



# SWX2210P series

## Technical Data

Rev.1.03.14



# 目次

重要なお知らせ .....	1
ログインセキュリティ .....	1
機能概要 .....	1
対象機種とリビジョン .....	1
ファームウェア更新時の注意点 .....	2
関連文書 .....	3
保守・運用機能 .....	4
ユーザーアカウント管理 .....	4
機能概要 .....	4
用語の定義 .....	4
機能詳細 .....	4
ユーザーアカウント機能の設定 .....	4
ユーザーの認証 .....	6
関連コマンド .....	8
コマンド実行例 .....	8
管理者パスワードを設定する .....	8
ユーザーを追加する .....	8
注意事項 .....	8
関連文書 .....	9
LEDインジケーター制御 .....	10
機能概要 .....	10
用語の定義 .....	10
機能詳細 .....	10
LEDインジケーター点灯仕様 .....	10
LED MODEについて .....	11
その他のLED表示 .....	12
関連コマンド .....	12
コマンド実行例 .....	12
LAN ポートの状態確認 .....	12
LAN ポートループ検出状態の確認 .....	13
初期LEDモードの設定 .....	13
注意事項 .....	13
関連文書 .....	14
起動情報の管理 .....	15
機能概要 .....	15
関連コマンド .....	15
コマンド実行例 .....	15
起動情報の表示 .....	15
起動情報のクリア .....	16
注意事項 .....	16
関連文書 .....	16
筐体情報の表示 .....	17
機能概要 .....	17
コマンドによる筐体情報の表示 .....	17
技術サポート情報のリモート取得 .....	17

---

関連コマンド.....	17
コマンド実行例.....	17
製品情報の表示.....	17
稼動情報の表示.....	18
技術サポート情報の表示.....	19
注意事項.....	19
関連文書.....	20
ケーブル診断機能.....	21
機能概要.....	21
用語の定義.....	21
機能詳細.....	21
ケーブル診断方法.....	21
関連コマンド.....	21
設定例.....	22
ケーブル診断の実行.....	22
前回の診断結果の確認.....	22
注意事項.....	22
関連文書.....	22
コンフィグ管理.....	23
機能概要.....	23
用語の定義.....	23
機能詳細.....	23
ランニングコンフィグ.....	23
スタートアップコンフィグ.....	23
デフォルトコンフィグ.....	23
起動時のコンフィグファイルの決定.....	24
TFTPによるコンフィグファイルの制御.....	24
関連コマンド.....	24
コマンド実行例.....	24
ランニングコンフィグの保存.....	24
スタートアップコンフィグの消去.....	25
注意事項.....	25
関連文書.....	25
リモートアクセス制御.....	26
機能概要.....	26
用語の定義.....	26
機能詳細.....	26
関連コマンド.....	27
コマンド実行例.....	27
TELNETサーバーに対するアクセス制御.....	27
HTTPサーバーに対するアクセス制限.....	28
TFTPサーバーに対するアクセス制限.....	28
SNMPサーバーに対するアクセス制限.....	28
注意事項.....	29
関連文書.....	29
時刻管理.....	30
機能概要.....	30

---

---

用語の定義	30
機能詳細	30
日付・時刻の手動設定	30
日付・時刻の自動設定	30
タイムゾーンの設定	31
関連コマンド	31
コマンド実行例	31
時刻の手動設定	31
時刻の自動設定	31
注意事項	32
関連文書	32
SNMP	33
機能概要	33
用語の定義	33
機能詳細	33
SNMPv1	33
SNMPv2c	34
SNMPv3	34
SNMPサーバーへのアクセス制限	35
プライベートMIB	35
関連コマンド	35
コマンド実行例	36
SNMPv1 設定例	36
SNMPv2c 設定例	36
SNMPv3 設定例	36
注意事項	37
関連文書	37
SYSLOG	38
機能概要	38
用語の定義	38
機能詳細	38
関連コマンド一覧	39
コマンド設定例	39
注意事項	40
関連文書	40
ファームウェア更新	41
機能概要	41
用語の定義	41
機能詳細	41
更新ファームウェア送付による更新	41
HTTPクライアントを使用した更新	42
書き込み後の再起動	44
関連コマンド	44
コマンド実行例	44
HTTPクライアントを使用した更新	45
注意事項	46
関連文書	46

---

---

L2MS (Layer2 Management Service).....	47
機能概要 .....	47
用語の定義 .....	47
機能詳細 .....	48
対応機種 .....	48
L2MSのプロトコル .....	48
エージェントの監視 .....	48
エージェントの占有 .....	48
エージェントの操作 .....	49
エージェントからの情報通知 .....	49
L2MSフィルター / non-L2MSフィルター .....	49
L2MSの有効化 / 無効化 .....	49
初期IPアドレスについて .....	49
関連コマンド .....	50
コマンド実行例 .....	50
L2MSフィルターの設定 .....	50
L2MSの設定 .....	50
注意事項 .....	50
他機能との併用について .....	50
SYSLOGメッセージ一覧 .....	51
関連文書 .....	51
LLDP .....	52
機能概要 .....	52
用語の定義 .....	52
機能詳細 .....	52
動作仕様 .....	52
TLV一覧 .....	53
関連コマンド .....	56
コマンド実行例 .....	56
LLDPフレームの送受信の設定 .....	56
LLDP インターフェース状態の表示 .....	57
LLDP 接続機器の情報の表示 .....	57
注意事項 .....	58
関連文書 .....	58
LLDP自動設定 .....	59
機能概要 .....	59
用語の定義 .....	59
機能詳細 .....	59
基本仕様 .....	59
Dante最適設定 .....	60
スケジュール機能による給電停止の事前通知 .....	60
関連コマンド .....	61
設定例 .....	61
注意事項 .....	61
関連文書 .....	62
スケジュール機能 .....	63
機能概要 .....	63

---

---

用語の定義	63
機能詳細	63
時刻トリガー	63
アクション	65
関連コマンド	65
設定例	65
特定の時間帯だけ無線LANアクセスポイントにPoE給電する場合（PoE対応モデルのみ）	65
特定の時間帯だけポートをシャットダウンする場合	66
実行可能コマンド	66
SYSLOG	66
注意事項	67
関連文書	67
Dante最適設定	68
機能概要	68
用語の定義	68
機能詳細	68
LLDPによる自動最適設定	71
Web GUIからの手動最適設定	71
関連コマンド	72
コマンド実行例	73
LLDPによる自動最適設定	73
注意事項	73
関連文書	73
ProAV設定	74
機能概要	74
用語の定義	74
ProAVプロファイル詳細	74
Danteプロファイル	74
NDIプロファイル	78
複数プロファイル併用時の設定	80
キッティングとトラブルシューティング	83
[キッティング] IPアドレスを意識せずに初期設定する	83
[キッティング] 複数のヤマハスイッチに同一設定を一括適用する	86
[トラブルシューティング] ネットワークの状態を確認する	89
[トラブルシューティング] Dante機器の状態を確認する	91
注意事項	92
関連文書	92
商標名称について	92
デフォルト設定一覧	93
インターフェース制御機能	96
インターフェース基本機能	96
機能概要	96
用語の定義	96
機能詳細	96
インターフェースの種類	96
インターフェース制御	96
LANポートの初期状態	98

---

ポートミラーリング	98
フレームカウンター	98
関連コマンド	100
コマンド実行例	100
LANポートに対する基本設定	100
ミラーリング設定	101
LANポートの情報表示	101
注意事項	102
関連文書	102
リンクアグリゲーション	103
機能概要	103
用語の定義	103
機能詳細	103
スタティック リンクアグリゲーション仕様	103
関連コマンド	104
コマンド実行例	105
スタティック論理インターフェースの設定	105
注意事項	108
関連文書	108
PoE制御	109
機能概要	109
用語の定義	109
機能詳細	109
PoE 納電機能の有効/無効 制御	109
給電クラスと同時給電可能なポートの最大数	109
ガードバンド	110
給電優先度	110
PoE給電動作	110
LLDPによる給電設定	111
関連コマンド	111
コマンド実行例	111
PoEポートの給電設定	111
注意事項	112
関連文書	112
Layer 2機能	113
フォワーディングデータベース	113
機能概要	113
用語の定義	113
機能詳細	113
FDBエントリー	113
MACアドレスの自動学習	114
MACアドレスの手動設定	115
関連コマンド	116
コマンド実行例	116
FDBの参照	116
ダイナミックエントリーの削除	116
ダイナミックエントリー エージング時間の変更	116

---

---

スタティックエントリーの登録	116
スタティックエントリーの削除	117
注意事項	117
関連文書	117
VLAN	118
機能概要	118
用語の定義	118
機能詳細	118
VLAN IDの定義	118
LANポートに対するVLAN設定	118
デフォルトVLAN	119
ネイティブVLAN	119
関連コマンド	120
関連コマンド一覧	120
コマンド実行例	120
ポートベースVLAN の設定	120
タグVLAN の設定	121
注意事項	123
関連文書	123
マルチプルVLAN	124
機能概要	124
用語の定義	124
機能詳細	124
基本動作仕様	124
マルチプルVLANグループ間の通信例	125
関連コマンド	125
関連コマンド一覧	125
コマンド実行例	126
マルチプルVLAN の設定	126
注意事項	127
関連文書	127
独自ループ検出	128
機能概要	128
用語の定義	128
機能詳細	128
ループ検出 動作仕様	128
ループ検出例	129
関連コマンド	131
コマンド実行例	131
注意事項	133
関連文書	133
パススルー	134
機能概要	134
用語の定義	134
機能詳細	134
BPDU/パススルー 動作仕様	134
EAP/パススルー 動作仕様	134

---

---

関連コマンド .....	135
コマンド実行例 .....	135
注意事項 .....	135
関連文書 .....	135
Layer 3機能 .....	136
IPv4/IPv6共通設定 .....	136
機能概要 .....	136
用語の定義 .....	136
機能詳細 .....	136
DNS クライアントの設定 .....	136
関連コマンド .....	137
コマンド実行例 .....	137
DNSクライアントの設定 .....	137
注意事項 .....	138
関連文書 .....	138
IPv4基本設定 .....	139
機能概要 .....	139
用語の定義 .....	139
機能詳細 .....	139
IPv4アドレスの設定 .....	139
Auto IP機能 .....	139
ルート情報の設定 .....	140
ARP テーブルの設定 .....	140
関連コマンド .....	141
コマンド実行例 .....	141
IPv4ネットワーク環境の設定 (DHCP) .....	141
注意事項 .....	142
関連文書 .....	142
IPv6基本設定 .....	143
機能概要 .....	143
用語の定義 .....	143
機能詳細 .....	143
IPv6アドレスの設定 .....	143
ルート情報の設定 .....	144
Neighbor キャッシュテーブルの設定 .....	144
関連コマンド .....	145
コマンド実行例 .....	145
IPv6ネットワーク環境の設定 (固定設定) .....	145
IPv6ネットワーク環境の設定 (RAによる自動設定) .....	146
注意事項 .....	146
関連文書 .....	146
IPマルチキャスト機能 .....	147
IGMP Snooping .....	147
機能概要 .....	147
用語の定義 .....	148
機能詳細 .....	149
関連コマンド .....	151

---

---

コマンド実行例 .....	151
IGMP Snooping の設定(マルチキャストルーターあり) .....	151
IGMP Snooping の設定(マルチキャストルーターなし) .....	153
IGMP Snooping の設定(双方向でデータ配信する場合) .....	155
注意事項 .....	159
関連文書 .....	159
MLD Snooping .....	160
機能概要 .....	160
用語の定義 .....	160
機能詳細 .....	161
関連コマンド .....	162
コマンド実行例 .....	163
MLD Snooping の設定(マルチキャストルーターあり) .....	163
MLD Snooping の設定(マルチキャストルーターなし) .....	164
注意事項 .....	167
関連文書 .....	167
トラフィック制御機能 .....	168
ACL .....	168
機能概要 .....	168
用語の定義 .....	168
機能詳細 .....	169
アクセスリストの生成 .....	169
インターフェースへの適用 .....	169
LANポートに対する設定 .....	169
関連コマンド .....	170
コマンド実行例 .....	170
IPv4アクセスリストの設定 .....	170
IPv6アクセスリストの設定 .....	171
MACアクセスリストの設定 .....	173
注意事項 .....	174
関連文書 .....	174
QoS .....	175
機能概要 .....	175
用語の定義 .....	175
機能詳細 .....	176
QoS の有効・無効制御 .....	176
QoS 処理フロー .....	176
送信キューの割り当て .....	176
リマーキング .....	177
送信キューへの格納 .....	178
スケジューリング .....	178
Web会議アプリケーション向け最適設定 .....	179
別表1. 標準 PHB (RFC 推奨値) .....	180
関連コマンド .....	181
コマンド実行例 .....	182
DSCP 値を使用した優先制御(SP) .....	182
CoS 値を使用した優先制御(WRR) .....	183

---

---

受信ポート毎に付与したDSCP値に基づく優先制御 . . . . .	183
ポート優先トラストモードを使用した優先制御 . . . . .	184
注意事項 . . . . .	185
関連文書 . . . . .	186
商標名称について . . . . .	186
フロー制御 . . . . .	187
機能概要 . . . . .	187
用語の定義 . . . . .	187
機能詳細 . . . . .	187
IEEE 802.3x フロー制御 . . . . .	187
バックプレッシャー . . . . .	188
関連コマンド . . . . .	189
コマンド実行例 . . . . .	189
注意事項 . . . . .	189
関連文書 . . . . .	189
ストーム制御 . . . . .	190
機能概要 . . . . .	190
用語の定義 . . . . .	190
機能詳細 . . . . .	190
関連コマンド . . . . .	190
コマンド実行例 . . . . .	191
注意事項 . . . . .	191
関連文書 . . . . .	191
その他の情報 . . . . .	192
SNMP MIBリファレンス . . . . .	192
コマンドリファレンス . . . . .	193
本製品で使われるオープンソースソフトウェアのライセンスについて . . . . .	194
オープンソースソフトウェア一覧 . . . . .	194
ライセンス条文一覧 . . . . .	195
GPLv2 . . . . .	195
OpenSSL . . . . .	201
Wide-DHCPv6 . . . . .	203
crypt-md5.c . . . . .	204
ExplorerCanvas . . . . .	204
jqCanvas . . . . .	205
jqPlot . . . . .	205
jQuery . . . . .	206
jQuery Datepicker plugin . . . . .	206
jQuery File Upload Plugin / jQuery Iframe Transport Plugin / jQuery XDomainRequest Transport Plugin . . . . .	206
jQuery Migrate . . . . .	207
jQuery UI . . . . .	208
jQuery UI Touch Punch . . . . .	208
jQuery UI Ympicker . . . . .	209
PowerTip . . . . .	209



# 重要なお知らせ

## ログインセキュリティー

### 機能概要

#### 基本機能

本製品では、サイバーセキュリティーに対する取り組みとして、以下のようにユーザーアカウント管理の強化を行っています。

サイバー攻撃に悪用されるおそれを排除し、より安全にご利用いただくため、本資料を十分に確認いただきて適切なユーザー・パスワードを設定してからご使用ください。

詳細については、[ユーザーアカウント管理](#)を参照してください。

#### ・ 管理者登録の必須化

- 本製品では管理者を必ず1アカウント以上登録する必要があります。  
このため、本製品に初めてログインする際に使用する 初期管理ユーザー（ユーザー名: admin、パスワード: admin）が設定されています。
- 本製品に初めてログインするときには、ユーザー名とパスワードに **admin** を指定してください。
- 初期管理ユーザーでログインするとパスワードの変更が促されます。

#### ・ ゲストユーザーによる操作の厳格化

- 特権パスワードが初期設定から変更されていない場合、特権/パスワードを使用する以下の操作に制限が発生します。
  - 管理者権限を持たないユーザーは特権EXECモードに遷移できません
  - CLI/GUIの操作により、工場出荷状態に戻すことはできません
  - TFTPサーバーとして接続を受け付けることはできません
- 上記の操作を行う場合には、特権パスワードを変更してください。

#### ・ ブルートフォースアタック（総当たり攻撃）への対策

- 本製品への総当たり攻撃の対策の一つとして、ログイン認証失敗時、制限を設けました。
- コンソールやWeb GUIなどで本製品にログインするとき、パスワードを3回連続で間違えると、その後 **1分間** は正しいパスワードを入力してもログインすることができません。
- パスワードの入力ミスがあった場合には、1分以上時間を空けてから再度ログインしてください。

### 対象機種とリビジョン

以下の機種、リビジョンでユーザーアカウント管理の強化が行われています。

機種	リビジョン
SWX3220-16MT SWX3220-16TMs	Rev.4.02.10以降
SWX3200-52GT SWX3200-28GT	Rev.4.00.25以降
SWX3100-18GT SWX3100-10G	Rev.4.01.29以降

機種	リビジョン
SWX2322P-16MT	Rev.2.06.10以降
SWX2320-16MT	Rev.2.05.10以降
SWX2310-52GT SWX2310-28GT SWX2310-18GT SWX2310-10G	Rev.2.04.11以降
SWR2310-28GT SWR2310-18GT SWR2310-10G	Rev.2.04.12以降
SWX2310P-28GT SWX2310P-18G SWX2310P-10G	Rev.2.02.24以降
SWR2311P-10G	Rev.2.02.25以降
SWP2-10SMF SWP2-10MMF	Rev.2.03.16以降
SWX2220P-26NT SWX2220P-18NT	Rev.1.05.06以降
SWX2221P-10NT	Rev.1.05.03以降
SWX2220-26NT SWX2220-18NT	Rev.1.04.06以降
SWX2220-10NT	Rev.1.04.03以降
SWX2210P-28G SWX2210P-18G	Rev.1.03.14以降
SWX2210P-10G	Rev.1.03.13以降
SWX2210-24G SWX2210-16G SWX2210-8G	Rev.1.02.14以降

## ファームウェア更新時の注意点

ユーザーアカウント管理を強化したファームウェアに更新してスイッチを利用する場合、以下の手順に従って必ず事前に管理者アカウントを登録してください。

1. ユーザーアカウント管理を強化する前のファームウェア起動環境で、管理者アカウントを登録する
  - 既に管理者アカウントが存在する場合は、登録は不要です。
  - ただし、管理者アカウントのパスワードが未設定の場合、パスワードを必ず設定してください。
  - 管理者アカウントのユーザー名は、初期管理ユーザーのユーザー名である admin でも問題ありません。

```

Yamaha>enable
Yamaha#configure terminal

```

```
Yamaha(config)#username (ユーザー名) privilege on password (パスワード)
```

## 2. ゲストユーザーを作成する

必要に応じて、ゲストユーザーを作成します。

- username コマンドで作成する場合は、privilege オプションを無効 (off) にして作成します。

```
Yamaha(config)#username (ユーザー名) privilege off password (パスワード)
```

## 3. 特権パスワードを変更する

- 特権パスワードは、デフォルトで admin が設定されています。
- 特権パスワードの変更をコマンドで行う場合は、enable password コマンドを使用します。

```
Yamaha(config)#enable password (特権パスワード)
```

## 4. 対策ファームウェアに更新する

- ファームウェア更新に従って、対策ファームウェアに更新します。

## 関連文書

- [ユーザーアカウント管理](#)
- [リモートアクセス制御](#)
- [ファームウェア更新](#)

# 保守・運用機能

## ユーザーアカウント管理

### 機能概要

本製品は、ユーザーアカウントを管理する仕組みとして、以下の機能を提供します。

- ・ユーザー情報を設定する機能
- ・ユーザー名とパスワードを使ったユーザー認証機能

### 用語の定義

#### 初期管理ユーザー

工場出荷状態で設定されている管理者権限を持つユーザー。

ユーザー名: admin、パスワード: admin

#### 管理ユーザー

管理者権限を持つユーザーです。

usernameコマンドでprivilegeオプションがonで設定されているユーザーが管理ユーザーになります。

#### 一般ユーザー

管理者権限を持たないユーザーであり、特権EXECモードに遷移するときに特権パスワードの入力が必要です。

usernameコマンドでprivilegeオプションがoffで設定されているユーザーが一般ユーザーになります。

#### 特権パスワード

管理者権限を付与するために使用するパスワードであり、enable passwordコマンドで設定することができます。

#### 無名ユーザー

ユーザー名が空のユーザー。

Rev.1.03.12以前のファームウェアでは工場出荷状態で利用できるアカウントでしたが、ユーザーアカウント管理の強化に伴って廃止されました。

### 機能詳細

#### ユーザーアカウント機能の設定

##### ユーザー情報の設定

username コマンドを使用して以下のユーザー情報を設定します。

- ・ユーザー名
- ・パスワード
- ・管理者権限の有無

工場出荷状態では、初期管理ユーザーとして admin (パスワード:admin) が設定されます。

##### 特権パスワードの設定

enable password コマンドを使用して特権パスワードを設定します。

---

特権パスワードは、以下の用途で使用します。

- ・機器を初期化するとき
- ・コンソールにて、管理者権限を持たないユーザーで特権EXECモードへ移行するとき
- ・本製品に対して、TFTPクライアントでコンフィグやファームウェアを送信するとき

工場出荷状態では特権パスワードとして **admin** が設定されていますが、特権パスワードが初期設定の状態では前述した操作を行うことはできません。

これらの操作を行う場合、特権パスワードを前もって変更してください。

### 管理者権限

ユーザーの管理者権限の有無によって、そのユーザーでログインしたときの操作を制限できます。

- ・管理ユーザー（管理者権限を持つユーザー）は、機器の設定を変更したり、ファームウェアを更新したりすることができます。
- ・一般ユーザー（管理者権限を持たないユーザー）は、設定の変更などは行えず、機器情報の参照だけできます。

具体的には、管理者権限を持っているか否かで以下の違いがあります。

	CLI		Web GUI	
	管理ユーザー(権限有り)	一般ユーザー(権限無し)	管理ユーザー(権限有り)	一般ユーザー(権限無し)
機器情報の表示	○	○	○	○
設定の閲覧	○	×	○	△ (※1)
設定の変更	○	×	○	×
機器の再起動、初期化	○	×	○	×
ファームウェアの更新	○	×	○	×

※1：パスワードなどセキュリティに関する設定については参照できません。

一般ユーザーでログインした場合でも、 **enable** コマンドを実行した後、特権パスワードを入力することで特権EXECモードへ移行でき、管理ユーザーと同等の操作が行えます。

各コマンドを実行するときに必要な権限については、コマンドリファレンスを参照ください。

### パスワードの暗号化

設定したパスワードは、 **password-encryption** コマンドによって暗号化することができます。

パスワードを暗号化したい場合は、 **password-encryption enable** を設定してください。

一度暗号化されたパスワードは、 **password-encryption disable** を設定しても、暗号化前の文字列に復号されません。

以下のコマンドで設定するパスワードが暗号化の対象となります。

- ・ **enable password** コマンド
- ・ **username** コマンド

## ユーザーの認証

### コンソールにログインする場合

コンソールに接続すると、以下のようにログインプロンプトが表示されるため、設定したユーザー名とパスワードを入力してログインします。

```
Username:  
Password:
```

工場出荷状態でログインする場合、初期管理ユーザー admin ( パスワード : admin ) でログインします。 admin でログインすると、パスワードの変更を要求されるため、新しいパスワードを設定します。

```
Username: admin  
Password: ①  
  
SWX2210P-10G Rev.1.03.14 (Fri Feb 7 14:37:29 2025)  
Copyright (c) 2018-2025 Yamaha Corporation. All Rights Reserved.  
  
Please change the default password for admin.  
New Password: ②  
New Password(Confirm): ③  
Saving ...  
Succeeded to write configuration
```

① adminを入力する

② 新しいパスワードを入力する

③ 同じパスワードを再度入力する

パスワードを3回続けて間違えた場合、1分間、同じユーザーでのログインが制限されます。

```
Username: User  
Password:  
% Incorrect username or password, or login as User is restricted.  
Password:  
% Incorrect username or password, or login as User is restricted.  
Password:  
% Incorrect username or password, or blocked upon 3 failed login attempts for User.  
% Please try again later.
```

ログイン制限がかかったときには以下のメッセージがINFOレベルのSYSLOGに出力されます。

接続方法	出力メッセージ
シリアルコンソール	Login access from serial console as {ユーザー名} was restricted
TELNET	Login access from TELNET as {ユーザー名} was restricted: {IPアドレス}
Web GUI	Login access from HTTP as {ユーザー名} was restricted: {IPアドレス}

ログインが制限されているユーザーで再びパスワードを間違えると、ログイン制限が解除されるまでの時間が残り1分に更新されるため、注意してください。

#### WebGUIにログインする場合

WebGUIにアクセスすると、以下のログインフォームが表示されるため、設定したユーザー名とパスワードを入力してログインします。

The screenshot shows the login interface for the SWX2210P-10G device. At the top, it says "SWX2210P-10G". Below that, the title "SWX2210P" is displayed. The main area contains two input fields: one for the username (labeled "ユーザー名を入力してください" and "Please enter your username") and another for the password (labeled "パスワードを入力してください" and "Please enter your password"). Both fields have placeholder icons (user for username, key for password). A "Login" button is located below the password field. At the bottom of the page, the text "Yamaha Corporation" is visible.

工場出荷状態でログインする場合、初期管理ユーザー admin ( パスワード : admin ) でログインします。工場出荷状態でログインすると、パスワードの変更を要求されるため、新しいパスワードを設定します。

The screenshot shows the password change interface for the SWX2210P-10G device. At the top, it says "SWX2210P-10G". Below that, the title "SWX2210P" is displayed. The main area contains a message about changing the initial password for the "admin" user, followed by a note to enter a new password. An input field for the new password is shown with a key icon. Below the input field is a "Password Strength" section with four buttons labeled "弱" (Weak), "中" (Medium), "強" (Strong), and "最強" (Very Strong). Another input field for confirming the new password is also present with a key icon. At the bottom, there are "Back" and "Save" buttons, and the text "Yamaha Corporation" at the very bottom.

