、TELNET/SSH の中からアドレスフィルタリングを行うプロトコルのチェックボックスにチェックを入れ選択します。
- 6) 「Save」ボタンをクリックして設定を保存します。
- 7) フィルタリングのリストを削除するには「Delete」ボタンをクリックします。

Access Management Configuration

Mode Disabled

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

Add new entry

Save Reset

## 11.8. SNMP の設定

Simple Network Management Protocol (SNMP)はネットワーク上のネットワーク機器を監視(モニタリング)・制御するための情報の通信プロトコルです。SNMPではルータ、スイッチ等のネットワーク機器や、PC端末などを監視・制御することができます。SNMPを使用することでネットワーク機器の状態把握、潜在的な問題点や障害の検知に利用できます。

SNMPで監視・制御できるネットワーク機器はエージェントと呼ばれるSNMPソフトウェアがインストールされています。SNMPエージェントはネットワーク機器のパフォーマンス状態を示す“Managed Objects”と呼ばれるパラメータを保持し、“Managed Objects”はManaged Information Base(MI B)により定義されています。

本スイッチはSNMPエージェントを実装しSNMP v1、v2c、v3をサポートしています。エージェントは継続的にスイッチのハードウェア状態とスイッチのポートを通るトラフィックをモニターしています。ネットワーク監視端末はHP Open View等のSNMP管理ソフトウェア(SNMPマネージャー)を導入することでスイッチの情報を収集することができます。

SNMP v1、v2cを使用してスイッチへのアクセスはcommunityと呼ばれる文字列により制御されています。スイッチにSNMPマネージャーがアクセスするにはSNMPエージェント同じcommunity文字列を設定する必要があります。

SNMPv3は認証、メッセージの暗号化、改ざん防止といったセキュリティ機能があり、セキュリティレベルを持ったセキュリティモデルにより構成されています。

セキュリティモデルは、SNMPv1、SNMPv2c、SNMPv3の3種が定義されています。

ユーザーはセキュリティモデルとセキュリティレベルによって定義された“group”に割り当てられます。それぞれの“group”がMIBを参照、書き込みといった“Views”として知られるアクセス権限を定義されます。本スイッチは初期設定で“Views”の値に全てのMIB objectsが設定され、セキュリティモデルにSNMPv1、SNMP v2cが設定されています。

下記に本スイッチで利用可能なセキュリティモデルとセキュリティレベル、スイッチのSNMP初期設定値を記します。

Model	Level	Community String	Group	Read View	Write View	Security
v1	noAuth NoPriv	public	default_ro_group	default_view	none	Community string only
v1	noAuth NoPriv	Private	default_rw_group	Default_view	default_view	Community string only
v1	noAuth NoPriv	user defined	user defined	user defined	user defined	Community string only
v2c	noAuth NoPriv	public	default_ro_group	default_view	none	Community string only
v2c	noAuth Nopriv	private	default_rw_group	default_view	default_view	Community string only
v2c	noAuth NoPriv	user defined	user defined	user defined	user defined	Community string only
v3	noAuth Nopriv	user defined	default_rw_group	default_view	default_view	A user name match only
v3	Auth NoPriv	user defined	user defined	user defined	user defined	Provides user authentication via MD5 or SHA Algorithms
v3	Auth Priv	user defined	user defined	user defined	user defined	Providers user authentication via MD5, or SHA algorithms and data privacy using DES 56-bit encryption

**注意：** 既存定義のデフォルト“Group”と“View”は削除が可能です。カスタマイズした“Group”と“View”の定義も可能です。

### 11.8.1. SNMP システムとトラップの設定

SNMP項目ではSNMPの基本設定、SNMPトラップの設定を行うことができます。SNMPでスイッチを管理するには最初にSNMPプロトコルを有効にする必要があります。トラップメッセージをSNMPマネージャに送るには、トラップ機能を有効にし、送信先のホストを設定する必要があります。

### 11.8.2. SNMP システムとトラップ設定パラメータ

#### SNMP システムの設定パラメータ

- 2) **Mode:** SNMP サービスを Enabled で有効、Disabled で無効にします。
  - デフォルト値: Enabled
- 3) **Version:** 使用する SNMP のバージョンを指定します。選択可能バージョンは SNMPv1、SNMPv2c、SNMPv3 です。
  - デフォルト値: SNMPv2c
- 4) **Read Community:** SNMP エージェントへ情報の参照のみでアクセスする際に使用するコミュニティ名を設定します。コミュニティ名には使用する文字と文字数に制限があります。
  - 設定値の範囲: 0～255文字、ASCIIキャラクタ33～126
  - デフォルト値: public
 

このパラメータはSNMPv1とSNMPv2にのみ適用され、SNMPv3は User-based Security Model (USM)を認証に使用します。
- 5) **Write Community:** SNMP エージェントへ情報の書き込み・参照でアクセスする際に使用するコミュニティ名を設定します。コミュニティ名には使用する文字と文字数に制限があります。
  - 設定値の範囲: 0～255文字、ASCIIキャラクタ33～126
  - デフォルト値: public
 

このパラメータはSNMPv1とSNMPv2にのみ適用され、SNMPv3は User-based Security Model (USM)を認証に使用します。
- 6) **Engine ID:** SNMPv3 engine ID はユーザーパスワードと一緒に使用され、SNMP パケットの認証や暗号化に使用されます。スイッチ上の SNMPv3 engine ID は自動で生成され、初期値の SNMPv3 engine ID となりますが、削除してしまうと全ての SNMP ユーザーが消去され、手動で既存ユーザーを設定する必要があります。Engine ID に使用する値は 10～64 桁の十六進数を使用し、そのうち全て 0 と全て F の ID は使用できません。
  - デフォルト値: 800007e5017f000001

(次ページに続く)

(前ページの続き)

### Trap の設定パラメータ

- 1) **Trap Mode:** SNMP Trap を Enabled で有効、Disabled で無効に設定します。SNMP Trap を有効にすることで障害発生時に SNMP マネージャーへメッセージを送ることができます。
  - デフォルト値: Disabled
- 2) **Trap Version:** SNMP Trap に使用する SNMP のバージョンを指定します。SNMPv1、SNMPv2c、SNMPv3 が選択可能です。
  - デフォルト値: SNMPv1
- 3) **Trap Community:** SNMP Trap パケット送信に使用する SNMP のコミュニティ名を指定します。コミュニティ名には使用する文字と文字数に制限があります。
  - 設定値の範囲: 0~255文字
  - ASCIIキャラクタ: 33~126
- 4) **Trap Destination Address:** SNMP Trap パケットの送信先の IP アドレスを IPv4 で指定します。
- 5) **Trap Destination IPv6 Address:** SNMP Trap パケットの送信先の IP アドレスを IPv6 で指定します。
- 6) **Trap Authentication Failure:** SNMP 認証に失敗した際に通知メッセージを送ります。
  - デフォルト値: Enabled
- 7) **Trap Link-up Link-down:** スイッチのポートがリンクアップ、リンクダウンした際に通知メッセージを送ります。
  - デフォルト値: Enabled
- 8) **Trap Inform Mode:** Informメッセージとして通知を送信するかしないかを設定します。Trap Inform ModeはSNMPv2cとSNMPv3でのみ利用可能です。

**注意:** Trap メッセージの受信者はスイッチに対して返信しないため、返信要求を行う Inform メッセージと比較してトラップメッセージは同等の信頼性がありません。

Inform メッセージは受信者が重要なメッセージを受信しているか確認する目的で使えますが、一方で、Informメッセージは返信メッセージを受信するまでメッセージを保存するため、スイッチのリソースを消費します。

また、Informメッセージはトラフィックを増加させる要因にもなるため、Inform か Trap かどちらを導入するかは効果を考えて導入してください。

(次ページに続く)

(前ページの続き)

- 9) **Trap Inform Timeout**: Informメッセージの再送間隔を設定します。
  - 設定値の範囲: 0～2147秒
  - デフォルト値: 1秒
- 10) **Trap Inform Retry Times**-Informメッセージ受信者から受信の通知が無い場合の最大再送回数を設定します。
  - 設定値の範囲: 0～255回
  - デフォルト値: 5回
- 11) **Trap Probe Security Engine ID**(SNMPv3): トラップまたはInformメッセージを使用する際に Engine IDを使用するかしないかを設定します。
  - デフォルト値: Enabled
- 12) **Trap Security Engine ID**(SNMPv3): SNMPのSecurity Engine IDを指定します。SNMPv3は認証に使用するUMSを利用してトラップまたはInformメッセージを送信します。トラップとInformメッセージは1意のEngine IDが必要となります。

“Trap Probe Security Engine ID”が有効に設定されると“Trap Security Engine ID”は自動的に調査されるか、“Trap Security Engine ID”で指定されたものが使用されます。Engine IDに使用する値は10～64桁の十六進数を使用し、そのうち全て0と全てFのIDは使用できません。

**注意:** Trap Security Engine ID に engine ID を手動で入力する場合は Trap Probe Security Engine ID を Disabled に設定しておく必要があります。

- 13) **Trap Security Name**(SNMPv3): Trap Security Nameを選択します。SNMPv3は認証に使用するUMSを利用してトラップまたはInformメッセージを送信します。トラップとInformメッセージは1意のsecurity nameが必要となります。

**注意:** Trap Security Name を指定する際には、最初に同じに engine ID を持った SNMPv3 ユーザーを入力してください。手動で入力する場合は Trap Probe Security Engine ID を Disabled に設定しておく必要があります。

### SNMPシステムとSNMP Trapの設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「SNMP」→「SYSTEM」を順にクリックします。
- 2) SNMP を有効にするには Mode を Enabled に選択します。使用する SNMP のバージョンを Version で指定し必要な場合はコミュニティ名( Read Community、Write Community)を変更してください。SNMPv3 を使用する場合は Engine ID を設定します。
- 3) SNMP Trap Configuration 設定 Table にて Trap Mode を Enabled に設定し、スイッチのトラップメッセージ送信を有効にします。  
Trap Version、Trap Type、Trap Community、SNMP マネージャーの IP アドレスを IPv4 または IPv6 で入力します。  
送信するトラップメッセージのタイプ(Trap Authentication Failure、Trap Link-up and Link-Down)を選択します。SNMPv2c、SNMPv3 を使用している場合は Trap Inform Mode を設定します。  
SNMPv3 を使用の場合は Trap Probe Security Engine ID、Trap Security Engine ID、Trap Security Name を設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

SNMP Trap Configuration

Trap Mode	Disabled
Trap Version	SNMP v3
Trap Community	public
Trap Destination Address	
Trap Destination IPv6 Address	::
Trap Authentication Failure	Enabled
Trap Link-up and Link-down	Enabled
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5
Trap Probe Security Engine ID	Enabled
Trap Security Engine ID	Probe Fail
Trap Security Name	None

Save Reset

## 11.9. SNMPv3 コミュニティーアクセスストリングの設定

SNMPv3 Community Configuration項目でコミュニティ名の設定を行います。SNMPv1とSNMPv2cで使用するコミュニティ名は全てSNMPv3 Community Configuration項目のテーブルに記述されなければなりません。

### 11.9.1. SNMPv3 コミュニティーアクセスストリング設定パラメータ

- 1) **Community:** SNMP エージェントへのアクセスを許可するコミュニティ名を入力してください。  
使用できる文字列数に制限があります。1～32 文字、ASCII キャラクタ 33～126 まで。SNMP サービスを Enabled で有効、Disabled で無効にします。  
➤ デフォルト値: public、private
- 2) **Source IP:** SNMP クライアントの IP アドレスを設定します。
- 3) **Source Mask:** SNMP クライアントのサブネットマスクを設定します。

#### SNMPv3コミュニティアクセスストリング設定の設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「SNMP」→「Communities」を順にクリックします。
- 2) 初期設定のコミュニティ名に Source IP と Source Mask を入力して使用するか、初期設定のコミュニティ名を削除し、SNMPv1 と SNMPv2 c 用に Add new community をクリックして新しいコミュニティ名を作成します。新規に作成したコミュニティ名に Source IP と Source Mask を入力してください。
- 3) 「Save」ボタンをクリックして設定を保存します。

**SNMPv3 Community Configuration**

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0



## 11.10. SNMPv3 ユーザーの設定

SNMPv3 ユーザー設定項目にてSNMPv3ユーザーのリモートEngine IDと一意のユーザー名を設定します。セキュリティレベル、認証タイプ、秘匿性保護のためのプロトコルも本項目にて設定する必要があります。

**注意：** ユーザーは SNMPv3 Group Configuration 上の USM Security Model と SNMPv3 Access Configuration で割り当てられたグループに関連づけられています。

### 11.10.1. SNMPv3 ユーザー設定パラメータ

- 1) **Engine ID:** リモートユーザーが登録しているSNMPエージェントの engine ID を登録します。  
engine ID に使用する値は 10～64 桁の十六進数を使用し、そのうち全て 0 と全て F の ID は使用できません。  
Inform メッセージをリモートの SNMPv3 ユーザーに送信するには、リモートユーザーが登録している SNMP エージェント機器の engine ID を設定する必要があります。リモートの engine ID は認証に使用するダイジェストの生成とリモートのエージェントにパケットを暗号化して送信する際に使用されます。
- 2) **User Name:** SNMP エージェントに接続するユーザー名を入力します。使用できる文字列数に制限があります。1～32 文字、ASCII キャラクタ 33～126 まで。
- 3) **Security Level:** ユーザーに割り当てられたセキュリティレベルを設定します。セキュリティレベルは以下になります。  
**NoAuth、Nopriv-SNMP**情報を認証、暗号化なしで通信します。SNMPv3は初期状態でこのセキュリティレベルに設定されています。  
**Auth、Nopriv-SNMP**情報を認証に使用し、暗号化なしで通信します。  
**Auth、Priv-SNMP**情報を認証に使用し、暗号化して通信します。
- 4) **Authentication Protocol:** ユーザー認証に使用される認証方法を設定します。選択可能認証方法は None、MD5、SHA。  
 ➤ デフォルト値: MD5
- 5) **Authentication Password:** 認証に使用されるパスフレーズを入力します。使用できる文字列数に制限があります。MD5 は 1-32 文字まで、SHA は 8-40 まで。
- 6) **Privacy Protocol:** 暗号化に使用するアルゴリズムを指定します。56bit-DES のみ利用可能です。None、DES が選択可能。  
 ➤ デフォルト値: DES
- 7) **Privacy Password:** プライバシーパスフレーズを入力します。使用できる文字列数に制限があります。1-32 文字、ASCII キャラクタ 33-126 まで。

### SNMPv3ユーザー設定の設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「SNMP」→「Users」を順にクリックします。
- 2) Add new user をクリックし新規ユーザーの設定を行います。
- 3) リモート側 Engine ID を十六進数で入力します。Engine ID は十六進数最大 64 桁まで。
- 4) User name、Security Level、Authentication Protocol、Authentication Password、Privacy Protocol、Privacy Password を適宜設定します。
- 5) 「Save」ボタンをクリックして設定を保存します。

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

## 11.11. SNMPv3 Group の設定

SNMPv3 Group項目にてSNMPv3 Groupを設定します。SNMPv3 Groupはグループに割り当てられたユーザーの権限を定義し、ユーザーのviewsに対する読み込み、書き込みを制限します。スイッチ初期状態で定義されたグループを使用するか、または新規にグループを作成することも可能です。

### 11.11.1. SNMPv3 Group パラメータ設定

- 1) **Security Model:** ユーザーのセキュリティモデルを設定します。選択可能なセキュリティモデルは SNMPv1、SNMPv2c、usm (User-based Security Model)になります。
- 2) **Security Name:** SNMP エージェントに接続しているユーザー名を入力します。使用できる文字列数に制限があります。1-32 文字、ASCII キャラクタ 33-126 まで。
- 3) **Group Name:** SNMP エージェントに接続しているユーザー名を入力します。使用できる文字列数に制限があります。1-32 文字、ASCII キャラクタ 33-126 まで。

#### SNMPv3 Groupsの設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「SNMP」→「Groups」を順にクリックします。
- 2) Add new user をクリックし新規グループの設定を行います。
- 3) Security Level を選択します。
- 4) Security name を選択します。SNMPv1、SNMPv2c に関しては SNMPv3 Communities 項目の設定に基づいて Security name が表示されます。USM に関しては SNMPv3 Users Configuration 項目の設定に基づき Security name が表示されます。
- 5) Group name を入力します。グループに割り当てられた views は後述の SNMP Access Configuration 項目設定されている必要があります。
- 6) 「Save」ボタンをクリックして設定を保存します。

**SNMPv3 Group Configuration**

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

## 11.12. SNMPv3 Views の設定

SNMPv3 View項目設定では特定のMIB情報へのユーザーアクセスを制限することができます。既存のview“default\_view”は全てのMIB情報にアクセスできます。

### 11.12.1. SNMPv3 Views パラメータ設定

- 1) **View Name:** SNMP view 名を入力します。ユーザーのセキュリティモデルを設定します。使用できる文字列数に制限があります。1-32 文字、ASCII キャラクタ 33-126 まで。
- 2) **View Type:** MIB 情報の OID (Object Identifier)を SNMP view に含むか、除外するか指定します。
- 3) **OID Subtree:** 参照する MIB ツリー内の OID を指定します。OID の入力は最初にピリオド“.”を入力します。Wild card はアスタリスク“\*”を使用することができます。

#### SNMPv3 Viewsの設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「SNMP」→「Views」を順にクリックします。
- 2) Add new views をクリックし新規 views の設定を行います。
- 3) view name、view type、OID Subtree を入力します。
- 4) 「Save」ボタンをクリックして設定を保存します。

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

### 11.13. SNMPv3 Group Access Rights の設定

SNMPv3 Group Access項目ではグループ毎にアクセスを認められた特定のMIB情報を設定します。

#### 11.13.1. SNMPv3 Group Access Rights パラメータ設定

- 1) **Group Name:** SNMP グループ名を入力します。使用できる文字列数に制限があります。  
1-32 文字、ASCII キャラクタ 33-126 まで。
- 2) **Security Model:** ユーザーセキュリティレベルを指定します。any、SNMPv1、SNMPv2c、usm (User-based Security Model)  
➤ デフォルト値: any
- 3) **Security Level:** グループに割り当てるセキュリティレベルをします。選択可能セキュリティレベルは以下になります。  
 NoAuth、Nopriv-SNMP情報を認証、暗号化なしで通信します。SNMPv3は初期状態でこのセキュリティレベルに設定されています。  
 Auth、Nopriv-SNMP情報を認証し、暗号化なしで通信します。  
 Auth、Priv-SNMP情報を認証し、暗号化ありで通信します。
- 4) **Read View Name:** 読み込み権限のアクセスを設定します。
- 5) **Write View Name:** 書き込み権限のアクセスを設定します。

#### SNMPv3 Group Accessの設定手順

- 1) メニューから「Configuration」→「Security」→「Switch」→「SNMP」→「Access」を順にクリックします。
- 2) Add New Access をクリックし新規 Group Access Rights の設定を行います。
- 3) Group Name、Security Model、Security level、Read View name、Write View Name を適宜設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

SNMPv3 Access Configuration

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

#### 11.14. RMON 統計の設定 (SMCGS18/26/50 のみ対応)

RMON Statistics Configurationでは、RMON(リモートモニタリング)に関する設定をします。

##### 11.14.1. RMON Statistics Configuration パラメータ設定

- 1) **Delete:** エントリを削除します。
- 2) **ID:** アラームのインデックス番号を設定します。
- 3) **Data Source:** モニターするポート番号を指定します。

##### RMON Statistics Configurationの設定手順

- 1) ID, Data Source を適宜設定します。
- 2) 「Save」ボタンをクリックして設定を保存します。

Delete	ID	Data Source
Delete		.1.3.6.1.2.1.2.2.1.1. 0

Add New Entry Save Reset

### 11.15. RMON ヒストリー情報の設定 (SMCGS18/26/50 のみ対応)

RMON History Configurationでは、RMONヒストリー情報を収集するための設定を行います。

#### 11.15.1. RMON History Configuration パラメータ設定

- 1) **Delete:** エントリを削除します。
- 2) **ID:** アラームのインデックス番号を設定します。
- 3) **Data Source:** モニターするポート番号を指定します。
- 4) **Interval:** ヒストリーの保存間隔を指定します。
  - 設定値の範囲: 1-3600秒
  - デフォルト値: 1800秒
- 5) **Buckets:** 保持するヒストリーの数を指定します。
  - 設定値の範囲: 1-3600
  - デフォルト値: 50

#### RMON History Configurationの設定手順

- 1) ID, Data Source, Interval, Buckets を適宜設定します。
- 2) 「Save」ボタンをクリックして設定を保存します。

RMON History Configuration						
Delete	ID	Data Source	Interval	Buckets	Buckets Granted	
<input type="button" value="Delete"/>	<input type="text"/>	.1.3.6.1.2.1.2.2.1.1.	<input type="text" value="0"/>	<input type="text" value="1800"/>	<input type="text" value="50"/>	
<input type="button" value="Add New Entry"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>						

## 11.16. RMON アラームの設定 (SMCGS18/26/50 のみ対応)

RMON Alarm Configurationでは、RMONのアラームの設定を行います。

### 11.16.1. RMON Alarm Configuration パラメータ設定

- 1) **Delete:** エントリを削除します。
- 2) **ID:** アラームのインデックス番号を設定します。
- 3) **Variable:** 監視対象の MIB オブジェクトを指定します。
- 4) **Sample Type:** サンプル値と閾値の比較方法を指定します。  
**Absolute:** サンプル値と閾値を直接比較します。  
**Delta:** サンプル値の違いを計算して閾値と比較します。
- 5) **Startup Alarm:** アラームの設定を行います。  
**Rising Or Falling:** 上限閾値を上回るか、下限閾値を下回った時  
**Rising:** 上限閾値を上回った時  
**Falling:** 下限閾値を下回った時
- 6) **Rising Threshold / Index:** 上限閾値とイベントインデックスを指定します。
- 7) **Falling Threshold / Index:** 下限閾値とイベントインデックスを指定します。

### RMON Alarm Configurationの設定手順

- 1) ID, Variable, Sample Type, Startup Alarm, Rising Threshold, Falling Threshold を適宜設定します。
- 2) 「Save」ボタンをクリックして設定を保存します。

RMON Alarm Configuration										
Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
<input type="button" value="Delete"/>	<input type="text"/>	<input type="text" value="30"/>	.1.3.6.1.2.1.2.2.1. <input type="text" value="0.0"/>	<input type="text" value="Delta"/>	<input type="text" value="0"/>	<input type="text" value="Rising Or Falling"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="button" value="Add New Entry"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>										



## 11.17. RMON イベントの設定 (SMCGS18/26/50 のみ対応)

RMON Event Configurationでは、RMONのイベントの設定を行います。

### 11.17.1. RMON Event Configuration パラメータ設定

- 1) **Delete:** エントリを削除します。
- 2) **ID:** アラームのインデックス番号を設定します。
- 3) **Description:** イベントの説明(0-127 文字)を入力します。
- 4) **Type:** イベントのタイプを指定します。
  - **None:** 何もしません。
  - **log:** RMON ログに記録します。
  - **snmptrap:** SNMPトラップを送信します。
  - **logandtrap:** RMON ログに記録を行い、SNMPトラップも送信します。
- 5) **Community:** SNMPトラップを送信するコミュニティを指定します。

#### RMON Event Configurationの設定手順

- 1) ID, Description, Type, Community を適宜設定します。
- 2) 「Save」ボタンをクリックして設定を保存します。

RMON Event Configuration					
Delete	ID	Description	Type	Community	Event Last Time
<input type="button" value="Delete"/>	<input type="text"/>	<input type="text"/>	snmptrap ▼	<input type="text" value="public"/>	0

## 11.18. Port Security Limit Controls の設定

Port Security Limit Controls 項目ではユーザーのアクセス制限を特定ポートに設定します。

ユーザーは、MACアドレスとVLAN IDを使用して判別されます。

Port Security Limit Controlsが有効の時には、特定ポートへのユーザーアクセスを指定した最大許容アクセス数までに制限し、最大許容数を超えた場合スイッチは設定で指定した動作に基づき処理します。

### 11.18.1. Port Security Limit Controls パラメータ設定

#### System Configuration

- 1) **Mode:** Port Security Limit Controls を Enabled で有効、Disabled で無効に設定します。  
Mode パラメータでの設定はスイッチ全体に反映され、ポートごとで Port Security Limit Controls 設定をしていても Mode での設定が反映されます。
- 2) **Aging Enabled:** Aging Enabled が有効な場合、一度安全とみなされた MAC address はスイッチに記憶され一定時間保持されます。スイッチに保持する時間は Aging Period にて設定します。
- 3) **Aging Period:** Aging Enabled は Aging Period で設定された値をもとに実効されます。
  - 設定値の範囲: 10~10000000秒
  - デフォルト値: 3600秒

#### Port Configuration

- 1) **Port:** スwitchのポート番号を表示しています。
- 2) **Mode:** 選択したポートで Security Limit Controls を有効 Enables、無効 Disabled で設定します。アクセス制限を掛けるには Port Security LimitControl System Configuration の Mode を有効、Port Configuration の設定で Mode を Enabled に設定する必要があります。
- 3) **Limit:** 選択したポートで MAC アドレスベースのアクセス制限を掛ける際の最大許容数。Limit に 1024 以上の数値を入れることはできません。もし、最大許容数を超えるアクセスがある場合には、スイッチは設定された動作に従い処理します。
- 4) **Action:** アクセス数がスイッチに設定した制限値に達したさいにスイッチがとる処理を設定します。スイッチが実行する処理は下記から選択します。
  - **None:** 制限数を超えたアクセスは禁止しますが、何も特別な処理は行いません。
  - **Trap:** 制限数を 1 つでも超えたアクセスがあった場合、SNMP Trap を送信します。
  - **Shutdown:** 制限数を 1 つでも超えたアクセスがあった場合、ポートを無効にします。Shutdown Action により無効になったポートは、MAC アドレスの学習をやめポートへのケーブル抜き差しを行ってもリンクダウンの状態のままになります。無効状態から復旧させるには次の 3 通りの方法があります。

(次ページに続く)

(前ページの続き)

- i) スイッチをリブートする
  - ii) 該当ポートのPort Security Limit Controlsを一度無効にして、再度有効にする。
  - iii) Reopenボタンをクリックする。
- **Trap & Shutdown:** 制限数を 1 つでも超えたアクセスがあった場合、Trap Action と Shutdown action を実行します。
- 5) **State:** Port Security Limit Controls 上でのポートの状態を表示します。ポートは次の 4 つの状態のうちの 1 つを表示します。
- **Disabled:** Security Port Limit Controls の Mode 設定がスイッチ全体もしくはポートで無効の状態。
  - **Ready:** 設定した制限にまだ達していない状態。
  - **Limit Reached:** アクセス数が制限値に達した状態。Limit Reached は Action の設定が None もしくは Trap の時に制限数に達すると表示されます。
  - **Shutdown:** Port Security Limit Controls によりポートが無効状態となっていることを示します。Shutdown は Action の設定が Shutdown もしくは Trap&Shutdown の時に制限数に達すると表示されます。
- 6) **Reopen:** Port Security Limit Controls によりポートが無効とされた時に Reopen ボタンをクリックすることでポートを有効にすることができます。Reopen ボタンによりポートを復旧させることができるのは Port Security Limit Control により生じたポートの無効時のみで、他の要因によりポートが無効になっても Reopen により復旧はできません。

**Port Security Limit Controlsの設定手順**

- 1) メニューから「Configuration」→「Security」→「Network」→「Limit Control」を順にクリックします。
- 2) System Configuration パラメータを設定することでスイッチ全体の Limit Control を設定できます。Mode パラメータを Enabled で MAC アドレスベースでのアクセス制限機能を有効、Disabled で無効に設定します。Aging Enabled と Aging Period を必要に応じて設定します。
- 3) Port Configuration でポートにアクセス制限設定を行います。Mode パラメータ Enabled でポートへのアクセス制限を有効、Disabled で無効に設定します。Limit でアクセスできる最大 MAC アドレス数を指定し、Action パラメータで制限数をこえた場合の処理を指定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

**Port Security Limit Control Configuration**

**System Configuration**

<b>Mode</b>	Disabled ▼
<b>Aging Enabled</b>	<input type="checkbox"/>
<b>Aging Period</b>	3600 seconds

**Port Configuration**

Port	Mode	Limit	Action	State	Re-open
1	Disabled ▼	4	None ▼	Disabled	Reopen
2	Disabled ▼	4	None ▼	Disabled	Reopen
3	Disabled ▼	4	None ▼	Disabled	Reopen
4	Disabled ▼	4	None ▼	Disabled	Reopen
5	Disabled ▼	4	None ▼	Disabled	Reopen
6	Disabled ▼	4	None ▼	Disabled	Reopen
7	Disabled ▼	4	None ▼	Disabled	Reopen
8	Disabled ▼	4	None ▼	Disabled	Reopen
9	Disabled ▼	4	None ▼	Disabled	Reopen
10	Disabled ▼	4	None ▼	Disabled	Reopen

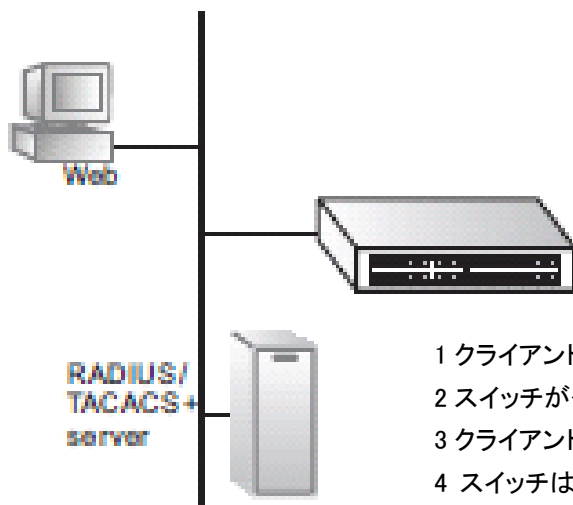
Save Reset

### 11.19. Network Access Server 認証の設定

スイッチに接続された端末はネットワークへのアクセスに制限がありません。ネットワークに誰でもアクセスをすることができると、ネットワークへ侵入して秘匿にしておきたい情報にアクセスされてしまいます。

Network Access Server項目では、IEEE802.1Xポートベース、MACアドレスベースの認証設定を行うことができます。

IEEE802.1Xはネットワークにアクセスするユーザーに対し認証要求を行うことで、アクセス権限の無いユーザーの侵入を防ぐプロトコルを定義しています。



- 1 クライアントがスイッチのポートにアクセス
- 2 スイッチがクライアントに認証要求
- 3 クライアントがスイッチに認証情報を返信
- 4 スイッチはクライアントの認証情報を認証サーバに転送
- 5 認証サーバはクライアントへチャレンジを送信
- 6 クライアントはサーバからのチャレンジに適切なレスポンスを返信
- 7 認証サーバはユーザーを認証
- 8 スイッチはユーザーにポートへのアクセスを許可

本スイッチはExtensible Authentication Protocol over LANs (EAPOL)をクライアントとの認証メッセージ交換に使用しています。外部のRADIUS認証サーバがユーザーのアクセス許可の可否を照会します。外部の認証サーバは後述のAAA項目にて設定します。

(次ページに続く)

(前ページの続き)

クライアントがスイッチポートへ接続するとスイッチはEAPOL identity要求を送信します。クライアントはEAPOL responseをスイッチに返信します。スイッチはクライアントからの情報をRADIUS サーバへ転送し、RADIUSサーバはユーザー情報を照会し、クライアントへアクセスチャレンジを送ります。RADIUSサーバからのExtensible Authentication Packet(EAP)パケットは認証に必要な情報だけでなく、使用される認証方法も含んでいます。RADIUSサーバとクライアント側で使用するIEEE802.1Xのソフトウェアによっては、クライアントは要求された認証方法を拒否し別の認証方法を要求することも可能です。

認証メッセージの交換に使用される暗号化方法はMD5 (Message Digest 5)、TLS (Tunneled Transport Layer Security)、PEAP (Protected Extensible Authentication)、そしてTTLS (Tunneled Transport Layer Security)を使用します。

**注意: MAC アドレスベースの認証をサポートしているのは MD5 だけです。**

クライアントは自信を証明する適切な方法(パスワードや証明書等)で返信します。RADIUS サーバはクライアントの身元を確認し、アクセスの許可、あるいはアクセスの拒否を返信します。認証が成功するとスイッチはクライアントにネットワークへのアクセスを許可しますが、失敗の時はアクセスを拒否します。

スイッチにIEEE802.1x設定を行うには以下の設定が必要になります。

- スwitchに IP アドレスを設定する。
- RADIUS 認証の設定がスイッチで有効になっている。また RADIUS サーバの IP アドレスが指定されている。
- 802.1X/MAC アドレスベースの認証がスイッチで有効になっている。

802.1Xを使用するには以下の条件を満たす必要があります。

- クライアントに dot1x クライアントソフトウェアがインストールされ、適切に設定されていること。
- 802.1X 認証を使用するには RADIUS サーバと 802.1X クライアントが EAP をサポートしていること(スイッチは EAP パケットをサーバからクライアントに転送するため EAPOL のみサポートしています)。
- RADIUS サーバとクライアントソフトウェアは EAP 認証に、MD5、PEAP、TLS、または TTLS のいずれかをサポートしていること。

MAC アドレスベース認証は 1 つのポートに複数のユーザーアクセスを許可し、IEEE802.1X の様にクライアントにソフトウェアをインストールする必要がありません。スイッチは認証に MAC アドレスを使用します。しかし、MAC アドレスの詐称でネットワークへのアクセスを許可してしまうので、MAC アドレスベース認証は 802.1X 認証方式ほどセキュリティが高くありません。

## 11.20. Network Access Server 認証の設定ガイドライン

802.1Xを有効にするにはクライアントとスイッチ間で実行される認証プロトコルを設定する必要があります。またスイッチと認証サーバ間で行われるクライアントの認証プロセスの設定を行う必要があります。

### 11.20.1. Network Access Server 認証パラメータ設定

#### Network Access Server認証システムの設定

- 1) **Mode:** IEEE802.1X 認証と MAC アドレスベース認証を Enabled で有効、Disabled で無効に設定します。Mode パラメータでの設定はスイッチ全体に反映され、Disabled に設定すると全てのポートでフレームの転送が許可されます。
  - デフォルト値: Disabled
- 2) **Reauthentication Enabled:** クライアントの再認証を Reauthentication Period で設定された間隔で行うかを設定します。チェックボックスをチェックで有効、チェックを外すと無効。
  - デフォルト値: Disabled
- 3) **Reauthentication Period:** クライアントが再認証する間隔を設定します。
  - 設定値の範囲: 1～3600秒
  - デフォルト値: 3600秒
- 4) **EAPOL Timeout:** スイッチがクライアントに Request Identity EAPOL を再送信するまでの間隔を設定します。
  - 設定値の範囲: 1～255秒
  - デフォルト値: 30秒
- 5) **Aging Period:** Aging Period はクライアントの接続有効期間を設定します。
  - 設定値の範囲: 10-1000000秒
  - デフォルト値: 3600秒
- 6) **Hold Time:** Hold Time は EAP 接続の失敗や RADIUS のタイムアウト後にクライアントからのアクセスを一定期間拒否する間隔です。
  - 設定値の範囲: 10-1000000秒
  - デフォルト値: 10秒

RADIUSサーバがクライアントのアクセスを拒否または、RADIUSサーバRequest time outが発生するとクライアントはアクセス権限の無いユーザーとしてホールドされます。

- 7) **RADIUS-Assigned QoS Enabled:** RADIUS Assigned QoS は、認証されたクライアントへトラフィックの優先を割り当てる機能です。この機能を使用するには RADIUS サーバ側に RADIUS 属性を送信するように設定を行う必要があります。

(次ページに続く)

(前ページの続き)

RADIUS-Assigned QoS チェックボックスにチェックを入れ RADIUS サーバに認証されたユーザーのトラフィックに割り当てる QoS クラスをスイッチ全体に有効にし、ポート毎の設定で QoS 設定を有効にすることで RADIUS-Assign QoS をポート単位で有効にしていきます。RADIUS-Assigned QoS にチェックが入っていないと全てのポートで RADIUS-Assigned QoS は無効となります。

RADIUS-Assigned QoS 設定がグローバルに有効で、かつポートで有効に設定されている場合、RADIUS サーバから送られる RADIUS Access-Accept パケット内の QoS クラス情報に基づきスイッチは動作します。

このオプションはsingle-clientモード(ポートベース802.1Xやシングル802.X) で利用可能です。

#### RADIUS属性で使用するQoSクラス

RFC4675で定義されているUser-Priority-Tableは、Access-Acceptパケット内のQoSクラスを見分けるのに使用されています。認証されたポートへのQoSクラス割り当ては、下記に説明するようにRADIUSサーバ上で設定することも可能です。

Filter-ID属性(attribute 11)はQoS情報を転送するのにRADIUSサーバ側で設定可能です。

Profile	Attribute Syntax	Example
DiffServ	Service-policy-in= <i>policy-map-name</i>	Service-policy-in=p1
Rate Limit	Rate-limit-input= <i>rate</i>	rate-limit-input=100 (単位はkbps)
802.1P	Switch-priority-default= <i>value</i>	Switch-priority-default=2

複数のプロファイルをセミコロン“;”の後に続けてFilter IDに記述することもできます。

例: service-policy-in=pp1;rate-limit-input=100

上記の例ではプロファイルネーム“pp1”をDiffservプロファイルに指定し、受信レートのプロファイルを100kbpsに指定しています。

プロファイルが重複して指定された場合は最初のプロファイルのみが適用されます。

例: service-policy-in=p1;service-policy-in=p2

上記の例ではプロファイルネーム“p1”のみをDiffservプロファイルに適用します。

Filter-ID属性内でサポートされていないプロファイルは適用されません。

例: map-id-dscp=2:3;service-policy-in=p1

上記の例ではmap-id-dscp=2:3はサポートされていないため、service-policy-in=p1のみが適用されます。

認証に成功したが、ダイナミックQoSの情報がRADIUSサーバから転送されない場合があります(ユーザーは認証された状態で変わりはありません)。その場合は以下の様なケースが考えられます。

- ユーザー情報を含む Filter-ID 属性が見つからなかった。
- Filter-ID 属性に情報が入っていない。
- Filter-ID 属性内の QoS 情報が認識できない。



ダイナミック QoS の割り当てに失敗して、ユーザーの認証が成功から失敗になった場合、以下の様なケースが考えられます。

- プロファイルに使用されている文字に使用できない文字が使用されている(例:802.1p に非デジタル文字が仕様されている)。
- 認証ポートで受信するプロファイルの設定ができていない。
- ダイナミック QoS 設定をされているユーザーがログオフすると、スイッチはポートの QoS 設定をオリジナルの状態に戻します。
- ユーザーがすでに認証されて同じポートを使用している他のユーザーと違う QoS 設定の場合アクセスを拒否されます。
- ポートがダイナミック QoS プロファイルを割り当てられている間は、手動の QoS 設定は認証されたユーザーがログオフしないと有効になりません。

- 8) **RADIUS-Assigned VLAN Enabled**: RADIUS Assigned VLAN は 認証されたクライアントのフレームに VLAN ID を割り当てる機能です。この機能を使用するには RADIUS サーバ側に RADIUS 属性を送信するように設定を行う必要があります。

RADIUS-Assigned VLAN チェックボックスにチェックを入れ認証されたユーザートラフィックへの VLAN 割り当てを有効にし、各ポートの設定で RADIUS-Assigned VLAN 設定を有効にするとポート単位で RADIUS-Assigned VLAN を有効にしていきます。RADIUS-Assigned VLAN にチェックが入っていないと全てのポートで RADIUS-Assigned VLAN は無効になります。

RADIUS-Assigned VLAN 設定がグローバルに有効かつポートで有効に設定されている場合、RADIUS サーバから送られる RADIUS Access-Accept パケット内の VLAN 情報に基づきスイッチはポートの Port VLAN ID を書き換えます。

このオプションは single-client mode (例: port-based 802.1X、Single 802.1X) で利用可能です。

#### RADIUS 属性で使用する VLAN ID

RFC2868 と RFC3580 で定義されている属性は Access-Accept パケット内の VLAN ID を識別に使用されています。VLAN ID 識別には以下の基準を使用します。

次の3つの属性、Tunnel-Medium-Type、Tunnel-Type、Tunnel-Private-Group-ID は全て一度 Access-Accept-Packet 内に含まれている必要があります。

-スイッチは最初にこれら3つの属性がおTagに同じ数値が入っているか、また次の条件を満たしているかをチェックします。(Tag==0 が使用されている、Tunnel-Group-ID は Tag を含んでいる必要はない。)

Tunnel-Medium-Type が 6 に設定されているか  
Tunnel-Medium-Type=6 はイーサネットを表しています。

Tunnel-Type は 13 に設定されているか。  
Tunnel-Type=13 は Vlan をあらわします。

Tunnel-Private-Group-ID は VLAN ID をあらわし 1-4095 までの数値が入っている必要があります。  
VLAN リストは複数の VLAN ID を含むことが可能です。リストする際のフォーマットは “1u,2t,3u” となり “u” は untagged VLAN を、“t” は tagged VLAN を意味します。

- 9) **Guest VLAN Enabled:** Guest Assigned VLAN は特殊な VLAN です。802.1 認証を使用していないクライアントが認証タイムアウト後に割り当てられる VLAN で、ネットワークアクセスが限定的になります。スイッチは条件に従いユーザーを Guest VLAN へ割り当てます。
- Guest VLAN Enabled のチェックボックスにチェックが入れると個々のポートでポートが Guest VLAN に移行するかを決定します。チェックを外すと Guest VLAN への移行機能は全てのポートで無効となります。
  - Guest VLAN Enabled にチェックが入り、ポート単位での設定で Guest VLAN Enabled となっている場合にスイッチはポートを Guest VLAN に移行させます。  
このオプションは EPAPOL-based モード(例: Port-based 802.1X、Single 802.1X、Multi 802.1X)でのみ有効です。

**注意:** VLAN の割り当てのトラブルシューティングには VLAN Membership と VLAN Port の項目を使用できます。Port VLAN の設定が一時的に書き換えられているかをチェックできます。これらの項目へのパスはメニューから「Monitor」→「VLANs」を順にクリックします。

### Guest VLANの操作方法

Guest VLAN Enabledが有効になるとポートがリンクアップしスイッチはEAPOLフレーム “Request Identity”の送信を開始します。

“Request identity”送信フレーム数がMax. Reauth. Countで設定された数値を超え、その間スイッチがEAPOLフレームを受信しないと、スイッチはGuest VLANへの移行を検討します。

EAPOL “Request Identity”フレームの送信間隔はEAPOL Timeout/パラメータで設定します。

“Allow Guest VLAN if EAPOL Seen”パラメータが有効の場合、ポートはGuest VLANへ移行します。

“Allow Guest VLAN if EAPOL Seen”設定が無効の場合、スイッチは該当ポートでEAPOLフレームを受信したことがあるかをチェックし、受信したことがない場合、ポートはGuest VLANへ移行します。

EAPOL フレーム受信の履歴はポートの状態がリンクダウンまたはポートのステートに変更があった場合消去されます。EAPOL “Request Identity”フレームを受信していない場合は Guest VLAN へポートは移行します。Guest VLAN に移行しない場合は継続して EAPOL “Request identity”フレームを EAPOL Timeout パラメータで指定した間隔で送信します。

Guest VLANに割り当てられるとポートは認証されたと認識され、ポートに接続された全てのクライアントはこのGuest VLANグループに割り当てられます。クライアントがGuest VLANグループに加わるとスイッチはEAPOL “Successful”フレームの送信を行いません。

クライアントがGuest VLANに割り当てられている間、スイッチはEAPOLフレームを監視し、もしEAPOLフレームを受信するとスイッチは即座にポートをGuest VLANから外し、認証を行います。

- 10) **Guest VLAN ID:** ポートが Guest VLAN に移行した場合に使用される VLAN ID を指定します。このパラメータは Guest VLAN Enabled が有効になっていないと設定できません。

➤ 設定値の範囲: 1~4095

- 11) **Max. Reauth. Count**: Guest VLAN に移行させるまでに、何回 EAPOL “Request Identity” フレームを送信するかを指定します。このパラメータは Guest VLAN Enabled が有効になっていないと設定できません。