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
特権パスワードの設定	enable password
パスワードの暗号化	password-encryption
ユーザーの設定	username
ユーザー情報の表示	show users

## コマンド実行例

### 管理者パスワードを設定する

管理者パスワードとして、**yamaha\_admin** を設定する。

```
Yamaha>enable
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#enable password yamaha_admin
```

### ユーザーを追加する

ユーザー **yamaha** に **特権オプション** を付与して、パスワード **yamaha\_pass** を指定して設定する。

```
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#username yamaha privilege on password yamaha_pass
Yamaha(config)#exit
Yamaha#exit

Username: yamaha
Password:

SWX2210P-10G Rev.1.03.14 (Fri Feb 7 14:37:29 2025)
Copyright (c) 2018-2025 Yamaha Corporation. All Rights Reserved.

Yamaha>enable
Yamaha#
```

## 注意事項

- 本製品が起動する際、startup-config 上に管理ユーザー(管理者権限を持つユーザー)が1人も存在しない場合、初期管理ユーザー admin (パスワード : admin)が自動的に追加されます。  
例えば、以下のようなケースが該当します。
  - 工場出荷状態で本製品を起動する
  - Rev.1.03.12 以前のファームウェアにて、無名ユーザーだけを使って本製品を運用している状態

---

で、Rev.1.03.12 より新しいファームウェアに更新する

- ・本製品が起動する際、startup-config 上にパスワードが空のユーザーが設定されている場合、ユーザー名と同じ文字列がパスワードとして自動的に追加されます。  
例えば、以下のようなケースが該当します。

- Rev.1.03.12 以前のファームウェアにて、パスワードが空のユーザーが設定されている状態で、Rev.1.03.12 より新しいファームウェアに更新する

#### Rev.1.03.12 以前のファームウェアでの設定

```
username yamaha1  
username yamaha2 privilege on
```

#### Rev.1.03.12 より新しいファームウェアにアップデートしたときの設定

```
username yamaha1 password yamaha1  
username yamaha2 privilege on password yamaha2
```

- ・初期管理ユーザー admin のパスワードが初期値(admin)のまま変更されていない場合、以下の制限があります。
  - IPv4アドレスもしくはIPv6アドレスが設定されているVLAN以外のネットワークセグメントからTELNET,HTTP,HTTPSで本製品にアクセスすることはできません。
  - 初期管理ユーザー以外でのログインが禁止されます。

```
Username: yamaha  
Password:  
% Please login as user "admin".
```

## 関連文書

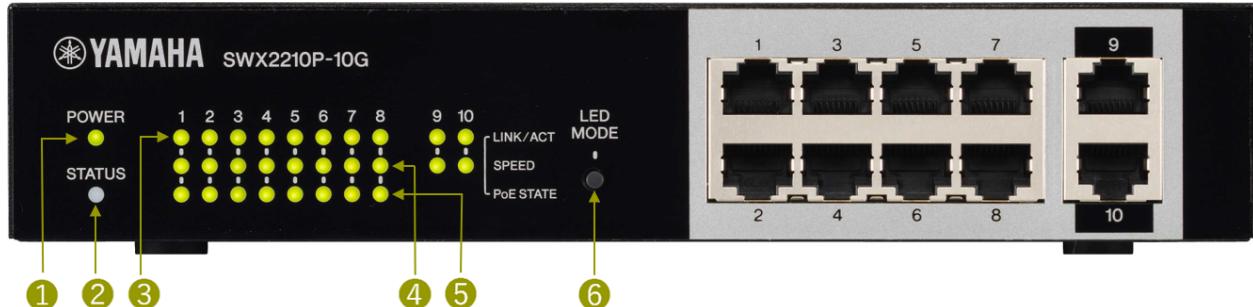
- ・[リモートアクセス制御](#)

# LEDインジケーター制御

## 機能概要

本製品には、[POWER], [STATUS], [LINK/ACT], [SPEED], [PoE STATE] の5種類のLED インジケーターと、LED MODEの切り替えに使用する LED MODEボタン が搭載されています。

- SWX2210P LED インジケーター



1. POWER LED
2. STATUS LED
3. LINK/ACT LED
4. SPEED LED
5. PoE STATE LED
6. LED MODE Button

## 用語の定義

特になし

## 機能詳細

### LEDインジケーター点灯仕様

本製品 の LED インジケーター点灯仕様について、以下に示します。

- SWX2210P LED インジケーター

インジケーター	点灯状態	説明
POWER	消灯	電源オフ
	緑色で点灯	電源オン
STATUS LED	消灯	正常
	橙色で点灯	<p>以下のいずれかの状態</p> <ul style="list-style-type: none"><li>- 総給能力オーバーにより給電を停止した</li><li>- ガードバンドにより給電を抑制した</li><li>- 過電流により給電を停止した</li><li>- ループを検出し、通信を遮断した</li></ul>
	橙色で点滅	システム異常を検出した(ファン異常/温度異常/電源異常)

インジケーター	点灯状態	説明
LINK/ACT	消灯	以下のいずれかの状態 - リンクダウン - 表示モードがOFFモードになっている
	緑色で点灯	リンクアップ
	緑色で点滅	データ転送中
	橙色で点滅	ループを検出し、通信を遮断した
SPEED	消灯	以下のいずれかの状態 - リンクダウン - 10BASE-T で接続中 - 表示モードがOFFモードになっている
	橙色で点灯	100BASE-TX で接続中
	緑色で点灯	1000BASE-T で接続中
PoE STATE	消灯	以下のいずれかの状態 - 給電していない - 表示モードがOFFモードになっている
	緑色で点灯	正常給電中
	橙色で点灯	以下のいずれかの状態 - 総給能力オーバーにより給電を停止した - ガードバンドにより給電を抑制した
	橙色で点滅	過電流により給電を停止した

## LED MODEについて

### 表示モードと表示モードの切り替え

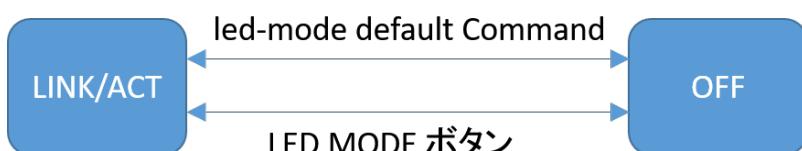
本製品は、以下に示す2つの表示モードを提供します。

モード名	機能概要
LINK/ACT モード	LINK/ACT LEDにリンク状態、SPEED LEDに接続速度、PoE STATE LEDに給電状態を表示します。
OFF モード	LINK/ACT LED、SPEED LEDおよびPoE STATE LEDを消灯し、消費電力を落とします。

表示モードの切り替えは、LED MODEボタンにより行います。

表示モードの切り替えの流れを以下に示します。

- 表示モードの切り替え (初期LEDモードが LINK/ACTモード の場合)



## OFFモードのLED表示

LEDモードがOFFモードのとき、LINK/ACT LED、SPEED LEDおよびPoE STATE LEDはリンク状態、ループ検出状態およびPoE給電状態に関係なくすべて消灯します。

## システム起動後のLEDモードの変更

本製品では、システム起動後のLEDモード(初期LEDモード)を設定することができます。初期LEDモードの初期値は、**LINK/ACT モード**に設定されており、**led-mode default**コマンドにより変更することができます。

**show led-mode**コマンドにより初期LEDモード、現在表示中のLEDモードを確認することができます。

## その他のLED表示

LED MODEボタンを押した状態で電源を入れて約10秒経過すると、LEDモードの状態に関係なく全ポートLEDは橙色に点灯し、工場出荷時の設定に戻ります。

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
LANポート状態表示	<b>show interface</b>
ループ検出設定状態の表示	<b>show loop-detect</b>
PoE給電情報の表示	<b>show power -inline</b>
初期LEDモードの設定	<b>led-mode default</b>
LEDモードの表示	<b>show led-mode</b>

## コマンド実行例

### LANポートの状態確認

LANポートの状態を**show interface**コマンドで確認します。

```
Yamaha#show interface
Interface port1.1
Link is UP
Hardware is Ethernet
HW addr: ac44.f230.02c9
MRU 1522
BPDU pass-through: Enabled
EAP pass-through: Enabled
Description:
ifIndex 5001
Speed-Duplex: auto(configured), 10-half(current)
Auto MDI/MDIX: on
Vlan info:
  Switchport mode      : access
  Ingress filter       : enable
```

```
Acceptable frame types : all
Default Vlan           :   1
Configured Vlans       :   1
Interface counter:
  input  packets          : 46290
    bytes              : 6834572
    drops              : 0
    broadcast-and-multicast-packets: 31605
  output packets          : 37816
    bytes              : 16869972
    drops              : 0
    broadcast-and-multicast-packets: 19050
:
```

(全LANポートの情報が表示される)

### LAN ポート ループ検出状態の確認

LANポートのループ検出状態を確認します。

```
Yamaha#show loop-detect
loop-detect: Enable

port      loop-detect      status
-----
port1.1    enable(*)      Normal
port1.2    enable(*)      Normal
port1.3    enable(*)      Detected
port1.4    enable(*)      Normal
port1.5    enable(*)      Blocking
port1.6    enable(*)      Normal
port1.7    enable(*)      Normal
port1.8    enable(*)      Normal
port1.9    enable(*)      Normal
port1.10   enable(*)      Normal
```

### 初期LEDモードの設定

初期LEDモードをOFFモードに設定します。

```
Yamaha#configure terminal
Yamaha(config)#led-mode default off ①
Yamaha(config)#exit
Yamaha#show led-mode ②
default mode : off
current mode : off
```

① 初期LEDモードの設定

② LEDモードの表示

### 注意事項

特になし

---

## 関連文書

特になし

# 起動情報の管理

## 機能概要

本製品は、システム起動情報として下表に示す情報を管理します。

管理項目	説明
システム起動時刻	システムが起動した時刻
起動中のファームウェア情報	現在起動中のファームウェアのバージョン、生成日時
前回起動したファームウェア情報	前回起動したファームウェアのバージョン、生成日時
起動要因	起動が行われた要因。以下を記録する。 * 電源投入による起動 * reloadコマンドによる再起動 * cold startコマンドによる再起動 * ファームウェア更新による再起動 * カーネルパニックによる再起動 * 原因不明の再起動

本製品は、現在の起動情報と過去4件の起動情報、あわせて5件の起動情報を保持します。

## 関連コマンド

関連コマンドについて、以下に示します。

詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
起動情報の表示	show boot
起動情報のクリア	clear boot list

## コマンド実行例

### 起動情報の表示

- 現在の起動情報を表示します。

```
Yamaha>show boot 0
Running EXEC: SWX2210P Rev.1.03.14 (Fri Feb 7 14:37:29 2025)
Previous EXEC: SWX2210P Rev.1.03.14 (Fri Feb 7 14:37:29 2025)
Restart by reload command
```

- 起動履歴の一覧を表示します。

```
Yamaha>show boot list
No. Date      Time      Info
-----
0 2025/02/12 15:38:15 Restart by reload command
1 2025/02/12 11:19:11 Power-on boot
```

## 起動情報のクリア

- ・起動情報をクリアします。

```
Yamaha#clear boot list
```

## 注意事項

特になし。

## 関連文書

特になし。

# 筐体情報の表示

## 機能概要

### コマンドによる筐体情報の表示

本製品は、下表に示す本体の表示機能を提供します。

表示項目	説明	コマンド
製品情報	製品名、型番、プロダクトIDなど本製品本体の情報を表示します。	show inventory
稼働情報	起動ソフトウェアの情報、CPU使用率、メモリ使用率、起動時刻など、本製品のプログラムの稼働情報を表示します。	show environment
技術サポート情報	技術サポートに必要な解析情報として、稼働情報がわかるものを全て出力します。	show tech-support

### 技術サポート情報のリモート取得

PCなどのリモート端末にインストールされた **TFTPクライアント** を使用して、本製品から **技術サポート情報(show tech-supportの出力結果)** を取得することができます。

本製品のtftpサーバーを機能させるために、以下の手順でリモートアクセス可能なネットワーク環境を整備してください。

1. 任意のVLAN( IPv4/IPv6アドレスを設定します。
2. tftp-server enableコマンドで、本製品のTFTPサーバー機能を起動します。
3. tftp-server accessコマンドを使用し、必要に応じてTFTPサーバーにアクセス可能なホストを設定します。

なお、TFTPクライアント使用時、技術サポート情報取得先のリモートパスには、 **techinfo** を指定します。

## 関連コマンド

関連コマンドについて、以下に示します。

詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
製品情報の表示	show inventory
稼働情報の表示	show environment
技術サポート情報の表示	show tech-support

## コマンド実行例

### 製品情報の表示

本体の製品情報を確認します。

- ・ 名称 (NAME)
- ・ 概要 (DESCR)

- ・ベンダー名 (Vendor)
- ・プロダクトID (PID)
- ・バージョンID (VID)
- ・シリアル番号 (SN)

```
Yamaha>show inventory
NAME: L2 PoE switch
DESCR: SWX2210P-10G
Vendor: Yamaha
PID: SWX2210P-10G
VID: 0000
SN: 1234567890
```

## 稼動情報の表示

システムの稼働状態(以下の情報)を確認します。

- ・ブートバージョン
- ・PoEバージョン
- ・ファームウェアリビジョン
- ・シリアル番号
- ・MACアドレス
- ・CPU使用率
- ・メモリ使用率
- ・ファンの稼働状態
- ・ファンの回転数
- ・RTCバージョン
- ・起動時刻
- ・現在時刻
- ・起動からの経過時間
- ・本体温度の状態
- ・本体温度

```
Yamaha>show environment
SWX2210P-10G BootROM Ver.1.05
SWX2210P-10G PoEROM Ver.1.2.0.15
SWX2210P-10G Rev.1.03.14 (Fri Feb 7 14:37:29 2025)
main=SWX2210P-10G ver=00 serial=1234567890 MAC-Address=ac44.f200.0000
CPU: 42%(5sec) 43%(1min) 43%(5min) Memory: 51% used
Fan status: Normal
Fan speed: FAN1=2689RPM FAN2=2561RPM
RTC version: 1
Boot time: 2024/09/18 16:47:54 +09:00
Current time: 2024/09/19 17:14:56 +09:00
Elapsed time from boot: 1days 00:27:27
Temperature status: Normal
```

Temperature: 49 degree C  
Yamaha>

## 技術サポート情報の表示

技術サポートに有用な以下のコマンド実行結果を表示します。

- show running-config
- show environment
- show inventory
- show boot all
- show logging
- show users
- show interface
- show frame-counter
- show vlan brief
- show loop-detect
- show mac-address-table
- show l2ms
- show qos queue-counters
- show ip igmp snooping groups
- show ip igmp snooping interface
- show ipv6 mld snooping groups
- show ipv6 mld snooping interface
- show power-inline

```
Yamaha#show tech-support
#
# Information for Yamaha Technical Support
#
*** show running-config ***
!
dns-client enable
!
!
...
#
# End of Information for Yamaha Technical Support
#
```

## 注意事項

特になし

---

## 関連文書

特になし

# ケーブル診断機能

## 機能概要

ケーブル診断機能では、本機のLANポートに接続されているLANケーブルの断線の有無を簡易的に調べることができます。

ネットワークトラブルが発生したときの問題の切り分けや、ネットワーク設営時の簡易的なケーブルチェックとしてご利用ください。

## 用語の定義

### TDR (Time Domain Reflector)

LANケーブルを介してパルス信号を送信し、反射信号からLANケーブルの長さや障害発生位置を測定する手法

## 機能詳細

### ケーブル診断方法

ケーブル診断機能では、TDR (Time Domain Reflector) 方式を用いてLANケーブルの簡易診断を行うことができます。

**test cable-diagnostics tdr interface** コマンドでケーブル診断を実行すると、以下の診断結果が表示されます。

項目	説明
ケーブルの状態	以下のケーブルの状態を検出することができます。 <ul style="list-style-type: none"><li>OK: 電気的に接続されています。</li><li>Open: 対向機が接続されていないか、ケーブルが故障しています。</li><li>Short: 短絡（ショート）が発生しています。</li></ul> 結果はペアごとに表示されます。
ケーブル障害位置までの距離	ケーブルの状態が Open もしくは Short のとき、障害位置までの距離を表示します。 結果はペアごとに表示されます。
推定ケーブル長	ケーブルの状態が全てのペアで OK のとき、推定ケーブル長を表示します。 リンクアップしている場合にのみ測定できます。

前回実行したケーブル診断実行結果は **show test cable-diagnostics tdr** コマンドで確認できます。

診断結果は直前の結果のみ保持され、再度ケーブル診断を実行した場合は結果が上書きされます。

**clear test cable-diagnostics tdr** コマンドで、直前の実行結果を削除することができます。

## 関連コマンド

関連コマンドについて、以下に示します。

コマンドの詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
ケーブル診断の実行	<b>test cable-diagnostics tdr interface</b>
ケーブル診断結果の表示	<b>show test cable-diagnostics tdr</b>

操作項目	操作コマンド
ケーブル診断結果のクリア	clear test cable-diagnostics tdr

## 設定例

### ケーブル診断の実行

port1.1に接続されているLANケーブルの診断を実行します。

```
Yamaha# test cable-diagnostics tdr interface port1.1 ↓
The port will be temporarily down during test. Continue? (y/N): y ↓
Cable-diagnostic is running...

Port      Pair  Status   Fault distance  Length
-----
port1.1  1      OK       -           50 +/- 15 m
          2      OK       -           -
          3      OK       -           -
          4      OK       -           -
```

### 前回の診断結果の確認

前回の診断結果を表示します。

```
Yamaha# show test cable-diagnostics tdr
Last run on Fri Feb 26 10:30:00 2021

Port      Pair  Status   Fault distance  Length
-----
port1.3  1      OK       -           -
          2      OK       -           -
          3      Open     5 +/- 3 m
          4      Open     5 +/- 3 m
```

## 注意事項

- ・本機能は簡易的な診断であり、専用計測機器ほど精密に計測することはできないため、予めご了承ください。
- ・診断対象ポートに **shutdown** コマンドが設定されているとき、ケーブルの診断を行うことはできません。
- ・ケーブル診断を実行すると一時的に通信断が発生するためご注意ください。
- ・対向ポートが1Gbps未満のリンク速度でリンクアップしているかシャットダウンしているとき、推定ケーブル長は測定できません。

## 関連文書

- ・特になし

# コンフィグ管理

## 機能概要

本製品では、以下のコンフィグを使用して設定値を管理します。

コンフィグの種類	説明	可能なユーザー操作
ランニングコンフィグ(running-config)	現在動作中の設定値。RAM上で管理する。	参照 / スタートアップコンフィグへの保存
スタートアップコンフィグ(startup-config)	保存した設定値。ROM上で管理する。	参照 / 消去
デフォルトコンフィグ(default-config)	デフォルトの設定値。ROM上で管理する。	操作不可

## 用語の定義

特になし

## 機能詳細

### ランニングコンフィグ

running-configは、現在動作中の設定で、RAM上で管理しているため再起動すると破棄されます。  
本製品では、コンフィギュレーションモードで実行したコマンドは、即座に running-config に反映され、設定した通りに機能します。

running-configの内容は、 **show running-config** コマンドで参照できます。

### スタートアップコンフィグ

startup-configは、Flash ROMに保存された設定で、再起動しても内容は保持されます。  
本製品を起動すると startup-config の設定が running-config の初期設定として展開されます。

**cold start** コマンド実行後など、startup-configが存在しない状態で起動しようとしたとき、自動的に default-config が適用されます。

running-config の設定は、 **copy running-config startup-config** コマンド、または **write** コマンドで startup-config に保存します。

本製品がFlash ROM上に保存できるスタートアップコンフィグの数は1つです。

スタートアップコンフィグが存在する状態で新しくスタートアップコンフィグを保存すると、古いスタートアップコンフィグは上書きされます。

startup-config の内容は、 **erase startup-config** コマンドで破棄、 **show startup-config** コマンドで参照できます。

### デフォルトコンフィグ

default-config は、本体Flash ROMに保存された本製品がスイッチとして最低限動作するための設定で、 startup-config 同様、再起動しても内容は保持されます。

工場出荷時の設定は、 default-config で管理します。

システム起動時、 startup-config が存在しない場合、 default-config が startup-config にコピーされ、 running-config に展開されます。

default-config の内容は、 参照することはできません。

## 起動時のコンフィグファイルの決定

本製品の起動時のコンフィグファイルを決定する流れは以下のとおりです。

1. startup-config が存在する場合、該当データをRAM上に running-config として展開する。
2. startup-config がROM上に存在しない場合、default-config をRAM上に running-config として展開する。

## TFTPによるコンフィグファイルの制御

本製品では、TFTPサーバー機能を有効にすることで、PCなどのリモート端末にインストールされた TFTP クライアントを使用して、以下を行うことができます。

1. 稼働中の running-config、startup-config を取得する
2. 予め準備した設定ファイルを、running-config、startup-config として適用させる

TFTPサーバーを正常に機能させるためには、本製品にアクセス可能な IP アドレスが設定されていることが条件となります。

リモート端末からの設定ファイルの取得／設定は、バイナリモードで行い、設定ファイルの取得先／送信先のリモートパスとして、以下を指定します。

取得／設定対象とする設定ファイル	取得先／送信先のリモートパス
running-config	config
startup-config # 0	config0
startup-config # 0 (設定のみ)	reconfig (送信先のみ)

- startup-config の設定は、システム再起動後に running-config として適用されます。
- 送信先のリモートパスに reconfig を指定した場合、本製品は設定ファイル受信後に自動的に再起動します。

## 関連コマンド

関連コマンドについて、以下に示します。

詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
ランニングコンフィグの保存	copy running-config startup-config
ランニングコンフィグの保存	write
スタートアップコンフィグの消去	erase startup-config
スタートアップコンフィグの表示	show startup-config

## コマンド実行例

### ランニングコンフィグの保存

running-configを保存する。

```
Yamaha#copy running-config startup-config
```

```
Building configuration...
```

```
[OK]
```

```
Yamaha#
```

## スタートアップコンフィグの消去

startup-configを消去する。

```
Yamaha#erase startup-config ①  
erasing...[OK]  
Yamaha#
```

① startup-configを消去

## 注意事項

特になし

## 関連文書

特になし

# リモートアクセス制御

## 機能概要

本製品では、ネットワークサービスを実現する以下のアプリケーションに対して、アクセス制限を行う機能を提供します。

- ・ TELNET サーバー
- ・ HTTP サーバー／セキュアHTTP サーバー
- ・ TFTP サーバー
- ・ SNMP サーバー

## 用語の定義

特になし

## 機能詳細

ネットワークサービスに対するアクセス制限として、以下の3つを可能とします。

- ・ 該当サービスをシステムに常駐させるかどうかの制御（起動・停止制御）
- ・ 受付ポート番号の変更
- ・ サービス起動中のアクセス元IPアドレスの限定

下表にネットワークサービスごとに応する機能を示します。

- ・ ネットワークサービスに対するアクセス制御

ネットワークサービス	起動・停止制御	受付ポート番号の変更	アクセス元の限定
TELNET サーバー	○	○	○
HTTP サーバー	×(常に起動)	○	○
セキュアHTTP サーバー	○	○	○
TFTP サーバー	○	○	○
SNMP サーバー	×(常に起動)	×(常に161)	○

1. ネットワークサービスを多重起動させることはできません。  
サービス起動中に同一サービスに対して起動制御を行うと、再立ち上げします。このため、接続中のセッションは **切断** されます。
2. ネットワークサービスに対してのアクセス元の限定では、**アクセス元のIPアドレス(\*1)** と **アクセスの許可/拒否(\*2)** を指定することができます。  
(\*1)…SNMPサーバーではアクセス先のコミュニティ名もしくはユーザー名も指定可能  
(\*2)…SNMPサーバーではアクセスの許可条件のみ指定可能。
3. ネットワークサービスの初期設定は下表のようになっています。

ネットワークサービス	起動・停止状態	受付ポート番号	アクセス元の限定
TELNET サーバー	起動	23	全て許可

ネットワークサービス	起動・停止状態	受付ポート番号	アクセス元の限定
HTTP サーバー	起動	80	全て許可
セキュアHTTP サーバー	起動	443	
TFTP サーバー	停止	69	全て許可
SNMP サーバー	起動	161	全て許可

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

ネットワークサービス	操作項目	操作コマンド
TELNETサーバー	起動停止および受付ポート番号変更	telnet-server enable (引数でポート番号を指定)
	IPアドレスアクセス制御	telnet-server access
	設定の表示	show telnet-server
HTTPサーバー	HTTPサーバーの受付ポート番号変更	http-server enable (引数でポート番号を指定)
	セキュアHTTPサーバー起動停止および受付ポート番号変更	http-server secure enable (引数でポート番号を指定)
	IPアドレスアクセス制御	http-server access
	設定の表示	show http-server
TFTPサーバー	起動停止および受付ポート番号変更	tftp-server enable (引数でポート番号を指定)
	IPアドレスアクセス制御	tftp-server access
SNMPサーバー	IPアドレスおよびコミュニティ名、ユーザー名でのアクセス制御	snmp-server access

## コマンド実行例

### TELNETサーバーに対するアクセス制御

TELNETサーバーに対するアクセス制限を実現します。

TELNETサーバーの受付ポートを1024に変更します。

TELNETサーバーへの接続は192.168.100.1からのクライアントのみ許可します。

telnet-server accessを設定した場合、条件に当てはまらないIPアドレスからのアクセスは拒否します。

```

Yamaha(config)#telnet-server enable 1024 ①
Yamaha(config)#telnet-server access permit 192.168.100.1 ②
Yamaha(config)#end
Yamaha#show telnet-server ③
Service:Enable

```

```
Port:1024  
Access:  
    permit 192.168.100.1
```

- ① 受付ポートを1024に変更し、TELNETサーバーを再起動する
- ② 192.168.100.1からのみアクセスを許可する
- ③ 設定状況の確認

### HTTPサーバーに対するアクセス制限

HTTPサーバーに対するアクセス制限を実現します。

HTTPサーバーの受付ポートを8000に、セキュアHTTPサーバーの受付ポートを9000に変更します。

HTTPサーバーへの接続は192.168.100.1からのクライアントのみ許可します。

http-server accessを設定した場合、条件に当てはまらないIPアドレスからのアクセスは拒否します。

```
Yamaha(config)#http-server enable 8000 ①  
Yamaha(config)#http-server secure enable 9000 ②  
Yamaha(config)#http-server access permit 192.168.100.1 ③  
Yamaha(config)#end  
Yamaha#show http-server ④  
HTTP :Enable(8000)  
HTTPS:Enable(9000)  
Access:  
    permit 192.168.100.1
```

- ① 受付ポートを8000に変更し、HTTPサーバーを再起動する
- ② 受付ポートを9000に変更し、セキュアHTTPサーバーを再起動する
- ③ 192.168.100.1からのみアクセスを許可する
- ④ 設定状況の確認

### TFTPサーバーに対するアクセス制限

TFTPサーバーに対するアクセス制限を実現します。

TFTPサーバーの受付ポートを2048に変更します。

TFTPサーバーへの接続は192.168.100.1からのクライアントのみ許可します。

```
Yamaha(config)#tftp-server enable 2048 ①  
Yamaha(config)#tftp-server access permit 192.168.100.1 ②
```

- ① 受付ポートを2048に変更し、TFTPサーバーを再起動する
- ② 192.168.100.1からのみアクセスを許可する

### SNMPサーバーに対するアクセス制限

SNMPサーバーに対するアクセス制限を実現します。

publicコミュニティへのアクセスを192.168.100.0/24からのクライアントのみに制限します。

加えて、privateコミュニティへのアクセスを192.168.100.1からのクライアントのみに制限します。

```
Yamaha(config)#snmp-server access permit 192.168.100.0/24 community public ①
```

```
Yamaha(config)#snmp-server access permit 192.168.100.1 community private ②
```

- ① コミュニティ名publicでは192.168.100.0/24からのみアクセスを許可する
- ② コミュニティ名privateでは192.168.100.1からのみアクセスを許可する

SNMPサーバーに対するアクセスを192.168.100.0/24から、かつユーザー名「user1」のクライアントのみに制限します。

```
Yamaha(config)#snmp-server access permit 192.168.100.0/24 user user1 ①
```

- ① 192.168.100.0/24かつユーザー名user1からのみアクセスを許可する

## 注意事項

IPv4/IPv6アドレスの設定を変更した場合、アクセス元IPアドレスの限定に関する設定がすべてリセットされます。

IPv4/IPv6アドレスの設定変更の際は十分にご注意ください。

## 関連文書

- [ユーザーアカウント管理](#)

# 時刻管理

## 機能概要

本製品は、日付・時刻を管理する仕組みとして、以下の機能を提供します。

- ・ユーザーが手動で日付・時刻情報を設定する機能
- ・ネットワークを介して日付・時刻情報を自動的に設定する機能
- ・タイムゾーンを設定する機能

なお、サマータイム(DST : Daylight Saving Time)を設定する機能は提供しません。

## 用語の定義

### UTC (Coordinated Universal Time)

全世界で時刻を記録する際に使われる公式な時刻のこと。

世界各国の標準時はこれを基準として決めています。

日本の場合、日本標準時（JST）で、協定世界時より9時間進んでおり、「+0900 (JST)」のように表示します。

### SNTP (Simple Network Time Protocol)

SNTPパケットを利用した、簡単な時計補正プロトコル。

RFC4330で規定されています。

## 機能詳細

### 日付・時刻の手動設定

**clock set** コマンドを使用して時刻を直接入力します。

### 日付・時刻の自動設定

指定したタイムサーバーから日付・時刻情報を収集し、本製品に設定します。

通信プロトコルとしては、RFC4330で規定されるSNTP(Simple Network Time Protocol)を利用します。

タイムサーバーは **2つまで** 指定でき、IPv4アドレス、IPv6アドレス、FQDN (Fully Qualified Domain Name) のいずれかを指定できます。

SNTPクライアントのポート番号は、123番を使用します。（ユーザーが設定を変更することはできません）  
日付・時刻の自動設定の方法として、**ntpdate** コマンドにより以下の2つから選択できます。

- ・ワンショット更新（コマンド入力時に更新をかける機能）
- ・インターバル更新（コマンド入力から更新を1~24時間の周期で行う機能）

タイムサーバーを2つ設定した状態で時刻同期を行った場合、**show ntpdate** コマンドで表示される NTP server 1, NTP server 2 の順番で問い合わせを行います。

NTP server 2への問い合わせは、NTP server 1との同期に失敗した場合のみ行われます。

初期状態では、インターバル更新を行わない設定がされています。

タイムサーバーおよびインターバル更新が設定されていてかつ、時刻の初回設定ができない状態では、インターバル周期時間に関係なく、ポートのリンクアップより1分後にタイムサーバーに対して問合せを行います。  
コマンド実行中はブロックされ、タイムアウトが発生すると、エラーメッセージを出力します。

## タイムゾーンの設定

生活拠点としている地域の時刻を管理するために、clock timezoneコマンドにより、使用するユーザーのタイムゾーンを管理し、時刻に反映します。  
タイムゾーンは、協定世界時（UTC）に対して±1時間単位で設定でき、その範囲は−12時間から+13時間とします。  
本製品のタイムゾーンの初期値は、**+9.0** となっています。

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
時刻の手動設定	clock set
タイムゾーンの設定	clock timezone
現在時刻の表示	show clock
NTPサーバーの設定	ntpdate server
NTPサーバーによる時刻同期(1ショット更新)	ntpdate oneshot
NTPサーバーによる時刻同期(周期更新設定)	ntpdate interval
NTPサーバーによる時刻同期設定情報の表示	show ntpdate

## コマンド実行例

### 時刻の手動設定

タイムゾーンを **JST** に設定し、現在時刻を **2018.11.01 15:50:59** に設定します。

```
Yamaha#configure terminal
Yamaha(config)#clock timezone JST ①
Yamaha(config)#exit
Yamaha#clock set 15:50:59 Nov 1 2018 ②
Yamaha#show clock ③
15:50:59 JST Thu Jan 1 2018
```

① タイムゾーンの設定

② 時刻の設定

③ 現在時刻の表示

### 時刻の自動設定

タイムゾーンを **+9.00** に設定し、NTPサーバーとしてローカルの **192.168.1.1** と **ntp.nict.jp** を設定します。

また、NTPサーバーとの更新周期を **24時間に1回** になるように変更します。

```
Yamaha#configure terminal
Yamaha(config)#clock timezone +9:00 ①
```

```
Yamaha(config)#ntpdate server ipv4 192.168.1.1 ②
Yamaha(config)#ntpdate server name ntp.nict.jp ③
Yamaha(config)#ntpdate interval 24 ④
Yamaha(config)#exit
Yamaha#show clock ⑤
10:03:20 GMT+9:00 Wed Oct 10 2018
Yamaha#show ntpdate ⑥
NTP server 1 : 192.168.1.1
NTP server 2 : ntp.nict.jp
adjust time : Wed Oct 10 11:46:30 2018 + interval 24 hour
sync server : 192.168.1.1
```

- ① タイムゾーンの設定
- ② NTPサーバーの設定
- ③ NTPサーバーの設定
- ④ NTPサーバーとの周期更新を24時間に設定
- ⑤ 現在時刻の表示
- ⑥ NTPによる時刻同期設定の表示

## 注意事項

特になし

## 関連文書

- [RFC 4330: Simple Network Time Protocol \(SNTP\) Version 4 for IPv4, IPv6 and OSI](#)

# SNMP

## 機能概要

SNMP (Simple Network Management Protocol) の設定を行うことにより、SNMP管理ソフトウェアに対してネットワーク管理情報のモニタと変更を行うことができるようになります。このとき本製品はSNMPエージェントとして動作します。

本製品はSNMPv1、SNMPv2c、SNMPv3による通信に対応しています。またMIB (Management information Base) として RFC1213 (MIB-II) およびプライベートMIB(yamahaSW) に対応しています。

SNMPv1およびSNMPv2cでは、コミュニティと呼ばれるグループの名前を相手に通知し、同じコミュニティに属するホスト間でのみ通信します。このとき、読み出し専用 (read-only) と読み書き可能 (read-write) の2つのアクセスモードに対して別々にコミュニティ名を設定することができます。

このようにコミュニティ名はある種のパスワードとして機能しますが、その反面、コミュニティ名は必ず平文でネットワーク上を流れるという特性があり、セキュリティ面では脆弱と言えます。よりセキュアな通信が必要な場合はSNMPv3の利用を推奨します。

SNMPv3では通信内容の認証、および暗号化に対応しています。SNMPv3はコミュニティの概念を廃し、新たにUSM (User-based Security Model) とVACM (View-based Access Control Model) と呼ばれるセキュリティモデルを利用することで、より高度なセキュリティを確保しています。本製品では、VACMによるアクセス制御は行いません。

本製品の状態を通知するSNMPメッセージをトラップと呼びます。本製品ではSNMP標準トラップを送信します。SNMPv1では通知メッセージの形式として、相手の受信確認応答を要求しないtrapリクエストを指定しますが、SNMPv2c、SNMPv3ではtrapリクエストか相手に受信確認応答を要求するinformリクエストかを選択できます。

SNMPv1およびSNMPv2cで利用する読み出し専用と送信トラップ用のコミュニティ名は、本製品では特にデフォルト値を決めていませんので、適切なコミュニティ名を設定してください。ただし、コミュニティ名はネットワーク上を平文で流れますので、コミュニティ名にログインパスワードや管理パスワードを決して使用しないよう注意してください。

初期設定では、各SNMPバージョンにおいてアクセスが一切できない状態となっています。また、トラップの送信先ホストは設定されておらず、どこにもトラップを送信しません。

本製品ではSNMPサーバーに対するアクセスを制限することができます。アクセス制限の設定を行うことで、意図しないホストからのアクセスを制限することができます。

## 用語の定義

特になし

## 機能詳細

各SNMPバージョンの主な特徴とSNMPに関する設定の設定方針について以下に説明します。  
具体的な設定例については後述する "[コマンド実行例](#)" をご覧ください。

### SNMPv1

コミュニティ名によりSNMPマネージャーとエージェント間の認証を行います。  
管理する本製品をコミュニティというゾーンで分割して管理を行います。

- MIBオブジェクトへのアクセス  
**snmp-server community** コマンドで設定されたコミュニティ名でのアクセスを許可します。  
IPアドレスが設定されているVLANインターフェースからアクセスすることができます。

- SNMPトラップ

**snmp-server host** コマンドで設定されたホストへ本製品の状態を送信することができます。

**snmp-server enable trap** コマンドでどのようなトラップを送信するか設定します。

## SNMPv2c

SNMPv1と同様に、コミュニティ名によりSNMPマネージャーとエージェント間の認証を行います。

**snmp-server community** コマンドでSNMPv2cによりアクセスするときに使用するコミュニティ名を設定します。

また、本バージョンから新たにGetBulkリクエストやInformリクエストに対応します。

MIBオブジェクトをまとめて効率よく取得したり、本製品からの通知パケットに対する応答確認を行うことができます。

- MIBオブジェクトへのアクセス

**snmp-server community** コマンドで設定されたコミュニティ名でのアクセスを許可します。

IPアドレスが設定されているVLANインターフェースからアクセスすることができます。

- SNMPトラップ

**snmp-server host** コマンドで設定されたホストへ本製品の状態を送信することができます。

またコマンドの設定により送信メッセージの形式をトラップかInformリクエストかを選択することができます。

Informリクエストでは相手に受信確認応答を要求します。

## SNMPv3

SNMPv3はSNMPv2までの全機能に加えてセキュリティ機能が強化されています。

ネットワーク上を流れるSNMPパケットを認証・暗号化することによって、SNMPv1、v2cでのコミュニティ名とSNMPマネージャのIPアドレスによるセキュリティ機能では実現できなかった盗聴、なりすまし、改竄、リプロイ攻撃などからSNMPパケットを守ることができます。

- セキュリティ

SNMPv3では以下のセキュリティ機能を提供します。

1. USM (User-based Security Model)

USMはメッセージレベルのセキュリティ確保を行うためのモデルで、共通鍵暗号に基づく認証と暗号化、メッセージストリーム改竄に対する防御を行います。

- セキュリティレベル

本製品は以下のセキュリティレベルに対応しています。通信内容の認証と暗号化は常に行われます。

- AuthPriv : 認証・暗号化を行う

- ユーザ認証

認証はデータの完全性(改竄されていないこと)とデータの送信元の認証を行うための手続きでHMACを使用します。

認証鍵でハッシュを取ることによりメッセージが改竄されていないことと送信者がユーザー本人であることを確認できます。

ハッシュアルゴリズムとしてHMAC-SHA-96をサポートします。

- 暗号化

SNMPv3では、管理情報の漏洩を防ぐ目的で、SNMPメッセージの暗号化を行います。

暗号方式はAES128-CFBをサポートします。

**snmp-server user** コマンドで、ユーザ名、アクセス権限、パスワードを設定することができます。

本製品では、ReadOnlyユーザーとReadWriteユーザーをそれぞれ一つずつ設定することができます。

## 2. VACM (View-based Access Control Model)

VACMはSNMPメッセージのアクセス制御を行うモデルです。

- 本製品ではVACMによるアクセス制御は行わないため、すべてのMIBビューに対してアクセスが可能です。

### • SNMPトラップ

**snmp-server host** コマンドで設定されたホストへ本製品の状態を送信することが可能です。

トラップを送信するには、あらかじめ **snmp-server user** コマンドでユーザを設定する必要があります。

またコマンドの設定により送信メッセージの形式をトラップかInformリクエストかを選択することができます。

Informリクエストでは相手に受信確認応答を要求します。

## SNMPサーバーへのアクセス制限

本製品のSNMPサーバーにアクセス可能なホストを **snmp-server access** コマンドで設定することができます。

意図したSNMPマネージャーからのアクセスのみを許可することで、意図しないホストからのアクセスを制限することができます。

デフォルトではすべてのホストからのアクセスを受け付けます。ご利用環境に応じてアクセス制限の設定をしてください。

アクセス制限についての詳細は [リモートアクセス制御](#)をご参照ください。

## プライベートMIB

本製品は、独自のスイッチ管理用プライベートMIBである yamahaSW に対応しています。

このプライベートMIBにより、ヤマハの独自機能に対する情報や、スイッチのより詳細な情報を得ることができます。

対応しているプライベートMIB、プライベートMIBの取得方法については、本文書のHTML版の「SNMP MIBリファレンス」章を参照願います。

## 関連コマンド

関連コマンドについて、以下に示します。

コマンドの詳細は、コマンドリファレンスを参照願います。

操作項目	操作コマンド
SNMP通知メッセージの送信先ホストの設定	<code>snmp-server host</code>
送信する通知メッセージタイプの設定	<code>snmp-server enable trap</code>
システムコンタクトの設定	<code>snmp-server contact</code>
システムロケーションの設定	<code>snmp-server location</code>
SNMPコミュニティの設定	<code>snmp-server community</code>
SNMPユーザーの設定	<code>snmp-server user</code>
SNMPサーバーのアクセス設定	<code>snmp-server access</code>
SNMPコミュニティの情報の表示	<code>show snmp community</code>
SNMPユーザーの情報の表示	<code>show snmp user</code>

## コマンド実行例

### SNMPv1 設定例

SNMPv1によるネットワーク監視を以下の条件で実現します。

- 読み出し専用のコミュニティ名"public"を設定します。
- トラップの送信先を"192.168.100.11"に設定し、トラップのコミュニティ名を"snmptrapname"とします。
- コミュニティ名"public"でアクセス可能なホストを192.168.100.0/24のみに制限します。

```
Yamaha(config)# snmp-server community public ro ... 1  
Yamaha(config)# snmp-server host 192.168.100.11 traps version 1 snmptrapname ... 2  
Yamaha(config)# snmp-server access 192.168.100.0/24 community public ... 3
```

### SNMPv2c 設定例

SNMPv2cによるネットワーク監視を以下の条件で実現します。

- 読み書き可能なコミュニティ名を "private" とします。
- 通知メッセージの送信先を"192.168.100.12"とし、通知タイプをinformリクエスト形式、通知先のコミュニティ名を "snmpinformsname" とします。
- コミュニティ名"private"でアクセス可能なホストを192.168.100.12のみに制限します。

```
Yamaha(config)# snmp-server community private rw ... 1  
Yamaha(config)# snmp-server host 192.168.100.12 informs version 2c snmpinformsname ... 2  
Yamaha(config)# snmp-server access 192.168.100.12 community private ... 3
```

### SNMPv3 設定例

SNMPv3によるネットワーク監視を以下の条件で実現します。

- ReadWrite権限を持つユーザー "admin1" を作成します。  
認証アルゴリズムは "HMAC-SHA-96" 固定、パスワードは "passwd1234" とします。  
暗号化アルゴリズムは "AES128-CFB" 固定、暗号パスワードは "passwd1234" とします。
- ReadOnly権限を持つユーザー "user1" を作成します。  
認証アルゴリズムは "HMAC-SHA-96" 固定、パスワードは "passwd5678" とします。  
暗号化アルゴリズムは "AES128-CFB" 固定、暗号パスワードは "passwd5678" とします。
- トラップ形式(応答確認なし)の通知メッセージを 192.168.10.3 に通知させます。
- Informリクエスト形式の通知メッセージを 192.168.20.3 に通知させます。

```
Yamaha(config)# snmp-server user admin1 admin auth sha passwd1234 priv aes passwd1234  
... 1  
Yamaha(config)# snmp-server user user1 guest auth sha passwd5678 priv aes passwd5678  
... 2  
Yamaha(config)# snmp-server host 192.168.10.13 traps version 3 priv admin1  
... 3  
Yamaha(config)# snmp-server host 192.168.20.13 informs version 3 priv admin1
```

## 注意事項

- ご使用のSNMPマネージャーが対応するSNMPバージョンを事前にご確認ください。使用するSNMPバージョンに合わせて本製品の設定を行う必要があります。
- コミュニティ名の文字列の仕様は以下の通りです。
  - ""で囲まれていたときに、""内の文字列が使用されます。
  - ""の外側に文字列があるケースはサポートしていません。
  - \の使用はサポートしていません。
  - ""のみの使用はサポートしていません。

## 関連文書

- [Yamaha RTpro SNMP](#)
- [Yamaha RTpro Private MIB](#)
- [SNMP MIBリファレンス](#)
- [リモートアクセス制御](#)

# SYSLOG

## 機能概要

本製品は、稼働状況を把握する仕組みとして、以下に示すSYSLOG機能を提供します。

1. ログを本製品の内部に蓄積し、参照、削除する機能
2. ログ蓄積と同じタイミングでTELNETコンソールに出力する機能
3. ログ蓄積と同じタイミングであらかじめ登録した通知先（SYSLOGサーバー）に送信する機能

ログの蓄積、TELNETコンソールへの出力、SYSLOGサーバーへの通知は、ユーザーが設定した出力レベルに従って行われます。許可されたメッセージのみが処理の対象となります。

ログの蓄積は、RAM上で行われ、Flash ROMに対して自動でバックアップ、またはコマンドにより手動でバックアップすることが可能です。

SYSLOGサーバーへの通知は、ログ蓄積と同じタイミングで行われますが、SYSLOGサーバーの登録が行われている場合に限定されます。

## 用語の定義

特になし

## 機能詳細

SYSLOG機能について、以下に示します。

1. ログの蓄積は、RAMに対して行われ、最大で1500件蓄積可能とします。  
Flash ROMへのバックアップは、以下の三つを提供します。
  - システム起動から1時間ごとに行われる定期的な自動バックアップ
  - save logging** コマンドによる手動バックアップ
  - reloadコマンドやファームウェア更新などで再起動が発生した場合の自動バックアップ
2. RAMに蓄積されたログは、**show logging** コマンドにより参照することができます。  
RAMおよびFlash ROMのログの削除は、**clear logging** コマンドにより行うことができます。  
バックアップ実行により、RAMのログ情報が消去されることはありません。  
また、Flash ROMにバックアップされたログは、システム起動時にRAM上に展開されます。  
そのため、reloadコマンドやファームウェア更新などで再起動を実施しても、前回起動時のログの続きから新たなログが蓄積されます。
3. ログの送信は、通知先（SYSLOGサーバー）の登録が行われている場合に限り、機能します。  
通知先は、**logging host** コマンドで2つまで登録できます。  
通知先の指定は、IPアドレス、またはFQDNで行います。  
通知先のポート番号は、デフォルトポート番号である514を使用します。（ユーザーが任意に設定することはできません）  
通知するログのフォーマットは**logging format** コマンドでヘッダ一部（タイムスタンプ、ホスト名）なしに変更できます。ログの例を以下に示します。
  - format 指定なし (no logging format)

```
<134>Jan 1 00:00:00 Yamaha [      IMI]:inf: Configuration file is saved in  
"config0"
```

- format 指定あり (logging format legacy)

```
<134>[      IMI]:inf: Configuration file is saved in "config0"
```

- 送信するログのレベル (SYSLOGのプライオリティ) は、**logging trap** コマンドで設定可能です。  
本製品では、ログのレベルごとに出力の有効・無効設定が可能です。  
工場出荷時の出力レベルは、Informational、Errorのみ有効です。

## 関連コマンド一覧

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

機能名	コマンド名
ログの出力レベル設定	logging trap
ログのTELNETコンソール出力設定	logging stdout
ログの通知先 (SYSLOGサーバ) の設定	logging host
ログの通知フォーマット変更	logging format
ログのバックアップ	save logging
ログの削除	clear logging
ログの参照	show logging

## コマンド設定例

- Debugレベルのログ出力を有効して、SYSLOGサーバー (192.168.1.100) にログ出力を開始します。  
さらにInformationalレベルのログをTELNETコンソールに出力します。

```
Yamaha(config)# logging trap debug ①
Yamaha(config)# logging host 192.168.1.100 ②
Yamaha(config)# logging stdout info ③
```

- ① Debugレベルのログ出力を有効にする
- ② SYSLOGサーバーの登録
- ③ InformationalレベルのログをTELNETコンソールに出力する

- SYSLOGサーバーへの通知を終了します。

```
Yamaha(config)# no logging host
```

- 蓄積されているログ情報を保存し、表示します。

```
Yamaha# save logging ①
Yamaha# show logging ②
2018/10/05 15:58:47:[      L2MS]:inf: Start L2MS(Agent)
```

```
2018/10/05 15:58:47:[    VLAN]:inf: Interface vlan1 changed state to up
2018/10/05 15:58:47:[        IF]:inf: Interface port1.4 changed state to up (10-half)
2018/10/05 15:58:49:[    L2MS]:inf: Start management by manager(00a0.dec9.d6d2)
2018/10/05 15:59:32:[    DHCPC]:inf: DHCP gets IP address: 192.168.1.9
2018/10/05 15:59:46:[ SESSION]:inf: Login succeeded as (noname) for TELNET: 192.168.1.6
:
```

- ① RAM上のログをROMに保存する
  - ② 蓄積されているログを表示する
4. 蓄積されているログ情報を削除します。

```
Yamaha# clear logging ①
Yamaha# show logging ②
③
```

- ① 蓄積されているログを全て削除する
- ② ログを表示する
- ③ 消去したため、何も表示されない

## 注意事項

特になし

## 関連文書

特になし

# ファームウェア更新

## 機能概要

本製品はプログラム不具合の吸収や機能追加を行うために、以下の2つのファームウェア更新機能を提供します。

1. PCなどのリモート端末に置かれた更新ファームウェアを本製品に送付して適用する機能
2. 本製品のHTTPクライアントがHTTPサーバーにアクセスし、最新のファームウェアをダウンロードして適用する機能

本更新機能を利用して、バージョンアップ、及び、バージョンダウンを行うことができます。

新部品対応により、Rev.1.03.13以降のファームウェアからRev.1.03.12以前のファームウェアへのバージョンダウンはできないため、ご注意ください。

更新ファームウェアの書き込みが正常に完了すると、**新しいファームウェアを有効にするため、システムを自動で再起動**します。

## 用語の定義

特になし

## 機能詳細

### 更新ファームウェア送付による更新

PCなどのリモート端末に置かれたファームウェアを本製品に送付し、起動ファームウェアとして適用させます。

本更新は、**TFTPクライアント** または **Web GUI** を使用して行います。

### TFTPクライアントを使用したファームウェア更新

PCなどのリモート端末にインストールされた **TFTPクライアント** を使用して、本製品に更新ファームウェアを送付し、更新することができます。

本製品のTFTPサーバーを機能させるために、以下の手順でリモートアクセス可能なネットワーク環境を整備してください。

1. 任意のVLANにIPv4/IPv6アドレスを設定します。
2. TFTPサーバーを有効にします。設定には、**tftp-server enable** コマンドを使用します。
3. **tftp-server access** コマンドを使用し、必要に応じてTFTPサーバーにアクセス可能なホストを設定します。

TFTPクライアントを使用して更新ファームウェアを送信する際は、以下のルールに従ってください。

- ・転送モードには、**バイナリモード**を指定してください。
- ・更新ファームウェアの送信先のリモートパスは下表を参照し指定してください。
- ・本製品に管理パスワードが設定されている場合、リモートパスの後ろに"/PASSWORD"という形式で管理パスワードを指定してください。

TFTPクライアントを使用するファームウェア更新では、以下の2種類の更新が行えます。

- ・更新ファームウェア

種類	リモートパス
本体ファームウェア	exec
ブートローダー	boot

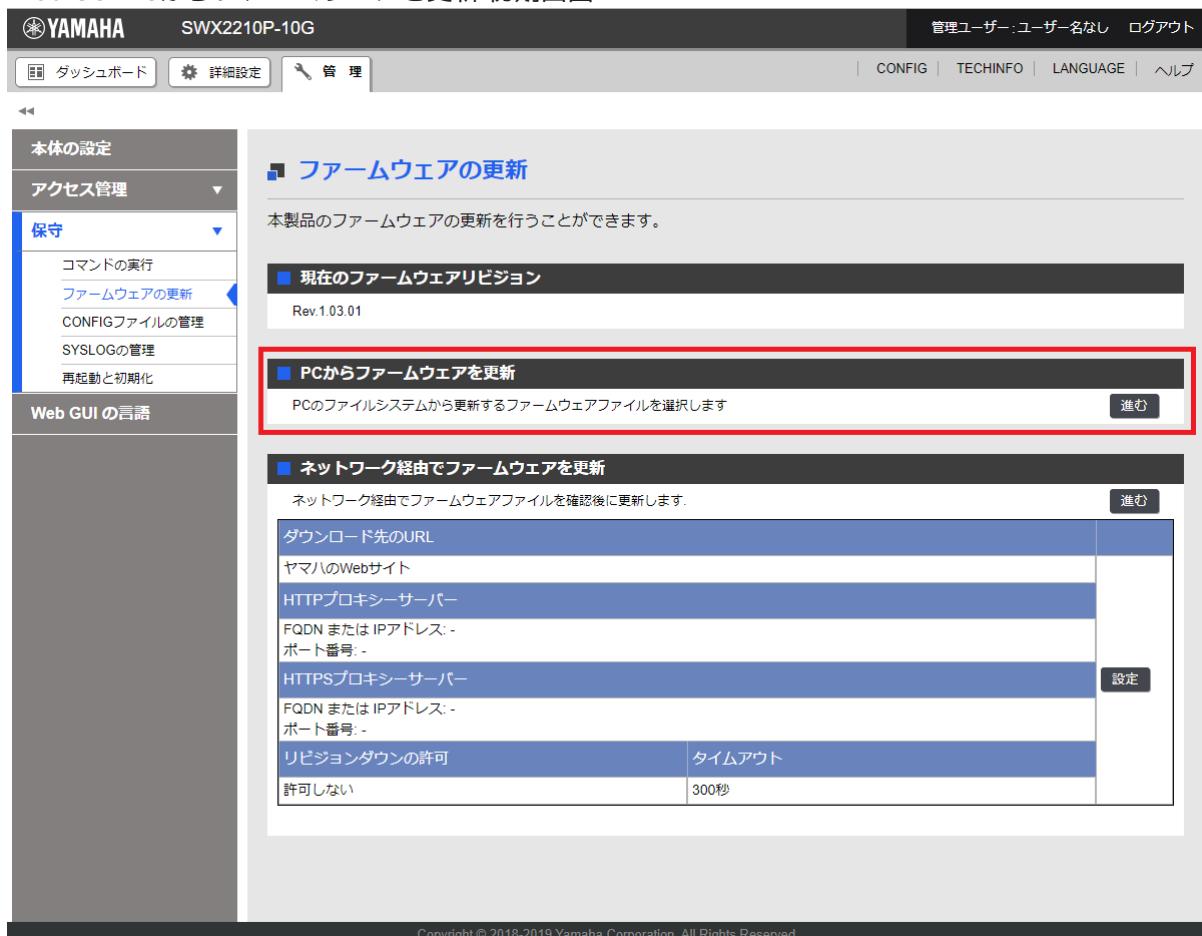
送付した更新ファームウェアに問題がなければ、更新ファームウェアの書き込みを行います。

### Web GUI ローカルファイル指定によるファームウェア更新

Web GUIアクセス中の端末に置かれた更新ファームウェアを指定して、本製品に適用させます。本機能では、新旧バージョンの確認は行わず、指定ファイルを強制的に書き換えます。

ローカルファイル指定によるファームウェアの更新は、Web GUI の [保守] - [ファームウェアの更新] のPCからファームウェアを更新 から行います。(下図の赤枠参照)  
具体的な操作方法は、GUI内のヘルプを参照ください。

- Web GUI PCからファームウェアを更新 初期画面



### HTTPクライアントを使用した更新

HTTPクライアントを使用したファームウェア更新は、指定したURLから更新ファームウェアを取得し、本製品に適用します。

本機能はバージョンアップが前提で、リビジョンダウンの許可が設定されている場合に限り、現バージョン以前のものを書き込むことができます。

同バージョンのファームウェアは書き込むことができません。

HTTPクライアントを使用したファームウェア更新は、以下の方法で実行することができます。

- CLI (Command-line interface) から **firmware-update** コマンドを使用する

- Web GUI の **ネットワーク経由でファームウェアを更新** を実行する

HTTPクライアントを使用したファームウェア更新は、下表の設定値に従って、動作します。

設定パラメータ	説明
ダウンロード先のURL	<p>ファームウェアのダウンロード先URLを設定します。URLは最大255文字まで設定することができます。</p> <p>初期値は、モデル毎に以下が設定されています。</p> <p>SWX2210P-10G: <a href="http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-10g.bin">http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-10g.bin</a>            SWX2210P-18G: <a href="http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-18g.bin">http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-18g.bin</a>            SWX2210P-28G: <a href="http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-28g.bin">http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-28g.bin</a></p>
HTTPプロキシサーバー	ファームウェア更新で使用するプロキシサーバーを設定します。 IPv4/IPv6アドレスまたはFQDNで指定します。FQDNの場合は最大255文字まで設定することができます。
HTTPSプロキシサーバー	初期設定では、プロキシサーバーの設定はありません。
リビジョンダウンの許可	<p>ファーム更新動作において、現在のバージョンより小さいバージョンの書き込みを許可するかどうかを設定します。</p> <p>初期設定では、“許可しない”に設定されています。</p> <p>なお、現在と同じバージョンの書き込みは許可しません。</p>
タイムアウト	<p>以下の処理を行う際の処理完了を監視するためのタイマーを指定します。</p> <ul style="list-style-type: none"> <li>* 新旧ファームウェアのバージョンチェック</li> <li>* 指定URLからのダウンロード</li> </ul> <p>監視タイマーは、<b>100秒～86,400秒</b>で指定可能で、初期設定は<b>300秒</b>に設定されています。</p>

**firmware-update** コマンドの使用方法は、 "[コマンド実行例](#)" または "[コマンドリファレンス](#)" を参照してください。

Web GUI の **ネットワーク経由でファームウェアを更新** は、Web GUI の [保守] - [ファームウェアの更新] から実行します。(下図の赤枠参照)

具体的な操作方法は、GUI内のヘルプを参照してください。

- Web GUI ネットワーク経由でファームウェアを更新 初期画面

The screenshot shows the Yamaha SWX2210P-10G device management interface. The left sidebar has a tree view with '本体の設定' (Main Unit Settings) expanded, showing '保守' (Maintenance) selected. Under '保守', 'ファームウェアの更新' (Firmware Update) is highlighted. The main content area is titled 'ファームウェアの更新' (Firmware Update). It includes sections for '現在のファームウェアリビジョン' (Current Firmware Revision) showing 'Rev.1.03.01', 'PCからファームウェアを更新' (Update Firmware via PC), and 'ネットワーク経由でファームウェアを更新' (Update Firmware via Network). The 'Network via Firmware Update' section is highlighted with a red box. It contains fields for 'ダウンロード先のURL' (Download source URL) with 'ヤマハのWebサイト' (Yamaha's website) selected, 'HTTPプロキシサーバー' (HTTP Proxy Server) with 'FQDN または IP アドレス: -' (FQDN or IP address: -) and 'ポート番号: -' (Port number: -), 'HTTPSプロキシサーバー' (HTTPS Proxy Server) with 'FQDN または IP アドレス: -' (FQDN or IP address: -) and 'ポート番号: -' (Port number: -), 'リビジョンダウンの許可' (Allow Revision Down) with '許可しない' (Do not allow) selected, and 'タイムアウト' (Timeout) set to '300秒' (300 seconds). A '進む' (Next) button is visible at the top right of this panel.