➤ 設定値の範囲: 1-255

- 12) **Allow Guest VLAN if EAPOL Seen**: スイッチはポートに EAPOL フレームを受信していたかを記録しています。スイッチはポートを Guest VLAN へ移行させるかどうかを判断するとき、このパラメータが有効か無効かを参照します。無効に設定されている場合、EAPOL フレームを受け取っていない場合にのみ Guest VLAN に移行します。有効の場合には EAPOL フレームを受信していた場合にのみ Guest VLAN に移行します。Allow Guest VLAN if EAPOL Seen パラメータは Guest VLAN Enabled が有効の時のみ利用可能です。

### Port Configurationの設定

- 1) **Port Identifier**: ポート番号を示します。
- 2) **Admin State**: 本項目の Mode パラメータが有効な場合、Admin State でポートの認証モードを指定します。以下の認証モードが選択可能です。

**Force Authorized**: ポートのリンクがアップ状態になるとスイッチは EAPOL Success フレームを一度だけ送信します。スイッチは全てのユーザーに対してアクセスを許可する状態になります。初期設定値は Force Authorized が使用されています。

**Force Unauthorized**: ポートのリンクがアップ状態になるとスイッチは EAPOL Failure フレームを送信します。スイッチは全てのユーザーに対してアクセスを拒否する状態になります。

**Port-based 802.1X**: クライアントは認証サーバに認証されるので 802.1X に対応している必要があります。802.1X に対応していないクライアントはアクセスを拒否されます。

**Single 802.1X**: 1ポートに1クライアントのみ認証されるモードです。複数のクライアントがアクセスすると最初にアクセスしたクライアントに優先権が与えられ、クライアントが一定時間内に正確な認証情報を提供できないと次にアクセスをしたクライアントに機会を与えます。クライアントが認証されると、そのクライアントのみがアクセスを許可されます。Single 802.1X モードは認証モードのなかで最もセキュリティの高いモードで、Port Security 機能を使用して安全性を高めます。

**Multi 802.1X**: 1ポートに1以上のクライアントからのアクセスを認証するモードです。クライアントを個々に認証し Port Security 機能を使用し MAC テーブルで安全性を高めます。Multi 802.1X モードではスイッチからクライアント向けに送る EAPOL フレームの送り先アドレスとしてマルチキャスト BPDU MAC アドレスを使用できません。これはスイッチから送られた EAPOL “Request” フレームに対して全クライアントが返信してしまうからです。

(次ページに続く)

(前ページの続き)

スイッチはクライアントの送信するEAPOL “Star”や“Response Identity フレームから学習したクライアントのMACアドレスを使用します。しかし例外が1つあり、クライアントがいない場合、スイッチはEAPOL “Request identity”フレームにBPDUマルチキャストフレームを宛先アドレスとして使用し送信します。

クライアントの最大接続数はPort Security Control機能で設定します。

**MAC-based Auth.**-ポートのMAC-based Authを有効にするとスイッチはポートにEAPOLフレームを送信、受信しなくなります。ポートにクライアントが認証されているかいないかにかかわらず、フラッドフレームやブロードキャストフレームがポートに送られます。その一方で認証に失敗したクライアントのユニキャストフレームは破棄されます。認証に失敗したクライアントのフレームはいかなるフレームの種類にかかわらず送信されません。

スイッチはクライアントに替わりサブリカントの役割をします。スイッチは最初にクライアントから送られたフレームを“のぞき見”(Snooping)して、クライアントのMACアドレスをRADIUSサーバとのEAP交換に使用するユーザー名とパスワードとして使用します。6バイトのMACアドレスは次の様な形態に変換されますXX-XX-XX-XX-XX-XX (“-”は小文字の16進数間を分割するセパレーターです)。スイッチは認証方式MD-5VChallengeのみをサポートしますので、RADIUSサーバもそれに従って設定してください。

認証が終了すると、RADIUSサーバはSuccess indicationかFailure indicationを送信します。送信されたindicationにしたがいスイッチは特定のクライアントに対しポートを解放または閉鎖します。この認証方式にはEAPOLフレームは使用されません。MAC-based認証は802.1Xとは別の認証方式です。

MAC-based認証の利点は1つのポートで複数のクライアントを個々に認証出来ることと、クライアントに802.1X対応のクライアントソフトをインストールする必要が無い事です。MAC-based認証で不利な点は悪意のあるユーザーがMACアドレスを詐称しアクセスされる可能性があることと、EAPにMD-5しかサポートされていないことです。クライアントの最大接続数はPort Security Control機能で設定します。

### Port Admin設定のガイドライン

ポートがSTP(Spanning Tree Protocol)に参加するにはPort AdminをForce-Authorizedに設定する必要があります。

802.1X認証がポートで有効な場合、MACアドレス学習機能はそのポートでは無効になります。ポートはMACアドレステーブルに表示されなくなります。

認証されたMACアドレスはスイッチのsecure MACアドレステーブルに記載され、MAC Table項目で設定されたStatic MACアドレスもSecure MACアドレステーブルに記載されます。

ポートステータスがダウンした場合、全てのMACアドレスがSecure MACアドレステーブルから削除されます。

- 3) **RADIUS Assigned QoS Enabled:** チェックボックスにチェックを入れて機能を個々のポートに有効、チェックを外して無効にします。機能に関しては“Network Access Server 認証システムの設定”に RADIUS Assigned QoS Enabled の解説がありますので、ご参照ください。

- 4) **RADIUS Assigned VLAN Enabled:** チェックボックスにチェックを入れて機能を個々のポートに有効、チェックを外して無効にします。機能に関しては“Network Access Server 認証システムの設定”に RADIUS Assigned VLAN Enabled の解説がありますのでご参照ください。
- 5) **Guest VLAN Enabled:** チェックボックスにチェックを入れて機能を個々のポートに有効、チェックを外して無効にします。機能に関しては“Network Access Server 認証システムの設定”に Guest VLAN Enabled の解説がありますのでご参照ください。
- 6) **Port State:** 現在のポートの状態を表示しています。このパラメータでは以下のいずれかが表示されます。

**Globally Disabled:** 802.1XとMAC-based認証がシステム全体で無効になった状態。初期状態ではGlobally Disabledが表示されます。

**Link Down:** 802.1XとMAC-based認証が有効に設定されているが、ポートはリンクアップしていない状態。

**Authorized:** ポートがForce Authorizedモードかsingle-supplicantモードに設定され、サブリカントが認証されている状態。

**Unauthorized:** ポートがForce Unauthorizedモードかsingle-supplicantモードに設定され、サブリカントがRADIUSサーバに認証されなかった状態。

**X Auth/ Y Unauth:** ポートがMultiple-supplicantモードに設定されXクライアントは認証され、Yクライアントは認証されていない状態。

- 7) **Restart:** クライアントを再認証する方法として以下に説明する方法のうち1つを実行して行うことができます。Restart ボタンは Network Access Server System の Enabled パラメータを Enabled に設定し、Admin State パラメータが EAPOL-based か MAC-Based モードのときのみ使用可能です。Restart パラメータの実効で他のパラメータ設定に変更されません。

**Reauthenticate:** EAPOL-based認証を使用している場合ポートのquiet-periodが終了の時点で再認証を行うよう設定できます。MAC-based認証を使用している場合再認証を即座に行います。

**Reinitialized:** クライアントを初期化します。初期化することで即座に再認証が行われます。クライアントは再認証の間Unauthorizedの状態になります。

## Network Access Configurationの設定手順

- 1) メニューから「Configuration」→「Security」→「Network」→「NAS」を順にクリックします。
- 2) 属性を必要に応じて変更してください。
- 3) 「Save」ボタンをクリックして設定を保存します。

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	QoS of VLAN Enabled	Port State	Revert
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate

## 11.21. Access Control List によるトラフィックコントロールの設定

Access Control List(ACL)はIPアドレスとMACアドレスに適用するトラフィック制限のリストです。スイッチは入ってきたパケットに対してACLに記述された条件をひとつひとつと照会していきます。パケットが許可のルールと一致するとスイッチはパケットを転送し、パケットが拒否のルールに一致すると破棄されます。ACLに記述されたルールにパケットが該当しない場合パケットは転送されます。ACLではスイッチに許可、拒否以外のパケット処理として帯域の制限、該当パケットをコピーして他のポートに送信する、システムログに記録、ポートをシャットダウンするといった動作を指定できます。

### 11.21.1. ACL ポリシーとパケット処理の設定

ACL Port Configuration項目では、ACLのリストに該当するパケットの処理(パケットをコピー転送、システムログに記録、ポートをシャットダウン)を定義します。帯域制限に関してはRate Limiter項目の設定と一緒に設定する必要があります。

**注意:** Rate Limiter は ACL のリストにマッチしたかどうかにかかわらず実行されます。

### 11.21.2. ACL Port Configuration の設定パラメータ

- 1) **Port**: Port ID を表示します。
- 2) **Policy ID**: Access Control List 項目で設定される Access List Entry(ACE)の Policy ID を指定します。
  - 設定値の範囲: 1-8
  - デフォルト値: 1(1は不定義をあらわします)
- 3) **Action**: Assign Policy で定義されたルールに当てはまるフレームに Permit(許可)、Deny(不許可)の処理を指定します。
  - デフォルト値: Permit
- 4) **Rate limiter ID**: Rate Limiter 項目で設定したトラフィック制限ポリシーをポート単位で設定します。
  - 設定値の範囲: 1-15
  - デフォルト値: Disabled
- 5) **Redirect to**: ポリシーにマッチしたフレームを転送するポートを指定します。
  - 設定値の範囲: 1-10
  - デフォルト値: Disabled

**注意:** Redirect toを使用するにはActionパラメータをDenyに設定する必要があります。

- 6) **Mirror**: ポリシーと一致したフレームを指定したポートへコピーしたフレームを転送します。1
  - デフォルト値: Disabled

**注意:** Mirrorを使用するには、コピーしたフレームの送り先ポートをMirror Configuration 項目でポートミラーリングの設定をしておく必要があります。ACL 項目で設定するミラーリング(Mirror パラメータでの設定)と Mirror 項目で設定するミラーリングは別々に機能します。ACL ベースでミラーリングを使用するには、ACL Port Configuration 項目で Mirror パラメータを Enabled に設定し、Mirror Configuration 項目の“Port to Mirror on”パラメータでコピーフレームの転送先ポートを指定し、“Mode”のパラメータを Disabled としておきます。

- 7) **Logging**: ポリシーと一致したフレームを受信時に sys log へ記録します。
  - デフォルト値: Disabled

**注意:** ログに記録された情報はSystem Log Information項目にて確認できます。System Log Information項目にはメニューから「Monitor」→「System」→「Log」を順にクリックします。ACLポリシーで記録された情報は“Info” または“All”のレベルで記録されます。

(次ページに続く)

(前ページの続き)

8) **Shutdown**: ポリシーに一致したフレームを受信するとポートをシャットダウンします。

➤ デフォルト値: Disabled

9) **Count**: ポリシーに一致したフレーム数を表示します。

#### ACL Port Configurationの設定手順:

- 1) メニューから「Configuration」→「Security」→「ACL」→「Port」を順にクリックします。
- 2) Access Control List Configuration 項目で設定した ACL Policy を割り当て、ポリシーに一致したフレームに対しての処理(フレームをコピーして他のポートに送信、一致したフレームをログに記録、ポートをシャットダウン)を指定します。パラメータ Rate Limiting はパケットがポリシーに一致したかにかかわらず実行されます。
- 3) 「Save」ボタンをクリックして設定を保存します。

Port	Policy ID	Action	Rate Limiter ID	Redirect to	Mirror	Logging	Shutdown	Counter
1	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	596
2	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0
9	1	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	0



## 11.22. ACL Rate Limiters の設定

ACL Rate Limiter Configuration項目ではポートに帯域制御を設定します。

### 11.22.1. ACL Rate Limiters の設定パラメータ

- 1) **Rate Limiter ID**: Rate Limiter ID です。
- 2) **Rate**: パケットを破棄する閾値を指定します。指定範囲 0-100pps、0、100、2\*100、3\*100、...1000000kbps)

**注意**: ASICの機能制限により指定された制限値より低い値で帯域制限を行います。  
**例**: 1Kppsの制限を掛けた場合に、スイッチが実行する閾値は1002.1ppsになります。

- 3) **Unit**: 設定に使用する単位。選択可能単位は pps と kbps  
 デフォルト値: pps

#### ACL Rate Limiter Configurationの設定手順

- 1) メニューから「Configuration」→「Security」→「ACL」→「Port」を順にクリックします。
- 2) Rate パラメータに ACL ポリシーに一致した場合にサポートする最大受信レートを設定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

ACL Rate Limiter Configuration		
Rate Limiter ID	Rate	Unit
1	1	pps ▼
2	1	pps ▼
3	1	pps ▼
4	1	pps ▼
5	1	pps ▼
6	1	pps ▼
7	1	pps ▼
8	1	pps ▼
9	1	pps ▼
10	1	pps ▼
11	1	pps ▼
12	1	pps ▼
13	1	pps ▼
14	1	pps ▼
15	1	pps ▼
16	1	pps ▼

Save Reset

## 11.23. Access Control List の設定

Access Control List Configuration項目では特定のポートまたは全てのポートに対してACLポリシーのフィルタリングルールを定義します。

### 11.23.1. Access Control List 設定ガイドライン

Access Control List は設定された順( Top から bottom) にチェックされます。パケットは permit ルールに一致すると受信され、deny ルールに一致すると破棄されます。

ACL ルールは最大 128 ルール作成が可能です。






ACL は以下の基準を使用してフレームをフィルタリングします。

- フレームタイプ(MAC アドレス、VLAN ID、VLAN Priority)
- Ethernet タイプ(Ethernet type の値、MAC アドレス、VLAN ID、VLAN Priority)
- ARP(ARP/RARP のタイプ、request/reply、sender/targetIP、hardware address matches ARP/RARP MAC アドレス、ARP/RARP hardware address length matches protocol address length、matches this entry when ARP/RARP hardware address is equal to Ethernet, matches this entry when ARP/RARP protocol address space setting is equal to IP (0x800))
- IPv4 フレームをフィルタリングします。(送信先 MAC アドレス、プロトコルタイプ、TTL、フラグメントパケット、IP のオプションフラグ、送信先/送信元 IP アドレス、VLAN ID、VLAN priority)

### 11.23.2. Access Control List 設定パラメータ

- 1) **Port**: 全てのポート、Port ID、policy を指定します。
- 2) **Frame Type**: 一致させるフレームタイプを表示します。
- 3) **Action**: ACL ルールに一致した際にフレームを許可するか、拒否するか表示します。
- 4) **Rate Limiter**: ACL ルールに一致した際にフレーム帯域制限を表示します。
- 5) **Redirect to**: ACL ルールに一致した際にフレームを指定したポートに転送するか表示します。
- 6) **Mirror**: ポートからのフレームを指定したポートにミラーリングするか表示します。
- 7) **Logging**: ACL ルールに一致したフレームを受信したときにシステムログに記録するかを表示します。
- 8) **Shutdown**: ACL ルールに一致したフレームを受信したときにポートをシャットダウンするか表示します。
- 9) **Counter**: ACL ルールに一致したフレーム数を表示します。

以下のボタンがACLエントリを編集、操作するのに使用されます。

ボタン	機能説明
	新規のACLエントリを現在の列に挿入
	ACLエントリを編集します。
	ACLエントリの順序を上げます。
	ACLエントリの順序を下げます。
	ACLエントリを削除します。
	ACLエントリ下部にあるプラスボタンは新規のACLエントリをリストの最後に追加します。

### ACE Configuration設定パラメータ

#### Ingress Port and Frame Type

- 1) **Ingress Port**: 全てのポート、ポート ID、ポリシーを選択します。選択可能オプションは Any Port、Port 1-10、Policy 1-8。  
➤ デフォルト値: Any
- 2) **Frame Type**: 一致させるフレームタイプを指定します。選択可能オプションは Any、Ethernet、ARP、IPv4。  
➤ デフォルト値: Any

#### 指定フレームタイプ別フィルタリング条件

##### Ethernet

**MACパラメータ**: SMAC Filter-送信元MACアドレスのタイプ。選択オプションはAny、Specific-ユーザー指定のMACアドレス。  
➤ デフォルト値: Any

**DMAC Filter**: 宛先MACアドレスのタイプ。選択オプションはAny、MC-マルチキャスト、BC-ブロードキャスト、UC-ユニキャスト、Specific-ユーザー指定のMACアドレス。  
➤ デフォルト値: Any

##### Ethernet タイプパラメータ

**Ethernet Filter**: このオプションはEthernet IIフォーマットのパケットのみをフィルタリングします。送信元MACアドレスのタイプ。選択オプションはAny、Specific (600-fff hex)。  
➤ デフォルト値: Any

**注意**: Ethernet プロトコルタイプの詳細なリストは RFC1060 に記述されています。一般的なタイプとして 0800(IP)、0806(ARP)、8137(IPX)があります。

## MACパラメータ

SMAC Filter: 送信元MACアドレスのタイプ。選択オプションはAny、Specific-ユーザー指定のMACアドレス。

➤ デフォルト値: Any

DMAC Filter: 宛先MACアドレスのタイプ。選択オプションはAny、MC-マルチキャスト、BC-ブロードキャスト、UC-ユニキャスト、Specific-ユーザー指定のMACアドレス。

➤ デフォルト値: Any

## ARPパラメータ

ARP/RARP-ARPパケットのタイプを指定します。選択オプションはAny-ARP/RARPのオペレーションコードを指定しません。ARP-フレームはARP/RARPオペレーションコードをARP設定の必要があります。RARP-フレームはARP/RARPオペレーションコードをRARP設定の必要があります。Other-フレームが不明なARP/RARPオペレーションコードを持つ場合。

➤ デフォルト値: Any

-Request/Reply-パケットがARP RequestなのかReplyまたは両方なのかを指定します。選択オプションはAny-ARP/RARPのオペレーションコードを指定しません、Request-フレームのオペレーションコードがARP RequestかRARP Requestに設定してある必要があります、Reply-フレームのオペレーションコードがARP ReplyかRARP Replyに設定してある必要があります。

➤ デフォルト値: Any

-Sender IP Filter-送信元のIPアドレスを指定します。選択オプションはAny-Sender IP Filterは指定されていません、Host-SIP Addressフィールドに送信元アドレスを入力します、Network-SIP Addressフィールドに送信元アドレスを入力し、SIP MASKフィールドにIPマスクを入力します。

➤ デフォルト値: Any

-Target IP Filter-送信先のIPアドレスを指定します。選択オプションはAny-Target IP Filterは指定されていません、Host-Target IP Addressフィールドに送信先アドレスを入力します、Network-Target IP Addressフィールドに送信先アドレスを入力し、Target IP MASKフィールドにIPマスクを入力します。

➤ デフォルト値: Any

-ARP SMAC Match-フレームが送信元のMACアドレスフィールド設定に従って一致しているかを指定します。選択可能オプションは、Any-全ての値が許可されます、0-ARPフレームの送信元MACアドレスフィールドがSMACアドレスと一致しない、1-ARPフレームの送信元MACアドレスフィールドがSMACアドレスと一致する。

➤ デフォルト値: Any

-RARP DMAC Match-フレームが送信先のMACアドレスフィールド設定に従って一致しているかを指定します。選択可能オプションは、Any-全ての値が許可されます、0-RARPフレームの送信先MACアドレスフィールドがDMACアドレスと一致しない、1-RARPフレームの送信先MACアドレスフィールドがDMACアドレスと一致する。

➤ デフォルト値: Any

–IP/Ethernet Length-フレームがARP/RARPハードウェアアドレス長とプロトコルアドレス長に従って一致しているかを指定します。選択可能オプションは、Any-全ての値が許可されます、0-ARP/RARPフレームのARP/RARPハードウェアアドレス長の値がEthernet(0x06)と一致し、プロトコルアドレス長の値がIPv4(0x04)と一致しない場合、1-ARP/RARPフレームのARP/RARPハードウェアアドレス長の値がEthernet(0x06)と一致し、プロトコルアドレス長の値がIPv4(0x04)と一致する場合

➤ デフォルト値: Any

–IP-フレームがARP/RARPハードウェアアドレスのデータベースと一致しているかを指定します。選択可能オプションは、Any-全ての値が許可されます、0-ARP/RARPフレームのARP/RARPハードウェアアドレススペースの値がEthernet(1)の場合一致しない、1-ARP/RARPフレームのARP/RARPハードウェアアドレススペースの値がEthernet(1)の場合一致する

➤ デフォルト値: Any

–Ethernet-フレームがARP/RARPプロトコルアドレスをもとに一致しているかを指定します。選択可能オプションは、Any-全ての値が許可されます、0-ARP/RARPフレームのARP/RARPプロトコルアドレススペースの値がIP(0x800)の場合一致しない、1-ARP/RARPフレームのARP/RARPプロトコルアドレススペースの値がIP(0x800)の場合一致する

➤ デフォルト値: Any

#### IPv4:

##### MACパラメータ

–DMAC Filter-送信先MACアドレスのタイプ。選択可能オプションはAny、MC-Multicast、BC-Broadcast、UC-Unicast

➤ デフォルト値: Any

##### IPパラメータ

–IP Protocol Filter-このルールでフィルタリングするIPプロトコルを指定します。選択可能オプションはAny、ICMP、UDP、TCP、Other

➤ デフォルト値: Any

プロトコルフィルターを選択すると以下のパラメータが追加で表示されます。

##### ICMPパラメータ

–ICMP Type Filter-このルールでフィルタリングするICMPパケットのタイプを指定します。選択可能オプションはAny、Specific-1～255

➤ デフォルト値: Any

–ICMP Code Filter-このルールでフィルタリングするICMPパケットのコードを指定します。選択可能オプションはAny、Specific-1～255、

➤ デフォルト値: Any

## UDPパラメータ

- Source Port Filter-このルールでフィルタリングするUDPソースフィルターを指定します。  
選択可能オプションはAny、Specific-1～65535、Range-0-65535  
➤ デフォルト値: Any
- Dest. Port Filter-このルールでフィルタリングするUDPデスティネーションフィルターを指定します。選択可能オプションはAny、Specific-1～65535、Range-0-65535  
➤ デフォルト値: Any

## TCPパラメータ

- Source Port Filter-このルールでフィルタリングするTCPソースフィルターを指定します。  
選択可能オプションはAny、Specific-1-65535、Range-0-65535  
➤ デフォルト値: Any
- Dest. Port Filter-このルールでフィルタリングするTCPデスティネーションフィルターを指定します。選択可能オプションはAny、Specific-1-65535、Range-0-65535  
➤ デフォルト値: Any
- TCP FIN-このルールでフィルタリングするTCP “No more data from sender”(FIN) の値を指定します。Any-全ての値が許可、0-FINがセットされたTCPパケットは一致しない、1- FINがセットされたTCPパケットは一致  
➤ デフォルト値: Any
- TCP SYN-このルールでフィルタリングするTCP “Synchronize sequence numbers”(SYN) の値を指定します。Any-全ての値が許可、0-SYNがセットされたTCPパケットは一致しない、1- SYNがセットされたTCPパケットは一致  
➤ デフォルト値: Any
- TCP RST-このルールでフィルタリングするTCP “Reset the Connection”(RST) の値を指定します。Any-全ての値が許可、0-RSTがセットされたTCPパケットは一致しない、1- RSTがセットされたTCPパケットは一致。  
➤ デフォルト値: Any
- TCP PSH-このルールでフィルタリングするTCP “Push Function”(PSH) の値を指定します。Any-全ての値が許可、0-PSHがセットされたTCPパケットは一致しない、1- PSHがセットされたTCPパケットは一致。  
➤ デフォルト値: Any
- TCP ACK-このルールでフィルタリングするTCP “Acknowledgment field significant”(ACK) の値を指定します。Any-全ての値が許可、0-ACKがセットされたTCPパケットは一致しない、1- ACKがセットされたTCPパケットは一致。  
➤ デフォルト値: Any
- TCP URG-このルールでフィルタリングするTCP “Urgent Pointer field significant”(URG) の値を指定します。Any-全ての値が許可、0-URGがセットされたTCPパケットは一致しない、1- URGがセットされたTCPパケットは一致。  
➤ デフォルト値: Any

-IP TTL-このルールに使用するtime-to-Liveの値を指定します。選択可能オプションはAny-全ての値を許可、Non-Zero-TTL値が0以上のIPv4フレームが一致、Zero-TTL値が0以上のIPv4フレームが一致しない。

➤ デフォルト値: Any

-IP fragment-このルールに使用するフラグメントオフセットの値を指定します。この設定にはIPv4フレームのMore Fragment (MF)ビットとFragment Offset(FRAG OFFSET)フィールドが用いられます。選択可能オプションはAny-全ての値を許可、Yes-IPv4フレームでMFビットがセットされているかFRAG OFFSETフィールドが1以上の物は一致、NO- IPv4フレームでMFビットがセットされているかFRAG OFFSETフィールドが1以上の物は一致しない。

➤ デフォルト値: Any

-IP Option-このルールに使用するOption Flagの値を指定します。選択可能オプションはAny-全ての値を許可、Yes-IPv4フレームでOption flagがセットされている物は一致、NO- IPv4フレームでOption flagがセットされている物は一致しない。

➤ デフォルト値: Any

-SIP Filter-このルールに使用するSource IP(SIP)フィルタを指定します。選択可能オプションはAny-SIPは指定されていない、Host-SIPフィールドのSource IPアドレスを指定。Network- SIPフィールドのSource IPアドレスと、SIP Maskフィールドのsource IP Maskを指定。

➤ デフォルト値: Any

-DIP Filter-このルールに使用するDestination IP(SIP)フィルタを指定します。選択可能オプションはAny-DIPは指定されていない、Host-DIPフィールドのDestination IPアドレスを指定。Network- DIPフィールドのDestination IPアドレスと、DIP MaskフィールドのDestination IP Maskを指定。

➤ デフォルト値: Any

### ルールに一致した際の処理設定

- 1) **Action-ACL**ルールに一致した際にフレームを許可(Permit)するか、拒否(Deny)するかを設定。  
➤ デフォルト値: Any
- 2) **Rate Limiter**–Rate Limiterをポートに適用するかを設定。指定可能範囲1-16。  
➤ デフォルト値: Any
- 3) **Port Copy**–ルールに一致したフレームのコピー転送先ポートを指定します。指定可能範囲1-10。  
➤ デフォルト値: Any
- 4) **Mirror**–ルールに一致したフレームをポートから見らリングを行うかを設定します。  
➤ デフォルト値: Any

このパラメータ設定のACLベースポートミラーリングとMirror Configuration項目でのポートミラーリングは別々に独立して実行されます。ACLベースのポートミラーリングを使用するにはACE Configuration項目のMirrorパラメータを有効にして、Mirror Configuration項目でPort to mirror onパラメータをミラーリングする先のポートを指定し、ModeパラメータをDisabledにしておきます。

- 5) **Logging**–一致した際にフレームをシステムログに記録するかを設定します。  
➤ デフォルト値: Any

System Log Informationメニューを開きLoggingルールに一致しシステムログに記録されたエントリを見ることができます。このルールで記録されたエントリは “Info”または “All”ロギングレベルで記載されます。

- 6) **Shutdown**–ルールに一致したフレームを検知したときにポートをシャットダウンするかを設定します。  
➤ デフォルト値: Any
- 7) **Counter**– ACLルールに一致したフレームの数を表示します。

### VLANパラメータ

- 1) **802.1Q Tagged**–フレームが802.1Q Tagフレームかを指定します。指定可能オプションAny、Disabled、Enabled  
➤ デフォルト値: Any
- 2) **VLAN ID Filter**–フィルタリングするVLAN IDを指定します。指定可能オプションAny、Specific-(1-4095)  
➤ デフォルト値: Any
- 3) **Tag Priority**–フィルタリングするVLAN Tag内のUser Priority値(IEEE802.1pで定義された3ビットの情報)を指定します。指定可能オプション Any、Specific-0-7  
➤ デフォルト値: Any



### Access Control List Configurationの設定手順

- 1) メニューから「Configuration」→「Security」→「Network」→「Access Control List」を順にクリックします。
- 2) ボタンをクリックし新規にアクセスリストを作成、または他の ACL 編集ボタンを使用して編集します(edit、delete、エントリの順序を↑↓ボタンで変更します)。
- 3) ACE 項目でエントリを編集するときに、選択項目によってアイテムは、フレームタイプ、IP プロトコルタイプ等が表示されます。適切な基準を指定しルールを作成し、ルールに一致した際の処理動作、Rate Limiter、Port Copy、Login、Shutdown を設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

The screenshot displays the 'Access Control List Configuration' window. At the top, there is a navigation bar with buttons for 'Ingress Port', 'Frame Type', 'Action', 'Rate Limiter', 'Redirect to', 'Mirror', 'Logging', 'Shutdown', and 'Counter'. To the right of these buttons are 'Auto-refresh', 'Refresh', 'Clear', and 'Remove All' options. A red arrow points from the 'Counter' button to a sub-dialog titled 'ACE Configuration'. This sub-dialog contains several configuration fields: 'Ingress Port' (set to 'Any'), 'Policy 1' (set to 'Policy 2'), 'Frame Type' (set to 'Any'), 'Action' (set to 'Permit'), 'Rate Limiter' (set to 'Disabled'), 'Redirect to' (set to 'Disabled'), 'Mirror' (set to 'Disabled'), 'Logging' (set to 'Disabled'), 'Shutdown' (set to 'Disabled'), 'Counter' (set to '0'), and 'VLAN Parameters' (including '802.1Q Tagged' set to 'Any', 'VLAN ID Filter' set to 'Any', and 'Tag Priority' set to 'Any'). At the bottom of the sub-dialog are 'Save', 'Reset', and 'Cancel' buttons.

## 11.24. DHCP Snooping の設定

DHCP Snoopingはスイッチのポートで偽のDHCP Replyパケットを送りつけ正規にDHCPサーバからIPアドレスを割り振ってもらうはずの端末になりすまして不正にネットワークへ侵入しようとする端末をブロックします。

### 11.24.1. DHCP Snooping 設定ガイドライン

ネットワークトラフィックは外部から悪意のあるDHCPメッセージを受信すると混乱する場合があります。DHCP Snooping は外部ネットワークやファイアーウォールから受信したDHCPメッセージをフィルタリングするのに使用します。DHCP Snoopingがシステム全体とVLANインタフェースで有効に設定されると、DHCP Snoopingテーブル上にない機器からのDHCPメッセージを破棄します。

テーブルにエントリされる機器はtrustedインタフェースからのみ登録されます。DHCP SnoopingテーブルのエントリはクライアントがDHCPサーバからのIPアドレスを受信、または解放したときに動的に追加・削除されます。エントリにはMACアドレス、IPアドレス、リース時間、VLAN IDとポートIDが含まれます。

DHCP Snoopingが有効の時、untrustedインタフェースからのDHCPメッセージはDHCP Snoopingで学習された動的エントリをもとにフィルタリングされます。

フィルタリングルールは以下に従って実行されます。

- DHCP Snooping がシステム全体で Disabled の時、全ての DHCP パケットはフォーワードされます。
- DHCP Snooping がシステム全体で有効の時、全ての DHCP パケットは trusted ポートに転送されます。受信したパケットが DHCP ACK の場合は、ダイナミック DHCP Snooping エントリはバインディングテーブルにも追加されます。
- DHCP Snooping がシステム全体で有効の時、ポートが trusted でない場合は次の様な処理過程になります。

-DHCPパケットがDHCPサーバからのReplyパケット(OFFER、ACK、またはNAKメッセージ)の場合、パケットが破棄されます。

-DHCP DECLINE、RELEASEまたは、INFORMメッセージがクライアントから受信されると、バインディングテーブルで該当のエントリが見つかった時のみパケットを転送します。

-DHCP DISCOVER、または、REQUESTメッセージがクライアントから受信されると、パケットを転送します。

-DHCPパケットが認識できない物の場合、パケットが破棄されます。

- クライアントからの DHCP パケットが上記のフィルタリング基準をパスすると、同じ VLAN の trusted ポートに転送されます。 Snooping がシステム全体で有効の時、ポートが trusted でない場合は下記の様な処理過程になります。

-サーバからのDHCPパケットがtrustedポートから受信すると、同じVLANのuntrustedとtrustedポートに転送されます。 Snoopingがシステム全体で有効の時、ポートがtrustedでない場合は下記の様な処理過程になります。

-DHCP Snoopingがシステム全体で無効の時、全ての動的バイディングはバイディングテーブルから削除されます。

-その他に考慮すべき点として、スイッチがDHCPクライアントとして設定されているとき。スイッチがクライアントRequestをDHCPサーバへ送信するポートをtrustedポートに設定する必要があります。スイッチはDHCPサーバからACKメッセージを受信しても自信をダイナミックエントリに追加しません。またスイッチがDHCPクライアントパケットを送信してもフィルタリングはされません。しかしながらスイッチはDHCPサーバからのメッセージを受信するときに、untrustedポートから受信したパケットは破棄されます。

#### 11.24.2. DHCP Snooping 設定パラメータ

- Snooping Mode:** システム全体で DHCP Snooping が有効の場合、DHCP Request は trusted ポートに転送されます。 Reply パケットは trusted ポートからのみ許可されます。
  - デフォルト値: Disabled
- Port:** ポート ID
- Mode**-DHCP の信頼できる送信元としてポートを登録(Trusted)、または信頼できない送信元としてポートの登録(Untrusted)を指定できます。
  - デフォルト値: Trusted

#### DHCP Snoopingの設定手順

- メニューから「Configuration」→「Security」→「Network」→「DHCP」→「Snooping」を順にクリックします。
- DHCP Snooping の処理プロセスを設定します。そして LAN ポートまたはファイヤーウォールへのポートを trusted に設定します。
- 「Save」ボタンをクリックして設定を保存します。

Port	Mode
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted
9	Trusted
10	Trusted

## 11.25. DHCP Relay の設定とオプション 82 に関して

DHCP Relay項目はDHCP Relayサービスを提供する設定に使用します。サブネットにDHCPサーバを持っていない場合に他のサブネットのDHCPサーバにDHCP Requestをリレーすることができます。

DHCP Relay機能が有効でスイッチがDHCP Requestのブロードキャストを検知すると、スイッチは自身のIPアドレスをRequestに挿入し(DHCPサーバはクライアントのサブネットを知っているため)、DHCPサーバにパケットを転送します。Requestを受け取ったDHCPサーバはクライアントのサブネットに定義したIPアドレスの範囲から未割当のIPアドレスを割り当て、DHCP Responseをスイッチに送ります。スイッチはクライアントにDHCP Responseをブロードキャストします。

DHCPはスイッチとDHCPクライアントに対してのDHCPサーバに関する情報を送信する機能を提供しています。これはOption 82として知られており、互換性のあるDHCPサーバ間で割り当てたIPアドレス、他のサービス設定、ポリシー、クライアント等に関する情報を使用できるようにしています。

DHCP Relay Option 82を使用することで、クライアントはMACアドレスだけでなく、どのVLAN IDに所属しているか、どのポートに接続されているか等で識別されます。DHCP クライアントとサーバ間のメッセージ交換はVLAN全体にブロードキャストされず、サーバとクライアント間で直接情報交換をします。

スイッチはクライアントからDHCP Option 82の情報を持ったDHCPパケットを受ける時があります。スイッチはこういったパケットに対してのアクションポリシーを設定しておく必要があります。スイッチはOption 82の情報を持つパケットを破棄、既存の情報を使用する、またはスイッチのrelay情報を更新する、のいずれかを選択できます。

### 11.25.1. DHCP Relay 設定パラメータ

- 1) **Relay Mode:** DHCP Relay 機能を有効(Enabled)、無効(Disabled)します。  
     ➤ デフォルト値: Disabled
- 2) **Relay Server:** スwitchの DHCP リレーエージェントに使用される DHCP サーバの IP アドレスを入力します。
- 3) **Relay Information Mode:** DHCP Relay Option 82 を有効(Enabled)、無効(Disabled)に設定します。Relay Information Mode を有効にするには Relay Mode を有効にしておく必要があります。  
     ➤ デフォルト値: Disabled
- 4) **Relay Information Policy:** DHCP Option 82 の情報を持つ DHCP クライアントパケットに対する DHCP Relay のポリシーを設定します。
  - Replace: DHCP クライアントパケットの情報をスイッチのリレー情報に書き換えます。Relay Information Policyの初期値は Replace です。
  - Keep: クライアントの情報を維持します。
  - Drop: DHCP リレー情報を持った DHCP パケットを破棄します。

**DHCP Relayの設定手順**

- 1) メニューから「Configuration」→「Security」→「Network」→「DHCP」→「Relay」を順にクリックします。
- 2) DHCP Relay機能を有効にし、DHCPサーバのIPアドレスを入力します。Option 82 Information modeを有効にして、クライアントのパケットにリレー情報を見つけた際のポリシーを設定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

The screenshot shows the 'DHCP Relay Configuration' page. It contains four configuration rows, each with a label on the left and a control on the right:

DHCP Relay Configuration	
Relay Mode	Disabled (dropdown menu)
Relay Server	0.0.0.0 (text input field)
Relay Information Mode	Disabled (dropdown menu)
Relay Information Policy	Replace (dropdown menu)

At the bottom of the configuration area, there are two buttons: 'Save' and 'Reset'.

## 11.26. IP SOURCE GUARD の設定

IP Source Guard機能は手動で設定したIP Source GuardエントリやDHCP Snoopingが有効の時にはDHCP Snooping エントリをもとにIPトラフィックをフィルタリングするセキュリティ機能です。IP Source Guardはネットワークアクセスを許可されたホストのなりすましを防ぐことができます。

IP Source Guardは外部ネットワークに接続されたポートやファイヤーウォールから受信するトラフィックをフィルタリングします。IP Source GuardはDHCP Snooping テーブル内にエントリされた送信元IPアドレスとそのMACアドレス情報や、静的にIP Source Guardテーブルに設定されたエントリ等といったトラフィックタイプ情報をもとにフィルタリングします。

### 11.26.1. IP SOURCE GUARD の設定ガイドライン

IP Source Guardがシステムおよびポートで有効時に、スイッチはVLAN ID、送信元IPアドレス、DHCP Snoopingバインディングテーブル内の全てのエントリに対するポート番号、IP Source Guardテーブルをチェックします。エントリに一致しない場合、パケットは破棄されます。

**注意：** Source Guard でマルチキャストアドレスは使用できません。

IP Source Guard有効時にはDHCP Snoopingで学習した動的なエントリ、Source Guardバインディングテーブルで設定された静的なアドレスをもとにトラフィックはフィルタリングされます。

IP Source Guard有効時にはインバウンドのIPパケットはバインディングテーブルをもとにチェックされます。エントリに一致しない場合、パケットは破棄されます。

フィルタリングルールは以下の処理動作を行います。

-DHCP Snoopingが無効で、IP Source GuardはVLAN ID、送信元IPアドレスとポート番号をチェックします。バインディングテーブルに一致したエントリがあり、エントリタイプが静的 IP Source Guardバインディングの場合、パケットは転送されます。

-DHCP Snoopingが有効で、IP Source GuardはVLAN ID、送信元IPアドレスとポート番号をチェックします。バインディングテーブルに一致したエントリがあり、エントリタイプが静的IP Source Guardバインディングか動的DHCP snoopingバインディングの場合、パケットは転送されます。

-IP Source GuardがIP Source Guardバインディングを設定していない(IP Source Guardバインディングテーブルへの静的な設定、DHCP Snoopingによる動的バインディングテーブルの作製のどちらも行っていない)ポートに対して有効にすると、DHCPを除くすべてのIPトラフィックは破棄されます。

### 11.26.2. IP SOURCE GUARD 設定パラメータ

- 1) **Global Mode**-IP Source Guard 機能をシステム全体で有効(Enabled)、無効(Disabled)に設定します。Global Mode を有効にすると ACE 項目の全設定が失われます。
- 2) **Port**-ポート ID
- 3) **Mode**-特定のポートで IP Source Guard を有効(Enabled)、無効(Disabled)に設定するか指定します。Global Mode と Port Mode の両方で IP Source Guard 有効となっているポートのみが ARP Inspection 機能を使用します。
- 4) **Max Dynamic Clients**-特定のポートで動的に学習できる最大クライアント数を指定します。設定可能値は 0、1、2、または unlimited です。Port Mode が有効で最大動的クライアント数が 0 の場合、スイッチは静的エントリに一致したパケットのみを転送します。

#### IP Source Guardの設定手順:

- 1) メニュー から「 Configuration 」→「 Security 」→「 Network 」→「 IP Source Guard 」→「Configuration」を順にクリックします。
- 2) IP Source Guard をシステム全体とポート毎に有効、無効の設定をします。
- 3) 動的クライアントの最大数をポートに設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

IP Source Guard Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode	Max Dynamic Clients
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited

Save Reset

## 11.27. IP SOURCE GUARD の STATIC BINDINGS 設定

Static IP Source Guard Tableを使用してポートに静的IPアドレスを結びつけます。テーブルのエントリにはポートID、VLAN ID、IPアドレスとサブネットマスクがあります。全てのエントリはリース時間に制限なしで設定されます。

### 11.27.1. IP SOURCE GUARD の STATIC BINDINGS ガイドライン

Source Guard Bindingテーブルにエントリされた静的IPアドレスはリース時間無制限で自動的に設定され、DHCP Snoopingで動的に学習されたエントリはDHCPサーバにより設定されます。

静的な結び付けは以下の処理動作を行います。

- 同じ VLAN ID と MAC アドレスを持ったエントリが無い場合、新しいエントリが Static IP Source Guard Binding テーブルに追加されます。
- 同じ VLAN ID、MAC アドレスでエントリタイプが Static IP Source Binding の場合、新しいエントリが古いエントリに差し替えられます。
- 同じ VLAN ID、MAC アドレスでエントリタイプが動的な DHCP Snooping binding の場合、新しいエントリが古いエントリに差し替えられ、エントリタイプが static IP Source Guard Binding に替わります。
- 静的な結び付けにはユニキャストアドレスのみが受け付けられます。

### 11.27.2. STATIC IP SOURCE GUARD TABLE 設定パラメータ

- 1) **Port**-静的なエントリが結び付けられるポート
- 2) **VLAN ID**-設定した VLAN ID。指定可能範囲 1-4095
- 3) **IP Address**-ユニキャスト IP アドレスでクラスフルタイプ、A、B、C
- 4) **MAC Address**-ユニキャスト MAC アドレス

Static IP Source Guard Tableの設定手順:

- 1) メニューから「Configuration」→「Security」→「Network」→「IP Source Guard」→「Static Table」を順にクリックします。
- 2) “Add new entry”をクリックします。
- 3) ポートへの結び付けに必要な情報を入力していきます。
- 4) 「Save」ボタンをクリックして設定を保存します。

Delete	Port	VLAN ID	IP Address	MAC address
Delete	1			
Delete	1			

Add new entry

Save Reset



## 11.28. ARP INSPECTION の設定

ARP InspectionはAddress Resolution Protocol(ARP)パケットで結びつけられたMACアドレスを検証するセキュリティ機能です。無効なMA-to-IPアドレスの結び付けをこない侵入する“なりすまし”行為からネットワークを守ります。全てのARP RequestとResponseをインタ-セプトし,ARPキャッシュをアップデートまたは送信先に転送する前にこれらのパケットを検証します。不正なパケットは破棄されます。

ARP InspectionはIP-to-MACアドレスの結び付けをデータベースに保存しており、このデータベース(DHCP Snoopingバインディングデータベース)をもとにARPパケットの有効性を決定します。このデータベースはDHCP Snoopingがシステム全体に有効でポートにも設定がされると作成されます。ARP Inspectionは静的に設定されたアドレスに対してもARPパケットの有効性をチェックします。

### 11.28.1. ARP INSPECTION ガイドライン

ARP Inspectionを有効、無効に設定します。ARP Inspectionはシステム全体に、またはポート毎で設定を行えます。

初期状態でARP Inspectionはシステム全体と全てのポートで無効の設定となっています。

ARP Inspectionがシステムで有効に設定されている場合、ARP Inspectionが有効のポートでのみ機能します。

ARP Inspectionがシステムで有効の際にはARP Inspectionが有効のポートで受信されるAPR Request、ResponseパケットはCPUに送られARP-Inspection Engineによりパケットの動作処理が行われます。

-ARP Inspectionが無効の場合、全てのARP Request、ResponseパケットがARP Inspection Engineを迂回し、他のパケットと同様に処理されます。

-ARP Inspectionを無効にして、再度有効にしてもポートのARP Inspection設定に影響はありません。

-ARP Inspectionをシステムで無効にしても、各ポートにARP Inspectionの設定をすることは可能です。設定はシステム全体のARP Inspection機能を有効にすると設定変更が反映されます。

### 11.28.2. ARP INSPECTION 設定パラメータ

- 1) **Mode:** システム全体に対し動的な ARP Inspection を有効(Enabled)、無効(Disabled)に設定します。
  - デフォルト値: Disabled
- 2) **Port:** ポート ID
- 3) **Mode:** 任意のポートに ARP Inspection を有効(Enabled)、無効(Disabled)に設定します。システム全体の ARP Inspection と任意のポートへの ARP Inspection が有効になった時にのみ ARP Inspection は有効になります。
  - デフォルト値: Disabled

**ARP Inspectionの設定手順**

- 1) メニュー から「 Configuration 」→「 Security 」→「 Network 」→「 ARP Inspection 」→「 Configuration 」を順にクリックします。
- 2) システム全体に ARP Inspection を有効に設定し、任意のポートに設定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

ARP Inspection Configuration

Mode: Disabled

Port Mode Configuration

Port	Mode
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Save Reset

## 11.29. STATIC ARP INSPECTION TABLE の設定

Static ARP Inspection Tableは静的アドレスをポートに結び付けるのに使用します。テーブルのエントリにはポートID、VLAN ID、ARP RequestパケットのSource MACアドレス、ARP Requestパケットのsource IPアドレスがあります。

ARP InspectionはIP-to-MACアドレスの結び付けリストとしてDHCP Snoopingバインディングデータベースを使用します。スイッチは最初にARPパケットをStatic ARPテーブルと比較します。パケットとテーブルのエントリで一致しない場合、DHCP Snoopingバインディングデータベースを使用して正当性を検証します。

### 11.29.1. STATIC ARP INSPECTION TABLE 設定パラメータ

- 1) **Port:** ポート ID
- 2) **VLAN ID:** 設定された VLAN ID
  - 設定値の範囲 1-4094
- 3) **MAC Address:** ARP Request パケットで許可する送信元 MAC アドレス
- 4) **IP Address:** ARP Request パケットで許可する送信元 IP アドレス

#### Static ARP Inspectionの設定手順

- 1) メニューから「Configuration」→「Security」→「Network」→「ARP Inspection」→「Static Table」を順にクリックします。
- 2) Add new entry をクリックします。
- 3) 任意のポートに必要なバインディング情報を入力します。
- 4) 「Save」ボタンをクリックして設定を保存します。

Delete	Port	VLAN ID	MAC Address	IP Address
Delete	1			

Add new entry

Save Reset

### 11.30. 認証サーバの指定

Authentication Server Configuration項目ではRADIUS、TACACS+リモートアクセス認証サーバで設定されたユーザー名とパスワードのリストをもとにアクセスの管理を行います、

**注意：** 本取扱説明書では RADIUS と TACACS+サーバは AAA をサポートするよう設定されていると想定しています。RADIUS と TACACS+サーバの設定は本取扱説明書の解説範囲外になります。RADIUS、TACACS+の設定に関しては、ご使用の RADIUS、TACACS+サーバに提供されている説明書をご参照ください。

#### 11.30.1. 11.26.1. authentication Server 設定パラメータ

##### Common Server Configuration

- 1) **Timeout:** スイッチが Request パケットを再送する前に認証サーバからの返信を待つ時間。
  - 設定値の範囲: 3-3600 秒
  - デフォルト値: 15 秒
- 2) **Dead Time:** スイッチから信が無い為認証サーバのサービスが停止していると判断するまでの時間。
  - 設定値の範囲: 0-3600 秒。
  - デフォルト値: 300 秒

##### RADIUS Server Configuration

- 1) **Enabled:** エントリに指定したサーバを有効にします。
- 2) **IP Address:** 認証サーバの IP アドレスまたは IP Alias
- 3) **Port:** 認証サーバが認証メッセージに使用するネットワークポート(UDP)。
  - 設定値の範囲 1-65535。
  - デフォルト値: 0

**注意：** UDP ポートを 0 に設定すると、スイッチは RADIUS 認証サーバに 1812 番ポートを、 1813 番ポートを RADIUS アカウンティングサーバに 1813 番ポートを、TACACS+認証サーバに 49 番ポートを使用します。

- 4) **Secret:** スイッチと認証サーバで共有される暗号鍵。最大長 29 文字。空の鍵を作成する場合はダブルクォーテーションマークを 2 つ("")使用してください。

### Authentication Serverの設定手順

- 1) エントリに指定したサーバを有効にします。
- 2) メニューから「Configuration」→「Security」→「AAA」を順にクリックします。
- 3) 認証方法を設定します。RADIUS、TACACS+サーバ、それぞれに必要な Common Server Configuration のパラメータ、アドレス、UDP ポート、Secret Key、を設定します「Save」ボタンをクリックして設定を保存します。

**Authentication Server Configuration**

Common Server Configuration

Timeout  seconds

Dead Time  seconds

RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1812	
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1813	
2	<input type="checkbox"/>		1813	
3	<input type="checkbox"/>		1813	
4	<input type="checkbox"/>		1813	
5	<input type="checkbox"/>		1813	

TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		49	
2	<input type="checkbox"/>		49	
3	<input type="checkbox"/>		49	
4	<input type="checkbox"/>		49	
5	<input type="checkbox"/>		49	

## 12. トランクグループ

本章では、トランクグループについて説明します。本スイッチは、静的なトランキングと動的なトランキング＝リンクアグリゲーション制御プロトコル（LACP）の両方をサポートしています。これにより複数のリンク、及びアグリゲートリンクを作成することができます。

### 12.1. トランクグループ設定のガイドライン

静的なトランク回線は、各リンクの両端のポートを手動で設定する必要があります。加えて、相互に接続されるスイッチは Cisco EtherChannel standard に適合しなければなりません。

一方、LACP を設定したポートは、他のデバイスで P-configured リンクを行ったトランクと自動的にネゴシエーションを行います。

まだ静的トランクを設定されていないポートならば、LACP を用いることにより、スイッチのどのポートにでも設定が可能です。

もし、他のデバイスの全てのポートが LACP を使うように設定されていた場合、スイッチと他のデバイスは、それらの間でトランクのネゴシエーションを行います。

LACP トランクが8ポート以上で構成されるなら、全ての他のポートは、スタンバイモードに移行します。トランク回線のうち、不良回線が1つでもあれば、スタンバイポートの一つが自動的に起動し、不良ポートと置き換わります。

まず、デバイス間の物理的な接続を始める前に、両端のデバイスのトランク回線の設定が必要になります。設定にあたっては、次のポイントに注意してください。

- 1) ループを作らないようにするため、スイッチ間のケーブルを接続する前に、ポートのトランクの設定を済ませます。
- 2) スイッチ 1 台につき最大 16 トランクを作成でき、トランクあたり最大ポート 14 を収容できます。(SMCG10X)
- 3) 接続の両端のポートは、トランクポートとして設定する必要があります。
- 4) 異機種あるいは他社製スイッチと本スイッチとの間で静的なトランク回線を設定する場合、それらは Cisco の EtherChannel 規格と互換性を持つ必要があります。
- 5) トランクの両端のポートは、通信モード、VLAN の割り当て及び CoS 設定が同等に設定されなければなりません。
- 6) フロントパネルのギガビットポート（RJ-45 及び SFP）は、各メディアタイプを混在させたトランク回線の作成が可能です。
- 7) あるトランク回線を構成する各ポートは、全て同じ VLAN の所属とするか、いずれも VLAN に所属させないかのどちらかに揃えてください。
- 8) STP、VLAN 及び IGMP は、トランク回線の中で共通に設定してください。

## 12.2. 静的トランク回線の設定

本章では、アグリゲーションモードと各静的トランクグループの要素の設定について説明します。

### 12.2.1. 静的トランク回線のガイドライン

- 1) 異なる種類のスイッチ同士が静的トランクでリンクできるかどうかは、各メーカーの実装に依存します。なお、本スイッチの静的トランクは、Cisco EtherChannel 互換です。
- 2) ネットワークのループを避けるため、ポートを接続する前に、静的トランクの設定インタフェースを確認してください。また、静的トランクを削除する前に、設定インタフェースを確認してポートを切断してください。
- 3) トランク回線における負荷分散のために、4 つの動作モードが用意されています。接続される環境において、モードを適切に選択されることを推奨いたします。
- 4) アグリゲーションモード設定は、LACP にも影響します。

### 12.2.2. 静的トランク回線のパラメータ

- 1) **Hash Code Contributors:** スwitchの全てのトランクに適用するロードバランスのモードを選択します。1 つ以上のオプションが選択されると、各要素はフレームを割り当てるべきトランク中のポートメンバーを決定するハッシュアルゴリズムで使われます。

➤ デフォルト値: IP Address

これには以下 4 つのオプションがサポートされています。

- |                                    |  |
|------------------------------------|--|
| i) <b>Source MAC Address</b>       | - 同じMACアドレスを発信元を持つ全てのトラフィックは、あるトランクの同じリンクから出力されます。このモードは、トラフィックがスイッチを通じて多くの異なるホストから受け取るような、スイッチ-スイッチ間のトランクリンクに最適です(デフォルトの一つです)   |
| ii) <b>Destination MAC Address</b> | <p>同じ送信先 MAC アドレスを持つ全てのトラフィックは、あるトランクの同じリンクから出力されます。</p> <p>このモードは、トラフィックがスイッチを通じて多くの異なるホストへ向けられるような、スイッチからスイッチへのトランクリンクに最適です。</p> <p>このモードを、全てのトラフィックの送信先MACアドレスが同じになる、スイッチ-ルータ間のトランクリンクに使わないでください。</p> |
| iii) <b>IP Address</b>             | <p>同じ発信元あるいは同じ送信先IPを持つ全てのトラフィックが、トランクの同じリンクから出力されます。</p> <p>このモードは、トラフィックがスイッチを通じて多くの異なるホストへ向けられるような、スイッチ-ルータ間のトランクリンクに最適となります。</p> <p>ただし、送信先IPアドレスが全てのトラフィックで同じになる、スイッチ-サーバ間のトランクリンクに使わないでください。</p>    |

(次ページに続く)

(前ページの続き)

- iv) **TCP/UDP Port Number** 同じ発振元と送信先のTCP/UDPポート番号を持つ全てのトラフィックは、トランクの同じリンクから出力されます。

- 2) **Group ID** – トランクの番号です。言い替えるとポートの集合体(グループ)の番号です。  
 3) **Port Members** – トランクグループに参加するポート番号の集合です。

### リンクアグリゲーションの設定手順

- 1) メニューから「Configuration」→「Aggregation」→「Static」を順にクリックします。
- 2) 1 つ以上のロードバランス方法を選びます。
- 3) ポートを使用する各トランクグループに割り当てます。
- 4) 「Save」ボタンをクリックして設定を保存します。

**Aggregation Mode Configuration**

**Hash Code Contributors**

Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

**Aggregation Group Configuration**

	Port Members									
Group ID	1	2	3	4	5	6	7	8	9	10
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1	<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"/>
2	<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"/>
3	<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"/>
4	<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"/>
5	<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"/>

Save Reset



## 12.3. 動的トランク回線 (LACP) の設定

本章ではLACPの設定について説明します。

### 12.3.1. 動的トランク回線 (LACP) のガイドライン

- 1) ネットワーク中にループを作らないように、ポートを接続する前に LACP を有効にするのを確認してください。また、LACP を禁止にする前に、ポートを切断してください。
- 2) 対向スイッチの接続ポートも同じように LACP が有効にされていると、トランクは自動的に起動します。
- 3) LACPを用いたもう一つのスイッチで形成されたトランクは、自動的に次の利用可能なトランク ID が割り当てられます。
- 4) 同じ対向スイッチに向けて 8 個を超える LACP ポートを設定した場合、超過したポートは待機状態となります。これらは、既に起動しているリンクがダウンすると、待機状態から稼働状態に切り替わります。
- 5) LACP トランクの両端にある全てのポートは、固定モードあるいはオートネゴシエーションによって、全二重に設定する必要があります。
- 6) LACP を通じて動的に確立したトランクは、モニターメニューの下、LACP システムステータスページと LACP ポートステータスページに現れます。
- 7) コモンリンクアグリゲーショングループ (LAG) に割り当てられたポートは、次の基準に一致しなければなりません。
  - 各ポートは同じLACP管理キーを持つ必要があります。管理キーの指定は自動生成 (Auto) の使用を推奨します。
  - ポートの近端か遠端のどちらか一つは、アクティブイニシエーションモードに設定しなければなりません。
- 8) Static Aggregation メニューの下にある Aggregation Mode Configuration は、LACP にも適用されます。

### 12.3.2. 動的トランク回線 (LACP) のパラメータ

- 1) **Port:** ポート番号に対応しています。
- 2) **LACP Enabled:** LACP を有効にするポートを設定します。LACP は 2 つ以上のポートが同じパートナーに接続される場合にアグリゲーションを形成します。LACP はスイッチあたり最大 12 個まで形成できます。
- 3) **Key:** あるリンクアグリゲーションに所属する各ポートは、いずれも同じ値の LACP 管理キーを持つ必要があります。  
動的トランクが 1 つしかない場合は、プルダウンメニューで Auto を選択すると、キーの値が自動的に決定されます。もし、動的トランクを複数存在させたい場合は、先にプルダウンメニューで Specific を指定した後、隣の欄に任意のキー値を入力します。
  - 設定値の範囲: 0-65535
  - デフォルト値: Auto
- 4) **Role:** LACP の初期化方法を、Active か Passive の何れかに設定します。あるポートの LACP ネゴシエーションの初期化を Active にすると、LACP ネゴシエーションパケットを自動的に送出します。(周期:1 回/秒)。  
初期化を Passive モードにすると、LACP ネゴシエーションパケットがパートナーから受信されるまでネゴシエーションを待つことになります。
  - 設定値の範囲: Active, Passive
  - デフォルト値: Active

#### LACPの設定手順

- 1) メニューから「Configuration」→「Aggregation」→「LACP」を順にクリックします。
- 2) リンクアグリゲーション(LAG)を行う全てのポートの「LACP Enabled」の欄にチェックを入れます。
- 3) 特定の LAG、ポートを制限するために LACP 管理キーを指定します。
- 4) 各 LAG を構成するポートの近端あるいは遠端のうち、少なくとも 1 つのポートをアクティブイニシエーションモードに設定します。
- 5) 「Save」ボタンをクリックして設定を保存します。

LACP Port Configuration

Port	LACP Enabled	Key	Role
1	<input type="checkbox"/>	Auto	Active
2	<input type="checkbox"/>	Auto	Active
3	<input type="checkbox"/>	Auto	Active
4	<input type="checkbox"/>	Auto	Active
5	<input type="checkbox"/>	Auto	Active
6	<input type="checkbox"/>	Auto	Active
7	<input type="checkbox"/>	Auto	Active
8	<input type="checkbox"/>	Auto	Active
9	<input type="checkbox"/>	Auto	Active
10	<input type="checkbox"/>	Auto	Active

Save Reset

## 13. Loop Protection (SMCGS18/26/50 のみ対応)

本章では、Loop Protection について説明します。

### 13.1. Loop Protection の設定

Loop Protectionでは、ループ保護の設定を行います。

#### 13.1.1. Loop Protection パラメータ設定

##### General Settings

- 1) **Enable Loop Protection:** 本スイッチのループ保護機能の有効/無効を選択します。
- 2) **Transmission Time:** loop protection PDU の送信間隔を指定します。
  - 設定値の範囲: 1-10秒
  - デフォルト値: 5秒
- 3) **Shutdown Time:** ループが検出された場合にポートをシャットダウンする時間を指定します。  
0を指定した場合はスイッチを再起動させるまでポートがシャットダウンされます。
  - 設定値の範囲: 0-604800秒
  - デフォルト値: 180秒

##### Port Configuration

- 1) **Port:** ポート番号を表示します
- 2) **Enable:** ポート毎にループ保護機能の有効/無効を選択します。
- 3) **Action:** ループが検出された際に実行するアクションを選択します。
- 4) **Tx Mode:** loop protection PDU を送信するかどうかを選択します。

#### Loop Protectionの設定手順

- 1) General Settings, Port Configuration を適宜設定します。
- 2) 「Save」ボタンをクリックして設定を保存します。

**Loop Protection Configuration**

**General Settings**

**Global Configuration**

Enable Loop Protection	Disable
Transmission Time	5 seconds
Shutdown Time	180 seconds

**Port Configuration**

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<>	<>
1	<input checked="" type="checkbox"/>	Shutdown Port	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port	Enable

## 14. スパニングツリーアルゴリズムの設定

本章では、スパニングツリーアルゴリズム(STA)の設定方法を説明します。

本スイッチは STA をサポートしていますが、この機能はネットワークループの検出や禁止に使うことができ、またスイッチ、ブリッジあるいはルータ間のバックアップリンクを作ることもできます。

これにより、ネットワーク上のあらゆる2拠点の間に唯一のルートだけが存在することを確実にするための、スイッチと他のブリッジ機器 (STA準拠のスイッチ、ブリッジまたはルータ) の情報のやりとりが可能になります。

そして、一次リンクがダウンした際に、自動的に引き継ぐバックアップリンクが提供されます。本スイッチがサポートするスパニングツリーアルゴリズムは以下の通りです。

- 1) STP: Spanning Tree Protocol (IEEE 802.1D)
- 2) RSTP: Rapid Spanning Tree Protocol (IEEE 802.1w)
- 3) MSTP: Multiple Spanning Tree Protocol (IEEE 802.1s)

### 14.1. スパニングツリー設定のガイドライン

#### 1) スパニングツリープロトコル

RSTP を内部状態マシンとして使用しますが、BPDU は 802.1D のみを送信します。これにより、ネットワーク全スパニングツリーインスタンスが 1 つ生成されます。

VLAN を複数操作する場合は、MSTP の選択を推奨します。

#### i) ラピッドスパニングツリープロトコル

この RSTP では、STP モードあるいは RSTP ノードのいずれかをサポートします。

- **STP モード:** ポートのマイグレーションディレイタイマーの経過後、スイッチが 802.1D BDU (STP BPDU) を受け取ると、スイッチは 802.1D ブリッジに接続されたと仮定して、802.1D BPDU のみを使用して動作します。
- **RSTP モード:** RSTP がポートで 802.1D BPDU を用い、マイグレーションディレイタイマーの経過後に RSTP BPDU を受け取ると、RSTP はマイグレーションディレイタイマーをリスタートさせ、RSTP BPDU をそのポートで使用開始します。

#### ii) マルチプル スパニングツリープロトコル

MSTP は各インスタンスに一意となるスパニングツリーを生成します。これによって、ネットワーク中に複数の経路を与え、トラフィックの負荷を平均化します。

さらに、単一インスタンスのブリッジノードが故障した際には、広範囲にわたる混乱を防ぎます。

#### 14.1.1. スパニングツリー設定のヒント

- 1) マルチプルスパニングツリーにネットワークを超えた動作をさせるためには、同じ MSTP 設定を関連するブリッジに設定しなくてはなりません。
- 2) スパニングツリーインスタンスは、VLAN-インスタンス割り当てに互換性を持つブリッジの上にしか存在できません。
- 3) スパニングツリーのモードを切り替えるときは注意が必要です。モードの変更は、以前のモードにあった全てのスパニングツリーインスタンスを停止し、新しいモードでシステムを再開させるので、ユーザーのトラフィックが一時的に中断します。

#### 14.1.2. スパニングツリー設定のパラメータ

- 1) **Protocol Version:** スパニングツリーアルゴリズムを STP、RSTP、MST の中から選択します。
  - 設定値の範囲:
    - STP: IEEE 802.1Dを使用します。RSTPをSTP強制互換モードで動作させます。
    - RSTP: ラピッドスパニングツリー (IEEE 802.1w)
    - MSTP: マルチプルスパニングツリー (IEEE 802.1s)
  - デフォルト値: MSTP
- 2) **Bridge Priority:** ブリッジ優先度はルートブリッジ、ルートポート、指定ポートの選択に用いられます。高い優先度を持つ装置はスパニングツリーアルゴリズムのルートブリッジになります。全てのブリッジが同じ優先度を持つならば、(数値として見た場合)、小さい MAC アドレスを持つブリッジがルートブリッジになります。(※ 低い数値ほど優先度が高くなります。)
  - 設定値の範囲: 0-240 ただし、16刻み。(0, 16, 32 ... 224, 240)
  - デフォルト値: 128
- 3) **Forward Delay:** 転送遅延タイマー。リスニングとラーニングの完了を待つ最大時間(秒)です。この時間が十分ないと、一時的にループ状態が残ります。
  - 設定の最小値: 4以上か、(メッセージ経過時間の最大値÷2) + 1
  - 設定の最大値: 30
  - デフォルト値: 15
- 4) **Max Age:** ルートスイッチからのコンフィギュレーション BPDU を待つ秒数を指定します。間に合わない場合は、スパニングツリーの再構築を試みます。指定ポートを除くブリッジのポートは、全てコンフィギュレーション BPDU を定期的に受け取るべきです。
  - 設定の最小値: 6 か、[ 2 x (Hello Time + 1) ] のどちらか大きいほう。
  - 設定の最大値: 40 か、[ 2 x (Forward Delay - 1) ] の小さいほう。
  - デフォルト値: 20
- 5) **Maximum Hop Count:** マルチプルスパニングツリーを使用する際のホップの最大値を指定します。
  - 設定値の範囲: 6-40
  - デフォルト値: 20

6) **Transmit Hold Count:** ポートが 1 秒あたりに送信できる BPDU の数です。これを超えた BPDU は送出が遅れます。

- 設定値の範囲: 1-10
- デフォルト値: 10

7) **Edge Port BPDU Filtering:** ブリッジの機能を持たない端末等が接続されたポート、即ち、エッジポートに対して BPDU の転送を無効にする場合、Enabled に設定します。この BPDU フィルタリングは、ポート毎の設定となります。

なお、スパンニングツリーアルゴリズムは、管理エッジポートの指定に関係なく、デフォルトで全てのポートに BPDU を送信します。

- デフォルト: チェックなし

8) **Edge Port BPDU Guard:** この機能を設定したエッジポートは、BPDU を受信するとシャットダウンします。エッジポートが BPDU を受け取る場合、無効な構成があると言えます。

- デフォルト: チェックなし

9) **Port Error Recovery:** 禁止状態 (Disabled) にあるポートを、ある時間の経過後(別途指定)、許可状態 (Enabled) に回復させます。回復された状態が Enabled でない場合、ポートは Disabled でなくてはならず、通常の STA 操作のために再度 Enabled にならなくてはなりません。スイッチのリブートによって、状態は消去されます。

- デフォルト: チェックなし

10) **Port Error Recovery Timeout:** Disabled の状態にあるポートを、指定した時間で Enabled にします。

- 設定値の範囲: 30-86400 秒

### STAのグローバル設定の手順

- 1) メニューから「Configuration」→「Spanning Tree」→「Bridge Settings」の順にクリックします。
- 2) 必要な属性を変更します。
- 3) 「Save」ボタンをクリックして設定を保存します。

STP Bridge Configuration

Basic Settings

Protocol Version	RSTP
Bridge Priority	128
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Save Reset

## 14.2. マルチプルスパニングツリーの設定

本章では、マルチプルスパニングツリーの設定について説明します。MSTI Mapping ページから、VLAN グループを MSTP インスタンス (MSTI) に参加させます。

### 14.2.1. マルチプルスパニングツリー

MSTP は各インスタンスに一意となるスパニングツリーを生成します。スパニングツリーを使う手順は以下の通りです。

- 1) スパニングツリーの種類から MSTP を選びます。
- 2) MSTI Mapping ページで、この MSTI を共有したい VLAN を追加します。
- 3) MSTI Priorities ページにある MST インスタンスと CIST を選択し、スパニングツリー優先度を入力します。

**注意:** 全ての VLAN は自動的に CIST (MST インスタンス 0) に追加されます。ネットワーク全域の接続性の維持を確実にするには、関連するブリッジのセットを、同じ MSTI の設定で揃えなければなりません。

### 14.2.2. マルチプルスパニングツリーのパラメータ

- 1) **Configuration Name:** MSTI の名前
  - 設定値の範囲: 最大文字長: 32 ASCII 文字
  - デフォルト値: スイッチの MAC アドレス。(例: 00-01-c1-01-02-03)
- 2) **Configuration Revision:** MSTI のリビジョン
  - 設定値の範囲: 0-65535
  - デフォルト値: 0
- 3) **MSTI:** スパニングツリーの識別子です。CIST は明示的なマッピングでは使用できないので、暗黙にマップされた VLAN を受け取ります。MSTI1-MSTI7 まで用意されています。
- 4) **VLANs Mapped:** この MST インスタンスに割り当てられた VLAN です。各 VLAN はコンマか、あるいはスペースで区切られなければなりません。VLAN は一つの MSTI のみ割り当てることができます。
  - 設定値の範囲: 1-4094

### マルチプルスパニングツリーの設定手順

VLAN グループを SMTP インスタンスに割り当てます。

- 1) メニューから「Configuration」→「Spanning Tree」→「MSTI Mapping」の順にクリックします。
- 2) VLAN マップの項目に、インスタンスに追加する VLAN グループを追加します。

**注意： 指定した要素は、設定された VLAN でなくても構いません。**

- 3) 「Save」ボタンをクリックして設定を保存します。

#### MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-01-c1-01-02-03
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Save

Reset



### 14.3. スパニングツリーブリッジプライオリティの設定

この章では、MSTI Prioritiesページでは、CISTと他の設定済MSITに対するブリッジの優先度の指定について説明します。

なお、RSTPは互いのMST インスタンスをブリッジノードとみなすことに注意してください。

#### 14.3.1. スパニングツリーブリッジプライオリティのパラメータ

- 1) **MSTI:** インスタンス識別子
  - MSTIの範囲: CIST, MST1-7
- 2) **Priority:** スパニングツリーインスタンスの優先度を指定します。
  - 設定値の範囲: 0-240、ただし16刻み(0, 16, 32 ... 240)
  - デフォルト値: 128

#### スパニングツリーブリッジプライオリティの設定

次の手順で MSTP インスタンスに VLAN を追加します。

- 1) メニューから「Configuration」→「Spanning Tree」→「MSTI Priorities」の順にクリックします。
- 2) CIST あるいは MSTI にブリッジ優先度を設定します。

The screenshot shows the 'MSTI Configuration' page with a sub-tab 'MSTI Priority Configuration'. It contains a table with two columns: 'MSTI' and 'Priority'. The table lists CIST and MSTI1 through MSTI7, all with a priority of 128. Below the table are 'Save' and 'Reset' buttons.

MSTI	Priority
CIST	128
MSTI1	128
MSTI2	128
MSTI3	128
MSTI4	128
MSTI5	128
MSTI6	128
MSTI7	128

### 14.3.2. STP/RSTP/CIST インタフェースの設定

CIST Port Configuration では、スパニングツリーがSTP、RSP、またはCISTにおけるインタフェースの属性を設定します。

### 14.3.3. STP/RSTP/CIST インタフェースのパラメータ

- 1) **Port:** ポート番号は静的なトランク、あるいは LACP によって作られた動的なトランクには適用されません。  
全てのトランクに適用できるのは、一組のインタフェースの設定だけです。
- 2) **STP Enabled:** インタフェースを、STA 許可(Enabled)、STA 禁止(Disabled)、BPDU 透過つきの STA 禁止、にします。
  - デフォルト: チェックあり (STP Enabled)
- 3) **Path Cost:** パラメータは、ブリッジ間のもっとも良い経路を決定するためにスパニングツリーアルゴリズムを使います。システムはデフォルトで、各ポートが使用する速度と二重化のモードを自動的に検出します。
  - 設定値の範囲: 上記の通り。  
ただし、プルダウンメニューで Specific を選択する必要があります。
  - デフォルト値: Auto

表: スパニングツリー推奨パスコスト範囲

速度	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50 ~ 600	200,000 ~ 20,000,000
Fast Ethernet	10 ~ 60	20,000 ~ 2,000,000
Gigabit Ethernet	3 ~ 10	2,000 ~ 200,000

表: スパニングツリー推奨パスコスト

速度	リンク	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

表: デフォルトSTAパスコスト

速度	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50 ~ 600	200,000 ~ 20,000,000
Fast Ethernet	10 ~ 60	20,000 ~ 2,000,000
Gigabit Ethernet	3 ~ 10	2,000 ~ 200,000

- 4) **Priority:** 該当スループートのスパニングツリーにおける優先度を指定します。
  - 設定値の範囲: 0-240, 16 刻み (0, 16,... 224, 240)
  - デフォルト値: 128
  
- 5) **Admin Edge (高速転送):** ポートがノードの終端(ブリッジが存在しない)の場合、このオプションを指定することにより、スパニングツリーの再構成に掛かる時間を低減できます。
  - 設定の範囲: Non-Edge, Edge
  - デフォルト値: Edge
  
- 6) **Auto Edge:** ポートがエッジポートかどうかを自動的に判断します。チェックボックスにチェックを入れると、BPDU を受け取るまでエッジポートとして扱います。
  - デフォルト: チェックあり
  
- 7) **Restricted Role:** チェックを入れたポートは、そのポートの優先度が最高に指定されていたとしても、CIST や MSTI のルートポートにはなりません。この機能は別名ルートガードと呼びます。
  - デフォルト: チェックなし
  
- 8) **Restricted TCN:** これにチェックが入っていると、トポロジ変更通知 (Topology Change Notice) を受け取っても通知せず、トポロジを他のポートに変更します。
  - デフォルト: チェックなし
  
- 9) **BPDU Guard:** ポートが BPDU の受信を受けた場合に、ループの生成を防ぐためポートをシャットダウンします。シャットダウンからの回復は管理者が手動で行う必要があります。Enabled にすると、ポートは有効な BPDU を受け取ると即座に禁止状態になります。ただし、ポートエッジステータスはこの設定に影響を与えません。この設定によって、エラーによる禁止状態に陥ったポートは、同様にブリッジの Port Error Recovery 設定に従います。
  - デフォルト: チェックなし(Disabled)
  
- 10) **Point-to-Point:** インタフェースに設定するリンクタイプを自動認識、ポイントツーポイントあるいは共有に設定することが可能です。
  - 設定値の範囲は以下の通り:
    - **Auto** - リンクタイプは接続のモードで決定されます。全二重ならばポイントツーポイント、半二重ならば共有リンクとします。
    - **Forced True** - 他のブリッジとポイントツーポイントで接続します。
    - **Forced False** - 2 つ以上のブリッジと共有接続します。
  - デフォルト値: Auto

**STP/RSTP/CIST インタフェースの設定:**

- 1) メニューから、「Configuration」→「Spanning Tree」→「CIST Ports」の順にクリックします。
- 2) 各属性を変更します。
- 3) 「Save」ボタンをクリックして設定を保存します。

STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		
-	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		
1	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input checked="" type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Save Reset

**14.4. MSTI インタフェースの設定**

この章では、MSTI Ports Configuration で特定のMSTIにおけるポート毎のスパニングツリーアルゴリズムの属性の設定について説明します。

**14.4.1. MSTI インタフェース設定のヒント**

好ましい経路を明示するため、同じメディアタイプに異なる優先度や、パスコストを与えても構いません。

**14.4.2. MSTI インタフェースのパラメータ**

- 1) **Port:** 設定を適用するポート番号です。この項目を、LACPを通じて生成される静的なトランクや動的なトランクに適用することはできません。
- 2) **Path Cost:** デフォルトでは自動設定になっています。パスコストを各ポートのメディアの速度や通信モードから決定します。

(次ページに続く)

(前ページの続き)

- 3) **Priority:** ポートの優先度を指定します。スイッチのポート全てのパスコストが等しければ、優先度の高いポートがスパンニングツリーでアクティブなリンクに設定されます。
- 1 つ以上のポートが高い優先度に設定されていると、より小さい番号を持つポートが有効になります。
- 設定値の範囲: 0-240 (16刻み)
  - デフォルト値: 128

### MSTI インタフェースの設定手順

- 1) メニューから「Spanning Tree」→「MSTI Ports」をクリックします。
- 2) プルダウンメニューから、MST1-MST7 のうち 1 つを選択します。ここで選択したインタフェースは、全トランクに影響を与える唯一のインタフェースとなります。
- 3) 「Get」ボタンを押します。
- 4) 必要な属性を設定します。
- 5) 「Save」ボタンをクリックして設定を保存します。

2) MST1～MST7 を選択

3) 「Get」ボタン

MSTI Port Configuration

Select MSTI  
MST1 Get

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration

Port	Path Cost	Priority
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
7	Auto	128
8	Auto	128
9	Auto	128
10	Auto	128

Save Reset

## 15. マルチキャスト VLAN レジストレーション (MVR)

本章では、マルチキャスト VLAN レジストレーションの設定について説明します。MVR はマルチキャストルーティングを使用することなくストリームを制御し、IGMP と同様の動作を行います。IGMP から独立した機能です。

### 15.1. MVR のヒント

MVR の一般的な設定の流れは次のようになります。

- 1) スイッチ全体の MVR を有効あるいは無効 (Enabled/Disabled) に設定します。次に、MVR に与える VLAN の ID を入力します。
- 2) MVR に参加するポートを有効に設定します。
- 3) マルチキャスト VLAN は、ソースポートとレシーバポートの組で作られる特殊な VLAN なので、関係するポートにはどちらか一方 (Source/Receiver) を指定します。基本的にマルチキャストはソースポートからレシーバポートに流れます。
- 4) 指定のポートにただ 1 台のホストしか接続されていないと確信できる場合は、IGMPv2 の即時脱退メッセージ (Immediate Leave) を Enabled にできます。これには、ホストがマルチキャストグループを抜けた後に不要なフラグディングを抑制する効果があります。

**注意:** MVR は IGMP スヌーピングの機能を利用して動作しますが、いずれ独立した機能であり、互いに影響を与えません。

なお、マルチキャストリーブメッセージを送信できるのは、IGMP ver.2 と ver.3 のホストだけであって、IGMP ver.1 のクライアントは 即時リーブメッセージを送信できません。

### 15.2. MVR のパラメータ

- 1) **MVR Mode:** MVR を許可(Enabled)すると、MVR グループに関係したどのマルチキャストデータも、ソースポートから、全てのレシーバポートに送信されます。なお、どちらのポートも MVR に登録する必要があります。
- 2) **MVR VLAN:** MVR にマルチキャスト用 VLAN として登録する VLAN の ID を設定します。
  - デフォルト値: 100

**注意:** ソースポートはMVRのVLANメンバーとして登録する必要がありますが、レシーバポートについては、スイッチが必要に応じて動的にVLANへ割り当てます。よって、レシーバポートを手動でVLANに割り当てないでください。

- 3) **Port:** 設定を適用するポートの番号です

(次ページに続く)

(前ページの続き)

- 4) **Mode:** MVR Mode はこのスイッチ全体に適用される設定ですが、このパラメータはその効果を個別のポートに反映させるためのものです。

MVR のグループからマルチキャストのトラフィックを受信する加入者がいた場合、そのレシーバポートを Enabled にする必要があります。

➤ デフォルト値: Disabled

- 5) **Type:** 以下のインタフェースタイプがサポートされています。

- **Source:** アップリンクしたポートは、MVR VLAN に割り当てられたグループのためにマルチキャストデータを送受信できます。

**注意:** ソースポートは手動でMVR VLANに登録しなければなりません。

- **Receiver:** MVR VLAN を通してマルチキャストデータを受信できる加入者ポートです。

レシーバポートとして設定されたポートは、IGMP レポートまたはホストのジョインメッセージを転送する際、動的にMVR VLANに追加されますので、手動でVLANに追加する必要はありません。

- 6) **Immediate Leave:** IGMP のバージョン 2 とバージョン 3 の機能にあたり、ホストから即時リーブメッセージを受けると、該当するポートをマルチキャストストリームから外します。

この機能により、不要なパケットがポートに流れなくなります。

ただし、このオプションが適用されるのは、MVR レシーバとして登録したポートだけです。IGMP のバージョン 2 と 3 に対応したホストは、マルチキャストグループから能動的なリーブが可能です。仮にバージョン 1 にしか対応していなければ、スイッチからの定期的な問合せに応答しないことでリーブしたとみなされます。

## MVRの設定手順

- 1) メニューから「Configuration」→「MVR」の順にクリックします。
- 2) MVR Mode」の全体的な設定を行った後、MVR VLAN の設定を行います。
- 3) MVR にソースポート、あるいはレシーバポートとして参加する各ポートを設定します。レシーバポートの先に存在するホストが、IGMP ver.2 あるいは ver3 に対応しているのであれば、Immediate Leave を Enabled に選択することにより、不要なトラフィックを削減できます。
- 4) 「Save」ボタンをクリックして設定を保存します。

Port	Mode	Type	Immediate Leave
1	Disabled	Receiver	Disabled
2	Disabled	Receiver	Disabled
3	Disabled	Receiver	Disabled
4	Disabled	Receiver	Disabled
5	Disabled	Receiver	Disabled
6	Disabled	Receiver	Disabled
7	Disabled	Receiver	Disabled
8	Disabled	Receiver	Disabled
9	Disabled	Receiver	Disabled
10	Disabled	Receiver	Disabled

## 16. IGMP スヌーピング

本スイッチは IGMP をサポートしており、マルチキャストストリームをフィルタリング制御することが可能です。この章では IGMP スヌーピングの設定について説明します。

### 16.1. IGMP スヌーピングのグローバル設定とポート設定

この章ではスイッチ全体と、ポート単位で行う IGMP スヌーピングの設定について説明します。

他のスイッチがマルチキャストルーティングをサポートしていない場合、IGMP スヌーピングと IGMP クエリを使って、マルチキャストサーバとクライアント間の IGMP サービスリクエストを監視することができます。

また、マルチキャストトラフィックを転送する必要があるスイッチのポートを、動的に設定することができます。

#### 16.1.1. IGMP スヌーピングの設定パラメータ

- 1) **Snooping Enabled:** チェックボックスにチェックを入れると、スイッチはマルチキャストパケットを解析し、どのホストがどのマルチキャストグループに参加しているかをチェックし、不要なフラディングを抑制します。
  - デフォルト: チェックなし (Disabled)
- 2) **Unregistered IPMC Flooding Enabled:** 未登録のマルチキャストストリームを VLAN に流すかどうかを設定します。
 

ただし、IGMP スヌーピングにより、マルチキャストグループと、それに参加するホストを記録するテーブルが満杯になると、新たな学習はされません。VLAN にルータポートが設定されていない場合、この項目が禁止(disabled)になっていると、テーブルにないマルチキャストトラフィックはドロップされます。

  - デフォルト: チェックあり (Enabled)
- 3) **Leave Proxy Enabled** – チェックを入れると、マルチキャストグループに参加している全てのメンバーポートからリーブメッセージを受信するまで、リーブメッセージを転送しません。
 

なお、リーブプロキシ機能は、スイッチがクエリアに設定されているときは機能しません。加えて、以下の条件が全て当てはまる場合、スイッチはグループ指定(GS)クエリを生成し、リーブメッセージを受け取ったメンバーポートに送信します。

この際、レシーバポートがルータポートである場合を除けばスイッチは GS クエリを送信しますが、ただちにポートの最終メンバークエリタイマーが動作します。

  - i) スwitchがクエリアでない。
  - ii) レシーバポートがグループの最後の動的メンバーポートではない。
  - iii) レシーバポートがルータポートではない。
  - iv) グループに IGMP ver.1 メンバーポートが存在しない。

(次ページに続く)



(前ページの続き)

Leave proxy もまた、以下に記す一般的なプロキシの機能に含まれます。

従って、Leave Proxy Enabled が選択されずに、代わりにProxy Enabledが選択されたならば、Leave proxyは実行されたままになります。

➤ デフォルト: チェックなし(Disabled: 転送を許可する)

- 4) **Proxy Enabled:** Proxy Reporting と共に IGMP スヌーピングを許可します。このコマンドがプロキシレポートと共に使われると、スイッチは IGMP スヌーピングとプロキシレポート、レポートの削減、ラストリーブ、クエリ削減を行います。

ラストリーブは、マルチキャストグループから最後のメンバーが抜けたときにプロキシクエリを送出し、クエリ削除は、特別のクエリや一般的なクエリを上流のマルチキャストルータからホストへ転送されません。

プロキシレポートが禁止 (Disabled) の場合は、スイッチが受け取った全ての IGMP レポートは上流のマルチキャストルータに転送されます。

➤ デフォルト: チェックなし(Disabled)

- 5) **Port:** 設定を適用するポート番号です。

- 6) **Router Port:** ポートをルータポート(IGMP クエリを受信するポート)に設定します。

もし、IGMP スヌーピングが IGMP クエリアの位置を正しく見つけられないのであれば、既知の IGMP クエリア (マルチキャストルータあるいはスイッチ)を手動で指定することもできます。このインタフェースは、スイッチ内の全ての適切なインタフェースにマルチキャストのトラフィックを確実に渡すため、後に全てのマルチキャストグループに参加します。

➤ デフォルト: チェックなし(Disabled)

- 7) **Fast Leave:** このオプションをチェックすると、ポートがリーブメッセージを受け取り次第、ただちにマルチキャストに参加しているメンバーポートを削除します。

これにより、IGMP グループ指定 (GS) クエリを送信することなく、ポートをマルチキャスト転送テーブルから削除できます。高速リーブが使われていないときに、IGMPv2/IGMPv3 グループリーブメッセージを受信すると、マルチキャストルータ (或いはクエリア) は GS クエリメッセージを送信します。

ルータやクエリアは、指定したタイムアウト時間内にクエリに対してリプライを返すホストが無くなると、グループのトラフィック転送を停止します。

高速リーブが可能な場合なポートは、IGMP が可能なホストが一台だけ接続されている場合、後はサービスホストあるいは近隣で IGMPv2 か IGMPv3 スヌーピングを使っている場合です。

高速リーブは、マルチキャストルータが接続されているかどうかスイッチが学習するまで適用されません。

➤ デフォルト: チェックなし(Disable)

➤

- 8) **Throttling:** ポートが所属できるマルチキャストグループの数を制限します。この数を越えた IGMP join レポートはドロップされます。

➤ 設定値の範囲: unlimited、1-10

➤ デフォルト: unlimited

### IGMPスヌーピングの設定手順

- 1) メニューから「Configuration」→「IPMC」→「IGMP Snooping」→「Basic Configuration」の順にクリックします。
- 2) 必要な IGMP 設定を行います。
- 3) 「Save」ボタンをクリックして設定を保存します。

IGMP Snooping Configuration

**Global Configuration**

Snooping Enabled ☐

Unregistered IPMC Flooding Enabled ☒

Leave Proxy Enabled ☐

Proxy Enabled ☐

**Port Related Configuration**

Port	Router Port	Fast Leave	Throttling
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▼

Save Reset

## 16.2. IGMP スヌーピングとクエリに関する LAN 設定

この章では、IGMP Snooping VLAN Configuration と、VLAN インタフェースのクエリの設定について説明します。

### 16.2.1. IGMP スヌーピングとクエリに関する設定パラメータ

- 1) **VLAN ID:** VLAN 番号
- 2) **Snooping Enabled:** チェックボックスをオンにすると、指定した VLAN インタフェースのトラフィックを監視して、どのホストがマルチキャストの受信を要求しているかを確認するようになります。

このスイッチ全体としての IGMP スヌーピングが許可されている場合は、VLAN インタフェースの IGMP スヌーピングの設定が優先されます。

逆に、スイッチ全体で IGMP スヌーピングが禁止されている場合、VLAN インタフェース毎のスヌーピング設定は可能ですが、スヌーピングはしません。

スヌーピングを行うには、このスイッチ全体としての設定が必要になります。

- デフォルト: チェックなし (Disabled)

**注意:** この項目にチェックを入れて、一旦 Save を行ってください。項4)以降の入力が可能になります。

- 3) **IGMP Querier:** チェックボックスをオンにすると、指定のポートがクエリアとして動作します。ルータ、あるいはマルチキャスト対応スイッチは、配下のホストがマルチキャストストリームの受信要求を出しているかどうかを定期的にチェックします。