## 書き込み後の再起動

更新ファームウェアの書き込みが正常に完了すると、即時再起動が開始されます。

## 関連コマンド

関連コマンドについて、以下に示します。

詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
ファームウェア更新サイトの設定	firmware-update url
ファームウェア更新で使用するHTTPプロキシサーバーの設定	firmware-update http-proxy
ファームウェア更新で使用するHTTPSプロキシサーバーの設定	firmware-update https-proxy
ファームウェア更新の実行	firmware-update execute
ファームウェアダウンロードタイムアウト時間の設定	firmware-update timeout
リビジョンダウンの許可	firmware-update revision-down
ファームウェア更新機能設定の表示	show firmware-update

## コマンド実行例

## HTTPクライアントを使用した更新

ローカルのHTTPサーバーに更新ファームウェアを置き、本製品のファームウェアを管理するようにして、ファームウェア更新を行います。

- ・ダウンロードのURLを **http://192.168.100.1/swx2210p-10g.bin** に変更します。
- ・リビジョンダウンは、**無効** のまとします。
- ・タイムアウト値は、**300秒** のまとします。

1. ダウンロードURLを変更し、ファームウェア更新の設定を確認します。

```
Yamaha(config)#firmware-update url http://192.168.100.1/swx2210p-10g.bin ①
Yamaha(config)#exit
Yamaha#show firmware-update ②
url:http://192.168.100.1/swx2210p-10g.bin
timeout:300 (seconds)
revision-down:disable
```

① ダウンロード先URLの設定

② ファームウェア更新機能設定の表示

2. ファームウェア更新を実行します。

```
Yamaha#firmware-update execute ①
Found the new revision firmware
Current Revision: Rev.1.03.01
New Revision:     Rev.1.03.02
Update to this firmware? (Y/N)y ②
Download...
%% Completed the firmware download
%% Updating...
```

③

① ファームウェア更新の実行

② yを入力

③ 自動でリブートします

3. 更新ファームウェアのダウンロード中に、"CTRL+C" で中断することができます。

```
Yamaha#firmware-update execute
Found the new revision firmware
Current Revision: Rev.1.03.01
New Revision:     Rev.1.03.02
Update to this firmware? (Y/N)y
Download... ①
%% Canceled the firmware download
```

① Ctrl-C を入力

---

## 注意事項

新部品対応により、Rev.1.03.13以降のファームウェアからRev.1.03.12以前のファームウェアへのバージョンダウンはできません。

## 関連文書

- [LEDインジケーター制御](#)

# L2MS (Layer2 Management Service)

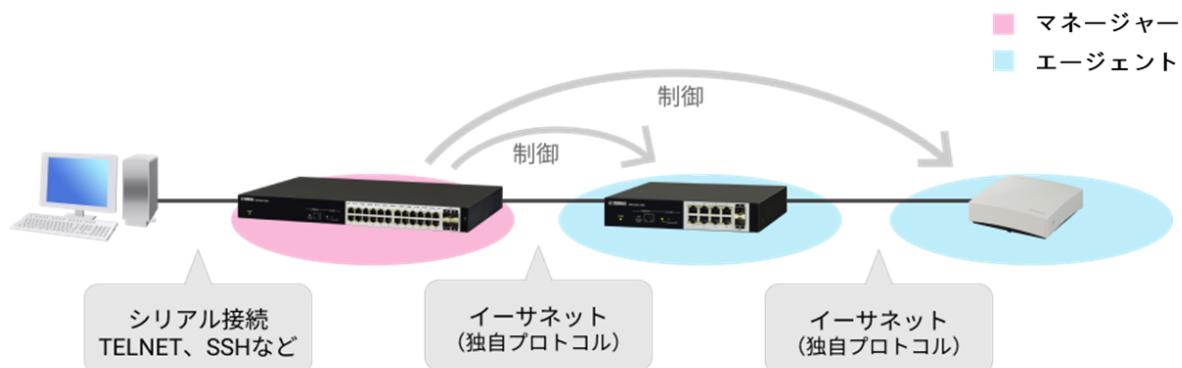
## 機能概要

L2MS (Layer2 Management Service)とは、ヤマハネットワーク機器をレイヤー2レベルで管理する機能です。L2MSは集中制御を行う1台のマネージャーと、マネージャーから制御される複数台のエージェントで構成されます。

SWX2210Pは、L2MSのエージェントとして動作します。

以下にPC、マネージャーおよびエージェントの接続方法を示します。

- L2MS 接続方法



L2MSのマネージャーには、エージェントの管理を行うためのコマンドや、エージェントの設定や状態取得を行うためのWeb GUIが用意されており、これらを利用してエージェントの操作を行います。

マネージャーとエージェントはイーサネットケーブルで接続し、通信には独自プロトコルを使用します。

本機能は次のような特徴を持っています。

- 初期設定が不要  
TELNETやWeb GUIを利用する場合、IPアドレスを設定する必要がありますが、本機能では独自プロトコルを使用して通信を行うため、エージェントへの初期設定は不要です。  
Ethernetケーブルを接続すると、マネージャーは、自動的に配下のエージェントを認識します。
- 複数の対応端末を同時制御  
マネージャーは同時に複数のエージェントを認識し、制御することができます。

SWX2210Pを管理できるマネージャーについての詳細は、各L2MSマネージャーの技術情報を参照してください。

- [技術資料 LANマップ/スイッチ制御GUI/Yamaha LAN Monitor 機能比較表](#)

## 用語の定義

### マネージャー

L2MSおよびスイッチ制御機能のエージェントとして動作している、ヤマハネットワーク機器を管理する機器。ネットワーク内のヤマハスイッチ、ヤマハ無線APを管理する。

### エージェント

L2MSおよびスイッチ制御機能のマネージャーによって管理されるヤマハスイッチ、およびヤマハ無線AP。マネージャーから設定の確認や変更を行うことができる。

## 機能詳細

### 対応機種

SWX2210Pをエージェントとして管理できるマネージャーは以下のリンクよりご確認ください。

- [技術資料 LANマップ/スイッチ制御GUI/Yamaha LAN Monitor 機能比較表](#)

### L2MSのプロトコル

L2MSの制御には以下に示す独自プロトコルのL2フレームを使用します。

- L2MSプロトコルのL2フレーム内容

項目	値
宛先MAC	01:a0:de:00:e8:12 ~ 01:a0:de:00:e8:15
EtherType	0xe812

マネージャーとエージェントとの間にファイアーウォールを設置する場合は、ファイアーウォールにこのL2フレームを通過させる設定を行う必要があります。

また、Yamaha LAN Monitor を使用してSWX2210PシリーズのファームウェアをL2MSで更新する場合、以下のユニキャストL2MSを使用します。

- ユニキャストL2MSプロトコルのL2フレーム内容

項目	値
宛先MAC	ユニキャスト送信先のMACアドレス
EtherType	0xe813

### エージェントの監視

マネージャーは定期的に探索フレームを送信することで配下のエージェントを監視します。

また、エージェントは探索フレームに対して応答フレームを送信することでマネージャーに自身の存在を通知します。

マネージャーから送信される探索フレームの設定についてはマネージャーの技術情報を参照してください。

### エージェントの占有

1つのエージェントを複数のマネージャーが同時に制御することはできません。

このため、マネージャーは同一ネットワーク内に1台となるように設定してください。

エージェントが起動後に探索フレームを受信すると、当該エージェントは探索フレームを送信したマネージャーに管理された状態となります。

この状態は、以下のいずれかの条件により解除されます。

- エージェントが探索フレームを30秒間受信しなかった場合
- マネージャーが再起動したり、L2MSの管理状態がリセットされたりした場合

## エージェントの操作

L2MSに対応したエージェントに対して、マネージャーから設定を行ったり、動作状態を取得したりすることを「エージェントを操作する」と言います。

各マネージャーには、エージェントを操作するためのコマンドやWeb GUIが提供されています。

詳しい操作方法については、各マネージャーの技術情報を参照してください。

## エージェントからの情報通知

マネージャーに管理されているエージェントは、自身の状態が変化したり異常を検出したりすると、マネージャーに情報を通知します。

エージェントからの情報は、マネージャーのSYSLOGやWeb GUIに出力されます。

詳しくは、各マネージャーの技術資料を参照してください。

SWX2210Pが通知する情報は以下のとおりです。

- ・ポートのリンクアップ/ダウン
- ・ループの検出
- ・ファンの異常停止
- ・ポート単位の給電機能の状態
- ・機器単位の給電機能の異常

## L2MSフィルター / non-L2MSフィルター

L2MSフィルター機能を使用することで、L2MS制御で使用するL2MS制御フレームの送受信を禁止することができます。

また、non-L2MSフィルター機能を使用することで、L2MS制御フレーム以外の送受信を制限することができます。

L2MSフィルター / non-L2MSフィルターはポート単位で設定することができ、それぞれ **l2ms filter**, **non-l2ms filter** コマンドを使用し、設定します。

## L2MSの有効化 / 無効化

**l2ms enable**, **l2ms disable** コマンドでL2MSの有効 / 無効を切り替えることができます。

L2MSを無効にした場合、L2MS制御フレームはL2MS制御フレーム以外のフレームと同様に転送され、L2MSマネージャーから管理することができなくなります。

初期設定でL2MSは有効です。

## 初期IPアドレスについて

工場出荷の状態や **cold start** コマンド実行直後は、固定のIPアドレスが設定されています。（L2MSはエージェントとして動作する）

この時、マネージャーに管理されると、**自動的にDHCPクライアントの設定が行われます。**

これは、エージェントが複数存在した場合に、IPアドレスが重複することを回避するためです。

IPアドレスは、ネットワーク内のDHCPサーバーから配布されるので、HTTP Proxy経由でエージェントのWeb GUIへアクセスすることができます。

ネットワーク内にDHCPサーバーが存在しない場合、IPアドレスが取得できませんので、マネージャーのLANマップにて、エージェントのIPアドレスの設定を行ってください。

設定が行われ、スタートアップコンフィグが保存されれば、以後、自動的にDHCPクライアントに設定されることはありません。

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

- ・インターフェース基本機能 関連コマンド一覧

操作項目	操作コマンド
L2MSモードへの移行	l2ms configuration
L2MS機能の設定	l2ms enable
L2MS制御フレームの送受信設定	l2ms filter
L2MS制御フレーム以外のフレームの送受信設定	non-l2ms filter
L2MS情報の表示	show l2ms

## コマンド実行例

### L2MSフィルターの設定

- ・LANポート#1 (port1.1)において、L2MS制御フレームを送受信しないようにします。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#l2ms filter enable
```

### L2MSの設定

- ・L2MSを無効化し、L2MSマネージャーから管理できないようにします。

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#l2ms disable
```

## 注意事項

L2MSを利用する際の注意事項については各マネージャーの技術情報を参照してください。

### 他機能との併用について

#### ループ検出機能との併用

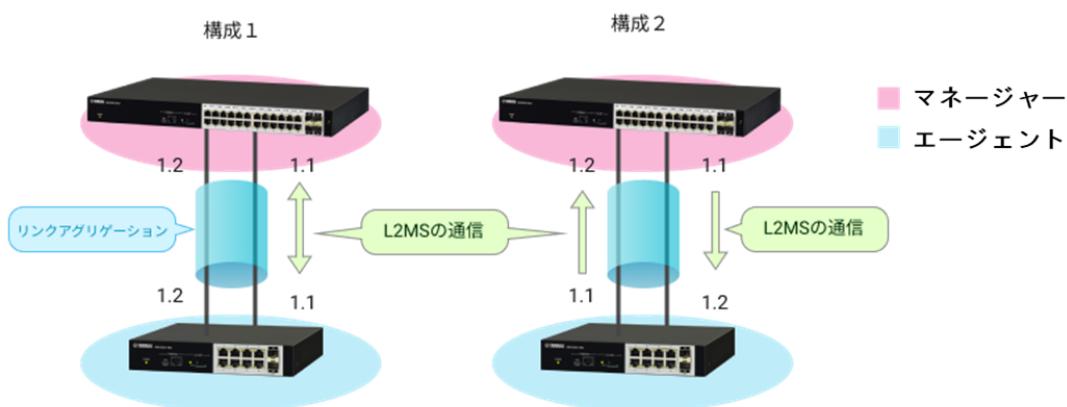
ループ検出機能でブロッキング状態になったポートではL2MSの通信を行うことができません。

#### リンクアグリゲーションとの併用

リンクアグリゲーションを使用している場合、L2MSの通信は「論理インターフェースに所属しているLANポートのうち、リンクアップしている最も小さい番号のポート」で行われているものと見なされます。また、リンクアグリゲーションと接続端末の監視機能を併用しているときに、論理インターフェースに繋がっている先で端末を発見した場合、端末は「論理インターフェースに所属しているLANポートのうち、リンクアップしている最も小さい番号のポート」に繋がっているものと見なされ、該当ポート番号が表示されます。

構成1の場合は、L2MSの通信がport1.1同士で行われているものと見なされます。

構成2の場合は、L2MSの通信がマネージャーのport1.1とエージェントのport1.1とで行われているものと見なされます。



### ルーターL2MSマネージャーのスイッチ制御コマンドの使用

ルーターL2MSマネージャーのスイッチ制御コマンドはSWX2200シリーズ用のコマンドであり、SWX2210Pシリーズに対しての使用は非対応です。

ただし、**switch control function execute start-poe-supply** コマンドおよび**switch control function execute stop-poe-supply** コマンドによる給電制御には対応しています。

### SYSLOGメッセージ一覧

L2MSによって出力されるSYSLOGを以下に示します。

出力されるメッセージには、"[ L2MS]"というプレフィックスが付与されます。

出力レベル	メッセージ	意味
Informational	Start L2MS(Agent)	エージェントとしてL2MSが起動した。
	Start management by manager (<Manager_MAC_Address>)	マネージャーの管理下に入った。
	Release from manager (<Manager_MAC_Address>)	マネージャーの管理下から外れた。
	Received config from manager (<Manager_MAC_Address>)	マネージャーからCONFIGを受信した。
	Restart for update settings.	マネージャーから受信したCONFIGを反映し、再起動を行った。
	Send config to manager (<Manager_MAC_Address>)	マネージャーにCONFIGを送信した。

### 関連文書

- ヤマハルーターのスイッチ制御機能

# LLDP

## 機能概要

LLDPは、隣接機器と自身の機器との間で、装置の管理情報を受け渡すためのプロトコルです。

## 用語の定義

### LLDP

Link Layer Discovery Protocol。  
IEEE 802.1ABで規定される。

### LLDP-MED

LLDP for Media Endpoint Devices。  
ANSI/TIA-1057で規定される。

## 機能詳細

### 動作仕様

#### 基本仕様

本製品では、以下の動作をサポートしています。

- 任意のLANポートからLLDPフレームを送信して、自身の機器の情報を通知する。
- 任意のLANポートでLLDPフレームを受信して隣接機器の情報を収集する。

LLDPは、TLVと呼ばれるタイプ(Type)、長さ(Length)、値(Value)の属性を使用して情報を送受信します。本製品で送信するTLVについては、[TLV一覧](#) を参照してください。

LLDP機能を使用するためには以下の設定が必要です。

- lldp run** コマンドで、システム全体のLLDP機能を有効にします。
- lldp-agent** コマンドで、対象のインターフェースにLLDPエージェントを作成します。
- set lldp** コマンドで、LLDPフレームの送受信モードを設定します。

本製品の初期設定では、LLDP機能は **有効** です。

LLDPフレームは、送信スイッチポートのVLAN設定にかかわらず、つねにタグなしで送信します。ネイティブVLANなしのトランクポートからもタグなしで送信します。

### 送信情報の設定

本製品では、基本管理TLVで送信する管理アドレスの種類のみ **set management-address-tlv** コマンドで設定することができます。その他の送信情報を変更することはできません。

自身の機器から送信するLLDPフレームには、常に以下のTLVが含まれます。詳細は [3.2 TLV一覧](#) を参照してください。

- 必須TLV
- 基本管理TLV

- 
- IEEE 802.1 TLV
  - IEEE 802.3 TLV
  - LLDP-MED TLV（隣接する機器からLLDP-MED TLVを含むLLDPフレームを受信した場合のみ）

### 送信タイマーの設定

LLDP フレームの送信間隔は、 **set timer msg-tx-interval** コマンドで設定します。

また、機器情報の保持時間(TTL)を算出するための乗数は、 **set msg-tx-hold** コマンドで設定します。

LLDPで送信するTTLは、以下の計算式の算出値となります。デフォルトは **121** 秒です。

- TTL = ( **set timer msg-tx-interval** コマンドの設定値 ) × ( **set msg-tx-hold** コマンドの設定値 ) + 1 (秒)

### 最大接続台数の設定

該当ポートで管理できる機器の最大接続台数は、 **set too-many-neighbors limit** コマンドで設定します。

最大接続台数の初期値は **5台** です。

### LLDP情報の確認

LLDPのインターフェース設定情報や受信した隣接機器の情報は、 **show lldp interface** コマンドや **show lldp neighbors** コマンドで確認できます。

また、LLDP フレームカウンターは、 **clear lldp counters** コマンドでクリアできます。

### TLV一覧

本製品で対応しているTLV一覧は以下のとおりです。

- 必須TLV
- 基本管理TLV
- IEEE 802.1 TLV
- IEEE 802.3 TLV
- LLDP-MED TLV

各TLVの詳細な仕様については、IEEE 802.1AB (LLDP)、ANSI/TIA-1057 (LLDP-MED) をご確認ください。  
以下では、本製品で送信するTLVについて説明します。

#### 必須TLV

LLDP対応機器が必ず送信するTLVです。

シャーシID、ポートID、TTLの3つを送信します。

必須TLVを以下に示します。

Type	説明	Length	Value (固定値のみ記載)
Chassis ID	シャーシID	6 Byte	機器のMACアドレス
Port ID	ポートID	7 ~ 8 Byte	ポート名(port1.X)
Time To Live (TTL)	機器情報の保持時間(秒)	2 Byte	

## 基本管理TLV

名称、保有する機能、アドレスなどのシステムに関する管理情報のTLVです。  
基本管理TLVを以下に示します。

Type	説明	Length	Value (固定値のみ記載)
Port Description	ポートの説明文字列	7 ~ 8 Byte	
System Name	システム名称文字列	10 ~ 10 Byte	
System Description	システムの説明文字列	28 Byte	SWX2210P-XXG Rev.1.03.XX
System Capabilities	システムがサポートする機能	2 Byte	0x0004 (bridge)
	有効状態になっているシステムの機能	2 Byte	0x0004 (bridge)
Management Address	管理用アドレス IP アドレス(4 Byte) または MACアドレス(6 Byte)	4 or 6 Byte	
	インターフェースサブタイプ	1 Byte	0x02 (ifIndex)
	インターフェース番号	1 ~ 2 Byte	ifIndex値

## IEEE 802.1 TLV

該当ポートのVLANやリンクアグリゲーションなどの情報のTLVです。  
IEEE 802.1 TLVを以下に示します。

Type	説明	Length	Value (固定値のみ記載)
Port VLAN ID	ポートVLAN番号	2 Byte	
Port and Protocol VLAN ID	プロトコルVLANのサポートおよび有効/無効	1 Byte	0x00 (no support)
	プロトコルVLAN番号	2 Byte	0x0000
Protocol Identity	プロトコルを特定するバイト列	0 ~ 255 Byte	
Link Aggregation	アグリゲーション能力の有無と状態	2 Byte	
	アグリケーション論理インターフェースのifIndex番号	1 ~ 2 Byte	
VLAN Name	ポートが所属するVLANの名称	0 ~ 32 Byte	

## IEEE 802.3 TLV

該当ポートのオートネゴシエーションサポート情報や最大フレームサイズの情報などを送信するTLVです。  
IEEE 802.3 TLVを以下に示します。

Type	説明	Length	Value (固定値のみ記載)
MAC/PHY Configuration/Status	オートネゴシエーションのサポートと有効/無効	1 Byte	
	オートネゴシエーション可能な通信方式	2 Byte	LANポート : 0x6C01(10/100 /1000M)
	Operational MAU Type 通信速度とデュプレックスモード (IETF RFC 4836)	2 Byte	
Power Via MDI	MDI パワーサポートステータス	1 Byte	
	PSE パワーペア 給電時に使用する配線の選択	1 Byte	0x01 (信号線)
	パワークラス Class0 ~ Class4	1 Byte	
	パワータイプ PSE Device/PD Device	2 bit	0b00 (PSE Device)
	パワーソース Primary/Secondary	2 bit	0b01 (Primary)
	優先度	2 bit	
	PD機器からの要求電力 (0.1 Watt 単位)	2 Byte	
	PSE機器の供給電力 (0.1 Watt 単位)	2 Byte	
Maximum Frame Size	最大フレームサイズ	2 Byte	

#### LLDP-MED TLV

隣接する機器からLLDP-MED TLVを含むLLDPフレームを受信した場合、本製品から送信されるLLDPフレームにもこのTLVが含まれるようになります。  
LLDP-MED TLVを以下に示します。

Type	説明	Length	Value (固定値のみ記載)
LLDP-MED Capabilities	送信可能な LLDP-MED TLV	2 Byte	0x0009 (LLDP-MED Capabilities, Extended Power-via-MDI TLV )
	デバイスタイプ	1 Byte	0x04 (Network Connectivity)

Type	説明	Length	Value (固定値のみ記載)
Extended Power-via-MDI	パワータイプ PSE Device/PD Device	2 bit	0b00 (PSE Device)
	パワーソース Primary/Secondary	2 bit	0b01 (Primary)
	パワー優先度	4 bit	
	PDからの要求電力(0.1 Watt 単位)	2 Byte	

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
LLDP機能の有効化	lldp run
LLDPエージェントの作成	lldp-agent
LLDP送受信モードの設定	set lldp
管理アドレスの種類の設定	set management-address-tlv
LLDP フレームの送信間隔の設定	set timer msg-tx-interval
機器情報の保持時間(TTL)を算出するための乗数の設定	set msg-tx-hold
ポート単位で管理できる機器の最大接続台数の設定	set too-many-neighbors limit
インターフェースの状態表示	show lldp interface
全てのインターフェースにおける接続機器の情報表示	show lldp neighbors
LLDP フレームカウンターのクリア	clear lldp counters

## コマンド実行例

### LLDPフレームの送受信の設定

port1.1でLLDPフレームの送受信を有効にします。  
LLDPフレームの送信間隔を60秒にします。LLDPフレームのTTLは181秒にします。  
ポートで管理する最大接続機器台数を10にします。

```

Yamaha#configure terminal
Yamaha(config)#interface port1.1
Yamaha(config-if)#lldp-agent ①
Yamaha(lldp-agent)#set timer msg-tx-interval 60 ②
Yamaha(lldp-agent)#set msg-tx-hold 3 ③
Yamaha(lldp-agent)#set too-many-neighbors limit 10 ④
Yamaha(lldp-agent)#set lldp enable txrx ⑤
Yamaha(lldp-agent)#exit

```

```
Yamaha(config-if)#exit  
Yamaha(config)#lldp run ⑥  
Yamaha(config)#exit
```

- ① LLDPエージェントの作成、モード遷移
- ② 送信間隔の設定
- ③ TTL算出の乗数の設定 : TTL = 60 × 3 + 1 = 181秒
- ④ 最大接続台数の設定
- ⑤ LLDP送受信モードの設定
- ⑥ LLDP機能の有効化

### LLDP インターフェース状態の表示

port1.1 のLLDP インターフェース情報を表示します。

```
Yamaha#show lldp interface port1.1 ①  
Agent Mode : Nearest bridge  
Enable (tx/rx) : Y/Y  
Message fast transmit time : 1  
Message transmission interval : 60  
Reinitialisation delay : 2  
MED Enabled : Y  
Device Type : NETWORK_CONNECTIVITY  
LLDP Agent traffic statistics  
Total frames transmitted : 1  
Total entries aged : 0  
Total frames received : 0  
Total frames received in error : 0  
Total frames discarded : 0  
Total discarded TLVs : 0  
Total unrecognised TLVs : 0
```

- ① インターフェース情報の表示

### LLDP 接続機器の情報の表示

LLDP 接続機器の情報を表示します。

```
Yamaha#show lldp neighbors ①  
Interface Name : port1.1  
System Name : SWX2210P  
System Description : SWX2210P-28G Rev.1.03.13  
Port Description : port1.1  
System Capabilities : L2 Switching  
Interface Numbering : 2  
Interface Number : 5001  
OID Number :  
Management IP Address : 192.168.100.241  
Mandatory TLVs  
CHASSIS ID TYPE  
Chassis MAC ADDRESS : ac44.f284.ef22  
PORT ID TYPE
```

```
INTERFACE NAME : port1.1
TTL (Time To Live) : 121
8021 ORIGIN SPECIFIC TLVs
Port Vlan id : 1
PP Vlan id : 0
Remote VLANs Configured
VLAN ID : 1
VLAN Name : default
Remote Protocols Advertised:
IPv4
Remote VID Usage Digest : 0
Remote Management Vlan : 0
8023 ORIGIN SPECIFIC TLVs
AutoNego Support : Supported Enabled
AutoNego Capability : 27649
Operational MAU Type : 30
Power via MDI Capability (raw data)
MDI power support : 0x2
PSE power pair : 0x1
Power class : 0x0
Type/source/priority : 0x0/0x1/0x3
PD requested power value : 0.0 W
PSE allocated power value : 0.0 W
Link Aggregation Status : Disabled
Link Aggregation Port ID : 0
Max Frame Size : 1522
```

① 接続機器の情報の表示

## 注意事項

特になし

## 関連文書

特になし

# LLDP自動設定

## 機能概要

LLDP自動設定は、独自のLLDPフレームを送受信し、LLDPで通知された情報をもとに自動的に設定を行ったり、ログ保存などの特定の処理を実行したりする機能です。

LLDP自動設定を使用することで自動設定および自動実行される内容は以下のとおりです。

- Dante最適設定
  - ヤマハの遠隔会議システムADECIAの構成機器が接続されたとき、「Dante」を利用する上での最適な設定を自動的に反映させます。
- スケジュール機能による給電停止の事前通知
  - ヤマハ無線APが接続されているポートでPoE給電の停止がスケジューリングされているとき、給電の停止タイミングを事前に通知し、ヤマハ無線APは給電が停止される直前にログの保存を行います。

ヤマハスイッチとヤマハ無線APのLLDP自動設定の対応機種については、[技術資料 LLDP自動設定の設定例](#) を参照してください。

ADECIAの構成機器については、[ADECIA製品情報](#) を参照してください。

## 用語の定義

### LLDP

Link Layer Discovery Protocol。  
IEEE 802.1ABで規定される。

### ADECIA

ヤマハの遠隔会議システム。遠隔会議用プロセッサー、マイク、スピーカーをLAN(Dante)で接続する。

### ADECIAコンポーネント

ADECIAを構成する機器（遠隔会議用プロセッサー、マイク、スピーカー）。

## 機能詳細

### 基本仕様

LLDP自動設定を有効にすると独自のLLDPフレームの送受信を行います。

LLDP自動設定全体の有効/無効は、**lldp auto-setting** コマンドで設定します。  
本製品の初期設定では**有効**に設定されています。

LLDP自動設定で有効にする機能の選択は、**lldp auto-setting function** コマンドで設定します。  
本製品の初期設定では、**すべての機能を使用**に設定されています。