- デフォルト: チェックなし (Disabled)

- 4) **RV:** ロバストネス変数(Robustness Variable) は、クエリアとホスト間で発生するパケットロスによって、ホストがマルチキャストグループから外されてしまう可能性を低減できます。ロバストネス変数は、クエリに対して返事のないポートにおけるクエリの数を増やします。

クエリアのロバストネス変数(QRV: Querier's Robustness Value) が 0 ならば、QVR フィールドはロバストネス変数が無指定であることを示しているため、スイッチはロバストネス変数をこのコマンドによって静的に設定します。

QVR に最大値7を超えた数値を入力すると、ロバストネス変数は 0 に設定されます。このデバイスは、その後続いて送られるその他のメッセージで QRV の通知を行いません。

- 設定値の範囲: 1-255
- デフォルト値: 2

**注意:** この項目は、先に項2) にチェックを入れて Save しないと、入力できません。

(次ページに続く)

(前ページの続き)

- 5) **QI:** クエリアが MLD General Query(IGMPv2)を送出する間隔です。マルチキャストグループに参加しているホストがこれを受け取ると、MLD レポートを構築します。
- 設定値の範囲: 1-255 (単位: 秒)
  - デフォルト値: 125

**注意:** この項目は、先に項2) にチェックを入れて Saveしないと、入力できません。

- 6) **QRI:** Query Response Interval は、定期的に通ずられる General Query クエリに対する最大応答時間です。QRI は、スイッチがクエリアとして General Query を通知する際、この通知への応答を何時まで待つかを周囲の機器に知らせるために使われます。
- 設定値の範囲: 10-31744 (単位: 100ミリ秒)

**注意:** この項目は、先に項2) にチェックを入れて Saveしないと、入力できません。

- 7) **LLQI:** Last Member Query Interval (RFC 3810 – MLDv2 for IP) には、group-specific あるいは group-and-source-specific クエリメッセージに対するレスポンスの待ち時間を設定します。LLQI に割り当てられた値とは、1 つのレスポンスを待つ時間全体を指し、Last Member Query Count (2 に固定)によって多重化されます。

ホストがマルチキャストグループから離れる際に、IGMP リーブメッセージを送信します。

スイッチがリーブメッセージを受け取ると、IGMP グループ指定あるいは group-and-source-specific クエリメッセージのいずれかを送ってタイマーを開始し、送信元であるホストがグループに残った最後のホストかどうかをチェックします。

タイマーが廃棄されるまで何も受信しなければ、グループの記録は削除され、レポートがアップストリームのマルチキャストルータへ送られます。

値が減少すると、グループまたはソースの最後のメンバーを失ったかどうかを検知する時間を減らす結果になりますが、より急なトラフィックを発生させます。この属性は、IGMP snooping proxy reporting が Enabled のときだけに有効になります。

- 設定値の範囲: 1-31744 (0.1秒単位)

**注意:** この項目は、先に項2) にチェックを入れて Saveしないと、入力できません。

- 8) **URI:** Unsolicited Report Interval は、レポート削減とプロキシーレポートが Enabled のとき、自動的にメンバーシップレポートを送信する間隔を指定します。
- 設定値の範囲: 0-31744 (単位: 秒)

**注意:** この項目は、先に項2) にチェックを入れて Saveしないと、入力できません。

### IGMP スヌーピング VLAN設定手順

- 1) メニューから「Configuration」→「IPMC」→「IGMP Snooping」→「VLAN Configuration」の順にクリックします。
- 2) Snooping Enabled にチェックを入れて、一旦 Save します。
- 3) 続けて各項目の設定を行います。
- 4) 「Save」ボタンをクリックして設定を保存します。

ここに入力するには、先に Snooping Enabled にチェックを入れて Save する必要があります。

### 16.3. IGMP フィルタリングの設定

このページでは、マルチキャストトラフィックをポート毎にフィルタリングする設定を行います。

例えば、IP による TV の有料チャンネル等、スイッチのポート単位で視聴の可否を設定したい場合に使用します。

#### 16.3.1. IGMP フィルタリングの設定のパラメータ

- 1) **Port:** 本スイッチのポート番号です。
- 2) **Filtering Groups:** 該当するポートで拒否したいマルチキャストグループを指定します。指定されたマルチキャストグループに対する Join レポートをポートが受け取ると、ドロップします。

#### IGMPフィルタリングの設定手順

- 1) メニューから「Configuration」→「IPMC」→「IGMP Snooping」→「Port Group Filtering」を順にクリックします。
- 2) 表中の「Add New Filtering Group」をクリックして、新しいエントリを表示します。
- 3) フィルタリングを適用したいポートをクリックします。
- 4) フィルタリングを適用したい IP アドレスを入力します。
- 5) 「Save」ボタンをクリックして設定を保存します。

IGMP Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups
Add new Filtering Group		

Save Reset

2) ボタンを押します。

IGMP Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups
Delete	1	

Add new Filtering Group

Save Reset

新しいエントリが追加されます。

## 17. MLD スヌーピング

本章ではMLDプロトコルの設定について説明します。

なお、使用する MLDv1 コントロールパケットは、リスナークエリ、リスナーレポート、及びリスナードーンメッセージを含んでいます。(これは IGMPv2 クエリ、レポート、リーブメッセージと同等です)

### 17.1. MLD スヌーピングのヒント

マルチキャストルーティングが他のスイッチでサポートされていない場合、MLD スヌーピングと MLD クエリを使って、MLD サービスリクエストがマルチキャストサーバとクライアントの間で渡されているかどうかをモニターすることができます。

インターネット全域に IP マルチキャストをサポートするため、マルチキャストルータはPIMv6 のようなマルチキャストルーティングプロトコルと一緒に、MLD スヌーピングと MLD クエリレポートの情報を uses。

#### 17.1.1. MLD スヌーピングのパラメータ (グローバルとポート単位)

- 1) **Snooping Enabled:** チェックボックスをオンにすると、スイッチはネットワークのトラフィックを監視して、どのホストがマルチキャストの受信を要求しているかを決定します。

このスイッチは、IP マルチキャストグループメンバーを判別するために、IP マルチキャストルータ・スイッチと IP マルチキャストホストグループの間で転送される、MLD リスナークエリと MLD レポートパケットの受動的なスヌープができます。

➤ デフォルト: チェックなし(Disabled)

- 2) **Unregistered IPMCv6 Flooding Enabled:** チェックボックスをオンにすると、登録されていないマルチキャストストリームを VLAN に流します。

ただし、MLD スヌーピングに使われる、マルチキャストエントリを格納するテーブルが一旦満杯になれば、新しいエントリは学習されません。

VLAN にルータのないポートが設定されて、未登録のIPMCv6の流れが禁止されると、後に発生したマルチキャストトラフィックがテーブルに見つからない場合、いずれもドロップされます。これ以外の場合、未登録のマルチキャストのトラフィックは VLAN に溢れます。

➤ デフォルト: チェックあり (Enabled)

- 3) **Leave Proxy Enabled:** チェックボックスをオンにすると、リーブメッセージを、グループ最後のメンバーポートから受け取るまで廃棄します。MLD リーププロキシは、最後の動的なメンバーポートがマルチキャストグループを抜ける時だけ、クエリアでないスイッチが MLD リーブメッセージを転送できるよう全ての不要な MLD リーブメッセージを削除します。

➤ デフォルト: チェックなし (Disabled)

**注意:** このリーブプロキシ機能は、スイッチがクエリアに設定されている場合は動作しません。

(次ページに続く)

(前ページの続き)

スイッチが以下の条件を満たす場合、スイッチはグループ指定 (GS) クエリを生成して、リーブメッセージを受け取ったメンバーポートに送ります。

その後、ポートのラストメンバークエリタイマーを動作させます。

- i) クエリアでない。
- ii) 受信ポートがマルチキャストグループの最後の動的メンバーポートではない。
- iii) 受信ポートがルータポートではない。

- 4) **Proxy Enabled:** チェックボックスをオンにすると、標準 MLD インタフェースを通して見つかったホストの代わりに、MLD ホストレポートメッセージを出力します。

MLD プロキシが Enabled の場合、スイッチはその上流インタフェースにあるルータと MLD メッセージを交換します。

上流インタフェースは、以下の MLD 作業のホスト部分を実行します。

- i) 問合せがあると、マルチキャストリスナーレポートをグループに送る。
- ii) 他のホストが参加していないマルチキャストグループにホストがジョインしたとき、Unsolicited Multicast Listener Report をグループに送る。
- iii) あるマルチキャストグループから最後に抜けるホストは、MLD v1 の Unsolicited Multicast Listener Done Report をマルチキャストアドレスに送る (全てのルータ用アドレス FF02::2)
- デフォルト: チェックなし (Disabled)

- 5) **Port:** ポート番号です。

- 6) **Router Port:** スwitchのポートを、レイヤ3マルチキャストデバイスまたは MLD クエリアへと繋がるルータポートに設定します。もし MLD スヌーピングが MLD クエリアを見つけられない場合、既知の MLD クエリアに接続している指定ポートをユーザーが設定することも可能です。

このインタフェースはその後、マルチキャストトラフィックが全ての適切なインタフェースを通過することを確実にするため、接続されたルータとスイッチに

よってサポートされた全ての現行のマルチキャストグループに参加します。

- デフォルト: チェックなし (Disabled)

(次ページに続く)



(前ページの続き)

- 7) **Fast Leave:** 高速リーブを使用すると、MLD ホストによる頻繁な参加とリーブリクエストを伴うネットワーク帯域の利用を改善できます。
- ポートがリーブメッセージを受信すると、マルチキャストサービスのメンバーポートを即座に削除します。
- 従ってスイッチは、ポートをマルチキャストのテーブルエントリから削除するために、そのインタフェースにグループ指定 (GS) クエリを送信しなくてもよいことになります。
- 高速リーブは、ただ一つの MLD 可能デバイス(サービスホストあるいは隣の MLD スヌーピングが動作しているデバイス)に繋がったインタフェースにのみ指定が可能です。
- ただし、マルチキャストルータが接続されたスイッチが学習したポートには適用できません。
- デフォルト: チェックなし (Disabled)
- 8) **Throttling:** ポートが同時に参加できるマルチキャストグループの数を制限します。参加グループ数が設定値に達すると、どの新しい MLD リスナーレポートもドロップされます。
- 設定値の範囲: Unlimited、1-10
  - デフォルト値: Unlimited

#### MLDスヌーピングの設定手順

- 1) メニューから「Configuration」→「IPMC」→「MLD Snooping」→「Basic Configuration」の順にクリックします。
- 2) MLD の設定を行います
- 3) 「Save」ボタンをクリックして設定を保存します。

MLD Snooping Configuration

**Global Configuration**

Snooping Enabled ☐

Unregistered IPMCv6 Flooding Enabled ☒

Leave Proxy Enabled ☐

Proxy Enabled ☐

**Port Related Configuration**

Port	Router Port	Fast Leave	Throttling
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Save Reset

## 17.2. MLD スヌーピングとクエリの VLAN 設定

本章ではMLDスヌーピングと、VLANインタフェースへのクエリの設定方法を説明します。

### 17.2.1. MLD スヌーピングとクエリの VLAN 設定のパラメータ

#### 1) VLAN ID: VLAN 番号

- 2) **Snooping Enabled:** チェックボックスをオンにすると、このスイッチ全体に対する(グローバルな)MLD スヌーピングが可能になります。

➤ デフォルト: チェックなし (Disabled)

**注意:** これとは別に、各インタフェースにも MLD スヌーピングの設定項目がありますが、こちらの項目にチェックを入れる (Enabled) にするまで各 VLAN インタフェースの MLD スヌーピングは動作しません。

一旦チェックボックスにチェックを入れて、Saveを行ってください。

- 3) **MLD Querier:** チェックボックスをオンにすると、VLAN 内にマルチキャストルータが存在しないか、あるいは他のスイッチやルータと競合した場合に、当該スイッチが MLD v2 のクエリアとして選ばれる場合があります。

クエリアとして選ばれると、どのホストがマルチキャストを受けたがっているかを確認するメッセージを定期的送信するようになります。

➤ デフォルト: チェックなし (Disabled)

- 4) **RV:** MLD クエリの回数に対して MLD レポートの応答が不足する場合、不足を許容できる数を指定します。この機能は、クエリに対してレポートの応答がある程度なければ、視聴者がいないポートと看做してマルチキャスト

サービスから削除するためのものです。

➤ 設定値の範囲: 1-255

➤ デフォルト値: 2

**参考:** クエリアのロバストネス変数が0の場合、そのクエリアのロバストネス変数 (QRV) にはここで設定された値が代入されます。

クエリアが持つ QRV が、その最大値7を超えると、QRV は0にセットされ、続いてそのデバイスは如何なるクエリメッセージに対しても、QRVを送信しないことを意味します。

- 5) **QI:** クエリアとして動作する場合に、一般クエリを送り出す間隔です。

➤ 設定値の範囲: 1-255

➤ デフォルト値: 25 (秒)

**注意:** 項2) にチェックを入れないと、入力できません。

(次ページに続く)

(前ページの続き)

- 6) **QRI:** クエリレスポンスインターバルは、通知した一般クエリに対する最大応答待ち時間です。このスイッチがクエリアとして動作する場合に使用されます。また、この設定値はクエリアによる一般クエリに対するレスポンスの待ち時間として、周囲の機器に通知されます。

- 設定値の範囲: 10-31744 (単位は1/10秒)
- デフォルト値: 100 (10秒)

**注意:** 項2) にチェックを入れないと、入力できません。

- 7) **LLQI:** (Last Listener Query Interval) マルチキャストアドレス指定クエリとマルチキャストアドレス・ソース指定クエリに対するレスポンスの最大待ち時間です。

ホストがグループを抜けるとき、MLD リープメッセージを送りますが、スイッチがこのメッセージを受け取ると、このホストが MLD グループ指定メッセージあるいはグループとソース指定クエリメッセージを送ることによってグループを抜けた最後かどうかをチェックし、タイマーをスタートさせます。もしタイマーが破棄される前にレポートを受けとらなかったら、グループレコードは削除され、レポートが上流のマルチキャストルータに送られます。

この属性は MLD スヌーピングプロキシレポーティングが有効でないと、効果がありません。

- 設定値の範囲: 1-31744 (1/10秒単位)
- デフォルト値: 10 (1秒)

- 8) **URI:** レポートの抑制とプロキシレポーティングが有効 (Enabled) の場合、このオプションによって、アンソリサイテッド MLD レポートを上流のインタフェースへ送る頻度を指定します。

### MLDスヌーピングの設定手順

- 1) メニューから「Configuration」→「IPMC」→「MLD Snooping」→「VLAN Configuration」の順にクリックします。
- 2) 必要な MLD の設定を行います。
- 3) 「Save」ボタンをクリックして設定を保存します。

MLD Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

VLAN ID	Snooping Enabled	MLD Querier	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input type="checkbox"/>	<input type="checkbox"/>	-	-	-	-	-

Save Reset

Refresh << >>

### 17.3. MLD フィルタリングのパラメータ

MLDスヌーピングポートグループフィルタリングでは、マルチキャストストリームをポート毎に制限することができます。例えば、IP/TV サービスなどのサービスを、指定のポート毎にフィルタリングすることができます。

- 1) **Port:** ポート番号です。
- 2) **Filtering Groups:** ポートを通させたくないマルチキャストグループを指定します。  
フィルタグループが定義されたとき、これらのグループに対してチェックがなされたポートで MLD リスナーレポートを受け取ります。

#### MLDフィルタリング設定手順

- 1) メニューから、「Configuration」→「IPMC」→「MLD Snooping」→「Port Group Filtering」を順にクリックします。
- 2) 「Add New Filtering Group」をクリックして、新しいフィルタのエントリを追加します。
- 3) フィルタリングを適用したいポート番号をクリックします。
- 4) フィルタリングを適用したいマルチキャストサービスの IP アドレスを入力します。
- 5) 「Save」ボタンをクリックして、設定を保存します。

MLD Snooping VLAN Configuration Refresh << >>

Start from VLAN  with  entries per page.

VLAN ID	Snooping Enabled	MLD Querier	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input type="checkbox"/>	<input type="checkbox"/>	-	-	-	-	-

Save Reset

MLD Snooping Port Group Filtering Configuration

Delete	Port	Filtering Groups
<span>Delete</span>	1 <input type="button" value="v"/>	<input type="text"/>

Add new Filtering Group

Save Reset

## 18. リンクレイヤ ディスカバリ プロトコル (LLDP)

本スイッチは、機器の管理情報を配信する LLDP(802.1AB-2005) 及び LLDP-MED をサポートしています。LLDP をサポートした各ネットワーク機器の管理情報をマルチキャストすることで、これら情報の取得が自動化できるため、管理効率の向上が期待できます。

基本的な管理情報には、TLV (Type Length Value) と呼ばれるフォーマットが用いられ、装置の LAN と VLAN についての情報が含まれています。さらに LLDP-MED では、より詳しい管理情報を含めることができます。

なお、LLDP は、発見した近隣のネットワークノードから収集した情報の保存や維持についても定義しています。

### 18.1. LLDP タイミングと TLV

本章では、LLDPを配信する時間の属性と、配信される情報の設定について説明します。

#### 18.1.1. LLDP のパラメータ

- 1) **Tx Interval:** LLDP の送信間隔(秒)を設定します。

- 設定値の範囲: 5-32758 (単位: 秒)
- デフォルト値: 30 (30秒はIEEE 802.1ABの推奨値)

ただし、Tx Interval の値は次のルールに沿う必要があります。

$$\begin{aligned} \text{Tx Interval} &\geq (4 \times \text{Tx Delay}) \\ \text{Tx Interval} \times \text{Tx Hold} &\leq 65536 \end{aligned}$$

- 2) **Tx Hold:** 送信保持係数 (time-to-live): 送信 LLDP エージェントが定期的に情報を更新できない場合に、受信 LLDP エージェントが情報を保持すべき時間の係数を指定します。

- 設定値の範囲: 2-10 (注: Tx Hold は秒ではなく係数です。)
- デフォルト値: 3

ただし、Tx Hold の値は次のルールに沿う必要があります。

$$\text{Tx Interval} \times \text{Tx Hold} \leq 65536$$

**参考:** このルールにより、デフォルトTTLの時間 は、Tx Interval: 30 × Tx Delay: 3 = 90 (秒) となります。

- 3) **Tx Delay:** 本スイッチの LLDP ローカルシステム MIB の値やステータスが短時間のうちに頻繁に変化する場合、LLDP の送信を一時的に遅延させる時間を指定します。この機能により、不要な送信を低減できます。

- 設定値の範囲: 1-8192 (単位: 秒)
- デフォルト値: 2

ただし、Tx Delay の値は次のルールに沿う必要があります。

$$4 \times \text{Tx Delay} \leq \text{Tx Interval}$$

(次ページに続く)

(前ページの続き)

- 4) **Tx Reinit:** LLDP ポートが禁止されるか、リンクダウンした後に行われる遅延時間を指定します。

なお、ポートの初期化はこの遅延時間の後に試みられます。

- 設定値の範囲: 1-10 (単位: 秒)
- デフォルト値: 2

**注:** あるポートが初期化されると、そのポートに関連した全ての LLDP リモートシステムMIB が削除されます。

- 5) **Port:** ポート番号に対応します。

- 6) **Mode:** LLDP の送信と、LLDPDU の受信モードを許可します

- 設定値の範囲: Disable、Enabled※、Rx only、Tx only
- デフォルト値: Enabled

※ Enabled は Tx と Rx の両方を含みます。

- 7) **CDP Aware:** チェックボックスをオンにすると、LLDP テーブルの項目に変換できる CDP TLV はデコードされますが、他は全て廃棄されます。

なお、LLDP に変換される CDP TLV については以下の通りです。

CDP TLV (変換前)	LLDP (変換後)
Device ID	Chassis ID
Address	Management Address ※1
Port ID	Port ID
Version and Platform	System Description
System capabilities	System capabilities ※2

※1. CDPは複数のアドレスを含む場合がありますが、先頭の1つだけがLLDPのテーブルに現れます。

※2. 名前は同じでも内容が異なります。CDPの"capability"は、LLDPの"others"に配置されます。

全てのポートで CDP awareness を禁止すると、スイッチは近隣のデバイスから受け取った CDP のフレームを転送します。少なくとも1つのポートで CDP awareness が許可されていれば、全ての CDP フレームはスイッチにおいて終端されます。

ポートの CDP awareness が禁止されている場合、CDP 情報はすぐに削除されません。情報の保持時間が過ぎてから削除されます。

- デフォルト: チェックなし。

(次ページに続く)

(前ページの続き)

- 8) **Port Descr:** チェックボックスをオンにすると、当スイッチのメーカー名、製品名、ハードウェアとソフトウェアインタフェースのバージョンが配信されます。この名前は RFC 2863 にある ifDescr から取られています。
  - デフォルト: チェックあり。
- 9) **Sys Name:** チェックボックスをオンにすると、ドメイン名が配信されます。この名前は、RFC 3418 の sysName から取られています。
  - デフォルト: チェックあり。
- 10) **Sys Descr:** チェックボックスをオンにすると、装置のフルネーム、ハードウェア、OS、ネットワークソフトウェアのバージョンが配信されます。この名前は、RFC 3418 の sysName から取られています。
  - デフォルト: チェックあり。
- 11) **Sys Capa:** チェックボックスをオンにすると、装置の主要な機能(ネットワーク機器の区分)を配信します。主要な機能が設定により停止されていても配信内容には影響がありません。この詳細は IEEE 802.1AB に記述されています。
  - デフォルト: チェックあり。
- 12) **Mgmt Addr:** 管理アドレスプロトコルパケットは、スイッチ自身の IPv4 アドレスを含みます。管理アドレスが一つも利用できない場合、アドレスは CPU か、配信するポートの MAC アドレスになります。
 

管理アドレス TLV は、このアドレスに関する特定のインタフェース、ハードウェアコンポーネントの種類を示すオブジェクト識別子、またはこのアドレスに関連したプロトコルの実体の情報を含みます。

インタフェース或いはエンティティ MIB のような、"enterprise specific" あるいは他の検索の開始点を示すことにより、ネットワーク探索における SNMP アプリケーションを補助するために、インタフェースの番号と OID が含まれています。

Layer 3 装置と関連する異なるアドレスは幾つも存在するので、個々の LLDP PDU は複数の管理アドレス TLV を含む場合があります。

  - デフォルト: チェックあり。

## LLDPの設定手順

- 1) メニューから「Configuration」→「LLDP」の順にクリックします。
- 2) Tx Interval 以下、タイミングのパラメータを変更します。
- 3) LLDP の送受信のモードを設定します。
- 4) CDP フレームのデコード動作を許可あるいは拒否します。
- 5) 「Optional TLV」以下の項目で、TLV に含める情報をチェックボックスで指定します。
- 6) 「Save」ボタンをクリックして設定を保存します。

LLDP Configuration

LLDP Parameters

Tx Interval: 30 seconds

Tx Hold: 3 times

Tx Delay: 2 seconds

Tx Reinit: 2 seconds

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Reset

## 18.2. LLDP-MED TLV の設定

この章では、LLDP-MEDの設定について説明します。LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery) は、VoIP 電話あるいはスイッチなどの設定を自動化するために、LLDP を拡張した規格です。

### 18.2.1. LLDP-MED のパラメータ

- 1) **Fast Start Repeat Count:** VoIP 機器など特定の機器に対して、設定情報等の送信を繰り返す回数を指定します。

VoIP 機器や緊急通報位置通知機能のある機器のように、素早い起動が必要な機器に対して設定情報などを送った場合、マルチキャストである LLDP-MED には、相手が確実に情報を受け取ったかどうかを確認する手段がありません。

そのため、特定の相手にユーザーデータを繰り返し送ることで、送信の成功率を高めようとしたのがこの機能です。

推奨値は4(回)で、この場合、1秒間隔で4つのLLDPUDが送信されます。

(次ページに続く)



(前ページの続き)

- 2) **Latitude:** 本スイッチが設置される場所の緯度を設定します。0-90 度に正規化された最大 4 桁の数値を設定します。
- 3) **Longitude:** 本スイッチが設置される場所の経度を設定します。0-180 度に正規化された最大 4 桁の数値を設定します。方向は、グリニッジ子午線から東向きあるいは西向きのいずれも指定できます。
- 4) **Altitude:** 本スイッチが設置される場所の高度を入力します。高度の単位は、階数(Floors)あるいはメートル(Meters) の 2 種類から選択します。  
建物等において地面からの正確な高度が判らないときは、階数の入力便利です。
  - 設定値の範囲: -32767-32767 (小数点以下は4桁まで使用可能)
  - 入力例:
    - 地面から10.0001mにある場合の入力例: 10.0001 [Meters]
    - 地面から10階にある場合の入力例: 10 [Floors]
    - 地下 -32766.9999mにある場合の入力例: -32766.9999 [Meters]
- 5) **Map Datum:** 上記の位置情報がどの測地系に準拠しているかを指定します。

- i) **WGS84** (世界測地系) – GPS に使われています。日本で GPS の値を使っている場合は、GPS の地域の設定に注意が必要です。  
(Map Datumの項を参照)
- ii) **NAD83/NAVD88** - アメリカで使われている現行の測地系です。
- iii) **NAD83/MLLW** - アメリカで使われている測地系のうち、垂直方向を平均既往最低潮位 (Mean Lower Low Water) を使って定義したものです。湖沼や河川、海上で使います。

なお、日本では 2002 年 4 月以降、世界測地系 (GRS80 及び ITRF94) を採用していますが、LLDP-MED には世界測地系の選択肢はありません。

GPS の出力を使って設定する場合は、GPS の設定を WGS84 にして測定し、次いでこれらの項目を WGS84 に設定してください。

これらの詳細につきましては、国土地理院のサイト、「GPS で地形図上の位置を確認するときの注意」のページをご覧ください。

( [http://www.gsi.go.jp/WNEW/LATEST/gpsmap-GPS\\_and\\_MAPs.htm](http://www.gsi.go.jp/WNEW/LATEST/gpsmap-GPS_and_MAPs.htm) )

(次ページに続く)

(前ページの続き)

6) **Civic Address Location:** 本スイッチの場所等の情報を記入します。これは RFC 4776 で定義されている位置情報 (Location Configuration Information: LCI) フォーマットを利用したものです。全ての項目を入力する必要はありません。  
詳細は本書の付録 2「位置情報 (Location Configuration Information: LCI) フォーマットの内容」をご覧ください。

7) **Emergency Call Service:** 緊急電話として使われる場合は、ELIN (Emergency Location Identification Number) の識別番号を登録します。これは電話番号ではありません。

8) **Policies:** VLAN に関する問題、特に VoIP やビデオサービスなどリアルタイム通信が用いられるトラフィックを監視し、診断するポリシーを設定します。  
なお、配信されるネットワークポリシーの属性は次の通りです。

- Layer 2 VLAN ID (IEEE 802.1Q-2003)
- Layer 2 priority value (IEEE 802.1D-2004)
- Layer 3 Differentiated services code point (DSCP) 値 (IEEE 802.1D-2004) ※

※ このネットワークポリシーは IP ヘッダーによって配信され、与えられたポートにおけるアプリケーションタイプの複数のセットに関係しています。

9) **Policy ID:** ポリシーの ID は「Add New Policies」のボタンを押すと自動的に生成されます。ここで作成したポリシーは、Policy Port Configuration の項目でポートに割り当てます。

(次ページに続く)

(前ページの続き)

10) Application Type: ここでいうアプリケーションタイプとは、次のものを指します。

アプリケーションタイプ	説明
音声	双方向の音声サービスをサポートするIP電話機と、それに類似した機器のために使われます。
音声伝送 (条件付き)	音声メディアのためというよりも、むしろ音声伝送のために異なるポリシーを要求するネットワーク網において使用します。
ゲスト音声	ゲストユーザーやビジターが所有するIPテレフォニー送受話器や他の同様の電気製品に、分離された‘制限付き機能セット’の音声サービスを提供する場合に使用します。
ゲスト音声伝送 (条件付き)	この項目はゲスト音声メディアよりも、ゲスト音声信号伝送のために別のポリシーを要求するネットワーク網で使用します。 もし、同様のネットワークポリシーを、ゲストボイスのアプリケーションポリシー内で配信されたそれらに適用するならば、このアプリケーションタイプは配信されるべきではありません。
ソフトフォン音声	PCのようにデータ処理中心の機器でソフトフォンアプリケーションを使う場合に選択します。このクラスの端末は多重VLANをサポートしていない場合があるので、タグ無し VLAN を指定するか、あるいは一つのVLANにだけ参加してタグ付きVLAN とします。 ネットワークポリシーがタグ無し VLAN を用いるよう定義された場合、L2の優先度の項目は無視されて、DSCPの値が妥当性を持ちます。
ビデオ会議	ビデオ会議専用機器か、あるいは、リアルタイムの双方向ビデオ・音声サービスをサポートする同様の機器に使われています。
ストリーミングビデオ	ブロードキャスト又はマルチキャストによるビデオ配信や、似たようなビデオ配信サービスをサポートするアプリケーションが、特定のネットワークポリシーによる扱いを要求する場合に選択します。 ただし、バッファリングされたTCPによるビデオアプリケーションでの使用は意図されていません。
ビデオ伝送(条件付き)	ビデオメディアよりもビデオ伝送に別のポリシーを要求するネットワーク網で使用します。

注意: 本表は、ANSI/TIA-1057 のApplication Type を意訳・引用

11) Tag: VLAN の使用状況に合わせて設定します。”untagged” を選択すると、VLAN ID とレイヤー2の優先度の項目が無視されて、DSCP の値のみが有効になります。

逆に“tagged”を選択された場合に、VLAN ID とレイヤー2の優先度の項目が同時に使用されると、DSCP の値と同様に、有効となります。

12) **VLAN ID:** ポートに与える VLAN ID です。

➤ 設定値の範囲: 1-4095

13) **L2 Priority:** L2 優先度はアプリケーションタイプの指定に使います。L2 優先度は 8 段階で与えます。ちなみに 0 は IEEE 802.1D-2004 においてデフォルト値の使用と定義されています。

➤ 設定値の範囲: 0-7

14) **DSCP:** DSCP 値は、Diffserv ノードの動作に、RFC 2474 で定義されたアプリケーションタイプを与えるために用います。

なお、0 は、RFC 2474 で定義されたデフォルトの DSCP 値を使用することを意味します。

➤ 設定値の範囲: 0-63

15) **Policy Port Configuration:** 全てのポートは、ユーザーID の認証あるいはポートの設定を元に、固有のネットワークポリシーのセット、あるいは異なる属性を持つ同じネットワークポリシーを配信します。

この設定には次の 2 つのパラメータがあります。

i) **Port** – ポリシーを適用させたいポートの番号です。

ii) **Policy ID** – [Add New Policy] で追加したポリシーの番号です。

## LLDP-MED プロトコル設定手順

- 1) メニューから「Configuration」→「LLDP-MED」の順にクリックします。
- 2) 各タイミングのパラメータを設定します。
- 3) Fast Start Repeat Count、Coordinates Location、Civic Address Location、Emergency Call Service を設定します。
- 4) 「Add new policy」ボタンを押して、適用したいポリシーを定義します。ポリシーの番号は自動的に採番されます。
- 5) 「Save」ボタンをクリックして、設定を保存します。

LLDPMED Configuration

Fast Start Repeat Count

Fast start repeat count

Coordinates Location

Latitude  degrees North Longitude  degrees East Altitude  Meters Map Datum WGS84

Civic Address Location

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

Emergency Call Service

Emergency Call Service

Policies

Policy Port Configuration

項 4)で、ポリシーを新たに作成すると、ここに表示されます。

(次ページに続く)

## (前ページの続き)

- 6) ポリシーを 1 つ以上定義し、「Save」ボタンを押すと、Policy Port Configuration の表が表示されます。
- 7) ポートとポリシーのチェックボックスが表示されていますので、ポートに適用したいポリシーにチェックを入れます。
- 8) 「Save」ボタンをクリックして設定を保存します。

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
<input type="checkbox"/>	0	Voice	Tagged	1	0	0
<input type="checkbox"/>	1	Voice	Tagged	1	0	0
<input type="checkbox"/>	2	Voice	Tagged	1	0	0
<input type="checkbox"/>	3	Voice	Tagged	1	0	0
<input type="checkbox"/>	4	Voice	Tagged	1	0	0
<input type="checkbox"/>	5	Voice	Tagged	1	0	0
<input type="checkbox"/>	6	Voice	Tagged	1	0	0
<input type="checkbox"/>	7	Voice	Tagged	1	0	0
<input type="checkbox"/>	8	Voice	Tagged	1	0	0
<input type="checkbox"/>	9	Voice	Tagged	1	0	0

Add new policy

Policy Port Configuration

Port	Policy ID									
	0	1	2	3	4	5	6	7	8	9
1	<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"/>
2	<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"/>
3	<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"/>
4	<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"/>
5	<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"/>
6	<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"/>
7	<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"/>
8	<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"/>
9	<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"/>
10	<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"/>

Save Reset

## 19. Power over Ethernet (SMCGSxxP のみ対応)

**注意：**本章は、SMCGSxxP-Smartシリーズが対象です。

本スイッチのうちPoEを搭載した製品は、IEEE 802.3af、IEEE 802.3at-2009 PoE Plus をサポートしています。

本章では、PoEに関連した以下の項目について説明します。

- 1) ポート毎の最大供給可能電力。
- 2) スイッチ全体の最大供給可能電力。
- 3) 電力割り当ての優先順位

**注意2：**受電機器の電力要求に対して、スイッチが供給する電力が不足した場合、スイッチは各ポートの優先順位設定に従って供給電力を制限します。

### 19.1. PoE 優先順位のヒント

ポートには4段階の優先順位を設定できます。優先度の高いほうから、Critical、high、medium、low(最優先、高、中、低)となります。PoEをスイッチの最大供給可能電力の範囲で制御するためには、最優先から中までに設定したいポートのPoE Modeを ”PoE+” あるいは ”PoE” にしておき、残りのポートを ”Disabled” に設定します。

優先度の低いポートには電力を供給しないようにすれば、スイッチの起動時に優先度の高いポートに電力を回すことができることになります。

## 19.2. PoE のパラメータ

- 1) **Reserved Power determined by:** スイッチが確保すべき供給電力を、何によって決定するかを指定します。これらは以下の項目で構成されています。

- i) **Class:** 各ポートに接続されている受電機器 (PD) のクラスを判別して、電力の供給量を決定します。  
ポートのクラスは4段階の 4、7、15.4 及び 34.2 ワットに分けられています。このモードを選択すると、“Maximum Power” の設定内容は無視されます。
- ii) **Allocation:** 各ポートの“Maximum Power”の項目に入力した電力の合計です。
- iii) **LLDP-MED:** LLDPによって配信されたPoEの情報から、確保すべき電力を決定します。このモードでは、“Maximum Power” の設定内容は無視されます。なお、LLDPの情報が利用できない場合は、Class モードの動作に準じます。

**注意:** 上記3つのどのモードにおいても、あるポートが供給する電力が、そのポートに指定された最大供給電力を超えた場合は、ポートがシャットダウンされます。

- 2) **Power Management Mode:** ポートをシャットダウンさせるモードを指定します。以下 2 通りの設定があります。

- i) **Actual Consumption:** 全てのポートが実際に供給する電力の合計が、スイッチの PoE の定格を超えた場合、すべてのポートをシャットダウンさせます。  
また、あるポートの供給電力が、そのポートに指定された“Maximum Power” を超えた場合には、そのポートのみをシャットダウンさせます。
- ii) **Reserved Power:** 予約した電力の合計が、スイッチの PoE の定格を超えた場合は、全てのポートがシャットダウンされます。  
このモードでは、受電側装置 (PD) がスイッチの供給可能電力を超える要求をしても、ポートに電力は供給されません。

- 3) **Primary Power Supply:** スイッチに接続された機器が、スイッチの最大供給可能電力を超える要求をした場合、ポートのパワー優先順位設定が電力供給の制御に用いられます。

- 4) **Port:** ポート番号です。

- 5) **PoE Mode:** 次のオプションを含む PoE 操作モードです。

- Disabled – このポートの PoE 動作を禁止します。
- PoE – IEEE 802.3af で動作させます。(クラス 4, 15.4W)
- PoE+ - IEEE 802.3at で動作させます。(クラス 4, 34.2W1)

(次ページに続く)



## (前ページの続き)

- 6) **Priority:** スイッチに接続された装置が、スイッチの能力を超えた電力を要求した場合、優先度の低いポートへの電力供給は、老番のポート番号から若番の順に止めていきます。

➤ 電力供給が停止する動作例: 24→23→22→..... 1

- 7) **Maximum Power:** スイッチに接続された装置へ供給できる電力の最大値を制限します。

➤ 設定値の範囲: 0-34.2 W

**PoE全体の設定とポート個別の設定手順**

- 1) メニューから「Configuration」→「PoE」をクリックします。
- 2) “Reserved Power determination”、“Reserved Power determined”、“Primary Power supply”の、グローバル設定を行います。
- 3) 各ポートにおける設定を行います。
- 4) 「Save」ボタンをクリックして設定を保存します。

Power Over Ethernet Configuration

Reserved Power determined by ☒ Class ☐ Allocation ☐ LLDP-MED

Power Management Mode ☐ Actual Consumption ☒ Reserved Power

Primary Power Supply [W]

Port	PoE Mode	Priority	Maximum Power [W]
1	PoE+ ▼	Low ▼	15.4
2	PoE+ ▼	Low ▼	15.4
3	PoE+ ▼	Low ▼	15.4
4	PoE+ ▼	Low ▼	15.4
5	PoE+ ▼	Low ▼	15.4
6	PoE+ ▼	Low ▼	15.4
7	PoE+ ▼	Low ▼	15.4
8	PoE+ ▼	Low ▼	15.4

Save Reset

## 20. MAC Address Table の設定

MAC Address Table ページではスイッチのMACアドレス学習方法を設定します。動的にMACアドレスを学習させる、特定のポートに静的にアドレスを登録するなどの設定が行えます。

スイッチは接続されたネットワーク機器のMACアドレスを保持します。保持したMACアドレス情報はポート間でフレーム転送に使用されます。データトラフィックをモニタリングすることでスイッチが学習したMACアドレスは動的にアドレステーブルに記録されます。MACアドレスは手動で静的にアドレスを登録することもできます。

### 20.1. MAC Address Table のパラメータ

#### Aging Configuration

- 1) **Disable Automatic Aging:** 動的に学習された MAC アドレスは一定時間を過ぎるとテーブルから消去されます。これを Aging と言います。スイッチは自動で Aging を行いますが Aging を行わないようにするには Disable Automatic Aging にチェックを入れます。
- 2) **Aging Time:** Aging 間隔を設定します。
  - 設定値の範囲: 10-1000000秒
  - デフォルト値: 300秒

#### MAC Table Learning

- 1) **Auto:** 自動的にMACアドレスを学習するように設定します。デフォルトで Auto が選択されています。
- 2) **Disabled:** MAC アドレスを学習せず、MAC アドレステーブルにも記録しません。
- 3) **Secure:** 静的な MAC アドレスエントリのみが学習され、他のフレームは破棄されます。  
ポートを Secure モードに変更する前にスイッチのマネジメントに使用するリンクが Static MAC アドレステーブルに登録されていることを確認してください。登録されていないとスイッチへのアクセスができなくなり、接続ポートを変更してログインすることになります。

**注意:** MAC Learning Tableでポートの表示がグレーで設定ができない状態にある場合は、他のスイッチ機能がポートのMACアドレス学習機能を設定し使用しています。そのためユーザーが変更をすることはできません。

(次ページに続く)

(前ページの続き)

### Static Table Configuration

静的にMACアドレスを登録します。登録できるエントリ数は64です。MACテーブルは最初にVLAN IDで区分し次にMACアドレスで区分します。

- 1) **VLAN ID:** VLAN ID を指定します。

➤ 指定値の範囲: 1-4095

- 2) **MAC Address:** 登録する機器の MAC アドレス。

静的なアドレスはスイッチの任意のポートの MAC アドレステーブルに登録できます。静的なアドレスは登録されたポートに結び付けられ、他のポートで使用することはできません。もし他のポートでそのアドレスを持ったフレームが検知されると、フレームは無視され、アドレステーブルに書き込まれません。

- 3) **Port Member:** Port ID を指定します。

### PoE全体の設定とポート個別の設定手順

- 1) メニューから「Configuration」→「MAC Table」をクリックします。
- 2) Aging Time を必要に応じて変更します。
- 3) MAC アドレスの学習方法を指定します。
- 4) 静的な MAC アドレスの登録が必要な場合は Add new static entry をクリックして新しいエントリをテーブルに追加します。追加時に VLAN ID、MAC アドレス、どのポートに結び付けるかを登録します。
- 5) 「Save」ボタンをクリックして設定を保存します。

**MAC Address Table Configuration**

**Aging Configuration**

Disable Automatic Aging ☐

Aging Time  seconds

**MAC Table Learning**

	Port Members									
	1	2	3	4	5	6	7	8	9	10
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<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"/>
Secure	<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"/>

**Static MAC Table Configuration**

			Port Members									
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10
Add new static entry												

Save Reset

## 21. IEEE802.1Q VLANs の設定

本スイッチではVLAN機能を使用することでLayer 2レベルでブロードキャストドメインを分離し、ブロードキャストトラフィックを減らします。

本スイッチでサポートするVLAN機能の概要を以下に示します。

- IEEE802.1Q で最大 256VLAN をサポートします。
- 明示的、暗示的にタグを使用して複数のスイッチ間で学習した VLAN 情報を配布します。
- Port OverLapping はポートを複数の VLAN に参加させます。
- 接続された端末は複数の VLAN に参加することができます。
- VLAN 機能を持つ機器、持たない機器間で通信することができます。
- Priority Tagging をサポートしています。

### 21.1. VLAN Membership 設定のパラメータ

- 1) **VLAN ID:** VLAN ID を設定します。
  - 設定値の範囲: 1-4095
- 2) **VLAN Name:** VLAN 名を設定します。
  - 設定値の範囲: アルファベット1-32文字
- 3) **Port Members:** このパラメータでは VLANID が行で表示されスイッチのポート毎にチェックボックスが表示されています。この VLAN にポートに参加させる場合は次の様にチェックボックスにチェックを入れます✓。VLAN 参加を禁じたポートには次の様にチェックを入れます✗。VLAN からポートを除外、削除する場合はチェックボックスのチェックを外します。

### IEEE802.1Q VLAN Groupの設定手順

- 1) メニューから「Configuration」→「VLANs」→「VLAN Membership」を順にクリックします。
- 2) 必要に応じてデフォルト VLAN(VLAN 1)の割り当てを変更します。
- 3) 新規に VLAN を作成する場合は Add New VLAN をクリックし VLAN ID を入力し新規に作成した VLAN に割り当てるポートにチェックを入れます。
- 4) 「Save」ボタンをクリックして設定を保存します。

**VLAN Membership Configuration**

Start from VLAN  with  entries per page.

Delete	VLAN ID	VLAN Name	Port Members									
			1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

## 22. ポートへの VLAN 属性の設定

VLAN Port Configuration ページでは特定のインタフェースに VLAN 属性の設定を行うことができます。属性設定ではデフォルト VLAN (PVID) の設定、受信フレームタイプの設定、受信時のフィルタリング、Queue-in-Queue フレーム処理の設定があります。

### 22.1. VLAN Port Configuration 設定パラメータ

- 1) **Ethertype for Custom S-ports:** Port Type が S-Custom-port に設定された場合に、受信されたフレームはここで指定された Ethertype に値を変更します。  
デフォルトで Ethertype は 0x88a8 (IEEE802.1ad) です。
- 2) **Port:** Port ID です。
- 3) **Port Type:** ポートが受信したフレームの VLAN ID に対してどのような処理を行うか設定します。
  - デフォルト値: Unaware
  - **C-port (Customer Port):** 受信したフレームの VLAN ID を確認し処理します。受信したフレームが Untag フレームの場合は、Port VLAN ID で指定した VLAN ID を元に処理を行います。
  - **S-port (Service Port):** 受信したフレームの Ethertype を 0x88a8 に変更しスイッチ内にダブルタグのフレームが転送されることを示します。スイッチは外側タグの VLAN ID に従いフレームを同一 VLAN グループに転送します。スイッチはフレームの Ether Type フィールド以外に変更は行いません。
  - **S-Custom-port (Service Custom Port):** 受信したフレームの Ethertype を Ethertype for S-Custom-port パラメータで指定した値に変更しスイッチ内にダブルタグのフレームが転送されることを示します。スイッチは外側タグの VLAN ID に従いフレームを同一 VLAN グループに転送します。スイッチはフレームの Ether Type フィールド以外に変更は行いません。
  - **Unaware:** 受信したフレームの VLAN ID を意識しません。受信したフレームが Tag フレームの場合でも Port VLAN ID で指定した VLAN ID を元に処理を行います。

4) **Ingress Filtering:** タグフレームを受信したポートがフレームの VLAN グループに属していない場合にどのような処理を行うか設定します。

- デフォルト値: Disabled
- Ingress Filtering はタグフレームに対してのみ処理を行います。
- Ingress Filtering が有効でポートが属していない VLAN グループのフレームを受信すると、フレームは破棄されます。
- Ingress Filtering が無効でポートが属していない VLAN グループのフレームを受信すると、フレームは他のポートへフラッディングされます。
- Ingress Filtering は VLAN に依存しない BPDU フレーム(GVRP や STP のBPDU)に影響しません。VLAN に依存した BPDU フレーム(GMRP)は影響をうけます。

5) **Frame Type:** 受信時に受け付けるフレームのタイプを選択します。

- 設定値の範囲:
  - All: 全てのフレーム(Tagged/Untagged にかかわらず)を受信します。
  - Tagged: Tag フレームのみを受け付けます。
  - Untagged: Untag フレームのみを受け付けます。
- デフォルト値: All

6) **Port VLAN Mode:** フレームの送信時と受信時に VLAN タグをどのように処理するか設定します。

- 設定値の範囲:
  - None: Port VLAN ID を設定しません。
  - Specific: ポート VLAN ID を設定できます。タグ無しフレームが受信されるとポートに設定された VLAN ID を割り当てます。
- デフォルト値: Specific

7) **Port VLAN ID:** ポートで受信したタグ無しフレームに割り当てる VLAN ID を設定します。

- 設定値の範囲: 1-4095
- デフォルト値: 1

8) **Tx Tag:** フレーム送信時に Tag を挿入するかどうかを設定します。

- 設定値の範囲
  - Untag\_pvid: PVID 以外は VLAN フレームにタグが付けられます。PVID と同じ場合はタグ無しフレームで送信します。
  - Tag\_all: タグ付きフレームで送信します。
  - Untag\_all: タグ無しフレームで送信します。
- デフォルト値: Untag\_pvid

### Port VLAN Configurationの設定手順

- 1) メニューから「Configuration」→「VLANs」→「Ports」を順にクリックします。
- 2) ポート毎に必要な設定を行います。
- 3) 「Save」ボタンをクリックして設定を保存します。

Ethertype for Custom S-ports 0x88A8

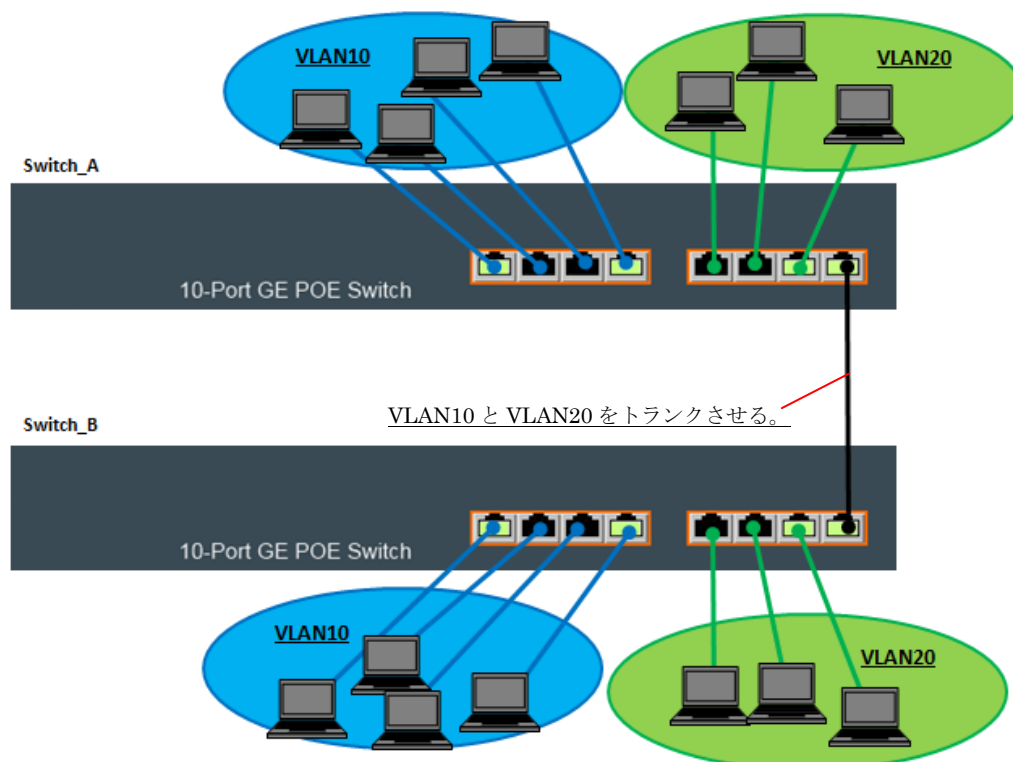
VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
1	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
2	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
3	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
4	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
5	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
6	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
7	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
8	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
9	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid
10	C-port	<input type="checkbox"/>	All	Specific	1	Untag_pvid

Save Reset

## 23. IEEE 802.1Q VLANs 設定例

ここでは次の様なネットワーク構成を例に説明します。



## VLANの作成

- 1) メニューから「Configuration」→「VLANs」→「VLAN Membership」を順にクリックします。
  - 2) VLAN10 と VLAN20 を作成し、VLAN10 に 1～4、8 ポート、VLAN20 に 5～8 ポートを所属させる。
- ※ Port8 はトランクポートなので、透過させる全ての VLAN に所属させる。

			Port Members							
Delete	VLAN ID	VLAN Name	1	2	3	4	5	6	7	8
<input type="checkbox"/>	1	default	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	10	VLAN10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	20	VLAN20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

トランクさせる VLAN が複数ある場合は、  
トランクさせる VLAN 全てにチェックを入れる

## ポートの設定

- 1) メニューから「Configuration」→「VLANs」→「Port」を順にクリックします。
- 2) 下図の様に 1～7 ポートは Untag ポートとし、8 ポートは Tag ポートとして設定します。

受信するフレームタイプの指定      Untag フレームに関連付ける VLAN ID を指定する。      送信時に Tag フレームで送信するか、Untag フレームで送信するか

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
1	C-port	<input type="checkbox"/>	Untagged	Specific	10	Untag_all
2	C-port	<input type="checkbox"/>	Untagged	Specific	10	Untag_all
3	C-port	<input type="checkbox"/>	Untagged	Specific	10	Untag_all
4	C-port	<input type="checkbox"/>	Untagged	Specific	10	Untag_all
5	C-port	<input type="checkbox"/>	Untagged	Specific	20	Untag_all
6	C-port	<input type="checkbox"/>	Untagged	Specific	20	Untag_all
7	C-port	<input type="checkbox"/>	Untagged	Specific	20	Untag_all
8	C-port	<input type="checkbox"/>	Tagged	Specific	1	Tag_all



## 24. PrivateVLANs の設定

Private VLAN(PVLAN)はVLAN内にポートベースのVLANを作成しブロードキャストドメインをさらに分割します。

### 24.1. Private VLAN Membership 設定パラメータ

- 1) **PVLAN ID:** Private VLAN ID を指定。
- 2) **Port Members:** ポート ID を指定。

#### Private VLAN Membershipの設定手順

- 1) メニューから「Configuration」→「Private VLANs」→「PVLAN Membership」を順にクリックします。
- 2) 既存の PVLAN 設定に追加、削除を行い、Add New Private VLAN をクリックしてポートメンバーを選択します。
- 3) 「Save」ボタンをクリックして設定を保存します。

Private VLAN Membership Configuration

		Port Members									
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New Private VLAN

Save Reset

## 25. Port Isolation の設定

Port IsolationページではPort Isolation機能をポート毎に有効、無効に設定します。

同一VLAN、PVLANメンバーを他のIsolatedポートと分離します。

PVLANを設定したポートは異なるPVLANグループと分離されます。Port Isolationは同一PVLAN間ポートでの通信を許可しません。Isolated Port同士はいかなるユニキャスト、マルチキャスト、ブロードキャストトラフィックも同一PVLANに属する他のPVLANポートに転送しません。

### 25.1. 23.1. Private VLAN Membership 設定パラメータ

- 1) **Port Number:** Port ID を指定。

#### Port Isolationの設定手順

- 1) メニューから「Configuration」→「Private VLANs」→「PVLAN Isolation」を順にクリックします。
- 2) 互いに通信を分離するポートを選択しチェックボックスにチェックを入れます。
- 3) 「Save」ボタンをクリックして設定を保存します。

The screenshot shows the 'Port Isolation Configuration' interface. It features a table with 10 columns labeled 'Port Number' from 1 to 10. Below each number is a checkbox. The first checkbox (for Port 1) is currently checked. At the bottom of the table are two buttons: 'Save' and 'Reset'.

Port Number									
1	2	3	4	5	6	7	8	9	10
<input checked="" 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"/>

Save Reset

## 26. MAC-Based VLANs の設定

MAC-based VLANsのページではMACアドレスをもとにVLANを設定します。MAC-based VLAN機能は送信元MACアドレスに従って受信したタグ無しフレームにVLAN IDを割り当てます。

MAC-based VLAN有効時にはフレームの送信元MACアドレスに定義したVLAN IDを割り当て、該当するMACアドレスが無い場合には、タグ無しフレームには受信したポートのPVIDを割り当てます。

### 26.1. MAC-Based VLANs 設定ヒント

- 送信元 MAC アドレスはひとつの VLAN ID にのみ割り当てることができます。
- ブロードキャストアドレス、マルチキャストアドレスは使用できません。
- MAC-based VLAN と Protocol-based VLAN の両方が有効の場合は、優先権は MAC-based VLAN、Protocol-based VALN、Port-based VLAN の順になります。

### 26.2. 24.2 MAC-Based VLAN Membership Configuration 設定パラメータ

- 1) **MAC Address:** 特定の VLAN に割り当てると送信元 MAC アドレス。
- 2) **VLAN ID:** 指定した送信元 MAC アドレスに一致した際に割り当てると VLAN ID。  
➤ 指定値の範囲: 1-4093
- 3) **Port Members:** VLAN に割り当てられたポート。

#### MAC-Based VLANs Membershipの設定手順:

- 1) メニューから「Configuration」→「VCL」→「MAC-based VLAN」を順にクリックします。
- 2) Add new entry をクリックします。
- 3) MAC アドレスパラメータに MAC アドレスを入力します。
- 4) VLAN パラメータに VLAN ID を入力します。
- 5) 作成した VLAN を割り当てるとポートを指定します。
- 6) 「Save」ボタンをクリックして設定を保存します。

MAC-based VLAN Membership Configuration			Port Members																									
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Delete	00-00-00-00-00-00	1	<input checked="" 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="checkbox"/>

## 27. Protocol VLANs の設定

Protocol VLANではプロトコル単位でVLANを割り当てます。

### 27.1. Protocol VLANs 設定ヒント

- Protocol VLAN を設定するには以下のステップで作成してください。
- プロトコル VLAN に使用する VLAN グループを最初に作成します。
- 各プロトコルに対応するプロトコルグループを作成します。
- 各ポートにプロトコルを割り振り、VLAN を割り当てます。
- MAC-based、IP subnet-based と Protocol-based VLAN が同時に使用される場合は、優先度は MAC-based、IP subnet-based、Protocol-based の順になり Port-based は最後になります。

### 27.2. Protocol VLAN Group 設定パラメータ

- 1) **Frame Type:** プロトコルに使用されるフレームタイプを指定します。選択可能フレームタイプは Ethernet、LLC(Logical Link Control)、SNAP(SubNetwork Access Protocol-RFC1042)になります。

- 2) **Value:** 特定プロトコルタイプを定義する値。Frame Type パラメータによって表示されるパラメータが変わります。

Ethernet-EtherType 値

- 指定値の範囲: 0x0600-0xffff
- デフォルト値: 0x0800

LLC-DSAP(Destination Service Access Point)値と SSAP(Source Service Access Point) 値

- 指定値の範囲: 0x00-0xff
- デフォルト値: 0xff

SNAP-OUI(Organizationally Unique Identifier)値と PID(Protocol ID)値

OUI-OUI 値は xx-xx-xx のフォーマットで xx には 16 進数を使用します。

- 指定値の範囲: 0x00-0xff

PID-PID 値は OUI 値が 00-00-00 の場合、PID値は EtherType(0x0600-0xffff)になります。OUI 値が 00-00-00 以外の場合、PID 値は 0x0000-0xffff の範囲内の値になります。

- 指定値の範囲: 0x0000-0xffff

(次ページに続く)

(前ページの続き)

- 3) **Group Name:** Protocol VLAN に割り当てるグループ名。Group Name は一意の名前で、アルファベット a-z または A-Z と整数値 0-9 を使用し最大 16 のキャラクタで作成します。

**注意:** IPプロトコルのEthernetフレームと一致したトラフィックはスイッチの管理IPに設定された VLANグループに割り当てられます(デフォルトではVLAN 1)。IPプロトコルEthernetトラフィックは別のVLANに設定しないでください。スイッチへの管理アクセスができなくなります。もしアクセスができなくなった場合は、Resetボタンを使用してスイッチを工場出荷時の状態に戻します。

#### Protocol to Group Mappingの設定手順

- 1) メニューから「Configuration」→「VCL」→「Protocol-based VLAN」→「Protocol to Group」を順にクリックします。
- 2) Add new entry をクリックします。
- 3) パラメータ、Frame Type、Value、Group Name を入力します。
- 4) 「Save」ボタンをクリックして設定を保存します。

**Protocol to Group Mapping Table**

Delete	Frame Type	Value	Group Name
<input type="button" value="Delete"/>	Ethernet ▼	Etype: 0x 0800	<input type="text"/>

## 28. Protocol Group のポートへの割り当て設定

Group Name to VLAN Mapping Tableを使用してプロトコルグループのVLANをポートに割り当てます。

### 28.1. Group Name to VLAN Mapping Table 設定ヒント

- Protocol-based VLAN を作成するには、Group Name to VLAN Mapping Table でのみをポートをプロトコルグループ別の VLAN に割り当てることができます。他の VLAN 機能でポートをVLANに割り当てると、ポートは全てのプロトコルをポートに割り当てられたVLANとして扱います。
- フレームが Protocol-based VLAN 設定ポートに受信されると、フレームは以下の処理動作で扱われます。
- タグフレームを受信すると、タグフレームに適用された処理動作を優先し扱われます。
- タグ無しでプロトコルタイプが一致したフレームが受信されると、フレームは設定された VLAN グループに転送されます。
- タグ無しでプロトコルタイプが一致しないフレームが受信されると、フレームはポートが所属するデフォルト VLAN に転送されます。

### 28.2. Group Name to VLAN Mapping Table 設定パラメータ

- 1) **Group Name:** Protocol VLAN に割り当てるグループ名。Group Name は一意の名前で、アルファベット a-z または A-Z と整数値 0-9 を使用し最大 16 のキャラクタで作成します。
- 2) **VLAN ID:** プロトコルが一致したトラフィックを転送する VLAN ID。  
➤ 設定値の範囲: 1-4095
- 3) **Port Members:** Protocol VLAN に割り当てられたポート ID。

#### Name Group to VLAN Mapping Tableの設定手順

- 1) メニューから「Configuration」→「VCL」→「Protocol-based VLAN」→「Group to VLAN」を順にクリックします。
- 2) Add new entry をクリックします。
- 3) プロトコルグループ ID を入力します。
- 4) 該当プロトコルを転送する VLAN を入力します。
- 5) プロトコル VLAN を割り当てるポートを選択します。
- 6) 「Save」ボタンをクリックして設定を保存します。

Group Name to VLAN mapping Table Auto-refresh ☐ Refresh

			Port Members																									
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Delete	<input type="text"/>	<input type="text"/>	<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="checkbox"/>
Add New Entry																												
Save Reset																												

### 28.3. Subnet-based VLAN の設定(SMCGS18/26/50 のみ対応)

Subnet-based VLANではサブネット単位でVLANを割り当てます。

### 28.4. Subnet-based VLAN Configuration 設定パラメータ

- 1) **VCE ID:** エントリのインデックスを表示します。
- 2) **IP Address:** サブネットアドレスを入力します。
- 3) **Mask Length:** サブネットマスクの長さを入力します。
- 4) **VLAN ID:** 指定したサブネットアドレスと一致した際に割り当てる VLAN ID を入力します。
- 5) **Port Members:** ポートを選択します。

#### Name Group to VLAN Mapping Tableの設定手順:

- 1) メニューから「Advanced Configuration」→「VCL」→「IP Subnet-based VLAN」を順にクリックします。
- 2) Add new entry をクリックします。
- 3) VCE ID, IP Address, VLAN ID, Port Members を適宜設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

IP Subnet-based VLAN Membership Configuration Auto-refresh ☐

Delete	VCE ID	IP Address	Mask Length	VLAN ID	Port Members																									
					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="button" value="Delete"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="24"/>	<input type="text" value="1"/>	<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"/>		

## 29. VoIP トラフィック管理設定

IPテレフォニーが企業ネットワークに導入される際には、Voice over IP(VoIP)ネットワークのトラフィックを他のデータトラフィックと分離することを推奨します。トラフィックを分けることで過度のパケット遅延、パケットロス、ジッター等を防ぎ音声品質を高くします。

Voice VLANの使用にはいくつかの利点があります。VoIPトラフィックを他のデータと分離することでセキュリティを高めることができます。End-to-EndでQoSポリシーおよび高い優先度をVoIP VLANトラフィックにネットワーク全体で適用ができ、VoIPトラフィックに必要な帯域を割り当てることができます。Voice VLANは音声品質に影響を及ぼすブロードキャスト、マルチキャストトラフィックからVoIPトラフィックを守ります。

本スイッチではネットワーク内にVoice VLANを作製しVoiceトラフィックにサービスプライオリティの設定を行うことが可能です。Voiceトラフィックはポート上でパケットの送信元MACアドレスまたはネットワークに接続されたVoIP機器の発見に使用するLLDP(IEEE802.1ab)で検知することができます。VoIPトラフィックが検知されると、スイッチは自動的にポートをVoice VLANのタググループに割り当てます。

### 29.1. Voice VLAN Configuration の設定

Voice VLANページでVoIPトラフィック用にスイッチ設定を行うことができます。最初にスイッチポートに接続されたVoIP機器を自動的に検出する機能を有効にします。次にネットワークで使用するVoice VLAN IDを設定します。一定期間ポートにVoIPトラフィックが受信されなくなるとポートがVoice VLAN グループからリブする、Voice VLAN aging timeも設定できます。

### 29.2. Voice VLAN Configuration 設定パラメータ

- 1) **Mode:** スイッチで Voice VLAN 機能を有効(Enabled)、無効(Disabled)に設定します。
  - デフォルト値: Disabled
- 2) **VLAN ID:** ネットワーク内の Voice VLAN ID を指定します。スイッチ上では Voice VLAN は 1 つだけサポートされます。
  - 設定値の範囲: 1-4095
  - デフォルト値: 1000
- 3) **Aging Time:** Aging Time を設定すると、Aging Time に設定した期間ポートに VoIP トラフィックが受信されなくなるとポートが Voice VLAN グループからリブします。
  - 設定値の範囲: 10-10,000,000秒
  - デフォルト値: 86,400秒

(次ページに続く)



(前ページの続き)

4) **Traffic Class:** Voice VLAN 上でのトラフィックのサービス優先度を設定します。

- 設定値の範囲: 0-7
- デフォルト値: 7 (High)

#### Port Configuration

1) **Mode:** ポートを Voice VLAN に参加させるか指定します。選択オプションは Disabled、Auto、Forced があります。

- デフォルト値: Disabled
- 設定値の範囲
  - **Disabled:** Voice VLAN 機能がポートで無効になります。ポートは VoIP トラフィックを検知せず、ポートは Voice VLAN に参加しません。
  - **Auto:** ポートは VoIP トラフィックを検知すると、Voice VLAN のタグメンバーとして追加されます。VoIP トラフィックの検知方法を OUI と LLDP(IEEE802.1ab)から選択します。OUI を選択する場合は、Telephony OUI リストに MAC アドレスの範囲を設定します。
  - **Forced:** Voice VLAN 機能がポートで有効になります。

2) **Security:** セキュリティフィルタリング機能を有効にします。セキュリティフィルタリングは VoIP 以外のパケットを受信したときにパケットを破棄します。VoIP トラフィックは Telephony list に設定された送信元 MAC アドレス、またはスイッチに接続された VoIP 機器検知に使用する LLDP で識別されます。

- デフォルト値: Disabled

3) **Discovery Protocol:** ポート上で VoIP トラフィックを検知する方法を設定します。

- デフォルト値: OUI

**OUI:** VoIP機器からのトラフィックは送信元MACアドレスのOUI(Organizationally Unique Identifier)で検知されます。OUIナンバーはMACアドレスの最初の3オクテットは製造メーカーに割り当てられています。MACアドレスのOUIナンバーはテレフォニーOUIリストに設定し、VoIP機器からのトラフィックだと検知ができるようにします。

**LLDP:** スイッチに接続された機器がVoIP機器だとわかるようにLLDPを使用します。LLDPはフレームのシステムケーパビリティのTLV(telephone bit)をチェックします。LLDPポートはVoIPTraフィックを検知すると、Voice VLANのタグメンバーとして追加されます。VoIPTraフィックの検知方法の詳細に関しては “Link Layer Discovery Protocol”を参照してください。

(次ページに続く)

(前ページの続き)

**Both:** OUIテーブルとLLDPがVoIPTraフィックの検知に使用されます。

- ※ Bothはディテクションモードが“Auto”の時にだけ機能します。  
Discovery ProtocolパラターにBoth、LLDPを選択する場合はLLDP機能を有効にする必要があります。Discovery ProtocolパラメータのOUI、LLDPに設定変更を行うと、自動検出プロセスはリスタートします。

#### Voice VLAN Configurationの設定手順:

- 1) メニューから「Configuration」→「Voice VLAN」→「Configuration」を順にクリックします。
- 2) VoIP に関してのスイッチ、ポートの設定を必要に応じて行います。
- 3) 「Save」ボタンをクリックして設定を保存します。

Voice VLAN Configuration

Mode	Disabled
VLAN ID	1000
Aging Time	86400 seconds
Traffic Class	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
1	Disabled	Disabled	OUI
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI

Save Reset

## 30. Telephony OUI の設定

スイッチに接続されたVoIP機器の識別をVoice VLAN OUIテーブルを使って行います。VoIP機器はMACアドレスのOUIを使用して識別されます。OUIナンバーは機器メーカーに割り当てられておりMACアドレスの最初の3オクテットを使用しています。VoIP機器のMAC OUIナンバーはスイッチで設定され、これらの機器からのトラフィックはVoIPTraフィックとして識別されます。

### 30.1. Voice VLAN OUI Table 設定パラメータ

- 1) **Telephony OUI:** VoIPトラフィックと識別されるよう、IEEEにより機器ベンダーに割り振られた一意のIDを入力します。OUIはキャラクタ長が6で、入力する際のフォーマットはxx-xx-xx(xは16進数値)です。
- 2) **Description:** VoIP 機器にユーザーが識別するために使用する説明文を入力します。

#### Voice VLAN OUI Tableの設定手順:

- 1) メニューから「Configuration」→「Voice VLAN」→「OUI」を順にクリックします。
- 2) Add new entry をクリックします。
- 3) VoIP 機器の OUI を入力し、機器の説明を Description に入力します。
- 4) 「Save」ボタンをクリックして設定を保存します。

Voice VLAN OUI Table

Delete	Telephony OUI	Description
<input type="checkbox"/>	00-01-e3	Siemens AG phones
<input type="checkbox"/>	00-03-6b	Cisco phones
<input type="checkbox"/>	00-0f-e2	H3C phones
<input type="checkbox"/>	00-60-b9	Philips and NEC AG phones
<input type="checkbox"/>	00-d0-1e	Pingtel phones
<input type="checkbox"/>	00-e0-75	Polycom phones
<input type="checkbox"/>	00-e0-bb	3Com phones

Add new entry

Save Reset

## 31. Quality of Service の設定

スイッチやルータがパケットを転送時、処理を同等に行うかどうかはパケットのクラス情報に依存しています。クラス情報はエンドの端末、ネットワーク経路にあるスイッチやルータによって割り当てられます。

スイッチやルータはクラスの異なるトラフィックに対してリソース配分を優先付けにクラス情報を使用します。ネットワーク機器毎でのトラフィック処理を “per-hop behavior” と呼び、ネットワーク経路に設置された機器には一致したQoS設定を行い一貫したend-to-endでのQoSサービスにする必要があります。

本章ではデータトラフィック量が増加し、トラフィックがバッファにため込まれた状態でデータパケットが高い優先度を持っているとスイッチがどのように処理するかを説明します。本スイッチはポートごとに4つのプライオリティキューがあります。データパケットは優先度の高いキューに入ると、優先度の低いキューに入ったパケットより先に送信されます。デフォルトの優先度をポート毎、キューイングモード、キューウェイトに設定できます。

### 31.1. Port Classification の設定

QoS Ingress Port Classificationページではポートに対する基本的なQoS情報(デフォルトトラフィッククラス、DP level(IEEE802.1P)、ユーザープライオリティ、ドロップエリジブルインディケーター、タグフレームのクラシフィケーションモード、DSCP-based QoSクラシフィケーション)を設定します。

### 31.2. QoS Ingress Port Classification の設定パラメータ

#### QoS Ingress Port Classification

- 1) **Port:** Port ID を指定します。
- 2) **QoS Class:** デフォルト QoS クラスを制御します。QoS クラスはキューとプライオリティに一対一でマッピングされており、QoS クラス 0 が一番低いプライオリティを持っています。
  - 設定値の範囲: 0-7
  - デフォルト値: 0
- 3) **DP level:** デフォルトのフレーム破棄を制御します。
  - 設定値の範囲: 0-7
  - デフォルト値: 0

(次ページに続く)

(前ページの続き)

- 4) **PCP:** タグ無しフレームのデフォルト Priority Code Point を制御します。
  - 設定値の範囲: 0-7
  - デフォルト値: 0
- 5) **DEI:** デフォルトの Drop Eligible Indicator を制御します。
  - 設定値の範囲: 0-7
  - デフォルト値: 0
- 6) **Tag Class:** ポートでのタグフレームのクラス分けモードを表示します。
  - 設定値の範囲
    - **Disabled:** デフォルトの QoS クラス、DP レベルをタグフレームに使用します。
    - **Enabled:** タグフレームにマッピングされた PCP と DEI を使用します。

モードをクリックしてモードまたはマッピングを設定します。
- 7) **DSCP Based:** ポートで DSCP ベースの QoS Ingress を有効にします。
- 8) **Tag Classification:** ポートでタグフレームのクラス分けモードを有効にします。
  - 設定値の範囲
    - **Disabled:** デフォルトの QoS クラス、DP レベルをタグフレームに使用します。
    - **Enabled:** タグフレームにマッピングされた PCP と DEI を使用します。
  - デフォルト値: Disabled
- 9) **PCP/DEI:** Tag Classification が有効時にクラス分けの設定オプション PCP、DEI に対しての QoS クラス、DP レベルを表示します。
- 10) **QoS Class:** Tag Classification が有効時に PCP と DEI に対しての QoS クラスのマッピングを制御します。
  - 設定値の範囲: 0-7
  - デフォルト値: 0
- 11) **DP level:** Tag Classification が有効時に PCP、DEI に対しての DP レベル値(破棄の優先度)のマッピングを制御します。
  - 設定値の範囲: 0-1
  - デフォルト値: 0

(次ページに続く)

(前ページの続き)

## Port Classificationの設定手順

### ポートの基本QoSパラメータの設定

- 1) メニューから「Configuration」→「QoS」→「Port Classification」を順にクリックします。
- 2) QoS パラメータをポートに設定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
1	0	0	0	0	Disabled	<input type="checkbox"/>
2	0	0	0	0	Disabled	<input type="checkbox"/>
3	0	0	0	0	Disabled	<input type="checkbox"/>
4	0	0	0	0	Disabled	<input type="checkbox"/>
5	0	0	0	0	Disabled	<input type="checkbox"/>
6	0	0	0	0	Disabled	<input type="checkbox"/>
7	0	0	0	0	Disabled	<input type="checkbox"/>
8	0	0	0	0	Disabled	<input type="checkbox"/>
9	0	0	0	0	Disabled	<input type="checkbox"/>
10	0	0	0	0	Disabled	<input type="checkbox"/>

Save Reset

### タグフレームのTag Classificationパラメータの設定

- 1) メニューから「Configuration」→「QoS」→「Port Classification」を順にクリックします。
- 2) Tag Classification パラメータに表示されている値をクリックします。
- 3) Tag フレームにデフォルトの QoS クラスと DP レベルを使用できるように Tag Classification モードを Disabled にセットします。もしくはタグフレームにマップされた PCP と DEI 使用できるように Tag Classification を Enabled に設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

QoS Ingress Port Tag Classification Port 1

Tagged Frames Settings

Tag Classification Disabled

(PCP, DEI) to (QoS class, DP level) Mapping

PCP	DEI	QoS class	DP level
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Save Reset Cancel

## 32. Ingress Port Policers の設定

Port Policingでは受信したトラフィックに関してポリシングを行うか否かの設定を行います。

### 32.1. QoS Ingress Port Policers の設定パラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **Enabled:** 受信したトラフィックに対してポリシングを行うか否かを選択します。
- 3) **Rate:** 帯域上限を設定します。
  - 設定値の範囲: 100-1,000,000kbps/fps、1-3,300Mbps/kfps
  - デフォルト値: 500kbps
- 4) **Unit:** 単位を設定します。
  - 設定値の範囲: kbps/Mbps/fps/kfps
  - デフォルト値: kbps
- 5) **Flow Control:** フローコントロールの有効/無効を設定します。

#### QoS Ingress Port Policersパラメータの設定

- 1) メニューから「Configuration」→「QoS」→「Port Policing」を順にクリックします。
- 2) 有効にしたいポートで Enable にチェックを入れ、Rate, Unit, Flow Control を適宜設定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

Port	Enabled	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<>	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

## 33. Egress Port Scheduler の設定

Egress Port Scheduler ページではキューや、ウェイトといったQoS送信ポートのスケジューリングを表示します。Port パラメータをクリックし、Egress キューや、キューモード、キューシェーパー(データレートや帯域制限超過時のアクセス)、ポートシェーパーを設定します。

### 33.1. Egress Port Scheduler の設定パラメータ

#### QoS Egress Port Scheduler の表示

- 1) **Port:** Port ID を指定します。
- 2) **Mode:** ポートのスケジューリングモードを表示します。
- 3) **Weight:** ポートで使用する egress キューのウェイトを表示します。

#### QoS Egress Port Scheduler、Queue Scheduler、Port Shapers の設定

- 1) **Scheduler Mode:** 優先度の低いキューがサービスを受ける前に優先度の高いキューのトラフィックを処理する厳密なルールなキューサービスをスイッチに設定するか、キューごとに重みづけ処理を指定する、Deficit Weighted Round-Robin(DWRR)を設定します。
  - 設定値の範囲: Strict、Weighted
  - デフォルト値: Strict

DWRR サービスはWRRに似たサービスですが、キューのDeficit Counterが送信されるパケットのサイズより小さい時のみ、次のキューがサービスをうけます。

注: Weighted Schedulingはキュー0-5、と高優先度キュー6-7、との組み合わせで使用します。

- 2) **Queue Sharper:** ポートのキューでキューシェーピングを有効にするかを設定します。
  - **Enable:** キューシェーピングを有効、無効に設定します。
    - デフォルト値: Disabled
  - **Rate:** キューシェーパーのデータレートを設定。
    - 設定値の範囲: 100-1000000kbps、1-3300Mbps
    - デフォルト値: 500
  - **Unit:** キューシェーパーのデータレート単位を設定。
    - 設定値の範囲: kbps、Mbps
    - デフォルト値: kbps
  - **Excess:** 帯域制限超過時の処理設定。
    - デフォルト値: Disabled

(次ページに続く)



(前ページの続き)

- 3) **Queue Scheduler:** Scheduler Mode が Weighted に設定されていた時に、ポート毎に相関的に重みづけをする必要があります。DWRR は次のキューに移る前にスイッチがサービスするそれぞれのキューのサービス時間のパーセンテージを決める既定義の重みづけを使用します。
- **Weight:** キューごとに割り当てられた重みづけ。
    - 設定値の範囲: 1-100
    - デフォルト値: 17
  - **Percent:** キューのパーセンテージの重み。
- 4) **Port Sharper:** ポートで送信できるトラフィックレート。
- **Enable:** Port Sharper を有効(Enabled)、無効(Disable)に設定します。
    - デフォルト値: Disabled
  - **Rate:** Port Sharper のレートを設定します。
    - 設定値の範囲: 100-1000000kbps、1-3300Mbps
    - デフォルト値: 500
  - **Unit:** ポートシェーパのデータレート単位を設定。
    - 設定値の範囲: kbps、Mbps
    - デフォルト値: kbps

(次ページに続く)

(前ページの続き)

#### QoS Egress Port Scheduler の設定手順:

- 1) メニューから「Configuration」→「QoS」→「Port Scheduler」を順にクリックします。
- 2) Port Scheduler と Sharper を設定するポートのパラメータをクリックします。

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-

送信ポートでScheduler Mode、Egress Queue Mode、Queue shaper、Port Shaperを設定するには

- 1) メニューから「Configuration」→「QoS」→「Port Scheduler」を順にクリックします。
- 2) Scheduler Mode、Queue shaper、Queue Scheduler(Scheduler Mode が Weighted の場合)、Port Shaper を設定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue Shaper				Port Shaper		
Enable	Rate	Unit	Excess	Enable	Rate	Unit
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>	<input checked="" type="checkbox"/>	500	kbps
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>			
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>			
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>			
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>			
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>			
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>			
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>			
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>			

Diagram: A central vertical oval labeled "STRICT" has arrows pointing to it from the Queue Shaper section. An arrow points from the "STRICT" oval to the Port Shaper section.

Buttons: Save, Reset, Cancel

## 34. Egress Port Shaper の設定

QoS Egress Port Shaper ページではキューやポートごとのレートを含む QoS Egress Port Shaper の情報を表示します。Egress Queue Mode、Queue Shaper (レートと帯域制限超過時のアクセス)、と Port Shaper を設定するには Port パラメータのエントリをクリックします。

### 34.1. Egress Port Shaper の設定パラメータ

#### QoS Egress Port Scheduler の表示

- 1) **Port:** Port ID を指定します。
- 2) **Shapers:** キューシェーパーレートとポートシェーパーレートを表示します。

#### QoS Egress Port Scheduler、Queue Scheduler、Port Shaper の設定

この設定ページは Port Scheduler か、Port Shaper のページからアクセスできます。パラメータの解説は“Egress Port Scheduler”のページを参照ください。

- 1) メニューから「Configuration」→「QoS」→「Port Shaper」を順にクリックします。
- 2) Port Scheduler と Sharper を設定するポートのパラメータをクリックします。

QoS Egress Port Shapers									
Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

## 35. Port Remarking Mode の設定

QoS Egress Port Tag Remarking ページではQoS Egress Port Tag Remarkingの概要を表示します。Port パラメータをクリックしPCP/DEI値、デフォルトのPCP/DEI値、マッピングされたQoSクラスやDrop Priority値を使用したRemarking Modeを設定します。

### 35.1. Port Remarking Mode の設定パラメータ

#### QoS Egress Port Remarking Modeの表示

- 1) **Port:** Port ID を指定します。
- 2) **Mode:** ポートで使用されている Tag Remarking Mode を表示します。
  - **Classified:** クラス分けされた PCP/DEI 値を使用します。
  - **Default:** PCP/DEI のデフォルト値を使用します。
  - **Mapped:** マッピングされた QoS クラスとフレーム破棄の優先度レベルを使用します。

#### Port Remarking Modeの設定

- 1) **Tag Remarking Mode:** ポートで使用する Tag Remarking Mode を設定します。
  - **Classified:** クラス分けされた PCP/DEI 値を使用します。
  - **Default:** PCP/DEI のデフォルト値を使用します。
    - 設定値の範囲: PCP 0-7、DEI 0-1
    - デフォルト値: PCP 0、DEI 0
  - **Mapped:** PCP/DEI 値をクラス分けされた QoS と DP level にマッピングします。
- 2) **QoS class/DP level:** QoS クラス値と DP level のマッピングオプションを表示します。
- 3) **PCP:** 指定した Code Point に一致した送信フレームを Remarking します。
  - 設定値の範囲: 0-7
  - デフォルト値: 0
- 4) **DEI:** 指定した Drop Eligible Indicator Code に一致した送信フレームを Remarking します。
  - 設定値の範囲: 0-1
  - デフォルト値: 0

(次ページに続く)

(前ページの続き)

**QoS Egress Port Tag Remarking の表示手順:**

- 1) メニューから「Configuration」→「QoS」→「Port Tag Remarking」を順にクリックします。
- 2) Port Tag Remarking Mode を設定するには、Port パラメータをクリックします。

QoS Egress Port Tag Remarking	
Port	Mode
<u>1</u>	Classified
<u>2</u>	Classified
<u>3</u>	Classified
<u>4</u>	Classified
<u>5</u>	Classified
<u>6</u>	Classified
<u>7</u>	Classified
<u>8</u>	Classified
<u>9</u>	Classified
<u>10</u>	Classified

**QoS Egress Port Tag Remarking の設定手順:**

- 1) メニューから「Configuration」→「QoS」→「Port Tag Remarking」を順にクリックします。
- 2) Port Tag Remarking Mode を設定するには、Port パラメータをクリックします。
- 3) 選択した Mode に関連したパラメータをと Remarking Mode を設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

Tag Remarking mode -&gt; Classified

QoS Egress Port Tag Remarking Port 1 Port 1 ▼

Tag Remarking Mode Classified ▼

Save Reset Cancel

Tag Remarking mode -&gt; Default

QoS Egress Port Tag Remarking Port 1 Port 1 ▼

Tag Remarking Mode Default ▼

PCP/DEI Configuration

Default PCP 0 ▼

Default DEI 0 ▼

Save Reset Cancel

(次ページに続く)

(前ページの続き)

Tag Remarking mode -> Mapped

QoS Egress Port Tag Remarking Port 1 Port 1 ▼

Tag Remarking Mode Mapped ▼

(QoS class, DP level) to (PCP, DEI) Mapping

QoS class	DP level	PCP	DEI
0	0	1 ▼	0 ▼
0	1	1 ▼	1 ▼
1	0	0 ▼	0 ▼
1	1	0 ▼	1 ▼
2	0	2 ▼	0 ▼
2	1	2 ▼	1 ▼
3	0	3 ▼	0 ▼
3	1	3 ▼	1 ▼
4	0	4 ▼	0 ▼
4	1	4 ▼	1 ▼
5	0	5 ▼	0 ▼
5	1	5 ▼	1 ▼
6	0	6 ▼	0 ▼
6	1	6 ▼	1 ▼
7	0	7 ▼	0 ▼
7	1	7 ▼	1 ▼

## 36. Port DSCP Translation と Rewriting の設定

QoS Port DSCP Configuration ページではフレーム受信時の Translation と Classification 設定と送信時の DSCP 値の書き換え設定を行います。

### 36.1. QoS Port DSCP の設定パラメータ

- 1) **Port:** Port ID を指定します。
- 2) **Ingress Translate:** 受信時に指定したクラス分け方法をもとに DSCP 値のトランスレーションを行えるようにします。
- 3) **Ingress Classify:** クラス分け方法を指定します。
  - **Disabled:** Ingress DSCP のクラス分けは実行されません。
  - **DSCP=0:** 受信する DSCP 値が 0 の時にクラス分けを行う。
  - **Selected:** DSCP テーブルで有効になっているクラスからのみ選択します。
  - **All:** 全ての DSCP をクラス分けします。
- 4) **Egress Rewrite:** 送信時の DSCP 値書き換えを設定します。
  - **Disabled:** Egress Rewriting は実行されません。
  - **Enabled:** 再マッピングせずに Egress Rewriting が実行されます。
  - **Remap DP Aware:** DSCP 値がリマップされ、フレームが DSCP 値のリマップによりリマークされています。フレームの DP level により、リマップされた DSCP 値は DSCP Translation Table から Egress Remap DP0 または DP1 フィールドが取られます。
  - **Remap DP Unaware:** DSCP 値がリマップされ、フレームが DSCP 値のリマップによりリマークされています。フレームの DP level により、リマップされた DSCP 値は DSCP Translation Table から Egress Remap DP0 が取られます。

### QoS Port DSCP Configuration の設定手順

- 1) メニューから「Configuration」→「QoS」→「Port DSCP」を順にクリックします。
- 2) 必要に応じて Ingress Translation と Egress Re-writing パラメータを設定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable
7	<input type="checkbox"/>	Disable	Disable
8	<input type="checkbox"/>	Disable	Disable
9	<input type="checkbox"/>	Disable	Disable
10	<input type="checkbox"/>	Disable	Disable

Save Reset

## 37. DSCP-Based QoS Ingress Classification の設定

DSCP-Based QoS Ingress Classification ページでは DSCP-Based QoS Classification を設定します。

### 37.1. DSCP-Based QoS Ingress Classification の設定パラメータ

- 1) **DSCP:** 受信パケットの DSCP 値。
  - 設定値の範囲: 0-63
- 2) **Trust:** 指定された DSCP 値が信頼すべきものか(Trust)を制御します。Trust の DSCP 値を持つフレームのみが指定の QoS クラスと Drop level をマッピングされます。信頼性のない(Untrusted)DSCP 値を持つフレームは、IP フレーム以外として処理されます。
- 3) **QoS Class:** DSCP 値に対応した QoS 値が受信処理時にクラス分けされます。
  - 設定値の範囲: 0-7
  - デフォルト値: 0
- 4) **DPL:** DSCP 値に対応した Drop Precedence Level が受信処理時にクラス分けされます。
  - 設定値の範囲: 0-1(1が高いDrop Priorityを持ちます)
  - デフォルト値: 0

#### DSCP-Based QoS Ingress Classification の設定手順

- 1) メニューから「Configuration」→「QoS」→「DSCP Based QoS」を順にクリックします。
- 2) DSCP 値が“Trust”であるかを指定し、受信時処理に使用する QoS 値と DP level を設定します
- 3) 「Save」ボタンをクリックして設定を保存します。

DSCP	Trust	QoS Class	DPL
0(BE)	<input type="checkbox"/>	0 ▼	0 ▼
1	<input type="checkbox"/>	0 ▼	0 ▼
2	<input type="checkbox"/>	0 ▼	0 ▼
3	<input type="checkbox"/>	0 ▼	0 ▼
4	<input type="checkbox"/>	0 ▼	0 ▼
5	<input type="checkbox"/>	0 ▼	0 ▼
6	<input type="checkbox"/>	0 ▼	0 ▼
7	<input type="checkbox"/>	0 ▼	0 ▼
8(CS1)	<input type="checkbox"/>	0 ▼	0 ▼
9	<input type="checkbox"/>	0 ▼	0 ▼
10	<input type="checkbox"/>	0 ▼	0 ▼
11	<input type="checkbox"/>	0 ▼	0 ▼
12	<input type="checkbox"/>	0 ▼	0 ▼
13	<input type="checkbox"/>	0 ▼	0 ▼
...	<input type="checkbox"/>	0 ▼	0 ▼



## 38. DSCP Translation の設定

DSCP Translation ページでは受信するデータトラフィックに対してDSCPを設定(Ingress Translation)もしくは、送信するデータトラフィックへのDSCP再マッピングを設定(Egress Re-mapping)します。