本機能を使用するためには、LLDPフレームを受信できるようにする必要があります。  
そのため、事前に以下が設定されていることを確認してください。

- **lldp run** コマンドで、システム全体のLLDP機能を有効にします。

- **lldp-agent** コマンドで、対象のインターフェースにLLDPエージェントを作成します。
- **set lldp** コマンドで、LLDPフレームの送受信モードを設定します。

本製品の初期設定では、LLDPフレームの送受信は **有効** です。

### Dante最適設定

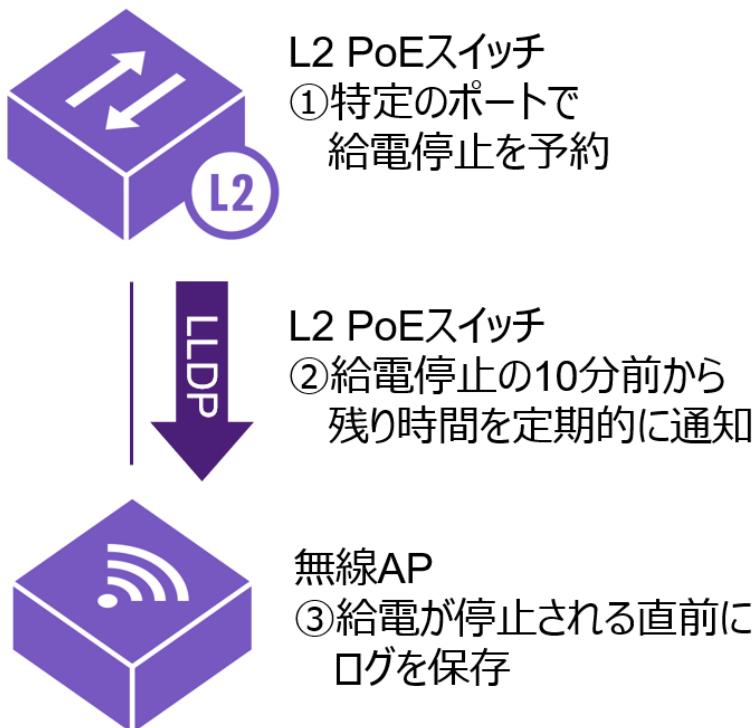
ADECIAコンポーネントから独自のLLDPフレームを受信することで、「Dante」を利用する上での最適な設定を自動的に反映させる機能です。

詳細については、[Dante最適設定](#)を参照してください。

### スケジュール機能による給電停止の事前通知

ヤマハスイッチの特定のポートでPoE給電停止がスケジュールされているとき、給電停止の10分前からスケジュール実行までの残り時間をLLDPで定期的に通知する機能です。

LLDPで給電停止までの残り時間を通知された無線APは、給電が停止される直前にログの保存を実行することで、電源断によるログの消失を防止できます。



特定のポートでLLDPの送信間隔が30秒よりも大きな値に設定されているとき、以下の条件を満たすとLLDPの送信間隔が強制的に30秒に変更されます。

- LLDPかつLLDP自動設定が有効になっている。
- 特定のポートでPoE給電の停止がスケジューリングされている。
- スケジュール実行までの残り時間が10分未満になっている。

なお、スケジュールが実行されるか、スケジュール設定が削除、もしくは10分以上後の時刻に設定変更された場合、LLDP送信間隔は元の設定値に戻ります。

本機能によってLLDPの送信間隔が強制的に30秒に変更されている場合、**show lldp interface** コマンドで表示されるLLDP送信間隔にアスタリスク (\*) が付与されます。

- **show lldp interface** コマンドによるLLDP送信間隔表示例

```

SWX#show lldp interface port1.2
Agent Mode : Nearest bridge
Enable (tx/rx) : Y/Y
Message fast transmit time : 1
Message transmission interval : 30*
Reinitialization delay : 2
MED Enabled : Y
Device Type : NETWORK_CONNECTIVITY
LLDP Agent traffic statistics
  Total frames transmitted : 0
  Total entries aged : 0
  Total frames received : 0
  Total frames received in error : 0
  Total frames discarded : 0
  Total discarded TLVs : 0
  Total unrecognised TLVs : 0

```

\* - Assigned by LLDP.

本機能を使用する場合、以下の点に注意してください。

- ・ **注意点**

- ・ 給電停止の事前通知は、特定のポートで給電停止がスケジュールされている場合にのみ通知されます。システム全体で給電の停止がスケジュールされている場合は通知されないためご注意ください。

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
LLDP自動設定の有効化	lldp auto-setting
LLDP自動設定で有効化する機能の設定	lldp auto-setting function
LLDP機能の有効化	lldp run
LLDPエージェントの作成	lldp-agent
LLDP送受信モードの設定	set lldp
インターフェースの状態表示	show lldp interface

## 設定例

ヤマハスイッチとヤマハ無線APのそれぞれの設定方法については以下を参照してください。

- ・ [技術資料 LLDP自動設定の設定例](#)

## 注意事項

特になし。

---

## 関連文書

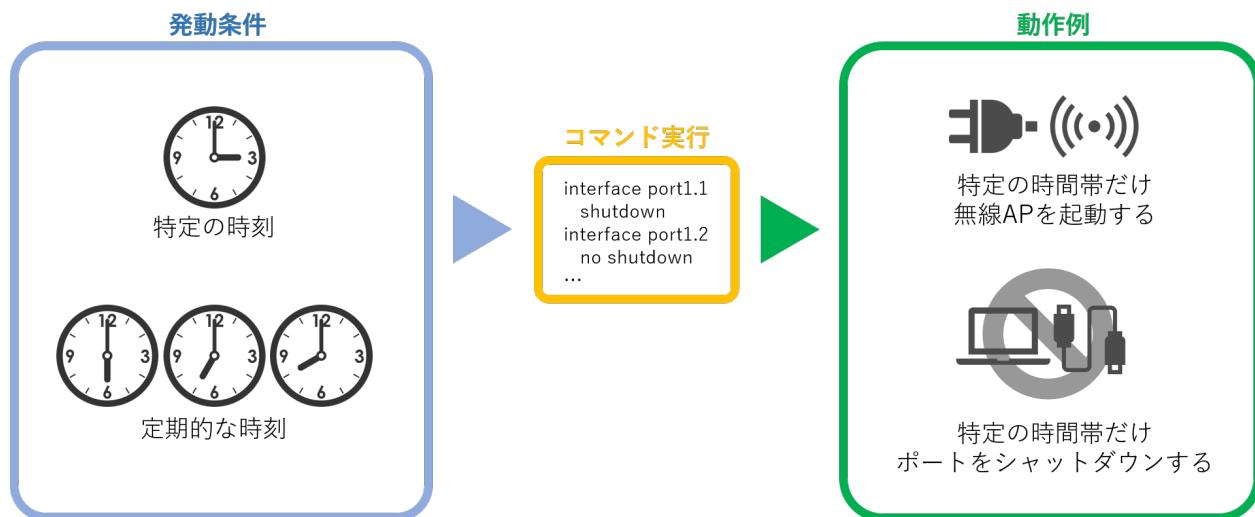
- [LLDP](#)
- [Dante最適設定](#)
- [スケジュール機能](#)
- [技術資料 LLDP自動設定の設定例](#)
- [ADECIA製品情報](#)

# スケジュール機能

## 機能概要

スケジュール機能は、任意の時刻やイベントの発生に起因して特定の処理を実行させる機能です。本機能を利用することで、以下のような動作をヤマハスイッチで行うことができます。

- ・ 特定の時間帯だけ無線LANアクセスポイントへのPoE給電を行う（PoE対応モデルのみ）
- ・ 特定の時間帯だけポートをシャットダウンする



本製品で実行できる機能については、[機能詳細](#) および [実行可能コマンド](#) を参照してください。

## 用語の定義

### トリガー

内部時計の時刻と指定時刻の合致や、任意のイベントの発生といった、特定の条件の総称

### 時刻トリガー

内部時計の時刻と指定時刻が合致するという条件

### アクション

トリガが起動したことによって実行される動作

## 機能詳細

スケジュール機能は、発動条件として「トリガー」、動作として「アクション」の2つを指定することによって、任意の時刻やイベントの発生に起因して特定の処理を実行させる機能です。本製品は **時刻トリガー** にのみ対応しています。

### 時刻トリガー

任意の年月日および任意の時分秒を時刻トリガーとして指定することができます。

時刻トリガーは **schedule** コマンドで設定します。

指定可能な条件は以下となります。

種別		指定方法	設定値の例
日付	月 1-12	任意の月のみ (例:12月のみ)	12
		任意の複数の月のみ (例:1月と2月のみ)	1,2
		任意の月から12月まで (例:2月から12月まで)	2-
		任意の月から任意の月まで (例:2月から7月まで)	2-7
		1月から任意の月まで (例:1月から7月まで)	-7
		毎月	*
	日 1-31	任意の日のみ (例:1日のみ)	1
		任意の複数の日のみ (例:1日と2日のみ)	1,2
		任意の日から月末まで (例:2日から月末まで)	2-
		任意の日から任意の日まで (例:2日から7日まで)	2-7
		1日から任意の日まで (例:1日から7日まで)	-7
		毎日	*
		任意の曜日のみ (例:月曜日のみ)	mon
		任意の複数の曜日のみ (例:土曜日と日曜日のみ)	sat,sun
		任意の曜日から任意の曜日まで (例:月曜日から金曜日まで)	mon-fri
		日曜日から任意の曜日まで (例:日曜日から金曜日まで)	-fri
時分秒	時 0-23	任意の時のみ (例:23時のみ)	23
		任意の複数の時のみ (例:1時と22時のみ)	1,22
		任意の時から23時まで (例:2時から23時まで)	2-
		任意の時から任意の時まで (例:2時から21時まで)	2-21
		0時から任意の時まで (例:0時から21時まで)	-21
		毎時	*
	分 0-59	任意の分のみ (例:59分のみ)	59
		任意の複数の分のみ (例:1分と50分のみ)	1,50
		任意の分から59分まで (例:2分から59分まで)	2-
		任意の分から任意の分まで (例:2分から50分まで)	2-50
		0分から任意の分まで (例:0分から50分まで)	-50
		毎分	*
	秒 0-59	任意の秒のみ (例:59秒のみ)	59
		省略可能	

## アクション

時刻トリガーが起動することによって実行される動作をアクションと呼びます。

アクションの指定は **schedule template** コマンドでスケジュールテンプレートモードに遷移してから **cli-command** コマンドで設定します。

本製品では以下のアクションに対応しています。

動作	設定コマンド	説明
指定コマンドの実行	cli-command コマンド	指定されたコマンドをIDが小さい方から順に実行する。

## 関連コマンド

関連コマンドについて、以下に示します。

コマンドの詳細は、コマンドリファレンスを参照してください。

操作モード	コマンド	説明
グローバルコンフィグレーションモード	schedule	トリガーの指定とアクションを定義したスケジュールテンプレートIDの指定
	schedule template	スケジュールテンプレートIDを指定し、スケジュールテンプレートモードへ遷移
スケジュールテンプレートモード	description	スケジュールテンプレートの説明の設定
	action	スケジュールテンプレートの有効・無効の設定 一時的にスケジュール機能を無効にしたい場合に disable とする。
	cli-command	トリガーの起動によって実行されるコマンド定義

## 設定例

### 特定の時間帯だけ無線LANアクセスポイントにPoE給電する場合（PoE対応モデルのみ）

平日の8:00から17:00だけport1.1とport1.2に接続されている無線LANアクセスポイントにPoE給電を行います。

```
Yamaha#
Yamaha# configure terminal
Yamaha(config)# schedule 1 time */mon-fri 8:00:00 1
Yamaha(config)# schedule template 1
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.1
Yamaha(config-schedule)# cli-command 3 power-inline enable
Yamaha(config-schedule)# cli-command 4 interface port1.2
Yamaha(config-schedule)# cli-command 5 power-inline enable
Yamaha(config-schedule)# exit
Yamaha(config)#
Yamaha(config)# schedule 2 time */mon-fri 17:00:00 2
Yamaha(config)# schedule template 2
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.1
Yamaha(config-schedule)# cli-command 3 power-inline disable
```

```
Yamaha(config-schedule)# cli-command 4 interface port1.2
Yamaha(config-schedule)# cli-command 5 power-inline disable
Yamaha(config-schedule)# end
Yamaha#
```

### 特定の時間帯だけポートをシャットダウンする場合

金曜日の17:00から翌週の月曜日の8:00までの間、port1.3とport1.4をシャットダウンします。

```
Yamaha#
Yamaha# configure terminal
Yamaha(config)# schedule 1 time */fri 17:00:00 1
Yamaha(config)# schedule template 1
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.3
Yamaha(config-schedule)# cli-command 3 shutdown
Yamaha(config-schedule)# cli-command 4 interface port1.4
Yamaha(config-schedule)# cli-command 5 shutdown
Yamaha(config-schedule)# exit
Yamaha(config)#
Yamaha(config)# schedule 2 time */mon 8:00:00 2
Yamaha(config)# schedule template 2
Yamaha(config-schedule)# cli-command 1 configure terminal
Yamaha(config-schedule)# cli-command 2 interface port1.3
Yamaha(config-schedule)# cli-command 3 no shutdown
Yamaha(config-schedule)# cli-command 4 interface port1.4
Yamaha(config-schedule)# cli-command 5 no shutdown
Yamaha(config-schedule)# end
Yamaha#
```

## 実行可能コマンド

スケジュール機能では、以下のコマンドのみ実行することができます。

- configure terminal
- interface
- shutdown
- no shutdown
- power-inline disable (PoE対応モデルのみ)
- power-inline enable (PoE対応モデルのみ)
- write
- end
- exit (特権EXECモードでは実行できません)

## SYSLOG

スケジュール機能では、以下のSYSLOGが outputされます。

レベル	出力	説明
Info	[SCHEDULE]:inf: ID:X command is done	トリガーの起動によりスケジュールテンプレートID:Xのコマンドが実行された
Error	[SCHEDULE]:err: Execution failed at schedule template ID: X, cli-command ID: Y.	スケジュールテンプレートID:Xでcli-command ID:Yの実行に失敗した

## 注意事項

- アクションが実行されるとき、cli-commandはIDが小さい方から実行されます。
- アクションが実行されるとき、cli-commandで指定したコマンドが実行エラーになったとしても残りのコマンドは実行されます。
- 複数のトリガーが同時に起動したときは、スケジュールテンプレートIDが小さい方から順にアクションが実行されます。
- clock setコマンドによる時刻手動設定およびNTPによる時刻更新によってトリガー起動の時刻が経過してしまった場合、現在時刻が変更された時点から59秒以内に起動すべきトリガーが存在した場合には、そのトリガーは起動されます。
- clock setコマンドによる時刻手動設定およびNTPによる時刻更新によって時刻が後退した場合、後退後の時刻から再度時刻トリガーのチェックが行われます。
- 本機能を用いることで、コンフィグの保存など定期的に行うことができますが、定期的な書き込みはROMの消耗を早めます。頻繁に書き込みを行ったことが原因でROMの故障に至った場合は、保証期間内であっても無償修理の対象外となりますのでご注意ください。

## 関連文書

- 特になし

# Dante最適設定

## 機能概要

Dante最適設定機能とは、デジタルオーディオネットワーク「Dante」に最適な環境を簡単に構築するための機能です。

ユーザーはDante用の個別の設定（QoSの設定、IGMPスヌーピングの設定、フロー制御の無効化設定、EEEの無効化設定など）を意識することなく、まとめて簡単に設定できます。

## 用語の定義

### Dante

Audinate社が開発したデジタルオーディオネットワークの規格。

### ADECIA

ヤマハの遠隔会議システム。遠隔会議用プロセッサーやマイク、スピーカーをLAN(Dante)で接続する。

### ADECIAコンポーネント

ADECIAを構成する機器（遠隔会議用プロセッサー、マイク、スピーカー）。

### LLDP

隣接機器に対して自身の機器情報を受け渡すためのプロトコル。

## 機能詳細

Dante最適設定は、次の2つの方法で適用できます。

- LLDPによる自動最適設定
  - ADECIAコンポーネントから独自のLLDPフレームを受信することで自動的に適用
- Web GUIからの手動最適設定
  - 本製品のWeb GUIのProAV設定ページからDanteプロファイルを適用

Dante最適設定機能によりまとめて設定される項目の一覧を以下に示します。LLDPによる自動最適設定の場合、ADECIAコンポーネントのファームウェアバージョンにより適用対象項目が異なります。

設定対象	機能	コマンド	適用対象項目		
			LLDP (ADECIA V2.5以前)	LLDP (ADECIA V2.8以降)	Web GUI
システム全体	フロー制御を無効	flowcontrol disable			○
	QoSを有効	qos enable	○	○	○
	DSCP値による送信キューの最適化	qos dscp-queue 8 2	○	○	○
		qos dscp-queue 26 3		○	○
		qos dscp-queue 34 4		○	○
		qos dscp-queue 46 5	○	○	○
		qos dscp-queue 48 5		○	○
		qos dscp-queue 56 7	○	○	○
		qos dscp-queue [上記以外] 0	○	○	○
	スケジューリング方式の設定	qos scheduling sp	○	○	○
	リンクローカルマルチキャストの常時転送	l2-unknown-mcast forward link-local		○	○
	MRUを設定	mru 1522			○
	LLDPを有効	lldp run		○	○
VLANインターフェース	プロファイル種別の設定	proav profile-type dante-primary/dante-secondary			○
	未知のマルチキャストをフラッディング	l2-unknown-mcast flood		○	○
	IGMPスヌーピングを有効	ip igmp snooping enable	○	○	○
	IGMPスヌーピングのバージョンを設定	ip igmp snooping version 3	○	○	○
	IGMPスヌーピングの高速脱退を有効	ip igmp snooping fast-leave auto-assignment		○	○

設定対象	機能	コマンド	適用対象項目		
			LLDP (ADECIA V2.5以前)	LLDP (ADECIA V2.8以降)	Web GUI
VLANインターフェース	IGMPクエリー送信機能を有効	ip igmp snooping querier	○	○	○
	IGMPクエリー送信間隔の設定	ip igmp snooping query-interval 30	○	○	○
	IGMP/パケットのTTL値検証機能を無効	ip igmp snooping check ttl disable	○	○	○
	IGMP/パケットのRA検証機能を無効	ip igmp snooping check ra disable		○	○
	IGMP/パケットのToS検証機能を無効	ip igmp snooping check tos disable		○	○
	IGMPレポート抑制機能を無効	ip igmp snooping report-suppression disable		○	○
	IGMPレポート転送機能を有効	ip igmp snooping report-forward enable		○	○
	マルチキャストルーターポート転送抑制機能を有効	ip igmp snooping mrouter-port data-suppression enable		○	○
	PTP/パケットの常時転送を設定	I2-mcast flood 224.0.1.129		○	○
		I2-mcast flood 224.0.1.130		○	○
		I2-mcast flood 224.0.1.131		○	○
		I2-mcast flood 224.0.1.132		○	○
		I2-mcast flood 239.254.3.3		○	○

LAN/SFPポート	QoSトラストモードをDSCPに設定	qos trust dscp	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
フロー制御を無効	flowcontrol disable		<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
EEEを無効	eee disable		<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
LLDPの送受信を有効	lldp-agent / set lldp enable tx rx			<input checked="" type="radio"/>	<input checked="" type="radio"/>

なお、Dante最適設定機能は、スイッチとしての基本的な設定(VLANやIPなど)をすべて行った上で使用してください。

新たに設定変更をした場合、Dante最適設定は追従しません。

### LLDPによる自動最適設定

ADECIAコンポーネントから独自のLLDPフレームを受信することで、「Dante」を利用する上での最適な設定を自動的に反映させることができます。

LLDPによる自動最適設定は、 **lldp auto-setting** コマンドで設定します。

本製品の初期設定では、LLDPによる自動最適設定は **有効** です。

本機能が有効、かつ、ADECIAコンポーネントからLLDPフレームを受信した場合、システム全体、受信したVLANインターフェース、受信したLAN/SFPポートのrunning-configに対して設定を自動的に反映します。ただし、ADECIA V2.8以降の場合、自動的に設定される項目のうちどれか一つでも工場出荷状態とは異なる設定がされている場合、本機能は動作しません。

**copy running-config startup-config** コマンドや **write** コマンドで保存すると、次回以降の起動時に使用する startup-config へも反映されます。

自動最適設定後に機器が接続されたポートをリンクダウンしても自動的に追加された設定はそのまま保持されます。

本機能は物理インターフェース (LAN/SFPポート) のみで利用できます。リンクアグリゲーション論理インターフェースでは利用できません。

また、LAN/SFPポートのモードはアクセスポートのみで利用できます。トランクポートでは利用できません。

本機能を使用するためには、LLDPフレームを受信できるようにする必要があります。  
そのため、事前に以下が設定されていることを確認してください。

- **lldp run** コマンドで、システム全体のLLDP機能を有効にします。
- **lldp-agent** コマンドで、対象のインターフェースにLLDPエージェントを作成します。
- **set lldp** コマンドで、LLDPフレームの送受信モードを設定します。

本製品の初期設定では、LLDPフレームの送受信は **有効** です。

### Web GUIからの手動最適設定

本製品のWeb GUIの **[ProAV設定] - [ProAVプロファイル]** ページからDanteプロファイルを適用します。  
詳細は[ProAV設定](#)を参照してください。

## 関連コマンド

関連コマンドについて、以下に示します。

コマンドの詳細は、コマンドリファレンスを参照願います。

操作項目	操作コマンド
LLDPによるDante自動最適設定機能の設定	lldp auto-setting
LLDP機能の有効化	lldp run
LLDPエージェントの作成	lldp-agent
LLDP送受信モードの設定	set lldp
フロー制御の設定(システム)	flowcontrol
フロー制御の設定(インターフェース)	flowcontrol
QoSを有効	qos
DSCP-送信キューID変換テーブルの設定	qos dscp-queue
QoSトラストモードの設定	qos trust
スケジューリング方式の設定	qos scheduling
EEE設定	eee
MRU設定	mru
リンクローカルマルチキャスト転送の設定	l2-unknown-mcast forward link-local
未知のマルチキャスト転送の設定	l2-unknown-mcast
マルチキャストフレームの転送設定	l2-mcast flood
IGMPスヌーピングの有効／無効設定	ip igmp snooping
IGMPスヌーピングのバージョンの設定	ip igmp snooping version
IGMPスヌーピング高速脱退の設定	ip igmp snooping fast-leave
IGMPクエリー送信機能の設定	ip igmp snooping querier
IGMPクエリー送信間隔の設定	ip igmp snooping query-interval
IGMP/パケットのTTL値検証機能の設定	ip igmp snooping check ttl
IGMP/パケットのRA検証機能の設定	ip igmp snooping check ra
IGMP/パケットのToS検証機能の設定	ip igmp snooping check tos
IGMPレポート抑制機能の設定	ip igmp snooping report-suppression
IGMPレポート転送機能の設定	ip igmp snooping report-forward enable
マルチキャストルーターポート転送抑制機能を有効	ip igmp snooping mrouter-port data-suppression enable
プロファイル種別の設定	proav profile-type

## コマンド実行例

### LLDPによる自動最適設定

LLDPによる自動最適設定を有効にします。  
port1.1でLLDPの送受信ができるようにします。

```
Yamaha#configure terminal  
Yamaha(config)#interface port1.1  
Yamaha(config-if)#lldp-agent ①  
Yamaha(lldp-agent)#set lldp enable txrx ②  
Yamaha(lldp-agent)#exit  
Yamaha(config-if)#exit  
Yamaha(config)#lldp run ③  
Yamaha(config)#lldp auto-setting enable ④
```

① LLDPエージェントの作成、モード遷移

② LLDP送受信モードの設定

③ LLDP機能の有効化

④ LLDPによる自動最適設定の有効化

## 注意事項

- Dante最適設定機能は、スイッチとしての基本的な設定(VLANやIPなど)を全て行った上で使用することが前提となっています。  
新たに設定変更をした場合(VLAN追加など)は、Dante最適設定の追従は行いません。
- Web GUIからの手動最適設定
  - すでにQoSの設定、フロー制御の設定、EEEの設定、IGMPスヌーピングなどの設定がされた状態で本機能を使用したとき、Dante最適設定に上書きされますのでご注意ください。
- LLDPによる自動設定
  - 本機能は物理インターフェース (LAN/SFPポート) のみで利用できます。リンクアグリゲーション論理インターフェースでは利用できません。
  - LAN/SFPポートのモードはアクセスポートのみで利用できます。トランクポートでは利用できません。
  - ADECIA V2.8以降の場合、自動的に設定される項目のうちどれか一つでも工場出荷状態とは異なる設定がされている場合、本機能は動作しません。

## 関連文書

- [ProAV設定](#)
- [LLDP](#)
- [QoS](#)
- [フロー制御](#)
- [IGMP Snooping](#)
- [インターフェース基本機能](#)
- [ADECIA製品情報](#)

# ProAV設定

## 機能概要

Web GUI「ProAV設定」ページから、DanteやNDIなどの音声・映像トラフィックを伝送するAVoIPネットワークに最適な設定を、簡単なGUI操作で一括で行うことができます。  
本製品では、以下のProAVプロファイルを設定することができます。

- Dante
- NDI

本技術資料では、ProAVプロファイル適用時に設定されるコマンドの詳細と、キッティング（初期設定）やトラブルシューティングについて説明します。

Web GUI「ProAV設定」ページの使い方の詳細については、GUI技術資料を参照してください。

## 用語の定義

### Dante

DanteはAudinate, Inc.によって開発された、プロオーディオ向けのオーディオネットワークソリューションです。

1本のLANケーブルで、多チャンネル音声伝送やクロック同期信号、制御信号の伝送など、デジタルオーディオシステムに必要な情報通信が双方向で行われます。

### NDI

NDIはNewtek, Inc.によって開発された、IP利用における新しいライブビデオ制作ワークフロー支援プロトコルです。

一般的なギガビットイーサネット環境において、映像、音声、メタデータなどの情報のリアルタイム相互伝送を可能とします。

### Yamaha LAN Monitor

Yamaha LAN Monitorは、パソコン上でヤマハスイッチの情報や接続機器を監視、制御することができるPCアプリケーションです。

## ProAVプロファイル詳細

### Danteプロファイル

Danteプロファイルでは以下のコマンドが一括で適用されます。

- Danteプロファイルで適用されるコマンド一覧

設定対象	機能	コマンド
システム全体	フロー制御を無効	flowcontrol disable
	QoSを有効	qos enable
	DSCP値による送信キューの最適化	qos dscp-queue 8 2
		qos dscp-queue 26 3
		qos dscp-queue 34 4
		qos dscp-queue 46 5
		qos dscp-queue 48 5
		qos dscp-queue 56 7
		qos dscp-queue [上記以外] 0
	スケジューリング方式の設定	qos scheduling sp
リンクローカルマルチキャストの常時転送	リンクローカルマルチキャストの常時転送	l2-unknown-mcast forward link-local
	MRUを設定	mru 1522
	LLDPを有効	lldp run

設定対象	機能	コマンド
VLANインターフェース	プロファイル種別の設定	proav profile-type dante-primary/dante-secondary
	未知のマルチキャストをフラッディング	l2-unknown-mcast flood
	IGMPスヌーピングを有効	ip igmp snooping enable
	IGMPスヌーピングのバージョンを設定	ip igmp snooping version 3
	IGMPスヌーピングの高速脱退を有効	ip igmp snooping fast-leave auto-assignment
	IGMPクエリー送信機能を有効	ip igmp snooping querier
	IGMPクエリー送信間隔の設定	ip igmp snooping query-interval 30
	IGMPパケットのTTL値検証機能を無効	ip igmp snooping check ttl disable
	IGMPパケットのRA検証機能を無効	ip igmp snooping check ra disable
	IGMPパケットのToS検証機能を無効	ip igmp snooping check tos disable
	マルチキャストルーターポート転送抑制機能を有効	ip igmp snooping mrouter-port data-suppression enable
	IGMPレポート抑制機能を無効	ip igmp snooping report-suppression disable
	IGMPレポート転送機能を有効	ip igmp snooping report-forward enable
PTP/ポート	PTP/パケットの常時転送	l2-mcast flood 224.0.1.129 l2-mcast flood 224.0.1.130 l2-mcast flood 224.0.1.131 l2-mcast flood 224.0.1.132 l2-mcast flood 239.254.3.3
	QoSトラストモードをDSCPに設定	qos trust dscp
	フロー制御を無効	flowcontrol disable
	EEEを無効	eee disable
	LLDPの送受信を有効	lldp-agent set lldp enable tx rx
L2MSフィルター	L2MSフィルターの設定	l2ms filter disable / enable (※1)

設定内容の詳細は以下のとおりです。

- フロー制御無効

- フロー制御を無効にすることで、帯域が混雑したときでもDanteトラフィックの送受信が止まらないようにします。

## ・ QoS有効

- **QoSを有効** にすることで、Danteトラフィックが優先して転送されるようにします。
- **DSCP値による送信キューの最適化** をすることで、Danteトラフィックに関わるDSCP値を高優先度の送信キューに割り当てます。
- **QoSトラストモードをDSCPに設定** することで、DSCP値を参照して優先制御するようにします。
- **スケジューリング方式をSP(絶対優先)に設定** することで、高優先度の送信キューから優先的に送信します。

## ・ IGMPスヌーピング有効

- **IGMPスヌーピングを有効** にすることで、マルチキャスト受信者が存在するポートにのみマルチキャストトラフィックを転送し、不要なトラフィックを転送しないようにします。
- **IGMPスヌーピングのバージョンをIGMPv3に設定** します。  
複数のスイッチを使用するネットワーク構成で、スイッチ間でバージョンが異なるときは、ProAV GUIの「マルチキャストページ」で警告メッセージが表示されます。  
Danteネットワークを使用するときは、IGMPv3に設定してください。
- **IGMPスヌーピングの高速脱退機能を有効** にすることで、マルチキャスト受信者が受信を停止したときに、マルチキャストトラフィックの転送を即時停止します。  
マルチキャスト受信者が音声・映像を切り替えたときに、切り替え前のマルチキャストトラフィックがノイズになることを防止することができます。
- **高速脱退機能のauto-assignmentオプションを有効** にすることで、複数のスイッチを使用するネットワーク構成で、スイッチ間を接続するポートでは高速脱退を行わないようにします。  
対向スイッチ配下にマルチキャストトラフィックを受信したい受信者がまだ存在するにも関わらず、マルチキャストトラフィックの転送が即時停止されることを防ぐことができます。
- **IGMPクエリー送信機能（クエリアー機能）を有効** にします。  
IGMPスヌーピングを使用する場合、同一ネットワーク内に必ずクエリアーが存在する必要があります。  
同一ネットワークに複数のクエリアーが存在する場合、最もIPアドレスの小さいクエリアーが代表クエリアーとなり、それ以外のクエリアーは自動的にクエリー送信を停止します。
- **IGMPクエリーの送信間隔を30秒に設定** することで、IGMPスヌーピングの学習状態をより早く収束させることができます。
- **IGMPパケットのTTL値/RA/ToS検証機能を無効** にすることで、不正なIGMPパケットを受信した場合でも、正しい情報に補正してIGMPパケットを転送します。
- **マルチキャストルーターポート転送抑制機能を有効** にすることで、複数のスイッチを使用するネットワーク構成で、スイッチ間の帯域を節約することができます。  
通常、マルチキャスト受信者の有無に関わらず、すべてのマルチキャストトラフィックはマルチキャストルーターポートに転送されるため、双方向伝送環境では、不必要的マルチキャストトラフィックがスイッチ間の帯域を圧迫します。  
本機能を使用することで、対向スイッチにマルチキャスト受信者が存在する場合のみマルチキャストトラフィックを転送するため、スイッチ間の帯域を節約します。
- **IGMPレポート抑制機能を無効** にすることで、複数のスイッチを使用するネットワーク構成で、IGMPレポート転送時にプロキシせずに、そのまま転送するようにします。
- **IGMPレポート転送機能を有効** にすることで、複数のスイッチを使用するネットワーク構成で、スイッチ間を接続するポートにIGMPレポートを転送するようにします。

## ・ 制御用マルチキャストパケットの常時転送

- **リンクローカルマルチキャストの常時転送** をすることで、IGMPスヌーピングが有効のとき、Danteで使用されるmDNSなどの制御パケットを常に転送するようにします。
- **PTPパケットの常時転送** をすることで、IGMPスヌーピングが有効のとき、Danteで使用される時刻同期の制御パケットを常に転送するようにします。

- 未知のマルチキャストをフラッディングすることで、IGMPスヌーピングが有効のとき、受信者が存在しないマルチキャストトラフィックを転送するようにします。

- ジャンボフレーム無効

- MRUを1522バイトに設定することで、ジャンボフレームの転送を無効にします。

- EEE無効

- 省電力機能を無効にすることで、省電力機能が転送性能に影響を与えないようにします。

- LLDP有効

- LLDPの送受信を有効にすることで、IGMPスヌーピングの高速脱退機能とIGMPレポート転送機能が動作するようにします。

これら2つのIGMPの機能は、LLDPを使用して、対向機器がスイッチかどうかを判定して動作するためです。

- L2MSフィルターの設定(※1)

- Danteネットワークの構成が「Danteプライマリー/セカンダリー回線を二重化する」構成の場合のみ、DanteセカンダリーポートでL2MSフィルターを有効にします。

L2MSとは、Yamaha LAN Monitorなどの統合管理アプリケーションで、ヤマハスイッチを監視・制御するために使用される、ヤマハ独自の制御パケットのことです。

二重化構成では、スイッチ間をプライマリー用ケーブルとセカンダリー用ケーブルの2本で接続するため、L2MSフィルターを有効にすることで制御パケットがループして輻輳が発生することを防止します。

なお、二重化構成以外のネットワーク構成では、L2MSフィルターを無効にします。

- プロファイル種別の設定

- ProAV GUIで、プロファイル種別を識別するための識別子として使用されます。

## NDIプロファイル

NDIプロファイルでは以下のコマンドが一括で適用されます。

- NDIプロファイルで適用されるコマンド一覧

設定対象	機能	コマンド
システム全体	フロー制御を有効	flowcontrol enable
	QoSを無効	qos disable
	リンクローカルマルチキャストの常時転送	l2-unknown-mcast forward link-local
	MRUを設定	mru 1522
	LLDPを有効	lldp run

設定対象	機能	コマンド
VLANインターフェース	プロファイル種別の設定	proav profile-type ndi
	未知のマルチキャストをフラッディング	l2-unknown-mcast flood
	IGMPスヌーピングを有効	ip igmp snooping enable
	IGMPスヌーピングのバージョンを設定	ip igmp snooping version 2
	IGMPスヌーピングの高速脱退を有効	ip igmp snooping fast-leave auto-assignment
	IGMPクエリー送信機能を有効	ip igmp snooping querier
	IGMPクエリー送信間隔の設定	ip igmp snooping query-interval 125
	IGMPパケットのTTL値検証機能を無効	ip igmp snooping check ttl disable
	IGMPパケットのRA検証機能を無効	ip igmp snooping check ra disable
	IGMPパケットのToS検証機能を無効	ip igmp snooping check tos disable
	マルチキャストルーターポート転送抑制機能を有効	ip igmp snooping mrouter-port data-suppression enable
	IGMPレポート抑制機能を無効	ip igmp snooping report-suppression disable
	IGMPレポート転送機能を有効	ip igmp snooping report-forward enable
LAN/SFPポート	フロー制御を有効	flowcontrol enable
	EEEを無効	eee disable
	LLDPの送受信を有効	lldp-agent set lldp enable tx rx

設定内容の詳細は以下のとおりです。

- ・ **フロー制御有効**
  - **フロー制御を有効** にすることで、帯域が混雑したときに、混雑が解消するまで一時的にトラフィックの送信を停止し、パケットロスが発生しないようにします。
- ・ **QoS無効**
  - **QoSを無効** にすることで、パケット転送の優先制御を行わずに転送します。
- ・ **IGMPスヌーピング有効**
  - **IGMPスヌーピングを有効** にすることで、マルチキャスト受信者が存在するポートにのみマルチキャストトラフィックを転送し、不要なトラフィックを転送しないようにします。
  - **IGMPスヌーピングのバージョンをIGMPv2に設定** します。  
複数のスイッチを使用するネットワーク構成で、スイッチ間でバージョンが異なるときは、ProAV GUIの「マルチキャストページ」で警告メッセージが表示されます。  
NDIネットワークを使用するときは、IGMPv2に設定してください
  - **IGMPスヌーピングの高速脱退機能を有効** にすることで、マルチキャスト受信者が受信を停止したときに、マルチキャストトラフィックの転送を即時停止します。

マルチキャスト受信者が音声・映像を切り替えたときに、切り替え前のマルチキャストトラフィックがノイズになることを防止することができます。

- **高速脱退機能のauto-assignmentオプションを有効** にすることで、複数のスイッチを使用するネットワーク構成で、スイッチ間を接続するポートでは高速脱退を行わないようにします。  
対向スイッチ配下にマルチキャストトラフィックを受信したい受信者がまだ存在するにも関わらず、マルチキャストトラフィックの転送が即時停止されることを防ぐことができます。

- **IGMPクエリー送信機能（クエリアー機能）を有効** にします。  
IGMPスヌーピングを使用する場合、同一ネットワーク内に必ずクエリアーが存在する必要があります。  
同一ネットワークに複数のクエリアーが存在する場合、最もIPアドレスの小さいクエリアーが代表クエリアーとなり、それ以外のクエリアーは自動的にクエリー送信を停止します。

- **IGMPクエリーの送信間隔をデフォルトの125秒に設定** します。
- **IGMPパケットのTTL値/RA/ToS検証機能を無効** にすることで、不正なIGMPパケットを受信した場合でも、正しい情報に補正してIGMPパケットを転送します。

- **マルチキャストルーターポート転送抑制機能を有効** にすることで、複数のスイッチを使用するネットワーク構成で、スイッチ間の帯域を節約することができます。  
通常、マルチキャスト受信者の有無に関わらず、すべてのマルチキャストトラフィックはマルチキャストルーターポートに転送されるため、双方向伝送環境では、不必要的マルチキャストトラフィックがスイッチ間の帯域を圧迫します。

本機能を使用することで、対向スイッチにマルチキャスト受信者が存在する場合のみ、マルチキャストトラフィックを転送するため、スイッチ間の帯域を節約します。

- **IGMPレポート抑制機能を無効** にすることで、複数のスイッチを使用するネットワーク構成で、IGMPレポート転送時にプロキシせずに、そのまま転送するようにします。
- **IGMPレポート転送機能を有効** にすることで、複数のスイッチを使用するネットワーク構成で、スイッチ間を接続するポートにIGMPレポートを転送するようにします。

#### • 制御用マルチキャストパケットの常時転送

- **リンクローカルマルチキャストの常時転送** をすることで、IGMPスヌーピングが有効のとき、NDIで使用されるmDNSなどの制御パケットを常に転送するようにします。
- **未知のマルチキャストをフラッディング** することで、IGMPスヌーピングが有効のとき、受信者が存在しないマルチキャストトラフィックを転送するようにします。

#### • ジャンボフレーム無効

- **MRUを1522バイトに設定** することで、ジャンボフレームの転送を無効にします。

#### • EEE無効

- **省電力機能を無効** にすることで、省電力機能が転送性能に影響を与えないようにします。

#### • LLDP有効

- **LLDPの送受信を有効** にすることで、**IGMPスヌーピングの高速脱退機能** と **IGMPレポート転送機能** が動作するようになります。  
これら2つのIGMPの機能は、LLDPを使用して、対向機器がスイッチかどうかを判定して動作するためです。

#### • プロファイル種別の設定

- ProAV GUIで、プロファイル種別を識別するための識別子として使用されます。

### 複数プロファイル併用時の設定

ProAVプロファイルの「カスタム」ページでは、任意のプロファイルをポートごとに設定することができます。

プロファイルの組み合わせによっては設定の衝突が発生するため、プロファイル単独使用時と比較して設定差

---

分が生じます。

#### DanteとNDI併用時

- DanteとNDI併用時に適用されるコマンド一覧

設定対象	機能	Danteプロファイル	NDIプロファイル
システム全体	フロー制御を有効	flowcontrol enable	
	QoSを有効	qos enable	
	DSCP値による送信キューの最適化	qos dscp-queue 8 2	
		qos dscp-queue 26 3	
		qos dscp-queue 34 4	
		qos dscp-queue 46 5	
		qos dscp-queue 48 5	
		qos dscp-queue 56 7	
		qos dscp-queue [上記以外] 0	
	スケジューリング方式の設定	qos scheduling sp	
	リンクローカルマルチキャストの常時転送	l2-unknown-mcast forward link-local	
	MRUを設定	mru 1522	
	LLDPを有効	lldp run	

設定対象	機能	Danteプロファイル	NDIプロファイル
VLANインターフェース	プロファイル種別の設定	proav profile-type dante-primary/dante-secondary	proav profile-type ndi
	未知のマルチキャストをフラッディング	l2-unknown-mcast flood	l2-unknown-mcast flood
	IGMPスヌーピングを有効	ip igmp snooping enable	ip igmp snooping enable
	IGMPスヌーピングのバージョンを設定	ip igmp snooping version 3	ip igmp snooping version 2
	IGMPスヌーピングの高速脱退を有効	ip igmp snooping fast-leave auto-assignment	ip igmp snooping fast-leave auto-assignment
	IGMPクエリー送信機能を有効	ip igmp snooping querier	ip igmp snooping querier
	IGMPクエリー送信間隔の設定	ip igmp snooping query-interval 30	ip igmp snooping query-interval 125
	IGMP/パケットのTTL値検証機能を無効	ip igmp snooping check ttl disable	ip igmp snooping check ttl disable
	IGMP/パケットのRA検証機能を無効	ip igmp snooping check ra disable	ip igmp snooping check ra disable
	IGMP/パケットのToS検証機能を無効	ip igmp snooping check tos disable	ip igmp snooping check tos disable
	マルチキャストルーターポート転送抑制機能を有効	ip igmp snooping mrouter-port data-suppression enable	ip igmp snooping mrouter-port data-suppression enable
	IGMPレポート抑制機能を無効	ip igmp snooping report-suppression disable	ip igmp snooping report-suppression disable
	IGMPレポート転送機能を有効	ip igmp snooping report-forward enable	ip igmp snooping report-forward enable
PTP/パケットの常時転送	l2-mcast flood 224.0.1.129	-	
	l2-mcast flood 224.0.1.130		
	l2-mcast flood 224.0.1.131		
	l2-mcast flood 224.0.1.132		
	l2-mcast flood 239.254.3.3		
LAN/SFPポート	QoSトラストモードの設定	qos trust dscp	qos trust port-priority qos port-priority-queue 2
	フロー制御の設定	flowcontrol disable	flowcontrol enable
	EEEを無効	eee disable	eee disable
	LLDPの送受信を有効	lldp-agent set lldp enable tx rx	lldp-agent set lldp enable tx rx
	L2MSフィルターの設定	l2ms filter disable	l2ms filter disable

---

プロファイル併用時とプロファイル単独使用時の差分は以下のとおりです。

- **フロー制御**

- システム全体で **フロー制御を有効** にします。
- Danteプロファイルが適用されたポートでは、 **フロー制御を無効** にします。
- NDIプロファイルが適用されたポートでは、 **フロー制御を有効** にします。

- **QoS**

- システム全体で **QoSを有効** にします。
- システム全体で **DSCP値による送信キューの最適化** をします。
- Danteプロファイルが適用されたポートでは、 **QoSトラストモードをDSCPに設定** することで、 DSCP値を参照して優先制御するようにします。
- NDIプロファイルが適用されたポートでは、 **QoSトラストモードをポート優先度に設定、かつ送信キューを2(デフォルト)に固定** することで、 パケット転送の優先制御が行われないようにします。

## キッティングとトラブルシューティング

ヤマハネットワーク機器の統合管理ツール「Yamaha LAN Monitor」を活用することにより、かんたんにキッティング（初期設定）やトラブルシューティングを行うことができます。

Yamaha LAN Monitor は無料でダウンロードすることができます。Yamaha LAN Monitorのインストール方法や使い方の詳細は、ユーザーガイドを参照してください。

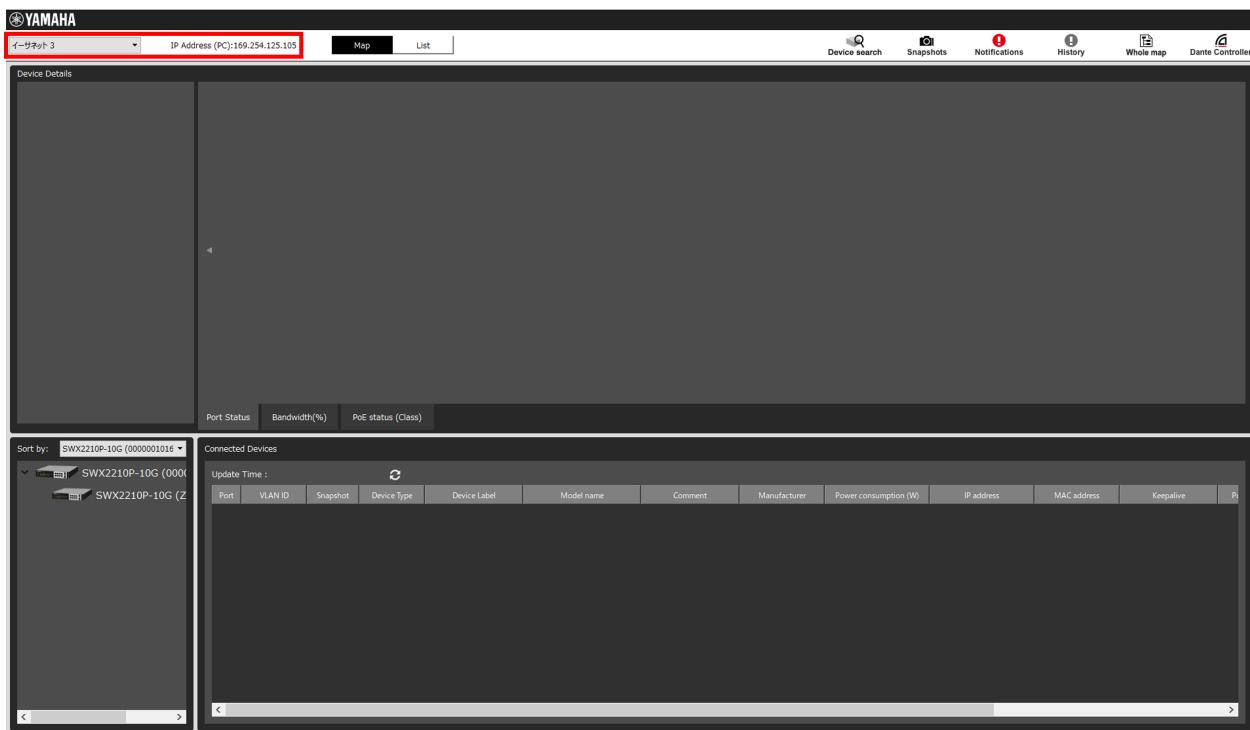
### [キッティング] IPアドレスを意識せずに初期設定する

通常、ネットワークで2台以上のスイッチを使用する場合、IPアドレスの重複が発生しないように、スイッチごとに適切にIPアドレスを設定する必要があります。

しかし、外部ネットワークに接続する必要のないクローズドなAVoIPネットワークであれば、スイッチの **Auto IP機能** によって、自動的にリンクローカルアドレスを割り当てることができます。

工場出荷状態のヤマハスイッチとYamaha LAN Monitorを組み合わせることで、IPアドレスの設定を意識することなく、かんたんにProAVプロファイルを適用することができます。

1. 事前準備として、PCにYamaha LAN Monitorをインストールし、PCの使用するネットワークアダプターのIPアドレスを「自動的に取得する」設定にします。  
この手順により、PCはリンクローカルアドレスで動作します。  
(※DHCPサーバーが存在する場合はDHCPでIPアドレスを取得しますが、今回はクローズドなAVoIPネットワークを想定するため、DHCPに関する説明は省略します。)
2. 工場出荷状態の複数のスイッチを接続し、PCを任意のスイッチのポートに接続してYamaha LAN Monitorを起動します。起動すると次のような画面が表示されます。  
画面左上のPCのネットワークアダプターに正しいものが選択されていることと、PCのIPアドレスが「169.254..」から始まるリンクローカルアドレスになっていることを確認してください。



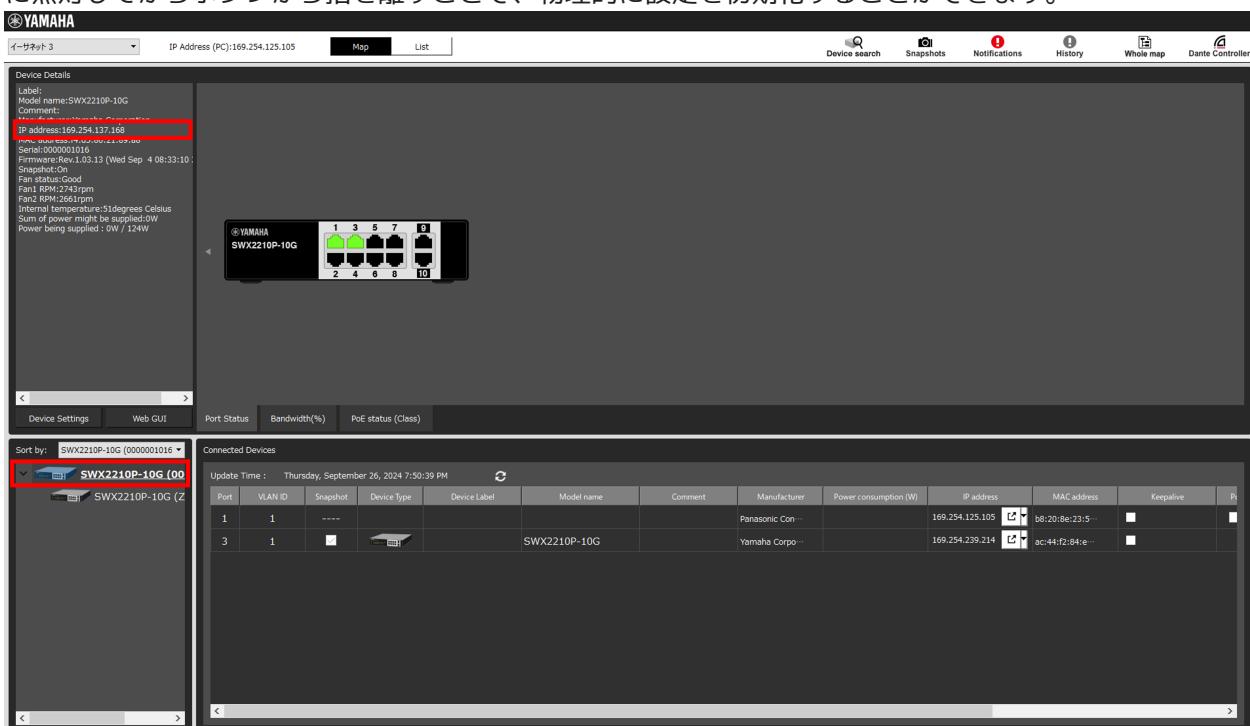
3. Yamaha LAN Monitor上のスイッチのアイコンをクリックすると、IPアドレスを確認することができます。

ヤマハスイッチの初期IPアドレスは「192.168.100.240/24」ですが、**工場出荷状態(何も設定が変更されていない状態)でYamaha LAN Monitorの管理下に入ると、自動的にリンクローカルアドレスに切り替わります。**

スイッチのIPアドレスが「169.254..」で始まっている場合は、リンクローカルアドレスで動作しています。「192.168.100.240」のままになっている場合は、リンクローカルアドレスに切り替わるまでしばらく待って、表示を更新してください。

**注意点として、ヤマハスイッチの設定が初期設定から既に変更されている場合は自動でリンクローカルアドレスに切り替わりません。** しばらく待ってもリンクローカルアドレスに切り替わらない場合は、スイッチの設定を初期化してください。

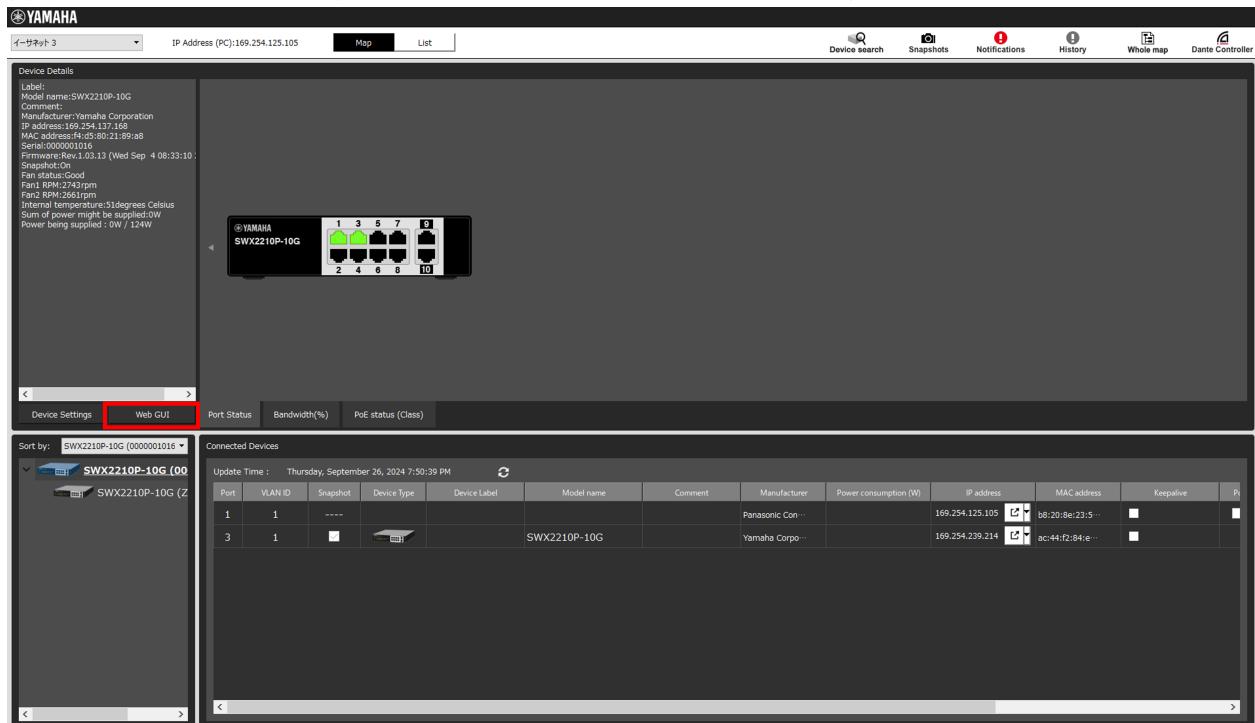
本製品では、筐体前面にあるLED MODEボタンを押したまま電源を投入し、すべてのポートLEDが橙色に点灯してからボタンから指を離すことで、物理的に設定を初期化することができます。



4. スイッチのIPアドレスがリンクローカルアドレスに切り替わったことを確認できたら、「Web GUI」ボ

タンをクリックしてください。

自動的にPCのブラウザーが開き、スイッチのWeb GUIが表示されます。



5. Web GUIのログイン画面で、ユーザー名「admin」、パスワード「admin」を入力してください。言語を選択した後、パスワードの変更が求められるため、任意のパスワードを設定してください。



6. Web GUIにログインできたら、画面上部のグローバルメニューの「ProAV設定」ボタンをクリックしてください。  
以下のように「ProAVプロファイル」ページが表示されます。

**YAMAHA SWX2210P-10G**

Dashboard ProAV settings Detailed settings Management ? | CONFIG | SYSLOG | TECHINFO Administrative User: admin Log out

ProAV profile Multicast

### ■ ProAV profile

All optimal settings for the AVoIP system can be specified at the same time.  
Refer to the [HELP](#) page for instructions on how to use this page.