### 38.1. DSCP Translation の設定パラメータ

- 1) **DSCP:** DSCP 値。
  - 設定値の範囲: 0-63
- 2) **Ingress Translate:** 指定されたクラス分け方法をもとにトラフィック受信時の DSCP Translation を有効にします。
- 3) **Ingress Classify:** 受信時のクラス分け(QoS Port DSCP Configuration Table ページで設定したクラス分け)を有効にします。
- 4) **Egress Remap DP0:** 選択した DSCP 値を DP0 パラメータ値に再マッピングします。DP0 は低い優先度での破棄を意味します。
- 5) **Egress Remap DP1:** 選択した DSCP 値を DP1 パラメータ値に再マッピングします。DP1 は高い優先度での破棄を意味します。

#### DSCP-Translationの設定手順

- 1) メニューから「Configuration」→「QoS」→「DSCP Translation」を順にクリックします。
- 2) 必要に応じて Ingress Translation と Egress Re-mapping のパラメータを設定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
0(BE)	BE	<input type="checkbox"/>	BE	BE
1	1	<input type="checkbox"/>	1	1
2	2	<input type="checkbox"/>	2	2
3	3	<input type="checkbox"/>	3	3
4	4	<input type="checkbox"/>	4	4
5	5	<input type="checkbox"/>	5	5
6	6	<input type="checkbox"/>	6	6
7	7	<input type="checkbox"/>	7	7
8(CS1)	CS1	<input type="checkbox"/>	CS1	CS1
9	9	<input type="checkbox"/>	9	9
10	10	<input type="checkbox"/>	10	10
11	11	<input type="checkbox"/>	11	11
12	12	<input type="checkbox"/>	12	12
13	13	<input type="checkbox"/>	13	13
14	14	<input type="checkbox"/>	14	14
15	15	<input type="checkbox"/>	15	15
16(CS2)	CS2	<input type="checkbox"/>	CS2	CS2
17	17	<input type="checkbox"/>	17	17
18	18	<input type="checkbox"/>	18	18
19	19	<input type="checkbox"/>	19	19
20	20	<input type="checkbox"/>	20	20
21	21	<input type="checkbox"/>	21	21
22	22	<input type="checkbox"/>	22	22

## 39. DSCP Classification の設定

DSCP Classification ページでは DSCP 値を QoS クラスと破棄優先権レベルにマッピングします。

### 39.1. DSCP Translation の設定パラメータ

- 1) **QoS class/DPL:** QoS クラス値と DP(Drop Precedence)レベル値のマッピングオプションを表示します。
- 2) **DSCP:** DSCP 値。
  - 設定値の範囲: 0-63

#### DSCP-Classification の設定手順

- 1) メニューから「Configuration」→「QoS」→「DSCP Classification」を順にクリックします。
- 2) QoS クラスと DPL に対応の DSCP 値をマッピングします。
- 3) 「Save」ボタンをクリックして設定を保存します。

**DSCP Classification**

QoS Class	DPL	DSCP
0	0	BE ▼
0	1	BE ▼
1	0	BE ▼
1	1	BE ▼
2	0	BE ▼
2	1	BE ▼
3	0	BE ▼
3	1	BE ▼
4	0	BE ▼
4	1	BE ▼
5	0	BE ▼
5	1	BE ▼
6	0	BE ▼
6	1	BE ▼
7	0	BE ▼
7	1	BE ▼

Save Reset

## 40. QoS Control List の設定

QoS Control List DSCPページではEthernet type、VLAN ID、TCP/UDPポート、DSCP、ToSまたはVLAN Priority Tagをもとに受信パケットの処理に関してQuality of Serviceポリシーを設定します。

ポートにQCE(QoS Control Entry)をマッピングすると、トラフィックは最初に一致したQoS Control Listのエントリで定義されたQoSクラス、Drop Precedence Level、DSCP値に割り当てられます。いずれのQCEに一致しなかったトラフィックはポートのデフォルトQoSクラスを割り当てられます。

### 40.1. QoS Control List の設定パラメータ







#### QoS Control List

- 1) **QCE:** Quality Control Entry インデックス。
- 2) **Port:** Port ID。
- 3) **Frame Type:** 受信フレームで選別するフレームタイプ。
  - 設定値の範囲: Any、Ethernet、LLC、SNAP、IPv4、IPv6
- 4) **SMAC:** 送信元 MAC アドレスの OUI フィールド(MAC アドレスの先頭から3オクテット部分)。
- 5) **DMAC:** 宛て先 MAC アドレスのタイプ。表示される値は Any、Broadcast、Multicast、Unicast
- 6) **VID:** VLAN ID。
  - 設定値の範囲: 1-4095
- 7) **ACTION:** 設定したパラメータがフレームの中身と一致したときのクラスわけ処理を指定します。設定可能処理動作は以下になります。
  - **Class(Classified QoS Class):** フレームが QCE に一致すると、指定された QoS クラスのキューに送られます。
  - **DPL:** DPL(Drop Precedence Level)が指定した値に設定されます。
  - **DSCP:** DSCP 値が指定した値に設定されます。

(次ページに続く)

(前ページの続き)

QCEを編集、追加、削除する際には以下のボタンを使用します。

ボタン	説明
	新規のQCEを現在の列に挿入します。
	QCEを編集します。
	QCEを上位に動かします。
	QCEを下位に動かします。
	QCEを削除します。
	テーブルの枠外下部にあるプラスボタンで新規のQCEを追加します。

### QCE Configuration

- 1) **Port Member:** QCE に割り当てられたポート。

### Keyパラメータ

- 1) **Tag:** VLAN タグタイプ。
  - 設定値の範囲: Any、Tag、Untag
  - デフォルト値: Any
- 2) **VID:** VLAN ID。
  - 設定値の範囲: Any、Specific(1-4095)、Range
  - デフォルト値: Any
- 3) **PCP:** Priority Code Point(User Priority)。
  - 設定値の範囲: Any、0、1、2、3、4、5、6、7、0-1、2-3、4-5、6-7、0-3、4-7
  - デフォルト値: 0
- 4) **DEI:** Drop Eligible Indicator 値
  - 設定値の範囲: 1、0、Any
- 5) **SMAC:** 送信元 MAC アドレスの OUI フィールド(MAC アドレスの先頭から 3 オクテット部分)。
  - 設定値の範囲: Any、Specific (OUI フィールドを手動入力)
  - デフォルト値: Any
- 6) **DMAC Type:** 宛て先 MAC アドレスのタイプ。
  - 設定値の範囲: Any、Broadcast、Multicast、Unicast
  - デフォルト値: Any

(次ページに続く)

(前ページの続き)

7) **Frame Type:** サポートされるフレームタイプは以下になります。

- **Any:** 全てのフレームタイプを許可します。
- **Ethernet:** Ethernet オプションは Ethernet II フォーマットの packets をフィルタする際に使用します。
  - 設定値の範囲: Any、Specific (16進数で範囲は:600-ffff)
  - デフォルト値: ffff

**注意:** 800(IPv4)と86DD(IPv6)は除外されています。Ethernet Protocol Typeの詳細はRFC1060をご参照ください。一般的に使用される0800(IP)、0806(ARP)、8137(ARP)は含まれています。

LLC-Link Logical Controlは以下の設定が必要です。

- **SSAP Address:** Source Service Access Point Address
  - 設定値の範囲: Any、Specific (16進数で範囲は:0x00-0xff)
  - デフォルト値: 0xff
- **DSAP Address:** Destination Service Access Point Address
  - 設定値の範囲: Any、Specific (16進数で範囲は:0x00-0xff)
  - デフォルト値: 0xff
- **Control:** LLC フレームタイプが Unnumbered、Supervisory、Information のいずれかの場合に、Control パラメータにはコマンド、レスポンス、シーケンス情報を含みます。
  - 設定値の範囲: Any、Specific (16進数で範囲は:0x00-0xff)
  - デフォルト値: 0xff
- **SNAP:** SubNetwork Access Protocol は OUI と PID によって区別されます。
  - 設定値の範囲: Any Specific(16進数で範囲は:0x00-0xffff)
  - デフォルト値: Any

OUIが16進数で000000の場合は、PID値はEther Type(0x0600-0xffff)になり、OUI値が00-00-00以外だと、PID値は0x0000-0xffffの任意の値になります。

- **IPv4:** IPv4 フレームタイプには以下の設定が必要です。
- **Protocol:** IP プロトコルナンバー。
  - 設定値の範囲: Any、UDP、TCP、Other(0-255)
  - デフォルト値: Any

(次ページに続く)

(前ページの続き)

- **Source IP:** Source IP アドレス。
  - 設定値の範囲: Any、UDP、TCP、Other(0-255)
  - デフォルト値: Any
- **IPv4:** IPv4 フレームタイプには以下の設定が必要です。
- **Protocol:** IP プロトコルナンバー
  - 設定値の範囲: Any、Specific
  - デフォルト値: Any

任意の送信元IPアドレスの設定には、クライアントIPアドレスとネットマスクを入力します。アドレスとネットマスクはX.X.X.Xのフォーマットで入力し、Xには10進数0-255の数値を入力します。  
なります。

- **IP Fragment:** Fragment パケットを受信許可するかを設定します。
  - 設定値の範囲: Any、Yes、No
  - デフォルト値: Any
- **DSCP :** Diffserv Code Point 値。
  - 設定値の範囲: Any、0-63、BE、CS1-CS7、EF、AF11-AF43、Range
  - デフォルト値: Any
- **IPv6:** IPv6 フレームタイプ設定には送信元 IP アドレス以外、IPv4 設定と同様のパラメータを使用します。
- **Sport:** Source TCP/UDP ポート。
  - 設定値の範囲: Any、Specific、Range
  - デフォルト値: Any
- **Dport:** Destination TCP/UDP ポート。
  - 設定値の範囲: Any、Specific、Range
  - デフォルト値: Any

(次ページに続く)


(前ページの続き)

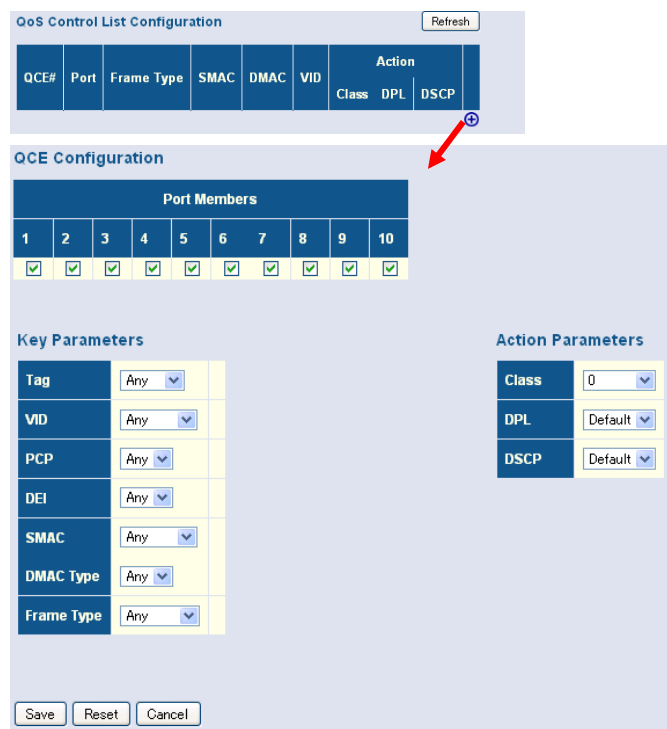
### Actionパラメータ

設定したパラメータとフレームのもつ情報とが一致した場合に、受信フレームに対するクラス分け処理を指定します。

- 1) **Class(Classified QoS Class):** QCE にフレームが一致した場合、指定された QoS クラスに対応した配置キューに配置されるか、クラス分けルールに基づいてキューに配置されます。
  - 設定値の範囲: 0-7、Default(Basic Classificationを使用)
  - デフォルト値: 0
- 2) **DPL:** DPL(Drop Precedence Level)は任意の値に設定するか、変更せずにしておきます。
  - 設定値の範囲: 0-1、Default
  - デフォルト値: Default
- 3) **DSCP:** DSCP 値は任意の値に設定するか、変更せずにしておきます。
  - 設定値の範囲: 0-63、BE、CS1-CS7、Default
  - デフォルト値: Default

### QoS Control Listの設定手順

- 1) メニューから「Configuration」→「QoS」→「QoS Control List」を順にクリックします。
- 2)  ボタンをクリックし新規に QCE を追加するか、他の QCE モディフィケーションボタンを使用して既存の QCE の内容変更を行います。
- 3) QCE Configuration ページのエントリに変更を行う際に、一致条件の基準と条件一致に対するレスポンスを設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。



QoS Control List Configuration

Refresh

QCE#	Port	Frame Type	SMAC	DMAC	VID	Action		
						Class	DPL	DSCP

QCE Configuration

Port Members

1	2	3	4	5	6	7	8	9	10
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Key Parameters

Tag	Any
VID	Any
PCP	Any
DEI	Any
SMAC	Any
DMAC Type	Any
Frame Type	Any

Action Parameters

Class	0
DPL	Default
DSCP	Default

Save Reset Cancel

## 41. Storm Control の設定

Storm Control Configuration ページではトラフィックストームを制御するためにブロードキャスト、マルチキャスト、不明なユニキャストトラフィックに制限を設けます。

Storm Control Configuration ページではブロードキャストトラフィック、マルチキャストトラフィック、不明なユニキャストトラフィックに Threshold(閾値)を設定してトラフィックストームを制御し、閾値を超えたパケットは破棄されます。

**注意:** Storm Control で設定された制限はそれぞれのポートに適用されます。

### 41.1. Storm Control の設定パラメータ

- 1) **Frame Type:** ブロードキャスト、マルチキャスト、不明なユニキャストトラフィックかフレームタイプを指定します。
- 2) **Status:** Storm Control を有効(Enabled)、無効(Disabled)に設定します。
  - デフォルト値: Disabled
- 3) **Rate(pps):** パケットが破棄される Threshold(閾値)。この制限値は  $2^n$  値 Packet Per Second(pps)か、選択値から選択します
  - 設定値の範囲:  $n=1, 2, 3, 4, 8, 16, 32, 64, 128, 256, 512$   
1, 2, 3, 4, 8, 16, 32, 64, 128, 256, 512, 1024Kpps
  - デフォルト値: 2pps

**注意:** ASICの制限により実際の制限値は設定値より低くなります。

**例:** 1Kppsは設定の制限値だと1002.1pps

#### Storm Controlの設定手順

- 1) メニューから「Configuration」→「QoS」→「Storm Control」を順にクリックします。
- 2) Unicast、Multicast、Broadcast で Storm Control を有効にしたいフレームタイプの Enable パラメータにチェックを入れます。
- 3) 制限値を設定します。
- 4) 「Save」ボタンをクリックして設定を保存します。

Frame Type	Enable	Rate (pps)
Unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

Save Reset



## 42. Mirroring の設定 (SMCGS10 のみ対応)

本スイッチでは指定したポートのトラフィックを別ポートにミラーリングを行うことができます。ミラーリングの設定はMirroring Configurationページで行います。

### 42.1. Mirroring 設定ヒント

Mirror ConfigurationページのミラーリングとACL-basedミラーリングは別々に実行されます。Mirror Configurationページで“Port to mirror”パラメータと“Mode”パラメータが設定されると、ACE Ports Configurationページ及び、ACE Configurationページでどのような設定をされていてもミラーリングを実行します。

### 42.2. Mirroring の設定パラメータ

- 1) **Port to mirror on:** 指定したポートのトラフィックのミラーリング先ポートを設定します。全てのミラーセッションは同じミラーリング先ポートを使用します。
- 2) **Port:** トラフィックの監視対象となるポートを指定します。
  - デフォルト値: Disabled
- 3) **Mode:** どのトラフィックがミラーリングされるかを設定します。
  - 設定値の範囲: Enabled(受信、送信の両方)、Disabled、Rx only(受信のみ)、Tx only(送信のみ)
  - デフォルト値: Disabled

#### Mirrorの設定手順

- 1) メニューから「Configuration」→「Mirroring」を順にクリックします。
- 2) ミラーリング先のポートを指定します。
- 3) ミラーリングするポートの Mode パラメータを選択します。
- 4) 「Save」ボタンをクリックして設定を保存します。

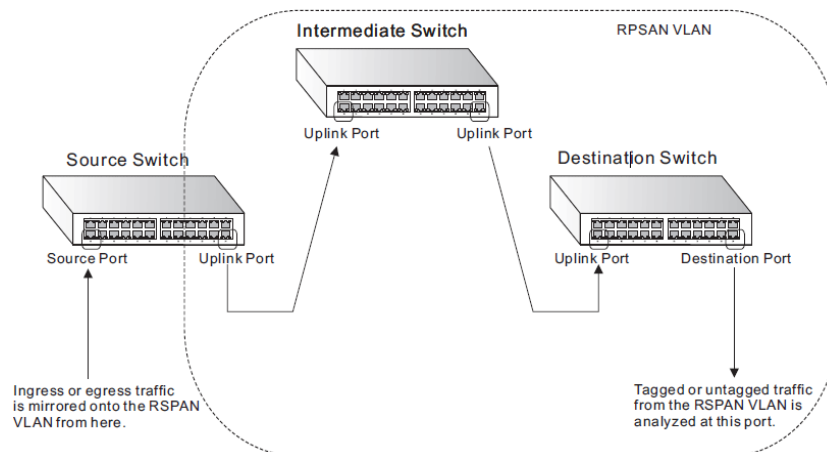
Port	Mode
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

## 43. Mirroring&RSPAN の設定 (SMCGS18/26/50 のみ対応)

本スイッチでは、Mirroring の設定に加えて RSPAN(Remote Switched Port Analyzer)の設定を行うことができます。RSPAN では指定する送信元ポート(Source)と宛先ポート(Destination)をネットワーク上の複数のスイッチにまたがるすることができます。

### 43.1. Mirroring&RSPAN 設定パラメータ

- 1) **Session Number:** ミラーリングのセッション番号を表示します。本スイッチではセッションは 1 つのみサポートしております。
- 2) **Mode:** ミラーリングの有効/無効を選択します。
- 3) **Type:** ミラーリングのタイプを選択します。
  - **Mirror:** ローカルポートのミラーリングを行います。
  - **Source:** RSPAN 機能を使用してモニターされるポートを設定します。
  - **Intermediate:** 対象の RSPAN VLAN のトラフィックを中継します。
  - **Destination:** RSPAN 機能を使用してモニターするポート(ネットワークアナライザを接続するポート)を設定します。



- 4) **VLAN ID:** RSPAN VLAN の ID を設定します。
- 5) **Reflector Port:** RSPAN VLAN にトラフィックをコピーするポートを選択します。
- 6) **Port:** ポート番号を表示します。
- 7) **Source:** ポートをミラーリング対象のポートにする場合のモードを選択します
  - **Disabled:** ミラーリング対象のポートにしません。
  - **Both:** 送受信のトラフィックを Intermediate/Destination ポートにコピーします。
  - **Rx Only:** 受信トラフィックを Intermediate/Destination ポートにコピーします。
  - **Tx Only:** 送信トラフィックを Intermediate/Destination ポートにコピーします。
- 8) **Intermediate:** 中継ポートを選択します。このポートには RSPAN VLAN に所属する他のスイッチが接続されます。
- 9) **Destination:** ソースポートでのトラフィックのコピーを受信するポートを選択します。このポートにはネットワークアナライザが接続されます。

**Mirroring&RSPANの設定手順**

- 1) メニューから「Advanced Configuration」→「Mirroring&RSPAN」を順にクリックします。
- 2) 適宜設定を行います。
- 3) 「Save」ボタンをクリックして設定を保存します。

**Mirroring & RSPAN Configuration**

<b>Session Number</b>	1
<b>Mode</b>	Enabled
<b>Type</b>	Mirror
<b>VLAN ID</b>	200
<b>Reflector Port</b>	Port 1

Port	Source	Intermediate	Destination
1	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
2	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
3	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
4	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
6	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
7	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
8	Disabled	<input type="checkbox"/>	<input type="checkbox"/>

## 44. UPnP の設定

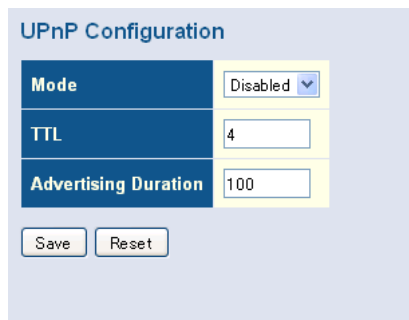
Universal Plug and Play(UPnP)機能を有効にするとスイッチにUPnPでアクセスが可能になります。

### 44.1. UPnP の設定パラメータ

- 1) **Mode:** スwitchの UPnP 機能を有効(Enabled)、無効(Disabled)に設定します。
  - デフォルト値: 4
- 2) **TTL:** スwitchから送信される UPnP メッセージの Time-to-Live 値を設定します。
  - 設定値の範囲: 4-255
  - デフォルト値: 4
- 3) **Advertising Duration:** スwitchは Simple Service Discovery Protocol(SSDP)パケット一定間隔で送信し他の UPnP 機器にスswitchに関する情報を伝えます。SSDP の送信間隔は Advertising Duration の半分から 30 秒引いた時間になります。
  - 設定値の範囲: 100-86400秒
  - デフォルト値: 100秒

#### UPnPの設定手順

- 1) メニューから「Configuration」→「UPnP」を順にクリックします。
- 2) UPnP を有効に設定し、TTL と Advertising Duration の値を設定します。
- 3) 「Save」ボタンをクリックして設定を保存します。

A screenshot of the 'UPnP Configuration' web interface. It features three rows of settings: 'Mode' with a dropdown menu set to 'Disabled', 'TTL' with a text input field containing '4', and 'Advertising Duration' with a text input field containing '100'. Below these fields are two buttons, 'Save' and 'Reset', side-by-side.

UPnP Configuration	
Mode	Disabled
TTL	4
Advertising Duration	100
<div>Save    Reset</div>	

## 45. ステータスの確認

この章では、スイッチの基本的な情報の確認について説明します。

### 45.1. システム情報の確認

本スイッチの、連絡先、システム名、スイッチの設置場所、及びタイムゾーンオフセットを確認する手順を説明します。

#### 45.1.1. システム情報のパラメータ

- 1) **Contact:** システムに責任を持つ管理者の名前を表示します。
- 2) **Name:** スイッチシステムに割り当てた名前を表示します。
- 3) **Location:** システムの設置場所を表示します。
- 4) **Chip ID:** ASIC チップのベンダーID を表示します。
- 5) **MAC Address:** スイッチの MAC アドレスを表示します。
- 6) **System Date:** 現在の日付と時間を表示します。
- 7) **System Uptime:** システムの稼働時間を表示します。
- 8) **Software Version:** システムのソフトウェアバージョンを表示します。
- 9) **Software Date:** ソフトウェアの公開日を表示します。

#### システム情報の確認手順

- 1) メニューから「Monitor」→「System」→「Information」の順にクリックします。
- 2) System Information 画面を自動更新するモードはデフォルトで禁止 (Disabled) になっています。Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

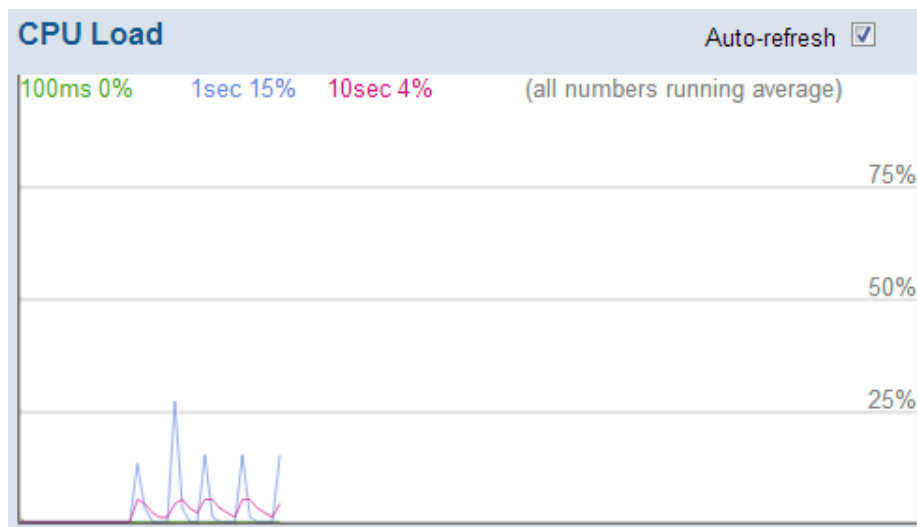
System Information		Auto-refresh <input type="checkbox"/>	Refresh
System			
Contact			
Name			
Location			
Hardware			
Chip ID	VSC7424		
MAC Address	78-cd-8e-b3-39-77		
Time			
System Date	1970-01-01T02:24:25+00:00		
System Uptime	0d 02:24:25		
Software			
Software Version	SMCGS10P-Smart (standalone) Version 1.0.0.3		
Software Date	2011-10-03 08:39:38 +0200		

## 45.2. CPU 使用率の確認

CPU Loadグラフの描写にはSVG(Scalable Vector Graphics)フォーマットを使用するため、IE8以前ではプラグインの追加が必要となります。

### CPU使用率の確認手順:

- 1) メニューから「Monitor」→「System」→「CPU Load」の順にクリックします。



## 45.3. システムログの確認

本スイッチに記録されたシステムログを確認する手順を説明します。

### 45.3.1. システムログのパラメータ

#### 表示フィルタ


- 1) **Level:** 表示するシステムログの種類を選択します。
  - 設定値の範囲:
    - Info      - 情報
    - Warning - 警告
    - Error     - エラー
    - All       - 全て
  - デフォルト値: All
- 2) **Start from ID:** どのシステムログの ID から表示するかを選択します。
- 3) **with #:** 一度に表示するシステムログの数を選択します。


#### 各種パラメータ


- 1) **ID:** システムログの ID を表示します。
- 2) **Level:** システムログの種類を表示します。
- 3) **Time:** システムログが記録された時間を表示します。
- 4) **Message:** システムログの内容を表示します。


#### システムログの確認手順

- 1) メニューから「Monitor」→「System」→「Log」の順にクリックします。
- 2) ページに表示させるシステムログの種類と ID を選択します。
- 3) ログメッセージをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。
 


 - 先頭のシステムログを表示します。


 - 現在表示されているIDより前のシステムログを表示します。


 - 現在表示されているIDより後のシステムログを表示します。


 - 最後に記録されたシステムログを表示します。

- 4) **Auto-refresh** をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは **Refresh** ボタンをクリックすると、直ちに画面を最新情報に更新します。  
 また、**Clear** ボタンをクリックすることで、全てのシステムログが消去されます。

**System Log Information**
Auto-refresh ☒ Refresh Clear |<< << >> >>|

Level

Info ▼

The total number of entries is 18 for the given level.

Start from ID  with  entries per page.

ID	Level	Time	Message
14	Info	1970-01-01T00:35:35+00:00	Link up on port 7
15	Info	1970-01-01T00:35:43+00:00	Link down on port 7
16	Info	1970-01-01T00:35:48+00:00	Link up on port 8
17	Info	1970-01-01T00:35:49+00:00	Link down on port 8
18	Info	1970-01-01T00:35:55+00:00	Link up on port 1

## 45.4. システムログの詳細の確認

本スイッチに記録されたシステムログの詳細情報を確認する手順を説明します。

### 45.4.1. システムログの詳細のパラメータ

#### 表示フィルタ

- 1) **ID:** 詳細を表示するシステムログの ID を選択します。

#### 各種パラメータ

- 1) **Level:** システムログの種類を表示します。
- 2) **Time:** システムログが記録された時間を表示します。
- 3) **Message:** システムログの内容を表示します。

#### システムログの詳細の確認手順

- 1) メニューから「Monitor」→「System」→「Detailed Log」の順にクリックします。
- 2) ログメッセージをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。



- 先頭のシステムログを表示します。



- 現在表示されているIDより前のシステムログを表示します。



- 現在表示されているIDより後のシステムログを表示します。



- 最後に記録されたシステムログを表示します。

- 3) Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

Detailed System Log Information							
ID	11						
<b>Message</b> <table border="1"> <tr> <td>Level</td> <td>Info</td> </tr> <tr> <td>Time</td> <td>1970-01-01T00:35:20+00:00</td> </tr> <tr> <td>Message</td> <td>Link down on port 5</td> </tr> </table>		Level	Info	Time	1970-01-01T00:35:20+00:00	Message	Link down on port 5
Level	Info						
Time	1970-01-01T00:35:20+00:00						
Message	Link down on port 5						



## 46. 熱保護状態の確認 (SMCGS10 のみ対応)

この章では、スイッチの熱保護の確認について説明します。

### 46.1. 熱保護状態の確認

本スイッチの熱保護の状態を確認する手順を説明します。

#### 46.1.1. 熱保護のパラメータ

- 1) **Local Port:** ポート番号を表示します。
- 2) **Port status:** ポートのリンクが通常動作しているか、シャットダウンされているかを表示します
- 3) **Temperature:** 本スイッチの ASIC チップの温度を表示します。

熱保護の確認手順:

- 1) メニューから「Monitor」→「Thermal Protection」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

Thermal Protection Status

Auto-refresh ☐ Refresh

Thermal Protection Port Status

Local Port	Port status
1	Port link operating normally
2	Port link is thermal protected (Link is down)
3	Port link operating normally
4	Port link operating normally
5	Port link operating normally
6	Port link operating normally
7	Port link operating normally
8	Port link operating normally
9	Port link operating normally
10	Port link operating normally

Chip Temperature

Temp.

60 °C

## 47. ポート状態の確認

この章では、スイッチのポートの状態確認について説明します。

### 47.1. パネル表示

本スイッチのフロントパネルの状態を確認する手順を説明します。

**パネル表示の確認手順：**

- 1) メニューから「Monitor」→「Ports」→「State」の順にクリックします。
- 2) 各ポートをクリックすることで、そのポートの詳細ステータスを確認する事が出来ます。
- 3) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。



## 47.2. ポートステータスの確認

本スイッチのポートステータスを確認する手順を説明します。

### 47.2.1. ポートステータスのパラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **Packets Received/Transmitted:** 送受信したパケットの総数を表示します。
- 3) **Bytes Received/Transmitted:** 送受信したデータの総数(Byte)を表示します。
- 4) **Errors Received/Transmitted:** 送受信したエラーフレームの総数を表示します。
- 5) **Drops Received/Transmitted:** 破棄されたフレームの総数を表示します。
- 6) **Filtered Received:** フィルタしたフレームの総数を表示します。

### ポートステータスの確認手順

- 1) メニューから「Monitor」→「Ports」→「Traffic Overview」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	61671	61906	92085180	92044404	0	0	0	0	493
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

### 47.3. QoS 統計情報の確認

本スイッチのQoSの統計情報を確認する手順を説明します。

#### 47.3.1. QoS 統計情報のパラメータ

- 1) Q # Rx/Tx: キューごとに送受信したパケットの総数を表示します。

#### QoS統計情報の確認手順

- 1) メニューから「Monitor」→「Ports」→「QoS Statistics」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

Queuing Counters																
Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	134	0	0	0	0	0	0	0	0	0	0	0	0	0	0	82
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	128	0	0	0	0	0	0	0	0	0	0	0	0	0	89
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

## 47.4. QoS Control List の確認

本スイッチのQoS Control Listを確認する手順を説明します。

### 47.4.1. QoS Control List のパラメータ

- 1) **User:** この QCE(QoS Control Entry)のユーザー(Static、Voice VLAN、Combined、Conflict)を表示します。
- 2) **QCE#:** QoS Control Entry の番号を表示します。
- 3) **Frame Type:** QoS を適用するフレームタイプを表示します。
  - 指定可能なフレームタイプは次の通りです： Any、Ethernet、LLC、SNAP、IPv4、IPv6
- 4) **Port:** ポート番号を表示します。
- 5) **Action:** 受信したフレームが、Frame Type の内容と適合した場合に実行されるアクションを表示します。
  - Class: ここで指定された QoS クラスのキューに置かれます。
  - DP: ここで指定された廃棄優先度が取り付けられます。
  - DSCP: ここで指定された DSCP 値が取り付けられます。
- 6) **Conflict:** 設定に矛盾が生じている場合には”Yes”が表示されます。

### QoSステータスの確認手順

- 1) メニューから「Monitor」→「Ports」→「QCL Status」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

QoS Control List Status

Combined

▼

Auto-refresh

☐

Resolve Conflict

Refresh

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DP	DSCP	
Static	1	Any	1-10	Class 0	Default	Default	No

## 47.5. 詳細ポートステータスの確認

本スイッチの詳細ポートステータスを確認する手順を説明します。

### 47.5.1. 詳細ポートステータスのパラメータ

#### Receive/Transmit Total

- 1) **Packets:** 送受信したパケットの総数を表示します。
- 2) **Octets:** FCS を含む送受信したデータの総数(Byte)を表示します。
- 3) **Unicast:** 送受信したユニキャストパケットの総数を表示します。
- 4) **Multicast:** 送受信したマルチキャストパケットの総数を表示します。
- 5) **Broadcast:** 送受信したブロードキャストパケットの総数を表示します。
- 6) **Pause:** 送受信した Pause フレームの総数を表示します。

**Receive/Transmit Queue Counters:** 送受信したパケットをキュー別に統計表示します。

#### Receive Error Counters

- 1) **Rx Drops:** リソース不足により破棄された受信パケットの総数を表示します。
- 2) **Rx CRC / Alignment:** 発生した FCS エラーとアラインメントエラーの総数を表示します。
- 3) **Rx Undersize:** 受信したデータのうち、長さが 64Byte に未満のフレームの総数を表示します。  
(FCS は含まれますが、フレーミングビットは含まれません)
- 4) **Rx Oversize:** 受信したデータのうち、Maximum Frame Size で設定した値よりも長いフレームの総数を表示します。(FCS は含まれますが、フレーミングビットは含まれません)
- 5) **Rx Fragments:** 受信しデータのうち、FCS エラーとアラインメントエラーがあった長さが 64Byte に未満のフレームの総数を表示します。
- 6) **Rx Jabber:** 受信しデータのうち、FCS エラーとアラインメントエラーがあった長さが Maximum Frame Size で設定した値よりも長いフレームの総数を表示します。
- 7) **Rx filtered:** フィルタされたフレームの総数を表示します。

#### Transmit Error Counters

- 1) **Tx Drops:** リソース不足により破棄されフレームの総数を表示します。
- 2) **Tx Late / Exc. Coll.:** 発生したレイトコリジョンの総数を表示します。

### 詳細ポートステータスの確認手順

- 1) メニューから「Monitor」→「Ports」→「Detailed Statistics」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

Detailed Port Statistics Port 1				Port 1	Auto-refresh <input type="checkbox"/>	Refresh	Clear
Receive Total		Transmit Total					
Rx Packets	2014	Tx Packets	3347				
Rx Octets	308674	Tx Octets	308085				
Rx Unicast	728	Tx Unicast	601				
Rx Multicast	587	Tx Multicast	2746				
Rx Broadcast	699	Tx Broadcast	0				
Rx Pause	0	Tx Pause	0				
Receive Size Counters		Transmit Size Counters					
Rx 64 Bytes	467	Tx 64 Bytes	2704				
Rx 65-127 Bytes	1160	Tx 65-127 Bytes	110				
Rx 128-255 Bytes	80	Tx 128-255 Bytes	399				
Rx 256-511 Bytes	124	Tx 256-511 Bytes	109				
Rx 512-1023 Bytes	173	Tx 512-1023 Bytes	12				
Rx 1024-1526 Bytes	10	Tx 1024-1526 Bytes	13				
Rx 1527- Bytes	0	Tx 1527- Bytes	0				
Receive Queue Counters		Transmit Queue Counters					
Rx Q0	2014	Tx Q0	0				
Rx Q1	0	Tx Q1	0				
Rx Q2	0	Tx Q2	0				
Rx Q3	0	Tx Q3	0				
Rx Q4	0	Tx Q4	0				
Rx Q5	0	Tx Q5	0				
Rx Q6	0	Tx Q6	0				
Rx Q7	0	Tx Q7	3347				
Receive Error Counters		Transmit Error Counters					
Rx Drops	0	Tx Drops	0				
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0				
Rx Undersize	0						
Rx Oversize	0						
Rx Fragments	0						
Rx Jabber	0						
Rx Filtered	0						

## 48. セキュリティの確認

この章では、セキュリティの確認について説明します。

### 48.1. アクセス統計情報

本スイッチのアクセス統計情報を確認する手順を説明します。

#### 48.1.1. アクセス統計情報のパラメータ

- 1) **Interface:** スwitchの管理に使用したプロトコルを表示します。  
(プロトコル: HTTP、HTTPS、SNMP、TELNET、SSH)
- 2) **Receive Packets:** 受信した管理パケットの総数を表示します。
- 3) **Allow Packets:** 受信を許可されたパケットの総数を表示します。
- 4) **Discard Packets:** 破棄されたパケットの総数を表示します。

#### アクセス統計情報の確認手順

- 1) メニューから「Monitor」→「Security」→「Access Management Statistics」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

Access Management Statistics				Auto-refresh <input type="checkbox"/>	Refresh	Clear
Interface	Received Packets	Allowed Packets	Discarded Packets			
HTTP	776	728	48			
HTTPS	380	380	0			
SNMP	1256	1256	0			
TELNET	357	354	3			
SSH	143	143	0			



## 48.2. スイッチセキュリティステータスの確認

スイッチセキュリティステータスを確認する手順を説明します。

### 48.2.1. スイッチセキュリティステータスのパラメータ

#### User Module Legend

- 1) **User Module Name:** ポートセキュリティで使用する可能性のあるユーザーモジュールを表示します。
- 2) **Abbr:** ユーザーモジュールを一文字に省略したもので、ポートステータステーブルで使用されます。

#### Port Status

- 1) **Port:** ポート番号を表示します。ポート毎の詳しいステータスを参照するにはポート番号をクリックしてください。
- 2) **Users:** 有効なユーザーモジュールを表示します。
- 3) **State:** 現在のポートの状態を表示します
  - 表示値は以下の4通りです。
    - Disabled: ポートセキュリティを使用しておりません。
    - Ready: 少なくとも1つのユーザーモジュールを使用中で、未知のMACアドレスからのフレームを待っています。
    - Limit Reached: 学習したMACアドレスの数がLimit Controlで設定した制限に達しているので、これ以上MACアドレスは学習されません。
    - Shutdown: 学習したMACアドレスの数がLimit Controlで設定した制限に達しているので、ポートをシャットダウンしています。
  - ※ シャットダウンから回復させるにはLimit ControlのウェブページでReopenボタンをクリックします。
- 4) **MAC Count:** このポートで学習した MAC アドレスの数と、学習出来る MAC アドレスの総数を表示します。Limit Control が設定されていない場合は、“-”が表示されます。

## スイッチセキュリティステータスの確認手順:

- 1) メニューから「Monitor」→「Security」→「Port Security」→「Switch」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

**Port Security Switch Status** Auto-refresh ☒ [Refresh](#)

**User Module Legend**

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

**Port Status**

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	L---	Ready	0	4
3	---	Disabled	-	-
4	---	Disabled	-	-
5	---	Disabled	-	-
6	---	Disabled	-	-
7	L---	Shutdown	0	1
8	L---	Ready	0	1
9	---	Disabled	-	-
10	---	Disabled	-	-

- 3) Limit Control にてシャットダウンになったポートを回復させるには、メニューから「Configuration」→「Security」→「Network」→「Limit Control」の順にクリックし、Shutdown 状態のポートの [Reopen](#) をクリックします。

**Port Configuration**

Port	Mode	Limit	Action	State	Re-open
1	Disabled	4	None	Disabled	<a href="#">Reopen</a>
2	Enabled	4	Trap & Shutdown	Ready	<a href="#">Reopen</a>
3	Disabled	4	None	Disabled	<a href="#">Reopen</a>
4	Disabled	4	None	Disabled	<a href="#">Reopen</a>
5	Disabled	4	None	Disabled	<a href="#">Reopen</a>
6	Disabled	4	None	Disabled	<a href="#">Reopen</a>
7	Enabled	1	Trap & Shutdown	Shutdown	<a href="#">Reopen</a>
8	Enabled	1	None	Ready	<a href="#">Reopen</a>
9	Disabled	4	None	Disabled	<a href="#">Reopen</a>
10	Disabled	4	None	Disabled	<a href="#">Reopen</a>

[Save](#) [Reset](#)

### 48.3. ポートセキュリティステータスの確認

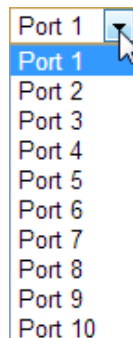
ポートセキュリティステータスを確認する手順を説明します。

#### 48.3.1. ポートセキュリティステータスのパラメータ

- 1) **MAC Address:** 学習している MAC アドレスを表示します。  
MAC アドレス一つも学習していない場合は、” *No MAC addresses attached* ”が表示されます。
- 2) **VLAN ID:** VLAN ID が表示されます。
- 3) **State:** 対応する MAC アドレスが転送されるか遮断されるかを表示します。State が blocked の場合はその MAC アドレスからはデータの送受信を行いません。
- 4) **Time of Addition:** MAC アドレスを学習した日時を表示します。
- 5) **Age/Hold:** 表示されている時間、記録されている MAC アドレスの情報を保持します。

#### ポートセキュリティステータスの確認手順

- 1) メニューから「Monitor」→「Security」→「Port Security」→「Port」の順にクリックします。
- 2) プルダウンメニューから情報を表示するポートを選択します。



- 3) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

Port Security Port Status Port 2				
		Port 2 ▼	Auto-refresh <input type="checkbox"/>	Refresh
MAC Address	VLAN ID	State	Time of Addition	Age/Hold
00-00-29-02-e4-32	1	Forwarding	1970-01-01T05:11:20+00:00	3597
00-05-6e-00-8b-da	1	Forwarding	1970-01-01T05:11:15+00:00	3591

#### 48.4. Network Access Server 認証のステータス

Network Access Server認証のステータスを確認する手順を説明します。

##### 48.4.1. Network Access Server 認証ステータスのパラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **Admin State:** ポートの認証モードを表示します。
- 3) **Port State:** 現在のポートの状態を表示します。
- 4) **Last Source:** 最後に受信した EAPOL 認証フレーム、または MAC-based 認証の新しいクライアントから受信したフレームの送信元アドレスを表示します。
- 5) **Last ID:** 最後に受信した EAPOL 認証フレームのユーザーID、または MAC-based 認証の新しいクライアントから受信したフレームの送信元アドレスを表示します。
- 6) **QoS Class:** 認証されたクライアントへ割り当てるトラフィックの優先度を表示します
- 7) **Port VLAN ID:** 認証されたクライアントへ割り当てる VLAN ID を表示します。  
VLAN ID が RADIUS サーバから割り当てられたものならば、(RADIUS-assigned)が表示され、RADIUS サーバとの認証がタイムアウトし、Guest VLAN ID が割り当てられている場合は (Guest)と一緒に表示されます。

##### Network Access Server 認証ステータスの確認手順

- 1) メニューから「Monitor」→「Security」→「NAS」→「Switch」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

Network Access Server Switch Status							Auto-refresh <input type="checkbox"/>	Refresh
Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID		
1	Force Authorized	Authorized						
2	Single 802.1X	Authorized				1 (Guest)		
3	Force Authorized	Link Down						
4	Force Authorized	Link Down						
5	Force Authorized	Link Down						
6	Force Authorized	Link Down						
7	Force Authorized	Link Down						
8	Force Authorized	Link Down						
9	Force Authorized	Link Down						
10	Force Authorized	Link Down						

## 48.5. Network Access Server 統計

Network Access Serverの統計情報を確認する手順を説明します。

※ 認証方式によって、表示される項目が変わります

### 48.5.1. Network Access Server 統計のパラメータ

#### Port State

- 1) **Admin State:** ポートの認証モードを表示します。
- 2) **Port State:** 現在のポートの状態を表示します
- 3) **QoS Class:** 認証されたクライアントへ割り当てるトラフィックの優先度を表示します。
- 4) **Port VLAN ID:** 認証されたクライアントへ割り当てる VLAN ID を表示します。VLAN ID が RADIUS サーバから割り当てられたものならば、(RADIUS-assigned)が表示され、RADIUS サーバとの認証がタイムアウトし、Guest VLAN ID が割り当てられている場合は(Guest)が一緒に表示されます。