#### ■ ProAV profile setting status

SWX2210P-10G

1 3 5 7 9  
2 4 6 8 10

■ Unset

#### ■ ProAV profile settings

Return to defaults

**Dante™** Select this option if only a Dante profile is used. **Select**

**NDI** Select this option if only a NDI profile is used. **Select**

**CUSTOM** Select this option if multiple profiles are used. **Select**

Copyright © 2018-2025 Yamaha Corporation. All Rights Reserved.

7. 最後に、設定ページでProAVプロファイルを適用すれば、ProAVプロファイルの設定完了です。

**YAMAHA SWX2210P-10G**

Dashboard ProAV settings Detailed settings Management ? | CONFIG | SYSLOG | TECHINFO Administrative User: admin Log out

ProAV profile Multicast

### ■ ProAV profile

#### Dante profile

The Dante primary profile is applied to all ports.

SWX2210P-10G

1 3 5 7 9  
2 4 6 8 10

■ Dante primary

Back OK

## [キッティング] 複数のヤマハスイッチに同一設定を一括適用する

Yamaha LAN Monitorは、設定ファイル（CONFIGファイル）を複数のヤマハスイッチに一括配布することができます。

IPアドレスにリンクローカルアドレスを使用していて、すべてのスイッチに同一の設定を適用したい場合、効率的に複数台のスイッチを設定することができます。

注意点として、スイッチを固定IPアドレスで運用している場合は、IPアドレスの重複を防ぐためにIPアドレス再設定が必要となるためご注意ください。

- 4.1の手順に従って、1台のスイッチにProAVプロファイルを適用してください。
- 画面上部の「List」タブをクリックしてください。検出しているヤマハスイッチの一覧が表示されます。

The screenshot shows the YAMAHA L2MS Agent List interface. At the top, there are tabs for 'L2MS Agent List', 'Firmware Update', and 'Config Import/Export'. The 'List' tab is selected, indicated by a red box. Below the tabs, it says '2 items' and 'Update Time : Friday, September 27, 2024 1:18:27 PM'. There are buttons for 'Refresh view', 'View settings', and 'CSV export'. A search bar is at the top right. The main area displays a table with columns: Route, Device Type, Device name, Device Label, Serial Number, Model name, MAC address, IP address, Date and time of last CONFIG import, CONFIG file of last import, and Comment. Two entries are listed:

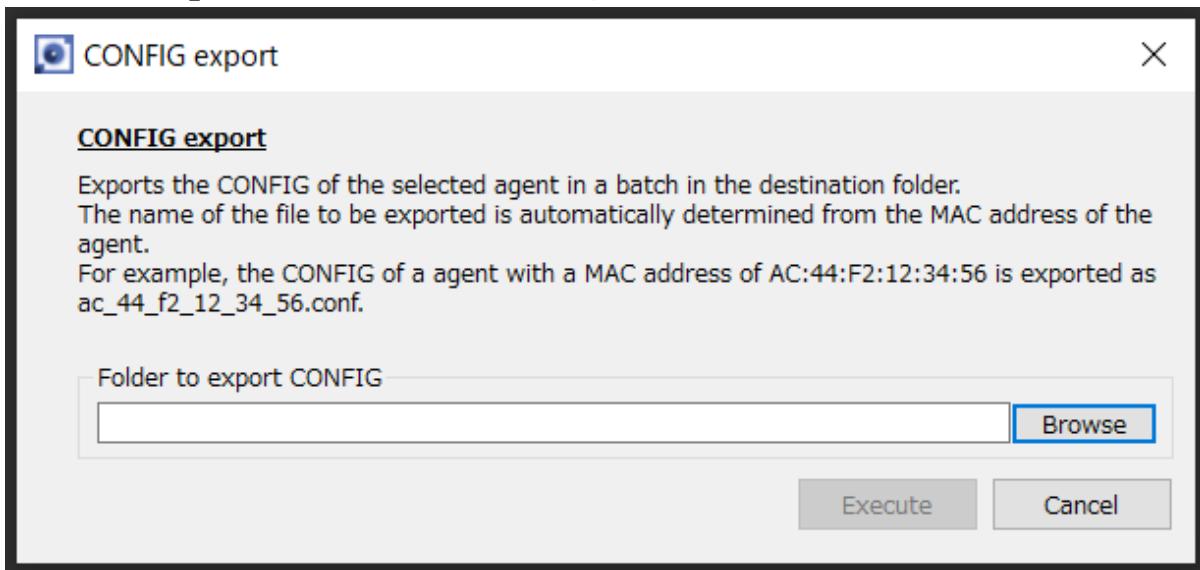
Route	Device Type	Device name	Device Label	Serial Number	Model name	MAC address	IP address	Date and time of last CONFIG import	CONFIG file of last import	Comment
Setting	PC	SWX2210P-10G_...		0000001016	SWX2210P-10G	f4:d5:80:21:89:a8	69.254.137.168	Rev.1.03.13 (We...)	-	-
Setting	PC-3	SWX2210P-10G_...		Z6800329ZM	SWX2210P-10G	ac:44:f2:84:ee:d6	69.254.239.214	Rev.1.03.13 (buil...)	-	-

- 画面上部の「Config Import/Export」タブをクリックしてください。  
さらに、既にProAVプロファイルを適用したスイッチをチェックし、「CONFIG export」ボタンをクリックしてください。

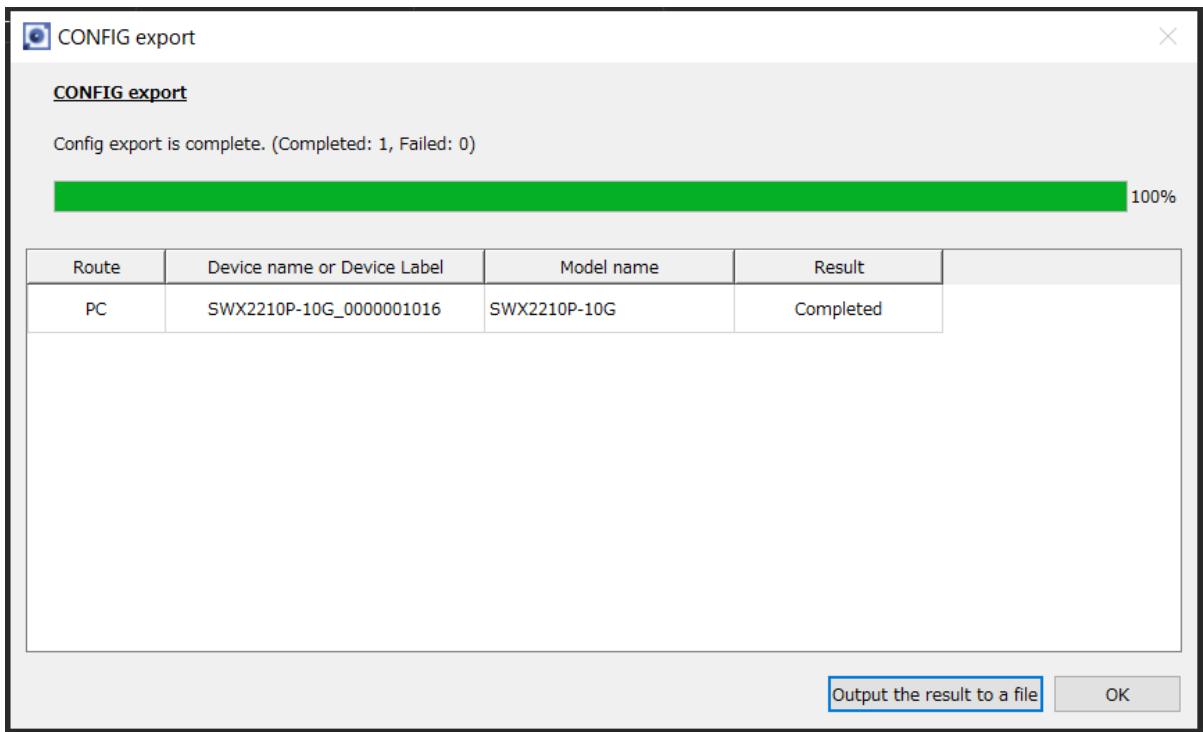
The screenshot shows the YAMAHA L2MS Agent List interface with the 'Config Import/Export' tab selected, indicated by a red box. Below the tabs, it says 'This screen shows agents only that supported CONFIG import/export.' and 'Select all' or 'Deselect all'. There are buttons for 'CONFIG import' and 'CONFIG export'. A red box highlights the 'CONFIG export' button. The main area displays a table with columns: Route, Device Type, Device name or Device Label, Model name, Date and time of last CONFIG import, and CONFIG file of last import. One entry has its checkbox checked, indicated by a red box.

Route	Device Type	Device name or Device Label	Model name	Date and time of last CONFIG import	CONFIG file of last import
<input checked="" type="checkbox"/> PC		SWX2210P-10G_000...	SWX2210P-10G	-	-
<input type="checkbox"/> PC-3		SWX2210P-10G_z68...	SWX2210P-10G	-	-

- 「CONFIG export」ダイアログが表示されるため、CONFIGファイルを保存するディレクトリを選択し、「Execute」ボタンをクリックしてください。



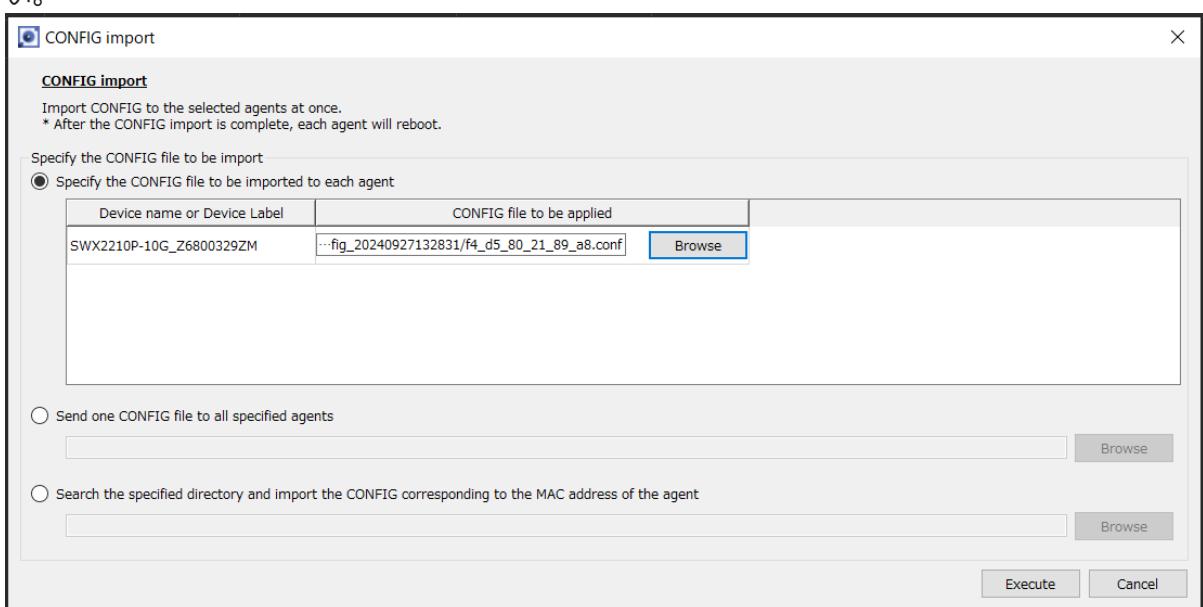
- ダイアログにExportの進捗状況と結果が表示されるため、完了したら「OK」ボタンをクリックしてください。



6. 続いて、ProAVプロファイルを適用したいスイッチをチェックし、「CONFIG import」ボタンをクリックしてください。

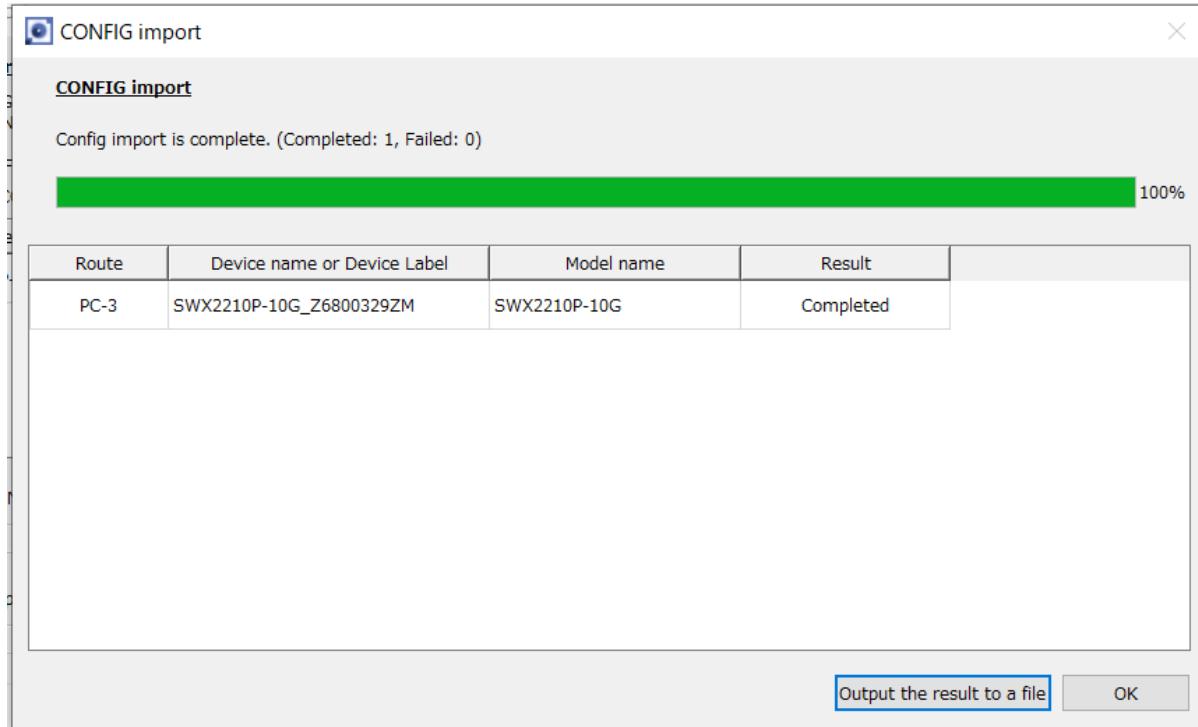
複数のスイッチに適用したい場合は、複数のチェックボックスをチェックしてください。

7. 「CONFIG import」ダイアログが表示されるため、インポートするファイルとして先ほど保存したCONFIGファイルを選択し、「Execute」ボタンをクリックしてください。  
選択したスイッチごとにCONFIGファイルを指定したり、選択した全てのスイッチに同一のCONFIGファイルを指定したりすることができます。  
異なるモデルのスイッチが混在する環境では、モデルごとに適切なCONFIGファイルを指定してください。



8. ダイアログにインポートの進捗状況と結果が表示されるため、完了したら「OK」ボタンをクリックしてください。

CONFIGを受信したスイッチは自動的に再起動し、起動後に新しい設定が適用されています。



なお、「Firmware Update」ボタンから、同じような手順で複数のヤマハスイッチに対して一括でファームウェア更新を行うこともできます。

このように、Yamaha LAN Monitorは多台数環境のキッティングツールとして使用することができるため、是非ご活用ください。

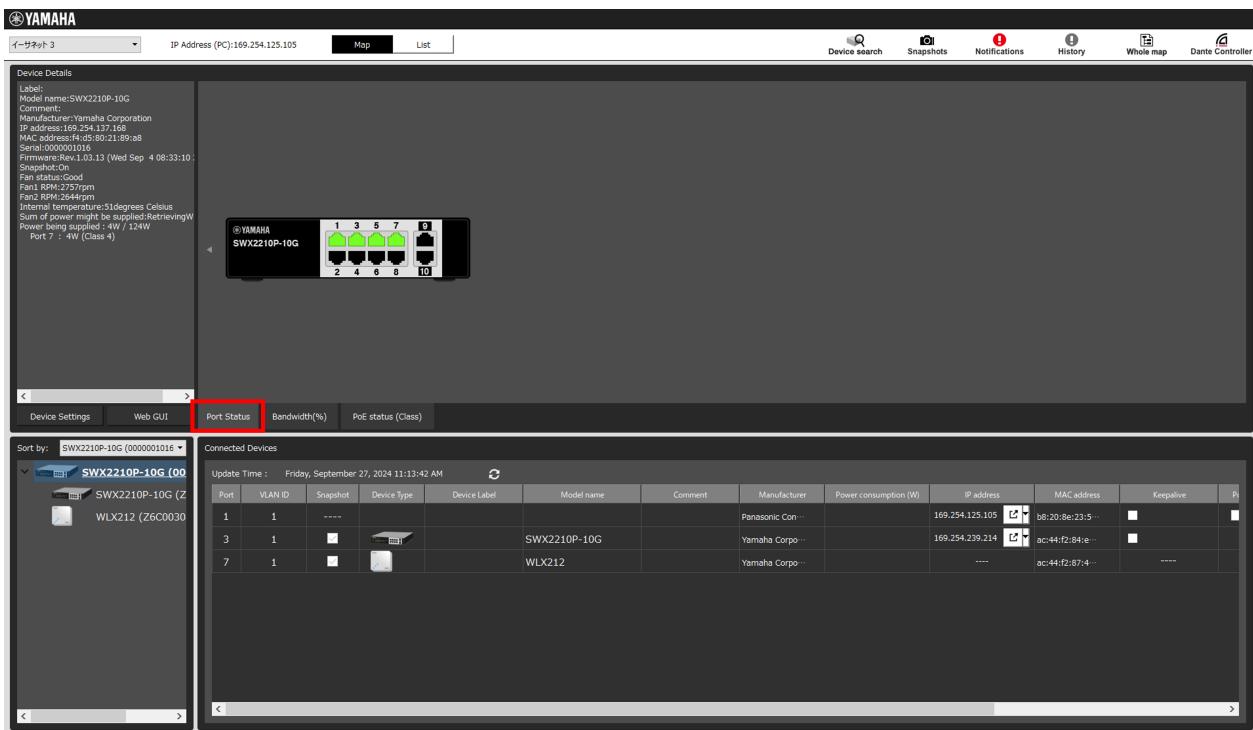
#### [トラブルシューティング] ネットワークの状態を確認する

Yamaha LAN Monitorを使用することで、ネットワーク全体の接続構成を見える化することができ、さらにトラフィックの帯域使用状況や、PoE給電状況を確認することができます。

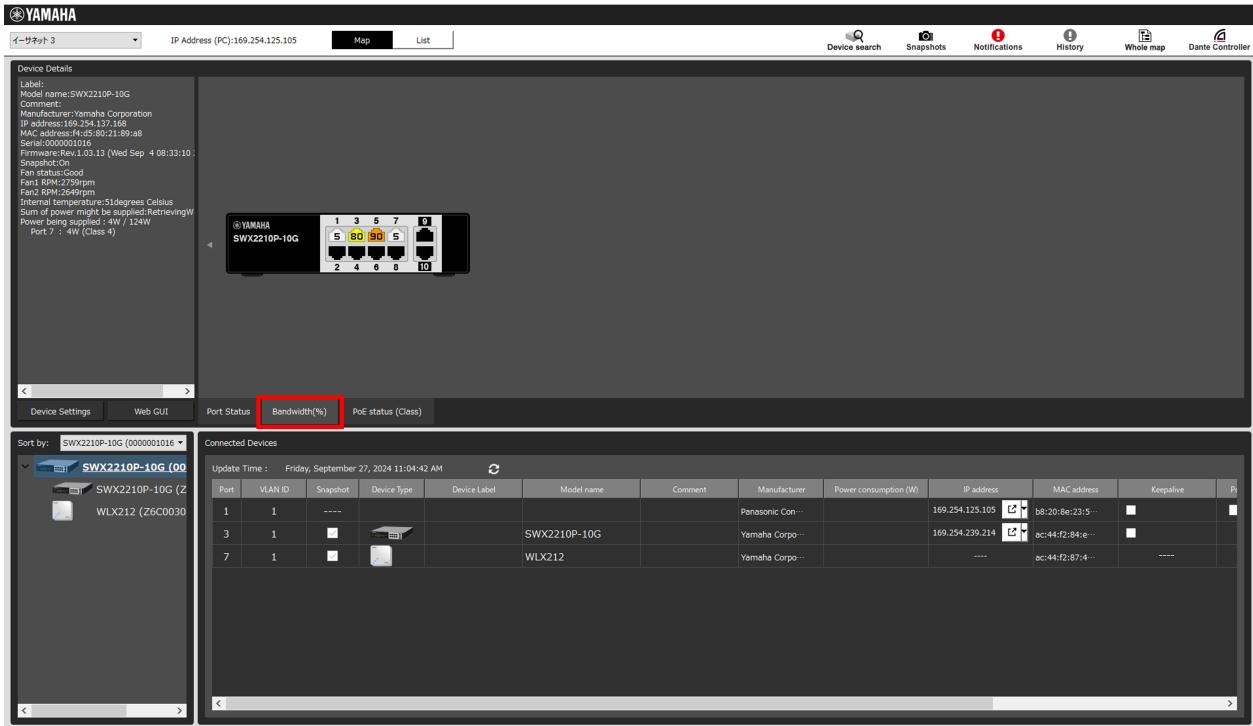
1. スイッチのアイコンをクリックします。

デフォルトでは「ポート状態」が選択されており、画面上部のフロントパネルにリアルタイムのリンク状態が表示されます。

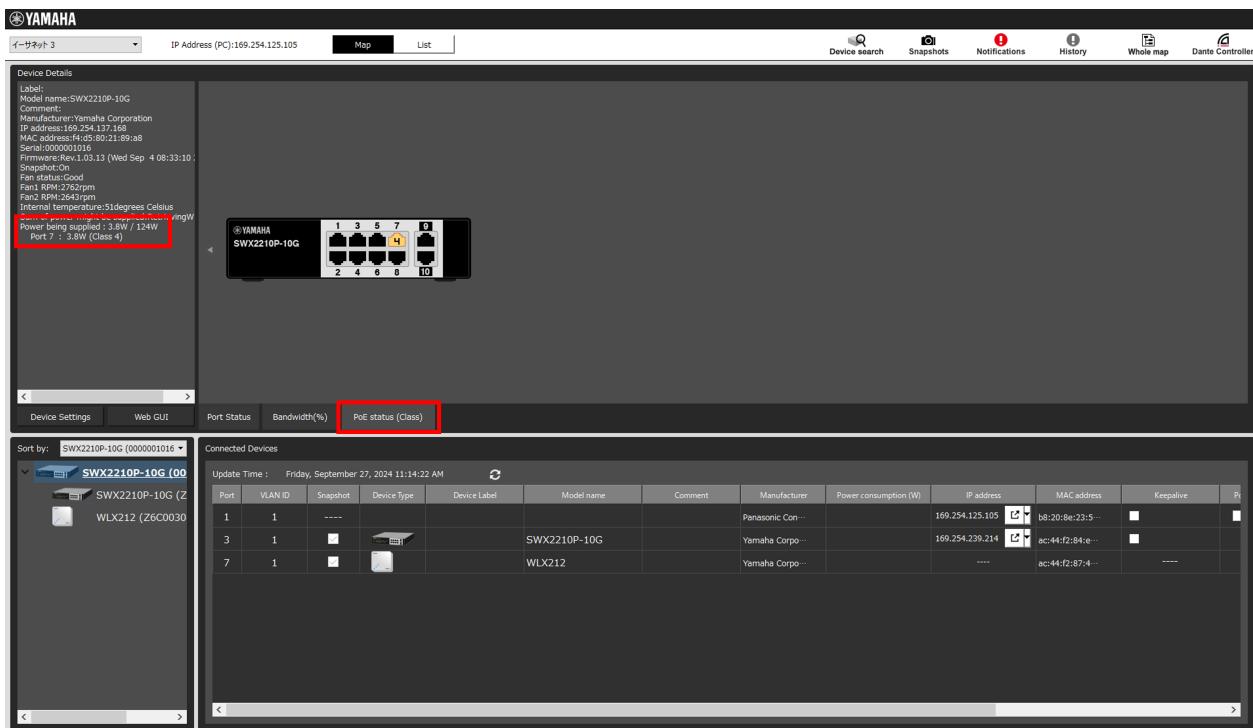
画面左下のツリービューでは現在のネットワーク接続構成を確認でき、画面右下の接続機器ビューではどのポートにどの機器が接続されているかを確認することができます。



2. トラフィックの帯域使用状況を確認するには、「帯域使用量(%)」ボタンをクリックしてください。各ポートの帯域使用率がリンク速度に対するパーセンテージで表示されます。  
帯域使用率が上限に近くなると、ポートアイコンが黄色やオレンジ、赤色で表示されます。



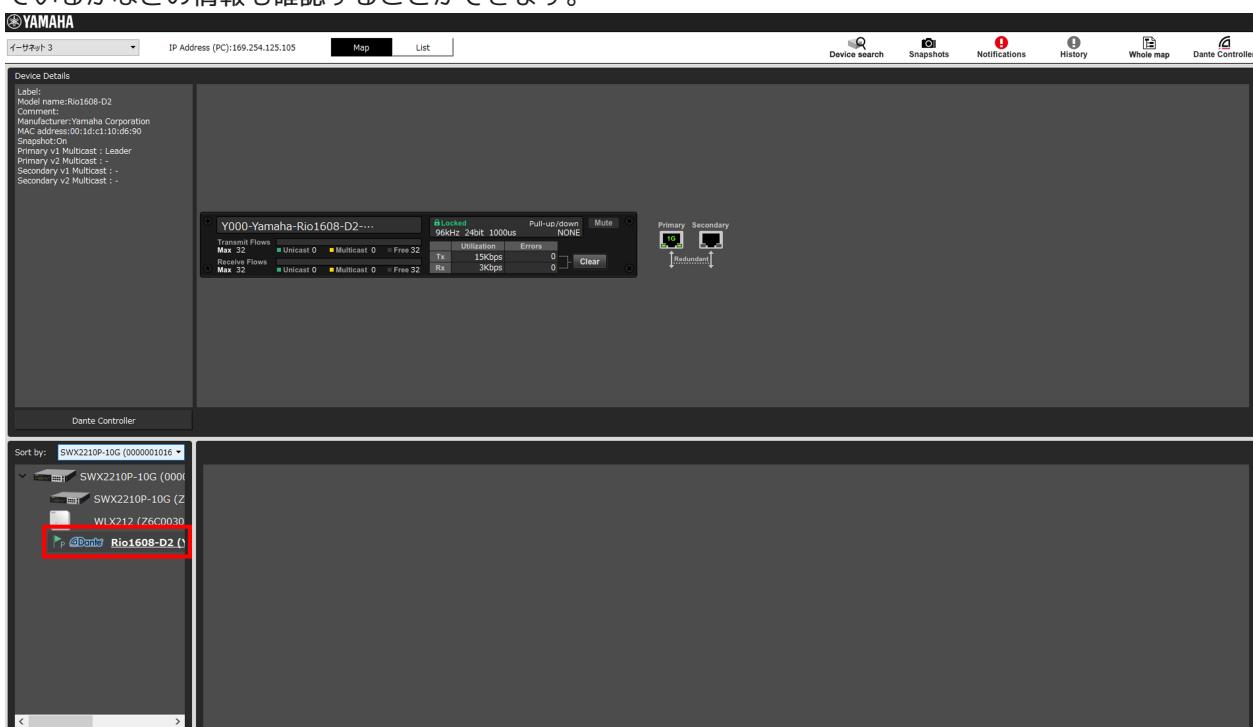
3. PoE給電状況を確認するには、「PoE給電状況(クラス)」をクリックしてください。  
給電中のポートに給電クラスが表示され、画面左上の機器詳細ビューには総供給電力量と、各ポートの給電量が表示されます。