#### Port Counters

##### Receive EAPOL Counters

- 1) **Total:** 受信した有効な EAPOL フレームの総数を表示します。
- 2) **Response ID:** 受信した有効な EAPOL Response Identity フレームの数を表示します。
- 3) **Responses:** 受信した有効な EAPOL Response Identity フレーム以外の EAPOL Response フレームの数を表示します。
- 4) **Start:** 受信した EAPOL Start フレームの数を表示します。
- 5) **Logoff:** 受信した EAPOL Logout フレームの数を表示します。
- 6) **Invalid Type:** 受信した EAPOL フレームのうち Type フィールドにエラーがあったものの数を表示します。
- 7) **Invalid Length:** 受信した EAPOL フレームのうち Body Length フィールドにエラーがあったものの数を表示します。

##### Transmit EAPOL Counters

- 1) **Total:** 送信した EAPOL フレームの総数を表示します。
- 2) **Request ID:** 送信した EAPOL Request Identity フレームの総数を表示します。
- 3) **Requests:** 送信した EAPOL Response Identity フレーム以外の EAPOL Response フレームの数を表示します。

##### Receive Backend Server Counters

- 1) **Access Challenges:**
  - 802.1X-based: RADIUS サーバからのアクセスチャレンジを受信した回数を表示します
  - MAC-based: サーバからのアクセスチャレンジを受信した数を表示します
- 2) **Other Requests:**
  - 802.1X-based: EAP-Request パケットを送信した数を表示します。
  - MAC-based: この項目は表示されません。
- 3) **Auth. Successes:** 認証に成功した回数を表示します。
- 4) **Auth. Failures:** 認証に失敗した回数を表示します。

(次ページに続く)

(前ページの続き)

#### Transmit Backend Server Counters

##### 1) Responses:

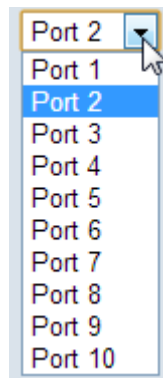
- 802.1X-based: サプリカントからの Response をサーバに送信した回数を表示します。再送信したものは数えません。
- MAC-based: スイッチからサーバにパケットを送信した回数を表示します。再送信したものは数えません。

#### Supplicant /client Info

- 1) **MAC Address** – 最後のクライアント/サプリカントの MAC アドレスを表示します。
- 2) **VLAN ID** – クライアント/サプリカントから最後に受信したフレームの VLAN ID を表示します。
- 3) **Version** –
  - 802.1X-based: 一番最近受信したフレームのプロトコルバージョンを表示します。
  - MAC-based: この項目は表示されません。
- 4) **Identity** –
  - 802.1X-based: 一番最近受信した Response Identity EAPOL フレームのユーザー名を表示します。
  - MAC-based: この項目は表示されません。

#### Network Access Server統計の確認手順

- 1) メニューから「Monitor」→「Security」→「NAS」→「Port」の順にクリックします。
- 2) プルダウンメニューから統計情報を表示させたいポートを選択します。



- 3) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

(次ページに続く)

(前ページの続き)

802.1X

**NAS Statistics Port 2** Port 2 ▼ Auto-refresh ☐ Refresh Clear

**Port State**

Admin State	Single 802.1X
Port State	Unauthorized
QoS Class	
Port VLAN ID	

**Port Counters**

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	1
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

Receive Backend Server Counters		Transmit Backend Server Counters	
Access Challenges	0	Responses	0
Other Requests	1		
Auth. Successes	0		
Auth. Failures	0		

**Supplicant Info**

MAC Address	
VLAN ID	
Version	0
Identity	

(次ページに続く)

(前ページの続き)

**MAC-based**

- 1) Attached Clients で統計を表示させたいクライアントの MAC Address をクリックすると、Selected Counters に選択したクライアントの統計情報が表示されます。
- 2) **Clear All** ボタンをクリックすることで、このポートの統計情報をクリアします。また、**Clear This** ボタンをクリックすると、現在選択されているクライアント(Selected counters に表示されている)の統計情報をクリアします。

**NAS Statistics Port 2** Port 2 Auto-refresh ☒ Refresh Clear All Clear This

**Port State**

Admin State	MAC-based Auth.
Port State	0 Auth/2 Unauth

**Port Counters**

Receive Backend Server Counters		Transmit Backend Server Counters	
Access Challenges	0	Responses	31
Auth. Successes	0		
Auth. Failures	0		
Last Client Info			
MAC Address	5c-26-0a-39-66-91		
VLAN ID	1		

**Selected Counters**

Receive Backend Server Counters		Transmit Backend Server Counters	
Access Challenges	0	Responses	2
Auth. Successes	0		
Auth. Failures	0		
Client Info			
MAC Address	00-1e-94-17-00-3f		
VLAN ID	1		

**Attached Clients**

MAC Address	VLAN ID	State	Last Authentication
<u>00-1e-94-17-00-3f</u>	1	Unauthorized	1970-01-01T19:37:52+00:00
<u>5c-26-0a-39-66-91</u>	1	Unauthorized	



## 48.6. Access Control List ステータスの確認

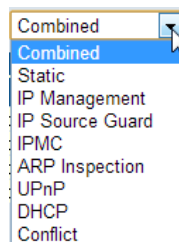
Access Control Listのステータスを確認する手順を説明します。

### 48.6.1. Access Control List ステータスのパラメータ

- 1) **User:** ACL ユーザーを表示します。
- 2) **Ingress Port:** ACL ルールが適用されるポートを表示します。
  - 表示値は以下の3通りです。
    - ・Any - 全てのポート
    - ・Policy - 指定したポリシー
    - ・Port - 指定したポート
- 3) **Frame Type:** ACL ルールが適用されるフレームタイプを表示します。
- 4) **Action:** ACL ルールを適用するフレームタイプを表示します。
  - 表示値は以下の2通りです。
    - ・Permit - ACLルールと一致した場合はフレームを転送し、MACアドレスを学習します。
    - ・Deny - ACLルールと一致した場合はフレームを破棄します。
- 5) **Rate Limiter :** ACL ルールと一致した場合に実行される Rate Limiter の ID を表示します。
- 6) **Redirect to:** ACL ルールに一致した場合にフレームを指定したポートに転送するかを表示します。
- 7) **Mirror:** ACL ルールに一致した場合にポートからのフレームを指定したポートにミラーリングするか表示します。
- 8) **CPU:** ACL ルールに一致した場合パケットは CPU で処理されます。
- 9) **CPU Once:** ACL ルールに一致した場合、最初のパケットは CPU で処理されます。
- 10) **Counter:** ACL ルールに一致したパケットの数を表示します。
- 11) **Conflict:** 設定に矛盾が生じている場合は”Yes”が表示されます。

### Access Control Listステータスの確認手順

- 1) メニューから「Monitor」→「Security」→「ACL Status」の順にクリックします。
- 2) プルダウンメニューからステータスを表示させたい ACL ユーザーを選択します。



- 3) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

ACL Status										
						Combined	Auto-refresh <input type="checkbox"/>		Refresh	
User	Ingress Port	Frame Type	Action	Rate Limiter	Redirect to	Mirror	CPU	CPU Once	Counter	Conflict
IP Management	Any	ARP	Permit	Disabled	Disabled	Disabled	Yes	No	16476	No
IP Management	Any	IPv4/UDP 68 DHCP Server	Permit	Disabled	Disabled	Disabled	Yes	No	16	No
Static	Policy 1	Any	Permit	Disabled	Disabled	Disabled	No	No	4612	No
Static	Port 6	Any	Permit	4	Disabled	Enabled	No	No	0	No

## 48.7. DHCP Snooping 統計情報の確認

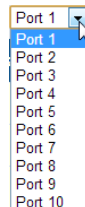
DHCP Snoopingの統計情報を確認する手順を説明します。

### 48.7.1. DHCP Snooping 統計情報のパラメータ

- 1) **Rx/Tx Discover:** 送受信した DHCP Discover メッセージの数を表示します。
- 2) **Rx/Tx Offer:** 送受信した DHCP Offer メッセージの数を表示します。
- 3) **Rx/Tx Request:** 送受信した DHCP Request メッセージの数を表示します。
- 4) **Rx/Tx Decline:** 送受信した DHCP Decline メッセージの数を表示します。
- 5) **Rx/Tx ACK:** 送受信した DHCP Ack メッセージの数を表示します。
- 6) **Rx/Tx NAK:** 送受信した DHCP Nak メッセージの数を表示します。
- 7) **Rx/Tx Release:** 送受信した DHCP Release メッセージの数を表示します。
- 8) **Rx/Tx Inform:** 送受信した DHCP Inform メッセージの数を表示します。
- 9) **Rx/Tx Lease Query:** 送受信した DHCP Lease Query メッセージの数を表示します。
- 10) **Rx/Tx Lease Unassigned:** 送受信した DHCP Lease Unassigned メッセージの数を表示します。
- 11) **Rx/Tx Lease Unknown:** 送受信した DHCP Lease Unknown メッセージの数を表示します。
- 12) **Rx/Tx Lease Active:** 送受信した DHCP Lease Active メッセージの数を表示します。

### DHCP Snooping統計情報の確認手順

- 1) メニューから「Monitor」→「Security」→「DHCP」→「Snooping Statistics」の順にクリックします。
- 2) プルダウンメニューから統計情報を表示させたいポートを選択します。



- 3) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

DHCP Snooping Port Statistics Port 1			
Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	1
Rx Offer	1	Tx Offer	0
Rx Request	1	Tx Request	1
Rx Decline	0	Tx Decline	0
Rx ACK	2	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	4	Tx Inform	4
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0

## 48.8. DHCP Relay 統計情報の確認

DHCP Relayの統計情報を確認する手順を説明します。

### 48.8.1. DHCP Relay 統計情報のパラメータ

#### Server Statistics

- 1) **Transmit to Server:** クライアントからサーバに中継したパケットの数を表示します
- 2) **Transmit Error:** クライアントに送信したエラーを含んでいるパケットの数を表示します。
- 3) **Receive from Server:** サーバから受信したパケットの数を表示します。
- 4) **Receive Missing Agent Option:** 受信したエージェント情報オプション無しのパケットの数を表示します。
- 5) **Receive Missing Circuit ID:** Circuit ID 無しで受信したパケットの数を表示します。
- 6) **Receive Missing Remote ID:** Remote ID 無しで受信したパケットの数を表示します。
- 7) **Receive Bad Circuit ID:** 受信したパケットのうち Circuit ID が不正だったものの数を表示します。
- 8) **Receive Bad Remote ID:** 受信したパケットのうち Remote ID が不正だったものの数を表示します。

#### Client Statistics

- 1) **Transmit to Client:** サーバからクライアントに中継したパケットの数を表示します。
- 2) **Transmit Error:** サーバに送信したエラーを含んでいるパケットの数を表示します。
- 3) **Receive from Client:** クライアントから受信したパケットの数を表示します。
- 4) **Receive Agent Option:** 受信したエージェント情報を含むパケットの数を表示します
- 5) **Replace Agent Option:** 受信したパケットのうち、エージェント情報を置き換えた数を表示します。
- 6) **Keep Agent Option:** 受信したパケットのうち、エージェント情報を変更しなかった数を表示します。
- 7) **Drop Agent Option:** リレー情報を既に含んでいたため破棄したパケットの数を表示します。

#### DHCP Relay統計情報の確認手順

- 1) メニューから「Monitor」→「Security」→「DHCP」→「Relay Statistics」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

DHCP Relay Statistics

Auto-refresh☐ Refresh Clear

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

## 48.9. ARP Inspection 情報の確認

ARP Inspection情報を確認する手順を説明します。

### ARP Inspection情報の確認手順

- 1) メニューから「Monitor」→「Security」→「ARP Inspection」の順にクリックします。
- 2) 表示させたいポート、VLAN、MAC アドレス、IP アドレスと表示させる数を指定します
- 3) ページをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。
  - 先頭のページを表示します。
  - 次ページを表示します。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

**Dynamic ARP Inspection Table** Auto-refresh ☐ Refresh |<< >>|

Start from Port 1 , VLAN 1 , MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

## 48.10. IP Source Guard Table の確認

IP Source Guard Tableを確認する手順を説明します。

### IP Source Guard Tableの確認手順

- 1) メニューから「Monitor」→「Security」→「IP Source Guard」の順にクリックします。
- 2) 表示させたいポート、VLAN、IP アドレスと表示させる数を指定します
- 3) ページをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。
  - 先頭のページを表示します。
  - 次ページを表示します。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

**Dynamic IP Source Guard Table** Auto-refresh ☐ Refresh |<< >>|

Start from Port 1 , VLAN 1 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	IP Address	MAC Address
No more entries			

## 48.11. 認証サーバー一覧の確認

認証サーバー一覧を確認する手順を説明します。

### 48.11.1. 認証サーバー一覧のパラメータ

- 1) #: RADIUS サーバの番号を表示します。クリックすることで詳細なステータスを確認する事が出来ます。
- 2) **IP Address:** RADIUS サーバの IP アドレスと UDP ポート番号を表示します。
- 3) **Status:** RADIUS サーバの現在の状態を表示します。
  - 表示値は以下の4通りです。
    - Disabled – 使用不可になっております。
    - Not Ready – サーバは有効ですが、通信が不可です。
    - Ready – サーバは使用可能です。
    - Dead (X seconds left) – サーバとの通信でタイムアウトが発生したため、dead-time(内の数字)が尽きるまでサーバへの問い合わせを行いません。

#### 認証サーバー一覧の確認手順

- 1) メニューから「Monitor」→「Security」→「AAA」→「RADIUS Overview」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

**RADIUS Authentication Server Status Overview** Auto-refresh ☐

#	IP Address	Status
<u>1</u>	0.0.0.0:1812	Disabled
<u>2</u>	0.0.0.0:1812	Disabled
<u>3</u>	0.0.0.0:1812	Disabled
<u>4</u>	0.0.0.0:1812	Disabled
<u>5</u>	0.0.0.0:1812	Disabled

**RADIUS Accounting Server Status Overview**

#	IP Address	Status
<u>1</u>	0.0.0.0:1813	Disabled
<u>2</u>	0.0.0.0:1813	Disabled
<u>3</u>	0.0.0.0:1813	Disabled
<u>4</u>	0.0.0.0:1813	Disabled
<u>5</u>	0.0.0.0:1813	Disabled

## 48.12. 認証サーバ詳細ステータスの確認

認証サーバ詳細ステータスを確認する手順を説明します。

### 48.12.1. 認証サーバ詳細ステータスのパラメータ

#### RADIUS Authentication Statistics

##### Receive Packets

- 1) **Access Accepts:** このサーバから受信した有効または無効な RADIUS Access-Accept パケットの数を表示します。
- 2) **Access Rejects:** このサーバから受信した有効または無効な RADIUS Access-Reject パケットの数を表示します。
- 3) **Access Challenges:** このサーバから受信した有効または無効な RADIUS Access-Challenge パケットの数を表示します。
- 4) **Malformed Access Response:** このサーバから受信した不正な形式の RADIUS Access-Response パケットの数を表示します。不正な形式のパケットには無効な長さのパケットが含まれます。無効な認証コード、無効な署名属性、不明なタイプのパケットは含まれません。
- 5) **Bad Authenticators:** このサーバから受信した無効な認証コードや無効な署名属性を含む RADIUS Access-Response パケットの数を表示します。
- 6) **Unknown Types:** このサーバの認証ポートから受信した不明なタイプの RADIUS パケットの数を表示します。
- 7) **Packets Dropped:** このサーバの認証ポートから受信した後、何らかの理由で破棄された RADIUS パケットの数を表示します。

##### Transmit Packets

- 1) **Access Requests:** このサーバに送信した RADIUS Access-Request パケットの数を表示します。(再送信したものは含みません。)
- 2) **Access Retransmissions:** このサーバに再送信した RADIUS Access-Request パケットの数を表示します。
- 3) **Pending Requests:** このサーバに送信した後、タイムアウトになっていないか、または応答を受信していないパケットの数を表示します。
- 4) **Timeouts:** このサーバへの認証タイムアウトの数を表示します。

##### Other Info

- 1) **State:** RADIUS サーバの現在の状態を表示します。
  - 表示値は以下の4通りです。
    - ・Disabled – 使用不可になっております。
    - ・Not Ready – サーバは有効ですが、通信が不可です。
    - ・Ready – サーバは使用可能です。
    - ・Dead (X seconds left) – サーバとの通信でタイムアウトが発生したため、dead-time(内の数字)が尽きるまでサーバへの問い合わせを行いません。
- 2) **Round-Trip Time** – 一番最近の、このサーバに対して送られた Access-Request パケットに対する応答時間を表示します。

(次ページに続く)

(前ページの続き)

## RADIUS Accounting Statistics

### Receive Packets

- 1) **Responses:** このサーバから受信した RADIUS パケットの数を表示します。
- 2) **Malformed Responses:** このサーバから受信した不正な形式の RADIUS Access-Response パケットの数を表示します。不正な形式のパケットには無効な長さのパケットが含まれます。無効な認証コード、無効な署名属性、不明なタイプのパケットは含まれません。
- 3) **Bad Authenticators:** このサーバから受信した無効な認証コードや無効な署名属性を含む RADIUS Access-Response パケットの数を表示します。
- 4) **Unknown Types:** このサーバから受信した不明なタイプの RADIUS パケットの数を表示します。
- 5) **Packets Dropped:** このサーバの認証ポートから受信した後、何らかの理由で破棄された RADIUS パケットの数を表示します。

### Transmit Packets

- 1) **Requests:** このサーバに送信した RADIUS パケットの数を表示します。
- 2) **Retransmissions:** このサーバに再送信した RADIUS パケットの数を表示します。
- 3) **Pending Requests:** このサーバに送信した後、タイムアウトになっていないか、または応答を受信していないパケットの数を表示します。
- 4) **Timeouts:** このサーバへの認証タイムアウトの数を表示します。

### Other Info

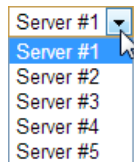
- 1) **State:** RADIUS サーバの現在の状態を表示します。
  - 表示値は以下の4通りです。
    - Disabled – 使用不可になっております。
    - Not Ready – サーバは有効ですが、通信が不可です。
    - Ready – サーバは使用可能です。
    - Dead (X seconds left) – サーバとの通信でタイムアウトが発生したため、dead-time(内の数字)が尽きるまでサーバへの問い合わせを行いません。
- 2) **Round-Trip Time:** 一番最近の、このサーバに対して送られた Access-Request パケットに対する応答時間を表示します。

(次ページに続く)

(前ページの続き)

#### 認証サーバ詳細ステータスの確認手順

- 1) メニューから「Monitor」→「Security」→「AAA」→「RADIUS Details」の順にクリックします。
- 2) ステータスを表示させるサーバの番号を選択します。



- 3) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812)			
Server #1		Auto-refresh <input type="checkbox"/>	Refresh Clear
Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
State	Disabled		
Round-Trip Time	0 ms		

RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)			
Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
State	Disabled		
Round-Trip Time	0 ms		



## 49. RMON 統計の確認

この章では、RMON 統計の確認について説明します。

### 49.1. RMON 統計のパラメータ

- 1) **ID:** エントリのインデックスを表示します。
- 2) **Data Source:** ポート ID を表示します。
- 3) **Drop:** リソース不足のため廃棄されたパケットの総数を表示します。
- 4) **Octets:** 受信したデータの総数(Byte)を表示します。
- 5) **Pkts:** 受信したパケットの総数を表示します。
- 6) **Broad-cast:** 受信したブロードキャストパケットの総数を表示します。
- 7) **Multi-cast:** 受信したマルチキャストパケットの総数を表示します。
- 8) **CRC Errors:** CRC エラーの総数を表示します。
- 9) **Under-size:** 受信したデータのうち、長さが 64Byte 未満のフレームの総数を表示します。
- 10) **Over-size:** 受信したデータのうち、長さが 1518Byte より長いフレームの総数を表示します。
- 11) **Frag.:** 受信したデータのうち、FCS エラーとアラインメントエラーがあった長さが 64Byte 未満のフレームの総数を表示します。
- 12) **Jabb.:** 受信したデータのうち、FCS エラーとアラインメントエラーがあった長さが 64Byte より長いフレームの総数を表示します。
- 13) **Coll.:** コリジョンの総数を表示します。

### RMON統計の確認手順

- 1) メニューから「Monitor」→「Switch」→「RMON」→「Statistics」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

RMON Statistics Status Overview

Auto-refresh ☒ Refresh 

<< >>

Start from Control Index  with  entries per page.

ID	Data Source (ifindex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
6	6	0	726096	3396	229	881	0	0	0	0	0	0	974	896	981	9	523	7
7	7	0	2647974	8556	627	2189	0	0	0	0	0	0	2671	2968	1228	217	357	1109

## 50. LACP ステータスの確認

この章では、LACP ステータスの確認について説明します。

### 50.1. LACP ステータス

本スイッチのLACPステータスを確認する手順を説明します。

#### 50.1.1. LACP ステータスのパラメータ

- 1) **Aggr ID:** LAG(Link Aggregation Group)のアグリゲーション ID を表示します。
- 2) **Partner System ID:** LAG パートナー機器の MAC アドレスを表示します。
- 3) **Partner Key:** LAG パートナー機器が、この LAG に割り当てた鍵を表示します。
- 4) **Last Changed:** 最後に情報を変更した時間を表示します。
- 5) **Local Ports:** この LAG に参加しているポート番号を表示します。

#### MACアドレス情報の確認手順

- 3) メニューから「Monitor」→「LACP」→「System Status」の順にクリックします。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

LACP System Status					Auto-refresh <input checked="" type="checkbox"/>	Refresh
Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports		
LLAG2	78-cd-8e-ae-07-3c	3	0d 02:58:45	5,6		

## 50.2. LACP ポートステータス

本スイッチのLACPポートステータスを確認する手順を説明します。

### 50.2.1. LACP ポートステータスのパラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **LACP:** LACP のステータスを表示します。
  - 表示値は以下の3通りです。
    - ・Yes - LACPが有効で、ポートがリンクアップしています。
    - ・No - LACPが無効になっているか、ポートがリンクダウンしています。
    - ・Backup - バックアップリンクとして動作し、他のポートがリンクダウンした時にLAGに参加します。
- 3) **Key:** このポートに割り当てられている key 番号を表示します。LAG は同じ key 番号を持つポートのみで構成されます
- 4) **Aggr ID:** LAG のアグリゲーション ID を表示します。
- 5) **Partner System ID:** LAG パートナー機器の MAC アドレスを表示します。
- 6) **Partner Port:** LAG パートナー機器のポート番号を表示します。

#### LACPポートステータス情報の確認手順

- 1) メニューから「Monitor」→「LACP」→「Port Status」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

LACP Status					
Auto-refresh <input type="checkbox"/> Refresh					
Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	Yes	4	LLAG2	78-cd-8e-ae-07-3c	5
6	Yes	4	LLAG2	78-cd-8e-ae-07-3c	6
7	No	-	-	-	-
8	Yes	4	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-

### 50.3. LACP ポート統計

本スイッチのLACPポート統計を確認する手順を説明します。

#### 50.3.1. LACP ポート統計のパラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **LACP Transmitted:** 送信した LACP フレームの数を表示します。
- 3) **LACP Received:** 受信した LACP フレームの数を表示します。
- 4) **Discarded:** 破棄された LACP フレームの数を表示します。
  - 表示値は以下の2通りです。
    - ・Unknown                    - 破棄された不明なLACPフレーム
    - ・illegal                    - 破棄された違法なLACPフレーム

#### LACPポートステータス情報の確認手順

- 1) メニューから「Monitor」→「LACP」→「Port Statistics」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

LACP Statistics				
Auto-refresh <input type="checkbox"/> Refresh Clear				
Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	5	0	0
5	46355	46354	0	0
6	15465	15459	0	0
7	0	0	0	0
8	34	42	0	0
9	0	0	0	0
10	0	0	0	0

## 50.4. Loop Protection ステータス (SMCGS18/26/50 のみ対応)

本スイッチのLoop Protectionのステータスを確認する手順を説明します。

### 50.4.1. Loop Protection Status のパラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **Action:** ループが検出された際に実行するアクションを表示します。
- 3) **Transmit:** Loop Protection PDU を送信するかどうかを表示します。
- 4) **Loops:** ループが検出された回数を表示します。
- 5) **Status:** 現在のポートのステータスを表示します。
- 6) **Loop:** 現在ループが検出されているかどうかを表示します。
- 7) **Time of Last Loop:** 最後にループが検出された時間を表示します。

### Loop Protection Statusの確認手順

- 1) メニューから「Monitor」→「Loop Protection」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown+Log	Enabled	1	Down	-	1970-01-02T02:44:35+09:00
2	Shutdown+Log	Enabled	2	Down	-	1970-01-02T02:40:29+09:00
3	Shutdown+Log	Enabled	4	Disabled	Loop	1970-01-02T10:16:33+09:00
4	Shutdown+Log	Enabled	0	Down	-	-
5	Shutdown+Log	Enabled	1	Down	-	1970-01-02T10:00:47+09:00
6	Shutdown+Log	Enabled	0	Up	-	-
7	Shutdown+Log	Enabled	2	Up	-	1970-01-02T10:10:26+09:00
8	Shutdown+Log	Enabled	0	Down	-	-
9	Shutdown+Log	Enabled	0	Down	-	-
10	Shutdown+Log	Enabled	0	Down	-	-
11	Shutdown+Log	Enabled	0	Down	-	-
12	Shutdown+Log	Enabled	0	Down	-	-
13	Shutdown+Log	Enabled	0	Down	-	-
14	Shutdown+Log	Enabled	0	Down	-	-
15	Shutdown+Log	Enabled	0	Down	-	-
16	Shutdown+Log	Enabled	0	Down	-	-
17	Shutdown+Log	Enabled	0	Down	-	-
18	Shutdown+Log	Enabled	0	Down	-	-
19	Shutdown+Log	Enabled	0	Down	-	-
20	Shutdown+Log	Enabled	1	Down	-	1970-01-02T02:43:45+09:00
21	Shutdown+Log	Enabled	0	Down	-	-
22	Shutdown+Log	Enabled	0	Down	-	-
23	Shutdown+Log	Enabled	1	Down	-	1970-01-02T02:43:11+09:00
24	Shutdown+Log	Enabled	3	Down	-	1970-01-02T03:05:50+09:00
25	Shutdown+Log	Enabled	0	Down	-	-
26	Shutdown+Log	Enabled	0	Down	-	-

## 51. スパニングツリーのステータス

この章では、スパニングツリーのステータスの確認について説明します。

### 51.1. ブリッジステータス

本スイッチのブリッジステータスを確認する手順を説明します。

#### 51.1.1. ブリッジステータスのパラメータ

- 1) **MSTI:** MST インスタンス ID を表示します。
- 2) **Bridge ID:** このブリッジの ID を表示します。  
(ブリッジプライオリティと MAC アドレスで構成される)
- 3) **Root ID:** ルートブリッジの Bridge ID を表示します。
- 4) **Root Port:** このスイッチのルートブリッジに一番近いポート番号を表示します。ルートブリッジとはこのポートで通信します。このスイッチ自体がルートブリッジの場合は、“-”が表示されます。
- 5) **Root Cost:** ルートブリッジまでのパスコストを表示します。
- 6) **Topology Flag:** このブリッジの TC フラグの状態を表示します。
- 7) **Topology Change Last:** 最後にトポロジが変更されてからの経過時間を表示します。

#### ブリッジステータスの確認手順

- 1) メニューから「Monitor」→「Spanning Tree」→「Bridge Status」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00:78:CD:8E:B3:39:77	80:00:78:CD:8E:AE:07:3C	5	20000	Steady	0d 00:33:55

- 1) また、MSTIの項目をクリックすることで、より詳細なステータスを確認することが出来ます。(次ページを参照)

**STP Detailed Bridge Status**

- 1) **Bridge Instance:** ブリッジインスタンスを表示します。
- 2) **Regional Root:** CIST リージョナルルート(MST リージョン内の CIST ツリーのルートブリッジ)のブリッジ ID を表示します。
- 3) **Internal Root Cost:** CIST リージョナルルートまでのパスコストを表示します。
- 4) **Topology Change Count:** トポロジの変更が発生した回数を表示します。

**CIST Ports & Aggregations State**

- 1) **Port:** ポート番号を表示します。
- 2) **Port ID:** RSTP で使用されるポート ID を表示します。
- 3) **Role:** ポートの役割を表示します。
- 4) **State:** ポートのステータスを表示します。
  - 表示値は以下の3通りです。
    - ・Discarding: STA設定メッセージを受信しますが、パケットは転送しません。
    - ・Learning: 矛盾している情報を受け取ることなく、フォワードディレイパラメータによって設定されている間隔の間、STA設定メッセージを送信しました。アドレステーブルはクリアされ、再びMACアドレスを学習し始めます。
    - ・Forwarding: パケットを転送し、MACアドレスを学習し続けます。
- 5) **Path Cost:** ルートブリッジまでのパスコストを表示します。
- 6) **Edge:** ポートがエッジポートかどうかを表示します。
- 7) **Point2Point:** 全二重接続の場合は Yes が表示されます
- 8) **Uptime:** ポートがリンクアップしてからの経過時間を表示します。

STP Detailed Bridge Status

Auto-refresh ☐ Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	80:00:78:CD:8E:B3:39:77
Root ID	80:00:78:CD:8E:AE:07:3C
Root Cost	20000
Root Port	5
Regional Root	80:00:78:CD:8E:B3:39:77
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	132
Topology Change Last	0d 00:37:34

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point2Point	Uptime
4	128:004	DesignatedPort	Forwarding	200000	Yes	Yes	0d 00:37:34
5	128:005	RootPort	Forwarding	20000	No	Yes	0d 00:37:34
6	128:006	AlternatePort	Discarding	20000	No	Yes	0d 00:37:34

## 51.2. STP ポートステータス

本スイッチのSTPポートステータスを確認する手順を説明します。

### 51.2.1. STP ポートステータスのパラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **CIST Role:** ポートの役割を表示します。
  - 表示値は以下の5通りです。
    - ・Alternate Port - Root Portの次にコストが小さいポートでルートブリッジまでの代替パスのポート
    - ・Backup Port - Designated Portが指定する経路の代替パスのポート
    - ・Root Port - ルートブリッジまでの到達コストが最小値のポート
    - ・Designated Port- ルートブリッジからのデータを転送するポート
    - ・Disabled - ポートがリンクダウンしているか、STPが無効になっています。
- 3) **CIST State:** このスイッチでのルートブリッジに一番近いポート番号を表示します
  - 表示値は以下の3通りです。
    - ・Discarding - STA設定メッセージを受信しますが、パケットは転送しません。
    - ・Learning - 矛盾している情報を受け取ることなく、フォワードディレイパラメータによって設定されている間隔の間、STA設定メッセージを送信しました。アドレステーブルはクリアされ、再びMACアドレスを学習し始めます。
    - ・Forwarding - パケットを転送し、MACアドレスを学習し続けます。
- 4) **Uptime:** ポートがリンクアップしてからの経過時間を表示します。

#### STPポートステータスの確認手順

- 1) メニューから「Monitor」→「Spanning Tree」→「Port Status」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

STP Port Status			
Auto-refresh <input type="checkbox"/>			Refresh
Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	DesignatedPort	Forwarding	0d 00:09:28
5	RootPort	Forwarding	0d 00:25:20
6	AlternatePort	Discarding	0d 00:25:26
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-



### 51.3. STP ポート統計

本スイッチのSTPポート統計を確認する手順を説明します。

#### 51.3.1. STP ポート統計のパラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **MSTP:** 送受信した MSTP BPDU の合計を表示します。
- 3) **RSTP:** 送受信した RSTP BPDU の合計を表示します。
- 4) **STP:** 送受信した STP BPDU の合計を表示します。
- 5) **TCN:** 送受信した TCN BPDU の合計を表示します。
- 6) **Discarded Unknown:** 受信後に破棄された未知の BPDU の合計を表示します。
- 7) **Discarded Illegal:** 受信後に破棄された違法な BPDU の合計を表示します。

#### STPポート統計の確認手順

- 1) メニューから「Monitor」→「Spanning Tree」→「Port Statistics」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

STP Statistics										
Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
4	0	0	871	0	0	0	0	0	0	0
5	0	0	2	19	0	0	1366	0	0	0
6	0	0	3	5	0	0	1354	0	0	0

## 52. MVR ステータス

この章では、MVR(マルチキャスト VLAN レジストレーション)のステータスの確認について説明します。

### 52.1. MVR ステータス

本スイッチのMVRステータスを確認する手順を説明します。

#### 52.1.1. MVR ステータスのパラメータ

- 1) **VLAN ID:** MVR でマルチキャスト用として使用している VLAN の ID
- 2) **V1 Reports Received:** 受信した IGMP V1 メンバーシップレポートの総数
- 3) **V2 Reports Received:** 受信した IGMP V2 メンバーシップレポートの総数
- 4) **V3 Reports Received:** 受信した IGMP V3 メンバーシップレポートの総数
- 5) **V2 Leaves Received:** 受信した IGMP V2 グループリーブメッセージの総数

#### MVRステータスの確認手順

- 1) メニューから「Monitor」→「MVR」→「Statistics」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

MVR Statistics					Auto-refresh <input type="checkbox"/>		Refresh	Clear
VLAN ID	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received				
100	0	0	25	0				

## 52.2. MVR グループステータス (SMCGS10 のみ対応)

本スイッチのMVRのグループ毎のステータスを確認する手順を説明します。

### 52.2.1. MVR グループステータスのパラメータ

- 1) **VLAN ID:** MVR でマルチキャスト用として使用している VLAN の ID を表示します。
- 2) **Groups:** マルチキャストグループアドレスを表示します。最大 128 のグループが登録されます。
- 3) **Port Members:** マルチキャストグループに参加しているポートを表示します

#### MVRグループステータスの確認手順

- 1) メニューから「Monitor」→「MVR」→「Group Information」の順にクリックします。
- 2) ページに表示させる VLAN ID と MAC Address 及び表示範囲を選択します。
- 3) ページをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。
 

|<<

- 先頭のページを表示します。

>>|

- 次ページを表示します。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

### MVR Groups Information

Auto-refresh ☐


|<<

>>|

Start from VLAN  add group address  with  entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
100	239.255.255.1				✓						

### 52.3. MVR Channels ステータス (SMCGS18/26/50 のみ対応)


本スイッチのMVRのグループ毎のステータスを確認する手順を説明します。

#### 52.3.1. MVR グループステータスのパラメータ


- 1) **VLAN ID:** MVR でマルチキャスト用として使用している VLAN の ID を表示します。
- 2) **Groups:** マルチキャストグループアドレスを表示します。最大 128 のグループが登録されます。
- 3) **Port Members:** マルチキャストグループに参加しているポートを表示します

#### MVRグループステータスの確認手順

- 1) メニューから「Monitor」→「MVR」→「MVR Channel Groups」の順にクリックします。
- 2) ページに表示させる VLAN ID と MAC Address 及び表示範囲を選択します。
- 3) ページをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。
 



- 先頭のページを表示します。



- 次ページを表示します。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

MVR Channels (Groups) Information

Auto-refresh ☐ Refresh  

Start from VLAN  and Group Address  with  entries per page.

		Port Members																									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
No more entries																											

## 52.4. MVR SFM Information (SMCGS18/26/50 のみ対応)

本スイッチのMVR SFM Informationを確認する手順を説明します。

### 52.4.1. MVR SFM Information パラメータ

- 1) **VLAN ID:** MVR でマルチキャスト用として使用している VLAN の ID を表示します。
- 2) **Group:** マルチキャストグループアドレスを表示します。
- 3) **Port:** ポート番号を表示します。
- 4) **Mode:** モードを表示します。
- 5) **Source Address:** 送信元 IP アドレスを表示します。
- 6) **Type:** タイプを表示します。

#### MVR SFM Informationの確認手順

- 1) メニューから「Monitor」→「MVR」→「MVR SFM Information」の順にクリックします。
- 2) ページに表示させる VLAN ID と MAC Address 及び表示範囲を選択します。

**MVR SFM Information**
Auto-refresh ☐
Refresh
|<<
>>

Start from VLAN  and Group Address  with  entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

## 53. IGMP スヌーピングステータス

この章では、IGMP スヌーピングのステータスの確認について説明します。

### 53.1. IGMP スヌーピングステータス

本スイッチのIGMPスヌーピングステータスを確認する手順を説明します。

#### 53.1.1. IGMP スヌーピングステータスのパラメータ

##### Statistics

- 1) **VLAN ID:** VLAN ID を表示します。
- 2) **Querier Version:** クエリアとして動作する時の IGMP バージョンを表示します。
- 3) **Host Version:** IGMP proxy モードで動作する時の IGMP バージョンを表示します。
- 4) **Querier Status:** クエリアとして動作しているかそうでないかを表示します。
  - 表示値は以下の2通りです。
    - **Active:** クエリアとして動作しており、配下のホストがマルチキャストストリームの受信要求を出しているかどうかを定期的にチェックします。
    - **IDLE:** クエリアとしては動作していません。
- 5) **Querier Transmitted:** 送信した IGMP クエリの総数を表示します。
- 6) **Querier Received:** 受信した IGMP クエリの総数を表示します。
- 7) **V1 Reports Received:** 受信した IGMP V1 メンバーシップレポートの総数を表示します。
- 8) **V2 Reports Received:** 受信した IGMP V2 メンバーシップレポートの総数を表示します。
- 9) **V3 Reports Received:** 受信した IGMP V3 メンバーシップレポートの総数を表示します。
- 10) **V2 Leaves Received:** 受信した IGMP V2 グループリーブメッセージの総数を表示します。

##### Router Port

- 1) **Port:** ポート番号
- 2) **Status:** マルチキャストルータが検出されたポートまたは、Router Port に設定したポートを表示します。

#### IGMP スヌーピングステータスの確認手順

- 1) メニューから「Monitor」→「IPMC」→「IGMP Snooping」→「Status」の順にクリックします。

IGMP Snooping Status

Auto-refresh ☐ Refresh Clear

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v3	v3	IDLE	7	0	0	0	64	0

Router Port

Port	Status
1	-
2	-
3	-
4	Static
5	-
6	-
7	-
8	-
9	-
10	-

## 53.2. IGMP グループステータス

本スイッチのIGMPグループステータスを確認する手順を説明します。

### 53.2.1. IGMP グループステータスのパラメータ

- 1) **VLAN ID** : VLAN ID が表示されます。  
IGMP グループを一つも学習していない場合は、” *No more entries* ”が表示されます。
- 2) **Groups** : マルチキャストグループの IP アドレスを表示します。
- 3) **Port Members** : マルチキャストグループに参加しているポートを表示します。

#### IGMP グループステータスの確認手順

- 1) メニューから「Monitor」→「IPMC」→「IGMP Snooping」→「Groups Information」の順にクリックします。
- 2) ページに表示させる VLAN ID とアドレス及び表示範囲を選択します。
- 3) ページをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。  

|<<

- 先頭のページを表示します。

>>|

- 次ページを表示します。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

### IGMP Snooping Groups Information

Auto-refresh ☒

Refresh

|<<

>>|

Start from VLAN  and group address  with  entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
1	239.255.0.1			✓	✓						

### 53.3. IGMP SSM ステータス

本スイッチのIGMP SSM(Source-Specific-Multicast)ステータスを確認する手順を説明します。

#### 53.3.1. IGMP SSM ステータスのパラメータ

##### Statistics

- 1) **VLAN ID:** VLAN ID が表示されます。  
IGMP グループを一つも学習していない場合は、”No more entries”が表示されます。
- 2) **Groups:** マルチキャストグループの IP アドレスを表示します。
- 3) **Port No.:** マルチキャストグループに参加しているポート番号を表示します。
- 4) **Mode:** フィルターモードを表示します。
  - 表示値は以下の2通りです。
    - ・INCLUDE – Source Addressに表示されているIPアドレスを送信元とするパケットだけを受信します。
    - ・EXCLUDE – Source Addressに表示されているIPアドレスを送信元とするパケット以外を受信します。
- 5) **Source Address:** 送信元の IP アドレス(最大 128 アドレス)を表示します。
- 6) **Type:** IGMP プロファイルのタイプを表示します。
  - 表示値は以下の2通りです。
    - ・Allow – Source Addressに表示されているIPアドレスを送信元とするパケットを許可します。
    - ・Deny – Source Addressに表示されているIPアドレスを送信元とするパケットは拒否します。

##### IGMP SSMステータスの確認手順

- 1) メニューから「Monitor」→「IPMC」→「IGMP Snooping」→「IPv4 SSM Information」の順にクリックします。
- 2) ページに表示させる VLAN ID とアドレス及び表示範囲を選択します。
- 3) ページをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。
 

|<<

 - 先頭のページを表示します。  

>>|

 - 次ページを表示します。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

**IGMP SSM Information**

Auto-refresh ☐ Refresh |<< >>|

Start from VLAN  and Group  with  entries per page.

VLAN ID	Group	Port No.	Mode	Source Address	Type
1	239.255.0.1	3	Exclude	None	Deny
1	239.255.0.1	4	Exclude	None	Deny
1	239.255.222.1	4	Exclude	None	Deny
1	239.255.255.1	3	Exclude	None	Deny
1	239.255.255.250	3	Exclude	None	Deny
1	239.255.255.250	4	Exclude	None	Deny



## 54. MLD スヌーピングステータス

この章では、MLD スヌーピングのステータスの確認について説明します。

### 54.1. MLD スヌーピングステータス

本スイッチのMLDスヌーピングステータスを確認する手順を説明します。

#### 54.1.1. MLD スヌーピングステータスのパラメータ

##### Statistics

- 1) **VLAN ID:** VLAN ID が表示されます。
- 2) **Querier Version:** クエリアとして動作する時の MLD バージョンを表示します。
- 3) **Host Version:** MLD proxy モードで動作する時の MLD バージョンを表示します。
- 4) **Querier Status:** クエリアとして動作しているかそうでないかを表示します。
  - 表示値は以下の2通りです。
    - ・Active – クエリアとして動作しており、配下のホストがマルチキャストストリームの受信要求を出しているかどうかを定期的にチェックします。
    - ・IDLE – クエリアとしては動作しておりません。
- 5) **Querier Transmitted:** 送信した MLD クエリの総数を表示します。
- 6) **Querier Received:** 受信した MLD クエリの総数を表示します。
- 7) **V1 Reports Received:** 受信した MLD V1 メンバーシップレポートの総数を表示します。
- 8) **V2 Reports Received:** 受信した MLD V2 メンバーシップレポートの総数を表示します。
- 9) **V1 Leaves Received:** 受信した MLD V1 グループリーブメッセージの総数を表示します。

##### Router Port

- 1) **Port:** ポート番号
- 2) **Status:** マルチキャストルータが検出されたポートまたは、Router Port に設定したポートを表示します。

#### MLD スヌーピングステータスの確認手順

- 1) メニューから「Monitor」→「IPMC」→「MLD Snooping」→「Status」の順にクリックします。

MLD Snooping Status								
Auto-refresh <input type="checkbox"/> Refresh Clear								
Statistics								
VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
Router Port								
Port	Status							
1	-							
2	-							
3	-							
4	-							
5	-							
6	-							
7	-							
8	-							
9	-							
10	-							

## 54.2. MLD グループステータス

本スイッチのMLDグループステータスを確認する手順を説明します。

### 54.2.1. MLD グループステータスのパラメータ

- 1) **VLAN ID** : VLAN ID が表示されます。  
MLD グループを一つも学習していない場合は、” *No more entries* ”が表示されます。
- 2) **Groups** : マルチキャストグループの IP アドレスを表示します。
- 3) **Port Members** : マルチキャストグループに参加しているポートを表示します。

#### MLD グループステータスの確認手順

- 1) メニューから「Monitor」→「IPMC」→「MLD Snooping」→「Groups Information」の順にクリックします。
- 2) ページに表示させる VLAN ID とアドレス及び表示範囲を選択します。
- 3) ページをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。  

|<<

- 先頭のページを表示します。

>>|

- 次ページを表示します。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

### MLD Snooping Groups Information

Auto-refresh ☐
Refresh

|<<

>>|

Start from VLAN  and group address  with  entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
No more entries											

### 54.3. MLD SSM ステータス

本スイッチのMLD SSM(Source-Specific-Multicast)ステータスを確認する手順を説明します。

#### 54.3.1. MLD SSM ステータスのパラメータ

##### Statistics

- 1) **VLAN ID** : VLAN ID が表示されます。  
MLD グループを一つも学習していない場合は、” *No more entries* ”が表示されます。
- 2) **Groups**: マルチキャストグループの IP アドレスを表示します。
- 3) **Port No.**: マルチキャストグループに参加しているポート番号を表示します。
- 4) **Mode**: フィルターモードを表示します。
  - 表示値は以下の2通りです。
    - ・INCLUDE – Source Addressに表示されているIPアドレスを送信元とするパケットだけを受信します。
    - ・EXCLUDE – Source Addressに表示されているIPアドレスを送信元とするパケット以外を受信します。
- 5) **Source Address**: 送信元の IP アドレス(最大 128 アドレス)を表示します。
- 6) **Type**: MLD プロファイルのタイプを表示します。
  - 表示値は以下の2通りです。
    - ・Allow – Source Addressに表示されているIPアドレスを送信元とするパケットを許可します。
    - ・Deny – Source Addressに表示されているIPアドレスを送信元とするパケットは拒否します。

##### MLD SSMステータスの確認手順

- 1) メニューから「Monitor」→「IPMC」→「MLD Snooping」→「IPv6 SSM Information」の順にクリックします。
- 2) ページに表示させる VLAN ID とアドレス及び表示範囲を選択します。
- 3) ページをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。
 

|<<

 - 先頭のページを表示します。  

>>|

 - 次ページを表示します。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

**MLD SSM Information**

Auto-refresh ☐ Refresh |<< >>|

Start from VLAN  and Group  with  entries per page.

VLAN ID	Group	Port No.	Mode	Source Address	Type
No more entries					

## 55. LLDP ステータス

この章では、LLDP ステータスの確認について説明します。

### 55.1. LLDP ステータス

本スイッチのLLDPステータスを確認する手順を説明します。

#### 55.1.1. LLDP ステータスのパラメータ

- 1) **Local Port:** 隣接デバイスに接続している本スイッチのポートを表示します。
- 2) **Chassis ID:** 隣接デバイスの MAC アドレスを表示します。
- 3) **Remote Port ID:** 本スイッチと接続している隣接デバイスのポートを表示します。
- 4) **System Name:** 隣接デバイスに設定されている名前を表示します。
- 5) **Port Description:** 隣接デバイスのポートの説明文を表示します。
- 6) **System Capabilities:** 隣接デバイスの機能を表示します。  
表示されている機能が使用可能な場合は(+)が、使用不可の場合は(-)が付けられます。
- 7) **Management Address** - 隣接デバイスの管理アドレスを表示します。IPv4 アドレスを持たないデバイスの場合、CPU もしくは接続されているポートの MAC アドレスが表示されます。  
隣接デバイスが WEB ブラウザでの管理アクセスに対応している場合、表示されている管理アドレスをクリックすることでデバイスの管理画面に入ることが出来ます。

#### LLDPステータスの確認手順

- 1) メニューから「Monitor」→「LLDP」→「Neighbors」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。
- 3) 隣接デバイスの 管理アドレス(Management Address) をクリックすることで、隣接デバイスの管理画面に入ることが出来ます。

The screenshot shows the 'LLDP Neighbour Information' page with a table of neighbors. A red box highlights the 'Management Address' column, specifically the entry '192.168.1.26 (IPv4)'. A red arrow points from this entry to the '隣接デバイス 管理画' (Neighbor Device Management Page) shown below. The management page is for the 'SMCGS-26C™ GigaBit Ethernet Switch' and features a 'Port State Overview' section with a diagram of the switch's ports.

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 5	00-1E-94-17-00-3F	Port 01	IPS-2042P	100TX	Bridge(+)	192.168.10.1 (IPv4) OID:
Port 6	78-CD-8E-AE-07-3C	8	SMCGS-26C	Port #8	Bridge(+)	192.168.1.26 (IPv4)

## 55.2. LLDP-MED ステータス

本スイッチのLLDP-MEDステータスを確認する手順を説明します。

### 55.2.1. LLDP-MED ステータスのパラメータ

- 1) **Port:** LLDP フレームを受信したポートを表示します。
- 2) **Device Type:** LLDP-MED 対応デバイスは主に 2 つのタイプから成ります。
  - i) **LLDP-MED Network Connectivity Devices** – Network Connectivity Deviceは End Point Deviceがネットワークにアクセスできるようにします。  
以下のデバイスが該当します。
    - ・スイッチ/ルータ
    - ・ブリッジ
    - ・リピータ
    - ・無線LANアクセスポイント
    - ・その他、TIA-1057によって定義されるIEEE 802.1ABとLLDP-MED機能をサポートしていて、Ethernetフレームを転送出来る装置
  - ii) **LLDP-MED Endpoint Device** –Endpoint Deviceは次の3つのLLDP-MEDクラスのうち1つに属します。
    - ・Class1 Generic Endpoint –基本的にLLDPをベースに動作しますが、IP メディアをサポートせず、またエンドユーザーの通信機器として動作しません。クラス1のエンドポイントは、IP通信コントローラ、通信関連のサーバまたはTIA-1057で定義されるLLDPサービスを必要とする他のデバイスが該当します。  
このクラスで定義されるディスカバリサービスには、LAN構成、設置場所、ネットワークポリシー、パワーマネジメント、Inventoryマネジメントが含まれます。
    - ・Class2 Media Endpoint – クラス1の機能に加えてメディアストリーミング機能をサポートし、特定のエンドユーザーと関連する場合があります。クラス2のエンドポイントは、音声/メディアゲートウェイ、カンファレンスブリッジ、メディアサーバー等が該当します。
    - ・Class3 Communication Endpoint – エンドユーザーIP通信をサポートします。クラス1とクラス2の機能に加えてロケーション識別、レイヤ2スイッチサポート、機器情報管理を提供します。  
クラス3のエンドポイントは、IP電話やソフトフォンなどが該当します。
- 3) **LLDP-MED Capabilities:** 隣接デバイスについて以下の情報を表示します。
  - ・LLDP-MED Capabilities
  - ・Network Policy
  - ・Location Identification
  - ・Extended Power vis MDI
  - ・Extended Power vis MDI
  - ・Inventory
  - ・Reserved
- 4) **Application Type:** MED Endpoint または Network Connectivity Device のアプリケーションタイプを表示します。表示されるアプリケーションタイプの詳細につきましては 19.2.1 章「LLDP-MED のパラメータ」をご参照下さい。

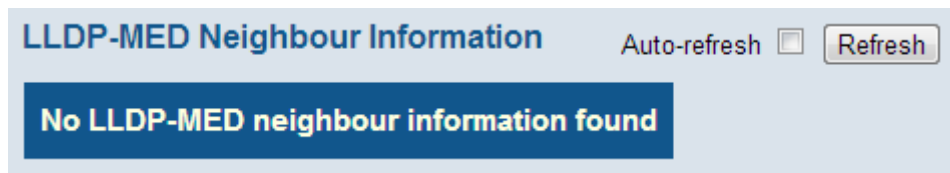
(次ページに続く)

**(前ページの続き)**

- 5) **Policy:** この項目には以下のいずれか一つが表示されます。
  - Unknown        - 定義されていない不明なポリシー
  - Defined        - 定義されているポリシー
- 6) **Tag:** Tag VLAN か Untag VLAN か表示します。
- 7) **VLAN ID:** VLAN ID を表示します。
- 8) **Priority:** 特定のアプリケーションタイプに関連付けられた優先度を表示します。
- 9) **DSCP:** 特定のアプリケーションタイプに関連付けられている DSCP 値を表示します。

**LLDP-MEDステータスの確認手順**

- 1) メニューから「Monitor」→「LLDP」→「LLDP-MED Neighbors」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。



### 55.3. LLDP PoE ステータス

本スイッチのLLDP PoEステータスを確認する手順を説明します。

#### 55.3.1. LLDP PoE ステータスのパラメータ

- 1) **Local Port:** LLDP フレームを受信したポートを表示します。
- 2) **Power Type:** デバイスの種類が、PSE(Power Sourcing Entity)か PD(Power Device)かどうかを表示します。
- 3) **Power Source:** デバイスが使用している電源を表示します。
- 4) **Power Priority:** 給電の優先度を表示します。
- 5) **Maximum Power:** PD が必要とする最大電力または、現在の構成に基づくケーブル長で PSE が給電することが出来る最小限の値を表示します。

#### LLDP PoEステータスの確認手順

- 1) メニューから「Monitor」→「LLDP」→「PoE」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

LLDP Neighbour Power Over Ethernet Information Auto-refresh ☐ Refresh

Local Port	Power Type	Power Source	Power Priority	Maximum Power
No PoE neighbour information found				

## 55.4. LLDP EEE ステータス

本スイッチのLLDP EEE (Energy Efficient Ethernet) ステータスを確認する手順を説明します。

### 55.4.1. LLDP EEE ステータスのパラメータ


- 1) **Local Port:** LLDP フレームを受信したポートを表示します。
- 2) **Tx Tw:** 隣接ポートにおいて LPI (Link Power Idle) アイドル状態回復から、送信開始までの遅延時間を表示します。※=IEEE802.3az Tw\_sys\_tx
- 3) **Rx Tw:** 隣接ポートにおいてアイドル状態回復から、レシーバ(受信機)回復までのトランスミッタ(送信機)待ち時間を表示します。 ※=IEEE802.3az Tw\_sys\_rx
- 4) **Fallback Receive Tw:** 隣接ポートから自ポートへの省エネのレベル通知(Tw\_sys\_tx)を表示します。

※ 本パラメータをサポートしていない場合は、Tw\_sys\_tx初期値を使用します。

- 5) **Echo Tx Tw:** 自ポートの Tx Tw 値を示す隣接ポートからのエコー(応答値)を表示します。
- 6) **Echo Rx Tw:** 自ポートの Rx Tw 値を示す隣接ポートからのエコー(応答値)を表示します。
- 7) **Resolved Tx Tw:** LLDP (EEE 情報含む) ネゴシエーションにより決まった、実際の Tx Tw 時間を表示します。
- 8) **Resolved Rx Tw:** LLDP (EEE 情報含む) ネゴシエーションにより決まった、実際の Rx Tw 時間を表示します。
- 9) **EEE activated:** 隣接デバイスにて EEE サポート有無を表示します。

### LLDP EEEステータスの確認手順

- 1) メニューから「Monitor」→「LLDP」→「EEE」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

LLDP Neighbors EEE Information								Auto-refresh <input checked="" type="checkbox"/>	Refresh
Local Port	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE activated	
1	17	17	17	17	17	17	17		



## 55.5. LLDP ポート統計

本スイッチのLLDPポート統計を確認する手順を説明します。

### 55.5.1. LLDP ポート統計のパラメータ

#### Global Counters

- 1) **Neighbor entries were last changed at:** LLDP エントリが最後に更新された時間と、それから経過した時間を表示します。
- 2) **Total Neighbors Entries Added:** 起動してから追加された LLDP エントリの数を表示します。
- 3) **Total Neighbors Entries Deleted:** 何らかの理由で削除された LLDP エントリの数を表示します。
- 4) **Total Neighbors Entries Dropped:** LLDP エントリテーブルが満杯のため LLDPDU を破棄した回数を表示します。
- 5) **Total Neighbors Entries Aged Out:** TTL が期限切れになったため LLDP エントリを削除した回数を表示します。

#### LLDP Statistics

- 1) **Local Port:** ポート番号を表示します。
- 2) **Tx Frames:** 送信した LLDPDU の総数を表示します。
- 3) **Rx Frames:** 受信した LLDPDU の総数を表示します。
- 4) **Rx Errors:** 受信した LLDPDU のうち、何らかのエラーを含んでいた物の数を表示します。
- 5) **Frames Discarded:** 不正な形式の TLV のため破棄された LLDPDU の総数を表示します。
- 6) **TLVs Unrecognized:** 破棄されたフレームの数を表示します。
- 7) **Age-Outs:** TTL が期限切れになったため LLDP エントリを削除した回数を表示します。

#### LLDPポート統計の確認手順

- 1) メニューから「Monitor」→「LLDP」→「Port Statistics」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

Global Counters									Auto-refresh <input type="checkbox"/> Refresh Clear	
Neighbour entries were last changed at 1970-01-01T00:05:23+00:00 (335027 sec. ago)										
Total Neighbours Entries Added		1								
Total Neighbours Entries Deleted		0								
Total Neighbours Entries Dropped		0								
Total Neighbours Entries Aged Out		0								

LLDP Statistics								
Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	11166	11168	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	171	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

## 56. PoE ステータス

この章では、PoE ステータスの確認について説明します。

### 56.1. PoE ステータス

本スイッチのPoEステータスを確認する手順を説明します。

#### 56.1.1. PoE ステータスのパラメータ

- 1) **Local Port:** ポート番号を表示します。
- 2) **PD Class:** 受電機器(PD)のクラスを表示します。

なお、各クラスの給電仕様は以下の通りです。

IEEE クラス	PSE 側出力	PD 側入力電力
0	15.4 W	0.44 ~ 12.95 W
1	4.0 W	0.44 ~ 3.84 W
2	7.0 W	3.84 ~ 6.49 W
3	15.4 W	6.49 ~ 12.95 W
4	30 W	12.95W ~ 25.5W

- 3) **Power Requested:** 受電機器(PD)が必要とする電力を表示します。
- 4) **Power Allocated:** スイッチが受電機器(PD)に割り当てた電力を表示します。
- 5) **Power Used:** 受電機器(PD)が使用している電力を表示します。
- 6) **Current Used:** 受電機器(PD)に出力している電流を表示します。
- 7) **Priority:** 給電の優先度を表示します。
- 8) **Port Status:** PoE サービスのステータスを表示します。

#### PoEステータスの確認手順

- 1) メニューから「Monitor」→「PoE」の順にクリックします。
- 2) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

Power Over Ethernet Status							
						Auto-refresh <input type="checkbox"/>	Refresh
Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	1	4 [W]	4 [W]	2.1 [W]	38 [mA]	Low	PoE turned ON
Total		4 [W]	4 [W]	2.1 [W]	38 [mA]		

## 57. MAC Address Table

この章では、MAC Address Table の確認について説明します。



### 57.1. MAC Address Table

本スイッチのMAC Address Tableを確認する手順を説明します。

#### 57.1.1. MAC Address Table のパラメータ

- 1) **Type** : MAC アドレスが登録された方法を表示します。
- 2) **VLAN**: VLAN ID を表示します。
- 3) **MAC Address**: MAC アドレスを表示します。
- 4) **Port Members**: ポート番号を表示します。

#### PoEステータスの確認手順

- 1) メニューから「Monitor」→「MAC Table」の順にクリックします。
- 2) ページに表示させる VLAN ID と MAC Address 及び表示範囲を選択します。
- 3) MAC Address Table をスクロールさせるには、画面右上の矢印ボタンを使用して下さい。
  -  - 先頭のページを表示します。
  -  - 次ページのMAC Address Tableを表示します。
- 4) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。  
また、Clear ボタンをクリックすることで、全てのステータスが消去されます。

**MAC Address Table** Auto-refresh ☐ Refresh Clear |<< >>

Start from VLAN  and MAC address  with  entries per page.

Type	VLAN	MAC Address	Port Members										
			CPU	1	2	3	4	5	6	7	8	9	10
Static	1	01-00-5E-7F-FF-FA		✓									

## 58. VLANs

この章では、VLAN ステータスの確認について説明します。

### 58.1. VLAN メンバーシップ

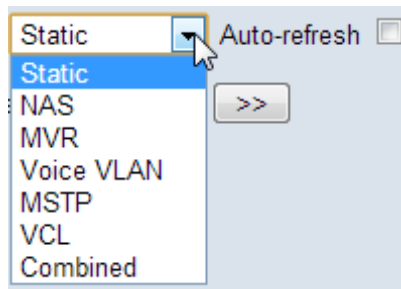
本スイッチのVLANメンバーシップを確認する手順を説明します。



#### 58.1.1. VLAN メンバーシップのパラメータ

- 1) **VLAN ID:** VLAN ID を表示します。
- 2) **Port Members:** VLAN に所属しているポート番号を表示します。

#### VLANメンバーシップの確認手順

- 1) メニューから「Monitor」→「VLANs」→「VLAN Membership」の順にクリックします。
- 2) プルダウンメニューから、VLAN メンバーシップを表示させたいソフトウェアモジュールを選択します。



- 3) ページに表示させる VLAN ID と表示範囲を選択します。
- 4) VLAN メンバーシップをスクロールさせるには、画面右上の矢印ボタンを使用して下さい。
  -  - 先頭のページを表示します。
  -  - 次ページのVLANを表示します。
- 5) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

**VLAN Membership Status for Static user**    Static    Auto-refresh    Refresh

Start from VLAN  with  entries per page.    <<<    >>>

VLAN ID	Port Members									
	1	2	3	4	5	6	7	8	9	10
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2								✓	✓	✓

## 58.2. VLAN ポートステータス

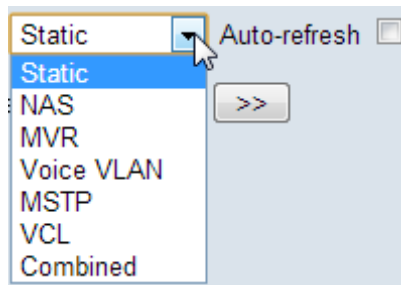
本スイッチのVLANポートステータスを確認する手順を説明します。

### 58.2.1. VLAN ポートステータスのパラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **PVID:** PVID を表示します。
- 3) **Port Type:** ポートタイプを表示します。
- 4) **Ingress Filtering:** Ingress フィルタリングの有効/無効を表示します。
- 5) **Frame Type:** ポートが許可するフレームのタイプを表示します。  
 “Tagged”と表示されている場合は、VLAN タグ付きフレームは受信しますが、タグ無しフレームは破棄されます。
- 6) **Tx Tag:** 出力するフレームに対してタグ付けを行うかどうかを表示します。
- 7) **UVID:** ここで表示されている VID と一致した場合はフレームから VLAN タグを取り外して転送します。
- 8) **Conflicts:** このポートに対する VLAN の設定に矛盾が生じている場合には”Yes”が表示されます。

#### VLANポートステータスの確認手順

- 1) メニューから「Monitor」→「VLANs」→「VLAN Port」の順にクリックします。
- 2) プルダウンメニューから、VLAN ポートステータスを表示させたいソフトウェアモジュールを選択します。



- 3) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	C-Port	Disabled	All	Untag_this	1	No
2	1	C-Port	Disabled	All	Untag_this	1	No
3	1	C-Port	Disabled	All	Untag_this	1	No
4	1	C-Port	Disabled	All	Untag_this	1	No
5	1	C-Port	Disabled	All	Untag_this	1	No
6	1	C-Port	Disabled	All	Untag_this	1	No
7	1	C-Port	Disabled	All	Untag_this	1	No
8	1	C-Port	Disabled	All	Untag_this	1	No
9	1	C-Port	Disabled	All	Untag_this	1	No
10	1	C-Port	Disabled	All	Untag_this	1	No

## 59. MAC ベース VLAN ステータス

この章では、MAC ベース VLAN の確認について説明します。

### 59.1. MAC ベース VLAN ステータス

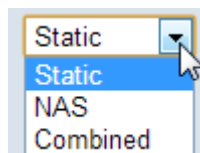
本スイッチのMACベースVLANステータスを確認する手順を説明します。

#### 59.1.1. MAC ベース VLAN ステータスのパラメータ

- 1) **MAC Address:** MAC アドレスを表示します。
- 2) **VLAN ID:** 関連付けされている VLANID を表示します。
- 3) **Port Members:** 割り当てられているポートを表示します。

#### VLANポートステータスの確認手順

- 1) メニューから「Monitor」→「VCL」→「MAC-based VLAN」の順にクリックします。
- 2) プルダウンメニューから、VLAN ポートステータスを表示させたいソフトウェアモジュールを選択します。



- 3) Auto-refresh をクリックすると、表示されたデータをおよそ 5 秒間隔で再表示します。あるいは Refresh ボタンをクリックすると、直ちに画面を最新情報に更新します。

MAC-based VLAN Membership Configuration for User Static

Static

Auto-refresh

Refresh

		Port Members									
MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10
00-00-00-00-00-00	1										✓

## 60. Diagnostics

この章では、スイッチの診断機能について説明します。

### 60.1. Ping/Ping6

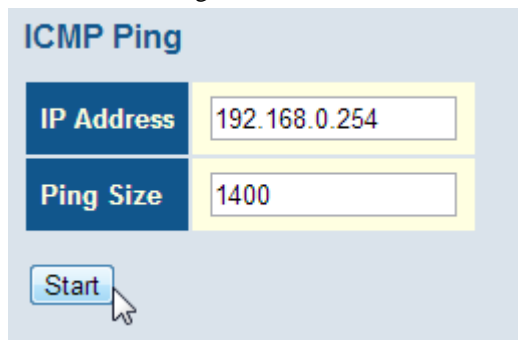
PingによるIPv4またはIPv6レベルでの疎通確認を行う手順を説明します。

#### 60.1.1. Ping/Ping6 のパラメータ

- 1) **IP Address:** 宛先の IP アドレスを指定します。
- 2) **Ping Size:** ICMP パケットのペイロードサイズを指定します。  
(設定値の範囲: 8 – 1400byte)

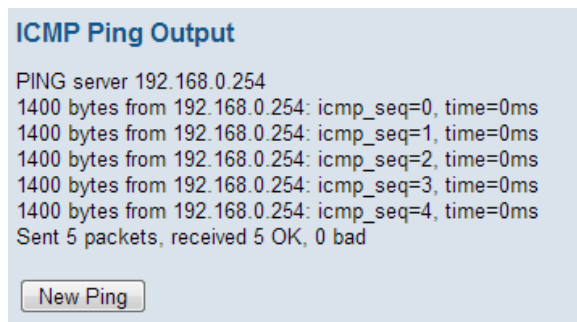
#### Ping/Ping6の確認手順

- 1) メニューから「Diagnostics」→「Ping」または「Ping6」の順にクリックします。
- 2) IP Address と Ping Size を入力し、**Start** をクリックしてください。



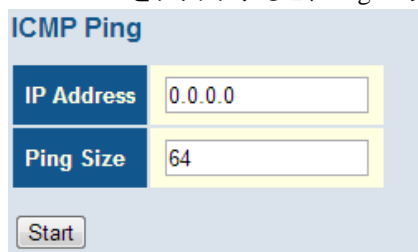
The screenshot shows the 'ICMP Ping' configuration interface. It has two input fields: 'IP Address' with the value '192.168.0.254' and 'Ping Size' with the value '1400'. Below these fields is a 'Start' button, which is being clicked by a mouse cursor.

- 3) Ping の結果が表示されます。



The screenshot shows the 'ICMP Ping Output' screen. It displays the results of a ping test to the server 192.168.0.254. The output shows five successful pings, each with a size of 1400 bytes and a time of 0ms. At the bottom, it states 'Sent 5 packets, received 5 OK, 0 bad'. There is a 'New Ping' button at the bottom.

- 4) **New Ping** をクリックすると、Ping パラメータの入力画面に戻ります。



The screenshot shows the 'ICMP Ping' configuration interface again, but with default values. The 'IP Address' field now contains '0.0.0.0' and the 'Ping Size' field contains '64'. The 'Start' button is visible at the bottom.

## 60.2. ケーブル診断

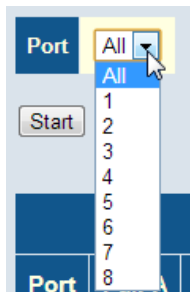
VeriPHYでは、指定したポートに接続されているLANケーブルの結線の確認や、線路長の測定をします。

### 60.2.1. ケーブル診断のパラメータ

- 1) **Port:** ポート番号を表示します。
- 2) **Cable Status:** 診断されたケーブル情報を表示します。

#### ケーブルの診断手順

- 1) メニューから「Diagnostics」→「VeriPHY」の順にクリックします。
- 2) 診断したいポートを選択して、**Start**をクリックします。



- 3) 診断結果が表示されます。

VeriPHY Cable Diagnostics

Port

All

Start

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	OK	15	OK	15	Short	15	Short	15
2	OK	0	OK	0	OK	0	OK	0
3	Open	0	Open	0	Open	0	Open	0
4	Open	0	Open	0	Open	0	Open	0
5	Open	0	Open	0	Open	0	Open	0
6	Open	0	Open	0	Open	0	Open	0
7	Open	0	Open	0	Open	0	Open	0
8	OK	0	OK	0	Short	0	Short	0



## 61. 製品仕様

### 60.1. SMCGS10P-Smart/SMCGS10C-Smart

製品名	SMCGS10P-Smart	SMCGS10C-Smart
規 格	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ah 1000BASE-BX IEEE 802.3at Power over Ethernet IEEE 802.3x Flow Control IEEE 802.3ad LACP(Link Aggregation) IEEE 802.1Q VLAN IEEE 802.1p CoS(Strict/WRR) IEEE 802.1D STP IEEE 802.1w RSTP IEEE 802.1s MSTP IEEE 802.1ab LLDP IEEE 802.1X Authentication IGMP snooping v1/v2/v3 ISO/IEC 8802-3	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ah 1000BASE-BX IEEE 802.3x Flow Control IEEE 802.3ad LACP(Link Aggregation) IEEE 802.1Q VLAN IEEE 802.1p CoS(Strict/WRR) IEEE 802.1D STP IEEE 802.1w RSTP IEEE 802.1s MSTP IEEE 802.1ab LLDP IEEE 802.1X Authentication IGMP snooping v1/v2/v3 ISO/IEC 8802-3
パケット転送能力	14.9Mpps	14.9Mpps
スイッチング容量	20Gpbs	20Gpbs
パケットバッファ	512KB	512KB
MAC アドレス登録数	8K	8K
SDRAM	64MB	64MB
フラッシュメモリ	8MB	8MB
VLAN 数	4000	4000
VLAN ID レンジ	1-4094	1-4094
フローコントロール	IEEE 802.3x (全二重)	IEEE 802.3x (全二重)
	バックプレッシャー(半二重)	バックプレッシャー(半二重)
スイッチング方式	Store and Forward	Store and Forward
最大フレーム長	9600byte	9600byte
インタフェース	RJ-45 x8 ポート	RJ-45 x8 ポート
	・10/100/1000BASE-T ・オートネゴシエーション ・オート MDI/MDI-X ・IEEE802.3at Power over Ethernet	・10/100/1000BASE-T ・オートネゴシエーション ・オート MDI/MDI-X

		SFP x2 ポート	SFP x2 ポート
		・100/1000BASE-FX/SX/LX/T	・100/1000BASE-FX/SX/LX/T
寸 法		(W)330 x (D)204 x (H)43mm (突起部含まず)	(W)196 x (D)116 x (H)37mm (突起部含まず)
重 量		2.2kg	0.74kg
電 源		100-240V, 50-60Hz, 1.7A	100-240V, 50-60Hz, 0.5A
消費電力	PoE 使用時	100W(最大)	PoE 非対応
	PoE 未使用時	20W(最大)	20W(最大)
動作温度		0～50℃	0～50℃
動作湿度		10～90%RH (結露なきこと)	10～90%RH (結露なきこと)
保存温度		-40～70℃	-40～70℃
保存湿度		10～90%RH (結露なきこと)	10～90%RH (結露なきこと)
安全規格		CSA (CSA 22.2 No 60950-1 & UL60950-1)、CB (IEC 60950-1/ EN60950-1)	
EMI 認定		FCC Class A, IEC 55022 Class A、CISPR 22 Class A、IEC 61000-3-2/3、VCCI Class A	
イミュニティ規格		EN 61000-4-2/3/4/5/6/8/11	
管理機能		HTTP/HTTPS、SNMPv1,v2c,v3、SSH、Telnet	
PoE	給電方式	Alternative A	PoE 非対応
	最大 1 ポートあたり	30W	
	装置全体	75W(最大)	

## 60.2. SMCGS18P-Smart/SMCGS18C-Smart

製品名	SMCGS18P-Smart	SMCGS18C-Smart
規 格	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ah 1000BASE-BX IEEE 802.3at Power over Ethernet IEEE 802.3x Flow Control IEEE 802.3ad LACP(LinkAggregation) IEEE 802.1Q VLAN IEEE 802.1p CoS(Strict/WRR) IEEE 802.1D STP IEEE 802.1w RSTP IEEE 802.1s MSTP IEEE 802.1ab LLDP IEEE 802.1X Authentication IGMP snooping v1/v2/v3 ISO/IEC 8802-3	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ah 1000BASE-BX IEEE 802.3x Flow Control IEEE 802.3ad LACP(LinkAggregation) IEEE 802.1Q VLAN IEEE 802.1p CoS(Strict/WRR) IEEE 802.1D STP IEEE 802.1w RSTP IEEE 802.1s MSTP IEEE 802.1ab LLDP IEEE 802.1X Authentication IGMP snooping v1/v2/v3 ISO/IEC 8802-3
パケット転送能力	26.8Mpps	26.8Mpps
スイッチング容量	36Gpbs	36Gpbs
パケットバッファ	512KB	512KB
MAC アドレス登録数	8K	8K
SDRAM	128MB	128MB
フラッシュメモリ	16MB	16MB
VLAN 数	4000	4000
VLAN ID レンジ	1-4094	1-4094
フローコントロール	IEEE 802.3x (全二重)	IEEE 802.3x (全二重)
	バックプレッシャー(半二重)	バックプレッシャー(半二重)
スイッチング方式	Store and Forward	Store and Forward
最大フレーム長	9600byte	9600byte
インタフェース	RJ-45 x16 ポート	RJ-45 x16 ポート
	・10/100/1000BASE-T ・オートネゴシエーション ・オート MDI/MDI-X ・IEEE802.3at Power over Ethernet	・10/100/1000BASE-T ・オートネゴシエーション ・オート MDI/MDI-X
	SFP x2 ポート	SFP x2 ポート
	・100/1000BASE-FX/SX/LX/T	・100/1000BASE-FX/SX/LX/T

寸 法		(W)440 x (D)350 x (H)44mm (突起部含まず)	(W)430 x (D)180 x (H)44mm (突起部含まず)
重 量		4.049kg	1.91kg
電 源		100-240V, 50-60Hz, 1.7A	100-240V, 50-60Hz, 0.5A
消費電力	PoE 使用時	250W(最大)	PoE 非対応
	PoE 未使用時	20W(最大)	20W(最大)
動作温度		0～50℃	0～50℃
動作湿度		10～90%RH (結露なきこと)	10～90%RH (結露なきこと)
保存温度		-40～70℃	-40～70℃
保存湿度		10～90%RH (結露なきこと)	10～90%RH (結露なきこと)
安全規格		CSA (CSA 22.2 No 60950-1 & UL60950-1)、CB (IEC 60950-1/ EN60950-1)	
EMI 認定		FCC Class A, IEC 55022 Class A、CISPR 22 Class A, IEC 61000-3-2/3、VCCI Class A	
イミュニティ規格		EN 61000-4-2/3/4/5/6/8/11	
管理機能		HTTP/HTTPS、SNMPv1,v2c,v3、SSH、Telnet	
PoE	給電方式	Alternative A	PoE 非対応
	最大 1 ポートあたり	30W	
	装置全体	190W(最大)	

## 60.3. SMCGS26P-Smart/SMCGS26C-Smart

製品名	SMCGS26P-Smart	SMCGS26C-Smart
規格	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ah 1000BASE-BX IEEE 802.3at Power over Ethernet IEEE 802.3x Flow Control IEEE 802.3ad LACP(LinkAggregation) IEEE 802.1Q VLAN IEEE 802.1p CoS(Strict/WRR) IEEE 802.1D STP IEEE 802.1w RSTP IEEE 802.1s MSTP IEEE 802.1ab LLDP IEEE 802.1X Authentication IGMP snooping v1/v2/v3 ISO/IEC 8802-3	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ah 1000BASE-BX IEEE 802.3x Flow Control IEEE 802.3ad LACP(LinkAggregation) IEEE 802.1Q VLAN IEEE 802.1p CoS(Strict/WRR) IEEE 802.1D STP IEEE 802.1w RSTP IEEE 802.1s MSTP IEEE 802.1ab LLDP IEEE 802.1X Authentication IGMP snooping v1/v2/v3 ISO/IEC 8802-3
パケット転送能力	38.7Mpps	38.7Mpps
スイッチング容量	52Gbps	52Gbps
パケットバッファ	512KB	512KB
MAC アドレス登録数	8K	8K
SDRAM	128MB	128MB
フラッシュメモリ	16MB	16MB
VLAN 数	4000	4000
VLAN ID レンジ	1-4094	1-4094
フローコントロール	IEEE 802.3x (全二重)	IEEE 802.3x (全二重)
	バックプレッシャー(半二重)	バックプレッシャー(半二重)
スイッチング方式	Store and Forward	Store and Forward
最大フレーム長	9600byte	9600byte
インタフェース	RJ-45 x24 ポート	RJ-45 x24 ポート
	・10/100/1000BASE-T ・オートネゴシエーション ・オート MDI/MDI-X ・IEEE802.3at Power over Ethernet	・10/100/1000BASE-T ・オートネゴシエーション ・オート MDI/MDI-X
	SFP x2 ポート	SFP x2 ポート
	・100/1000BASE-FX/SX/LX/T	・100/1000BASE-FX/SX/LX/T

寸 法		(W)440 x (D)350 x (H)44mm (突起部含まず)	(W)430 x (D)180 x (H)44mm (突起部含まず)
重 量		4.5kg	2.01kg
電 源		100-240V, 50-60Hz, 1.7A	100-240V, 50-60Hz, 0.5A
消費電力	PoE 使用時	250W(最大)	PoE 非対応
	PoE 未使用時	25W(最大)	20W(最大)
動作温度		0～50℃	0～50℃
動作湿度		10～90%RH (結露なきこと)	10～90%RH (結露なきこと)
保存温度		-40～70℃	-40～70℃
保存湿度		10～90%RH (結露なきこと)	10～90%RH (結露なきこと)
安全規格		CSA (CSA 22.2 No 60950-1 & UL60950-1)、CB (IEC 60950-1/ EN60950-1)	
EMI 認定		FCC Class A, IEC 55022 Class A、CISPR 22 Class A、IEC 61000-3-2/3、VCCI Class A	
イミュニティ規格		EN 61000-4-2/3/4/5/6/8/11	
管理機能		HTTP/HTTPS、SNMPv1,v2c,v3、SSH、Telnet	
PoE	給電方式	Alternative A	PoE 非対応
	最大 1 ポートあたり	30W	
	装置全体	190W(最大)	

#### 60.4. SMCGS50P-Smart/SMCGS50C-Smart

製品名	SMCGS50P-Smart	SMCGS50C-Smart
規 格	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ah 1000BASE-BX IEEE 802.3at Power over Ethernet IEEE 802.3x Flow Control IEEE 802.3ad LACP(LinkAggregation) IEEE 802.1Q VLAN IEEE 802.1p CoS(Strict/WRR) IEEE 802.1D STP IEEE 802.1w RSTP IEEE 802.1s MSTP IEEE 802.1ab LLDP IEEE 802.1X Authentication IGMP snooping v1/v2/v3 ISO/IEC 8802-3	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-SX/LX IEEE 802.3ah 1000BASE-BX IEEE 802.3x Flow Control IEEE 802.3ad LACP(LinkAggregation) IEEE 802.1Q VLAN IEEE 802.1p CoS(Strict/WRR) IEEE 802.1D STP IEEE 802.1w RSTP IEEE 802.1s MSTP IEEE 802.1ab LLDP IEEE 802.1X Authentication IGMP snooping v1/v2/v3 ISO/IEC 8802-3
パケット転送能力	74.4Mpps	74.4Mpps
スイッチング容量	100Gpbs	100Gpbs
パケットバッファ	512KB	512KB
MAC アドレス登録数	8K	8K
SDRAM	128MB	128MB
フラッシュメモリ	16MB	16MB
VLAN 数	4000	4000
VLAN ID レンジ	1-4094	1-4094
フローコントロール	IEEE 802.3x (全二重)	IEEE 802.3x (全二重)
	バックプレッシャー(半二重)	バックプレッシャー(半二重)
スイッチング方式	Store and Forward	Store and Forward
最大フレーム長	9600byte	9600byte
インタフェース	RJ-45 x48 ポート	RJ-45 x48 ポート
	・10/100/1000BASE-T ・オートネゴシエーション ・オート MDI/MDI-X ・IEEE802.3at Power over Ethernet	・10/100/1000BASE-T ・オートネゴシエーション ・オート MDI/MDI-X
	SFP x2 ポート	SFP x2 ポート
	・100/1000BASE-FX/SX/LX/T	・100/1000BASE-FX/SX/LX/T

寸 法		(W)440 x (D)350 x (H)44mm (突起部含まず)	(W)430 x (D)180 x (H)44mm (突起部含まず)
重 量		5.19kg	2.986kg
電 源		100-240V, 50-60Hz, 1.7A	100-240V, 50-60Hz, 0.5A
消費電力	PoE 使用時	525W(最大)	PoE 非対応
	PoE 未使用時	25W(最大)	20W(最大)
動作温度		0～50℃	0～50℃
動作湿度		10～90%RH (結露なきこと)	10～90%RH (結露なきこと)
保存温度		-40～70℃	-40～70℃
保存湿度		10～90%RH (結露なきこと)	10～90%RH (結露なきこと)
安全規格		CSA (CSA 22.2 No 60950-1 & UL60950-1)、CB (IEC 60950-1/ EN60950-1)	
EMI 認定		FCC Class A, IEC 55022 Class A、CISPR 22 Class A, IEC 61000-3-2/3、VCCI Class A	
イミュニティ規格		EN 61000-4-2/3/4/5/6/8/11	
管理機能		HTTP/HTTPS、SNMPv1,v2c,v3、SSH、Telnet	
PoE	給電方式	Alternative A	PoE 非対応
	最大 1 ポートあたり	30W	
	装置全体	375W(最大)	



## 62. 製品保証

◆ 故障かなと思われた場合には、弊社カスタマサポートまでご連絡ください。

- 1) 修理を依頼される前に今一度、この取扱説明書をご確認ください。
- 2) 本スイッチの保証期間内の自然故障につきましては無償修理させていただきます。
- 3) 故障の内容により、修理ではなく同等品との交換にさせて頂く事があります。
- 4) 弊社への送料はお客様の負担とさせていただきますのでご了承ください。

初期不良保証期間: 納品日より **3ヶ月** (交換機器発送による対応)

製品保証期間: ご購入日より **3年間** (お預かりによる修理対応)

◆ 保証期間内であっても、以下の場合は有償修理とさせていただきます。

(修理できない場合もあります)

- 1) 使用上の誤り、お客様による修理や改造による故障、損傷
- 2) 自然災害、公害、異常電圧その他外部に起因する故障、損傷
- 3) 本スイッチに水漏れ・結露などによる腐食が発見された場合

◆ 保証期間を過ぎますと有償修理となりますので御注意ください。

◆ 一部の機器は、設定を本体内に記録する機能を有しております。これらの機器は修理時に設定を初期化しますので、お客様が行った設定内容は失われます。

◆ 恐れ入りますが、修理をご依頼頂く前に、設定内容をお客様にてお控えください。

◆ 本スイッチに起因する損害や機会の損失については補償致しません。

◆ 修理期間中における代替品の貸し出しは、基本的に行っておりません。別途、有償サポート契約にて対応させて頂いております。有償サポートにつきましてはお買い上げの販売店にご相談ください。

◆ 本スイッチの保証は日本国内での使用においてのみ有効です。

製品に関するご質問・お問い合わせ先

ハイテクインター株式会社

カスタマサポート

TEL 0570-060030

E-mail [support@hytec.co.jp](mailto:support@hytec.co.jp)

受付時間 平日 9:00～17:00

**付録 1: デフォルト設定一覧**

本スイッチのデフォルト設定は、ファイル名: “Factory\_Default\_Config.cfg.” によって与えられます。スイッチをデフォルト設定でリセットするためには、このファイルをスタートアップコンフィギュレーションファイルとして設定しなければなりません。

以下に、基本的なデフォルト設定の一覧を挙げます。

機 能	パラメータ	デフォルト値
ユーザー認証	User Name	admin
	Password	admin
	RADIUS Authentication	Disabled
	TACACS+ Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Enabled
	Port Security	Disabled
	IP Filtering	Disabled
Web GUI による管理	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Disabled
	HTTP Secure Server Redirect	Disabled
SNMP	SNMP Agent	Disabled
	Community Strings	“public” (read only) “private” (read/write)
	Traps	Global: disabled Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: default_view Group: default_rw_group
ポート設定	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input and output limits	Disabled
ポートトランッキング	Static Trunks	None
	LACP (all ports)	Disabled

(次ページに続く)

## (デフォルト設定一覧の続き)

機 能	パラメータ	デフォルト値
ストームプロテクション	Status	Broadcast: Enabled (1 kpps) Multicast: disabled Unknown unicast: disabled
スパニングツリー アルゴリズム	Status	Enabled, RSTP (デフォルト: RSTP standard)
	Edge Ports	Enabled
アドレステーブル	Aging Time	300 seconds
VLAN	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Access
トラフィック優先順位	Ingress Port Priority	0
	Queue Mode	Strict
	Weighted Round Robin	Queue: 0 1 2 3 4 5 6 7 Weight: Disabled in strict mode
	Ethernet Type	Disabled
	VLAN ID	Disabled
	VLAN Priority Tag	Disabled
	ToS Priority	Disabled
	IP DSCP Priority	Disabled
	TCP/UDP Port Priority	Disabled
LLDP	Status	Enabled
IP 設定	Management. VLAN	VLAN 1
	IP Address	192.168.1.10 ::192.168.1.10 (IPv6 の場合)
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP	Client: Disabled Snooping: Disabled
	MLD Snooping	Disabled
	Multicast VLAN Registration	Disabled
システムログ (コンソールのみ)	Status	Disabled
	Messages Logged to Flash	All levels
NTP	Clock Synchronization	Disabled

## 62.1. 付録 2: 位置情報 (Location Configuration Information: LCI)フォーマットの内容

No.	項目名	説明
1	Country code	ISO 3166-1 alpha-2 で規定されている、国毎に割り当てられた 2 文字のラテン大文字コードです。 日本では JP を指定します。
2	State	海外では州、郡、地方、省、県を指します。日本では都道府県に相当します。
3	County	海外では郡 (County)、教区 (Parish)、地区 (District)を指します。日本では郡に相当します。
4	City	海外では市(City)、郡区・町区(Township) を指します。日本では市に相当します。
5	City District	海外では町 (City division)、区 (Borough)、地区 (City district)、郡や市の行政区 (Ward) を指します。日本では町に相当します。
6	Block (Neighborhood)	日本では丁に相当します。
7	Street	海外では通りの名前を指定しますが、日本では番地に相当します。
8	Leading street direction	通りを進む向き。(東西南北: E, W, S, N)
9	Trailing street suffix	Trailing street suffix. (例: SW) ※
10	Street suffix	Street suffix. (例: Ave, Platz) ※
11	House no.	家屋や棟の番号. (例: 2 号棟)
12	House no. suffix	家屋や棟の添え字
13	Landmark	ランドマーク名 (例: 東京都庁)
14	Additional location info	追加の位置情報
15	Name	氏名 (居住者と賃借人)
16	Zip code	郵便番号
17	Building	ビル名
18	Apartment	共同住宅の区画名
19	Floor	階数
20	Room no.	部屋番号
21	Place-type	当該住所の使用形態 (例: Office ) ※
22	Postal community name	郵便サービスの団体名
23	P.O.Box	私書箱の名前
24	Additional code	追加コード

記入例は RFC 4676 より引用。

### 62.1.1. 引用・参考文献、及び商標表示

本書は以下の文献を意識し引用、または参考にしております。各文献における著作権は該当する団体および個人に帰属します。

IEEE: “802.1AB-2005™ Link Layer Discovery Protocol”, 2005.

RFC 2236 : “Internet Group Management Protocol, Version 2”, W. Fenner. Nov. 1997.

RFC 4676 : “Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information”, H. Schulzrinne, Oct, 2006.

RFC 4604: “Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast”, H. Holbrook - Arastra, Inc., B. Cain - Acopia Networks, B. Haberman - JHU APL, Aug. 2006.

本書の文中に挙げられる固有名詞は、該当する団体の商標又は登録商標です。

- ・EZ Smart™ は SMC Networks, Inc. の登録商標です。
- ・CISCO は CISCO Systems, Inc. の登録商標です。
- ・CISCO EtherChannel Technology は CISCO Systems, Inc.の登録商標です。