## [トラブルシューティング] Dante機器の状態を確認する

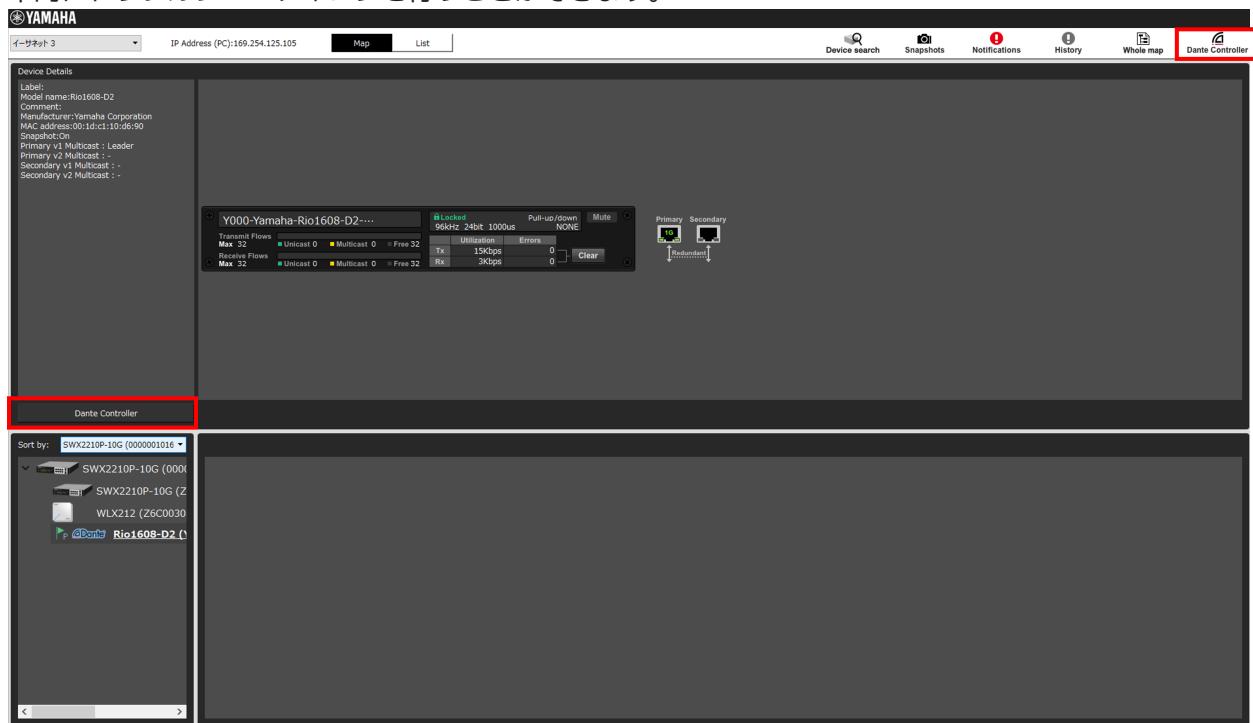
Yamaha LAN Monitorでは、Dante機器の状態を確認したり、Dante ControllerがPCにインストールされていればワンクリックでDante Controllerを開くことができます。  
Dante機器を表示するには、Yamaha LAN Monitorのインストール時にDante Control and MonitoringとDante Discoveryをインストールしている必要があります。

- Dante機器がヤマハスイッチに接続されている状態で、Dante機器のアイコンをクリックします。  
PrimaryポートとSecondaryポートの状態、送受信のフロー数などを監視することができます。  
また、Dante機器の動作モードが「リダンダントモード」と「デイジーチェーンモード」のどちらになっているかなどの情報も確認することができます。



- 画面右上もしくは画面中央の「Dante Controller」ボタンをクリックすると、Dante Controllerを起動することができます。（あらかじめDante Controllerがインストールされている必要があります。）

1台のPCでYamaha LAN MonitorとDante Controllerをシームレスに行き来することができます。より効率的にトラブルシューティングを行うことができます。



## 注意事項

- ProAV設定で一括設定される設定内容は、本機をAVoIPネットワーク専用のスイッチとして使用することを想定しています。  
既存の社内ネットワークとAVoIPネットワークを混在させるなど複雑なネットワークを構築する場合は、GUI 詳細設定ページやコマンドを使用して適切に設定してください。
- ProAVプロファイルを適用する際、論理インターフェースに所属するポートは、所属を外す必要があります。  
必要な場合は、一旦、所属をはずし、プロファイルを割り当てた後に、改めて、論理インターフェースに所属させてください。
- ProAVプロファイルはヤマハスイッチのみで構成されるAVoIPネットワークを想定しています。  
マルチベンダー環境でIGMPスヌーピング機能を使用する際、LLDPによる対向機器判定が動作しない可能性があるため、ご注意ください。

## 関連文書

- 特になし。

## 商標名称について

- Dante™は、Audinate Pty Ltd. の登録商標です。
- NDI®は Vizrt NDI AB の登録商標です。

## デフォルト設定一覧

SWX2210Pシリーズのデフォルト設定について、以下に示します。

- システム全体のデフォルト設定

カテゴリ	設定項目	設定値
コンソール	TELNETコンソールタイムアウト	600 sec
	VTY数	4
	表示行数	24
パスワード	初期管理ユーザー	ユーザー名：admin パスワード：admin
	管理者パスワード	admin
	パスワードの暗号化	暗号化しない
時刻管理	タイムゾーン	JST (UTC +9.0)
	NTPサーバー	なし
	NTP更新周期	なし
SNMP	動作	無効
SYSLOG	debugレベルログ出力	OFF
	informationレベルログ出力	ON
	errorレベルログ出力	ON
	SYSLOGサーバー	なし
ファームウェア更新	ダウンロードURL	SWX2210P-10Gの場合：firmware-update url <a href="http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-10g.bin">http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-10g.bin</a> SWX2210P-18Gの場合：firmware-update url <a href="http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-18g.bin">http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-18g.bin</a> SWX2210P-28Gの場合：firmware-update url <a href="http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-28g.bin">http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2210p-28g.bin</a>
	リビジョンダウンの許可	許可しない
	タイムアウト	300 sec
LLDP	動作	有効
	自動設定機能	有効
L2MS	動作	有効
	役割	エージェント

カテゴリ	設定項目	設定値
アクセス制御	TELNETサーバー状態	起動する (ポート23)
	TELNETサーバーアクセス	すべてのホストからのアクセスを許可
	TFTPサーバー状態	起動しない
	HTTPサーバー状態	起動する (ポート80)
	セキュアHTTPサーバー状態	起動する (ポート443)
	HTTP/HTTPSサーバーアクセス	すべてのホストからのアクセスを許可
	SNMPサーバー状態	起動する (ポート161)
インターフェース制御	SNMPサーバーアクセス	すべてのホストからのアクセスを許可
	MRU	1,522 Byte
	BPDUsスルー	有効
	EAPスルー	有効
L2スイッチング	リンクアグリゲーション	なし
	MACアドレス自動学習	有効
	MACアドレス自動学習エージング時間	300 sec
	独自ループ検出	有効
IPマルチキャスト	マルチプルVLAN	なし
	IGMPスヌーピング	無効
DNSクライアント	MLDスヌーピング	無効
	動作	有効
トラフィック制御	QoS	無効
	フロー制御 (IEEE 802.3x)	無効
PoE給電	給電動作	有効
	ガードバンド	7 W
Web GUI	言語設定	日本語

- ・ LANポート単位のデフォルト設定

カテゴリ	設定項目	設定値
基本設定	速度/通信モード設定	auto
	クロス/ストレート自動判別	有効
	ポートの説明	なし
	EEE	無効
	Port Mode	Access
	所属VLAN ID	1 (default VLAN)
L2MS	L2MSフィルター	無効
	non-L2MSフィルター	無効
L2スイッチング	独自ループ検出	有効
トラフィック制御	QoSトラストモード	CoS
	フロー制御 (IEEE 802.3x)	無効
	ストーム制御	無効
LLDPエージェント	送受信モード	有効
PoE給電	給電動作	有効
	給電優先度	低

- デフォルトVLAN (vlan1) に対する設定

設定項目		設定値
IPv4 Address		192.168.100.240/24
IGMP Snooping	動作	無効
MLD Snooping	動作	無効

# インターフェース制御機能

## インターフェース基本機能

### 機能概要

本製品のインターフェース基本機能について説明します。

### 用語の定義

特になし

### 機能詳細

#### インターフェースの種類

本製品では、下表の5種類のインターフェースを扱います。

インターフェースの種類	インターフェースID	説明
LANポート	port	本製品の物理ポート。 本インターフェースは、 <b>port</b> に続けて"筐体に印刷されているポート番号"で表現します。  LANポート#1の指定: <b>port1.1</b>
VLANインターフェース	vlan	ユーザーが定義したVLAN。 本インターフェースは、 <b>vlan</b> に続けて"VLAN ID"で表現します。 VLAN1の指定: <b>vlan1</b>
スタティック論理インターフェース	sa	ユーザーが定義したリンクアグリゲーション。 複数のLANポートを束ねて1つのインターフェースとして使用することができます。 本インターフェースは、 <b>sa</b> に続けて"論理リンクID"で表現します。  論理リンクID #1のスタティック論理インターフェースの指定 : <b>sa1</b>

### インターフェース制御

本製品では、インターフェースに対して下表の制御を行うことができます。

- 各ポートに対するインターフェース制御項目

制御項目	コマンド	説明
説明文の設定	<b>description</b>	インターフェースに対して説明文を設定します。

制御項目	コマンド	説明
有効化 / 無効化	<b>shutdown</b>	インターフェースを有効化 / 無効化します。
通信速度/通信モード	<b>speed-duplex</b>	インターフェースの通信速度と通信モードを設定します。(以下から選択します。) <ul style="list-style-type: none"> <li>・オートネゴシエーション</li> <li>・1Gbps / 全二重</li> <li>・100Mbps / 全二重</li> <li>・100Mbps / 半二重</li> <li>・10Mbps / 全二重</li> <li>・10Mbps / 半二重</li> </ul>
クロス/ストレート自動判別 (Auto MDI/MDI-X機能)	<b>mdix</b>	接続先のポートタイプ(MDI or MDI-X)を自動判別し、ケーブルの種別(クロス or ストレート)に依存することなく相互接続できるようにする機能です。
速度ダウンシフト	-	1000BASE-Tで使用できないLANケーブルが接続された時に、自動で速度を落としてリンクを試みる機能です。 本機能は、LANポートに対して常に有効となっています。(無効にすることはできません)
EEE	<b>eee</b>	Ethernet向け省電力技術 (EEE: Energy Efficient Ethernet) を使用するかどうかを設定します。 IEEE 802.3az として標準化されています。

- システム全体（全ポート共通）のインターフェース制御項目

制御項目	コマンド	説明
MRU	<b>mru</b>	インターフェースで受信可能な最大フレームサイズを <b>1,522～10,240 Byte</b> の範囲で設定します。
BPDU/パスルール	<b>pass-through bpdu</b>	BPDUフレーム（スパニングツリーで使用する制御フレーム）の転送の有効化 / 無効化を設定します。
EAP/パスルール	<b>pass-through eap</b>	EAPフレーム（IEEE802.1X認証で使用する認証フレーム）の転送の有効化 / 無効化を設定します。

各インターフェースに対するコマンド制御は、下表のようになっています。

- インターフェース制御 対応表

インターフェース名	説明文の設定	有効化 / 無効化	通信速度/通信モード	クロス/ストレート自動判別	EEE
LANポート	○	○	○	○	○
VLANインターフェース	○	×	×	×	×
スタティック論理インターフェース	○	○	×	×	×

## LANポートの初期状態

本製品のLANポートは、初期状態で以下のようになっています。

- 全てのLANポートは、アクセスポート(タグなしフレームを扱うポート)として機能し、デフォルトVLAN(VLAN #1)に所属しています。
- 全てのLANポートが所属するデフォルトVLAN(VLAN #1)に対して、IPv4アドレス(192.168.100.240/24)が付与されています。

## ポートミラーリング

本製品は、任意のLANポートのトラフィックを、指定したポートにコピーするポートミラーリング機能を提供します。

コピーされたパケットを採取することで通信状況の解析を行うことができます。

本製品では、4つのミラーポートを設定することができ、ミラーポートに対してそれ以外のすべてのLANポートをモニターとして、割り付けることが可能です。

ただし、以下の制限事項があります。

- 1つのモニターとして複数のミラーポートにミラーリングすることはできません。
- ミラーポートに設定されているポートをモニターとして使用することはできません。
- 論理インターフェースに所属しているLANポートをミラーポートとして使用することはできません。

また、モニターとして監視方向（送受信・送信のみ・受信のみ）を選択することができます。

ポートミラーリングの設定は、**mirror** コマンドで行うことができます。

初期設定では、ミラーポートの設定は無効となっています。

## フレームカウンター

本製品は、LANポートごとに送受信したフレーム数をカウントしています。(これをフレームカウンターといいます)

フレームカウンターの参照は、**show frame-counter** コマンドで行います。

下表にフレームカウンタの表示項目とその最大値を示します。

- 受信フレームカウンターの表示項目

表示項目	説明	最大値
packets (*1)	受信パケット数	4,294,967,295
octets	受信オクテット数	18,446,744,073,709,51,615
total-good-packets (*2)	正常に受信されたパケット数	4,294,967,295
total-error-packets (*2)	受信エラーパケット数 (CRCエラー、アライメントエラー、フレームサイズエラー)	4,294,967,295
drops (*2)	フィルター機能等によって受信時に破棄されたパケット数	4,294,967,295
broadcast-and-multicast-packets	ブロードキャストおよびマルチキャストのパケット受信数	4,294,967,295
64octet packets	64オクテット長のパケット受信数	4,294,967,295

表示項目	説明	最大値
65-127octet packets	65～127オクテット長のパケット受信数	4,294,967,295
128-255octet packets	128～255オクテット長のパケット受信数	4,294,967,295
256-511octet packets	256～511オクテット長のパケット受信数	4,294,967,295
512-1023octet packets	512～1,023オクテット長のパケット受信数	4,294,967,295
1024-MAXoctet packets	1,024～最大オクテット長 (*3) のパケット受信数	4,294,967,295

(\*1) : Packetsは (\*2) のパケットを合計した値になります。

(\*3) : 設定された **MRU** の値に依存し、変動します。

- 送信フレームカウンターの表示項目

表示項目	説明	最大値
packets (*1)	送信パケット数	4,294,967,295
octets	送信オクテット数	18,446,744,073,709,551,615
total-good-packets (*2)	正常に送信されたパケット数	4,294,967,295
total-error-packets (*2)	送信エラーパケット数 (フレームサイズエラー)	4,294,967,295
drops (*2)	送信時に破棄されたパケット数 (送信側での破棄が行われないため、カウンタの値は常に0となる)	-
broadcast-and-multicast-packets	ブロードキャストおよびマルチキャストのパケット送信数	4,294,967,295
64octet packets	64オクテット長のパケット送信数	4,294,967,295
65-127octet packets	65～127オクテット長のパケット送信数	4,294,967,295
128-255octet packets	128～255オクテット長のパケット送信数	4,294,967,295
256-511octet packets	256～511オクテット長のパケット送信数	4,294,967,295
512-1023octet packets	512～1,023オクテット長のパケット送信数	4,294,967,295
1024-MAXoctet packets	1,024～最大オクテット長 (*3) のパケット送信数	4,294,967,295

(\*1) : Packetsは (\*2) のパケットを合計した値になります。

(\*3) : 設定された **MRU** の値に依存し、変動します。

フレームカウンターは、**clear counters** コマンドで消去することもできます。

LANポートの状態を表示する **show interface** コマンドを実行したときに表示されるフレームカウンター値は、

**show frame-counter** コマンドと同じフレームカウンターの値です。

## 関連コマンド

関連コマンドについて、以下に示します。  
コマンドの詳細は、コマンドリファレンスを参照してください。

- ・ インターフェース基本機能 関連コマンド一覧

操作項目	操作コマンド
説明文の設定	description
シャットダウン	shutdown
通信速度・通信モードの設定	speed-duplex
クロス／ストレート自動判別設定	mdix auto
EEE設定	eee
EEEステータス情報を表示する	show eee status
MRU設定	mru
BPDU／パススルーの設定	pass-through bpdu
EAP／パススルーの設定	eap-through bpdu
ポートミラーリングの設定	mirror
ミラーリングポートの状態表示	show mirror
インターフェースの状態表示	show interface
インターフェースの状態簡易表示	show interface brief
フレームカウンター表示	show frame-counter
フレームカウンターのクリア	clear counters

## コマンド実行例

### LANポートに対する基本設定

LANポートに対する基本的な設定例を以下に示します。  
詳細な設定方法については、コマンドリファレンスを参照してください。

- ・ LANポート#1 (port1.1) に説明文を設定します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#description Connected to rtx1210-router
```

- ・ LANポート#1 (port1.1) を無効化します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#shutdown
```

- ・ LANポート#1 (port1.1) を有効化します。

```
Yamaha(config)#interface port1.1  
Yamaha(config-if)#no shutdown
```

- LANポート#1 (port1.1)の通信速度/通信モードを **100Mbps/Full** に設定します。

```
Yamaha(config)#interface port1.1  
Yamaha(config-if)#speed-duplex 100-full
```

## ミラーリング設定

LANポート#1 で LANポート#4 の送受信フレーム、 LANポート#5 の送信フレームを監視できるようにします。

ポートの役割としては、以下のようになります。

- ミラーポート: LANポート#1 (port1.1)
- モニターポート: LANポート#4 (port1.4)、 LANポート#5 (port1.5)
  1. ミラーポートであるLANポート#1 (port1.1) に対して、モニターポートの設定を行います。

```
Yamaha(config)#interface port1.1  
Yamaha(config-if)#mirror interface port1.4 direction both ①  
Yamaha(config-if)#mirror interface port1.5 direction transmit ②
```

① 送受信フレームの監視

② 送信フレームの監視

2. ミラーリング設定を確認します。

```
Yamaha#show mirror  
Monitor Port Mirror Port Direction  
===== ===== =====  
port1.1      port1.4      both  
                  port1.5      transmit
```

## LANポートの情報表示

- LANポート#1 (port1.1) の状態を確認します。

```
Yamaha#show interface port 1.1  
Interface port1.1  
Link is UP  
Hardware is Ethernet  
HW addr: 00a0.deae.b89f  
MRU 1522  
BPDU pass-through: Enabled  
EAP pass-through: Enabled  
Description: Connected to router  
ifIndex 5001  
Speed-Duplex: auto(configured), 1000-full(current)  
Auto MDI/MDIX: on
```

```
Vlan info :  
  Switchport mode      : access  
  Ingress filter       : enable  
  Acceptable frame types : all  
  Default Vlan         : 1  
  Configured Vlans     : 1  
Interface counter:  
  input  packets        : 34753  
  bytes              : 7806026  
  drops               : 12535  
  broadcast-and-multicast-packets: 21176  
  output  packets       : 10351  
  bytes              : 864389  
  drops               : 0  
  broadcast-and-multicast-packets: 7039
```

## 注意事項

特になし

## 関連文書

特になし

# リンクアグリゲーション

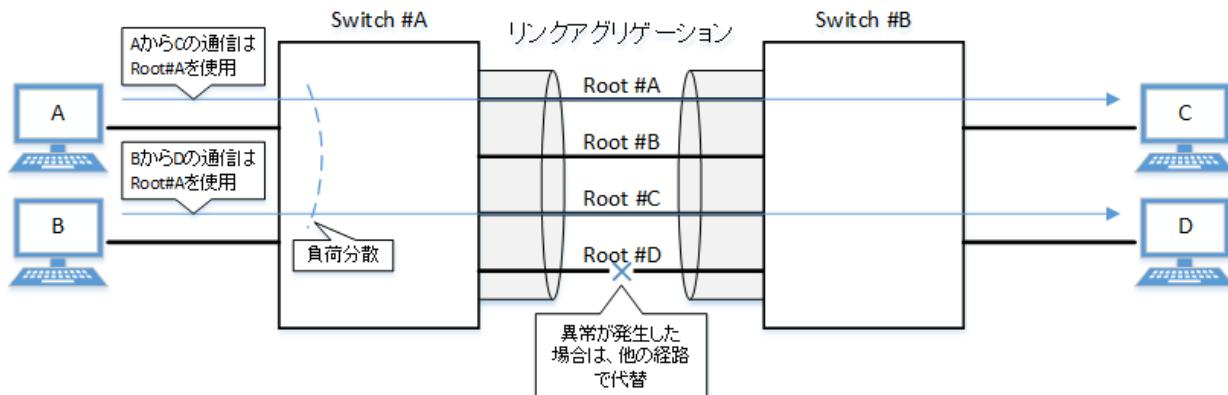
## 機能概要

リンクアグリゲーションは、ネットワーク機器間を接続する複数のLANポートを束ねて、一つの論理インターフェースとして扱う機能です。

リンクアグリゲーションは、複数の通信が発生する場合に有効な技術です。束ねた回線内でロードバランス機能を利用することで通信を分散させることができます。

また、リンクアグリゲーションで束ねた1つのLANポートで障害が発生し、通信不可になった場合でも残りのポートで通信を継続します。

- リンクアグリゲーション機能概要



本製品で提供するリンクアグリゲーションについて以下に示します。

- リンクアグリゲーション提供機能

提供機能	内 容
スタティックリンクアグリゲーション	束ねるLANポートを手動で設定するリンクアグリゲーション。LANポートがリンクアップしたタイミングで論理インターフェースとして動き始めます。

## 用語の定義

### ロードバランス

論理インターフェースに所属している LANポート 間で転送フレームを分散する機能。  
分散するためのルールとしてフレーム内の L2/L3/L4 情報を使用する。

## 機能詳細

### スタティック リンクアグリゲーション 仕様

本製品のスタティック リンクアグリゲーションの仕様について、以下に示します。

- 本製品のリンクアグリゲーションは、**8インターフェース** 定義することができます。  
インターフェース番号は、**1～8** の範囲で付与することができます。  
また、1つの論理インターフェースに対して **最大8つのLANポート** を所属させることができます。
- 収容するLANポートは、以下の設定が同じである必要があります。
  - ポートの動作

- ポートのモード (アクセス / トランク(ネイティブVLAN設定含む))
- 所属しているVLAN
- 所属しているマルチプルVLANグループ

3. 以下の設定については、収容するLANポート間で統一することを推奨します。

- 通信速度 / 通信モード
- フロー制御
- ストーム制御
- L2MSフィルター / non-L2MSフィルター

4. 論理インターフェースに対して、以下の操作を行うことができます。

- 説明文の追加 (**description** コマンド)
- インターフェースの有効化/無効化 (**shutdown** コマンド)
- VLAN、マルチプルVLANの設定

5. **port-channel load-balance** コマンドで、[ロードバランス](#)のルールを以下の中から選択することができます。

ロードバランスの設定は全論理インターフェース共通の設定となります。  
デフォルト設定値は、**宛先/送信元MACアドレス** です。

- 宛先MACアドレス
- 送信元MACアドレス
- 宛先/送信元MACアドレス
- 宛先IPアドレス
- 送信元IPアドレス
- 宛先/送信元IPアドレス
- 宛先ポート番号
- 送信元ポート番号
- 宛先/送信元ポート番号

6. LANポートをスタティック論理インターフェースに所属させるには、**static-channel-group** コマンドで行います。

- スタティック論理インターフェースが存在しないインターフェース番号に対してLANポートを所属させると、新たに論理インターフェースが生成されます。
- スタティック論理インターフェースからLANポートを脱退させた結果、所属するポートが無くなった場合、該当論理インターフェースが削除されます。
- 1つのLANポートを複数の論理インターフェースに所属させることはできません。
- また、ポートミラーリングのミラーポートとして使用しているLANポートは、スタティック論理インターフェースに所属させることができません。

7. スタティック論理インターフェースの状態表示は、**show static-channel-group** コマンドで行います。

## 関連コマンド

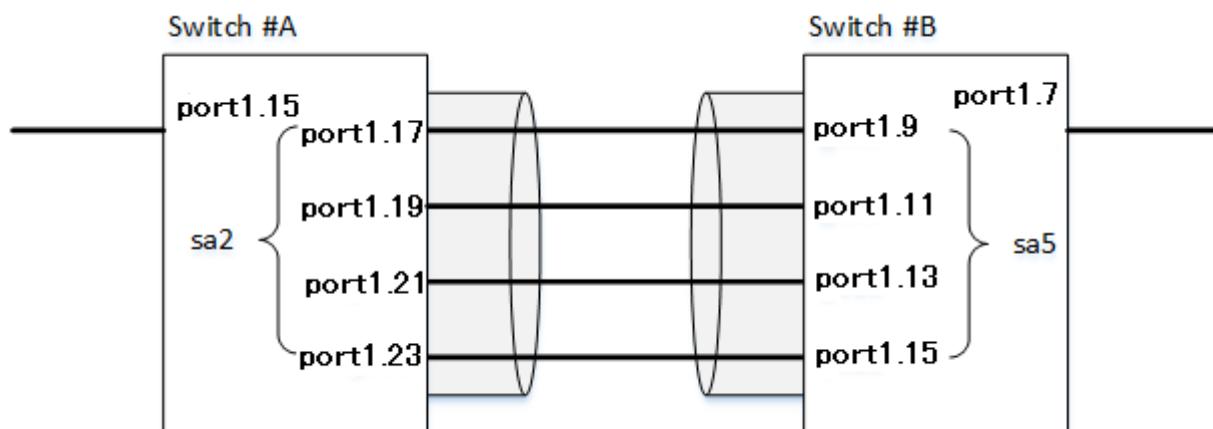
関連コマンドについて、以下に示します。  
コマンドの詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
スタティック論理インターフェースの設定	static-channel-group
スタティック論理インターフェースの状態表示	show static-channel-group
ロードバランス機能のルールの設定	port-channel load-balance

## コマンド実行例

### スタティック論理インターフェースの設定

L2スイッチ間の通信のために、LANポート4本を使用したリンクアグリゲーションを設定します。



- リンクアグリゲーションはスタティック設定とします。  
論理インターフェース番号は、スイッチA: #2、スイッチB: #5とします。
  - 論理インターフェースに所属するLANポートはすべてアクセスポートとし、VLAN #1000に所属します。
- [スイッチA] VLAN #1000を定義し、LANポート(#15, #17, #19, #21)を所属させます。  
あわせて、LANポート(#17, #19, #21, #23)を論理インターフェース #2 に所属させます。

```

Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.15 ②
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#interface port1.17 ④
Yamaha(config-if)#switchport access vlan 1000 ⑤
Yamaha(config-if)#static-channel-group 2 ⑥
Yamaha(config-if)#interface port1.19
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
Yamaha(config-if)#interface port1.21
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
Yamaha(config-if)#interface port1.23
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2

```

① VLAN #1000 の定義

- 
- ② LANポート #15 の設定
  - ③ アクセスポートに設定し、VLAN #1000 に所属させる
  - ④ LANポート #17 の設定
  - ⑤ アクセスポートに設定し、VLAN #1000 に所属させる
  - ⑥ 論理インターフェース #2 に所属させる

2. [スイッチA] 論理インターフェース #2 の設定状態を確認します。

```
Yamaha#show static-channel-group
% Static Aggregator: sa2
% Member:
  port1.17
  port1.19
  port1.21
  port1.23
```

3. [スイッチB] VLAN #1000 を定義し、LANポート(#07, #09, #11, #13, #15)を所属させます。  
あわせて、LANポート(#09, #11, #13, #15)を論理インターフェース #5 に所属させます。

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.7
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#interface port1.9
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.11
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.13
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.15
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
```

4. [スイッチB] 論理インターフェース #5 の設定状態を確認します。

```
Yamaha#show static-channel-group
% Static Aggregator: sa5
% Member:
  port1.9
  port1.11
  port1.13
  port1.15
```

5. [スイッチA] 論理インターフェースを有効化します。

```
Yamaha(config)#interface sa2 ①  
Yamaha(config-if)#no shutdown ②
```

① 論理インターフェース #2 の設定

② 論理インターフェースの有効化

6. [スイッチB] 論理インターフェースを有効化します。

```
Yamaha(config)#interface sa5 ①  
Yamaha(config-if)#no shutdown ②
```

① 論理インターフェース #5 の設定

② 論理インターフェースの有効化

7. [スイッチA] 論理インターフェースの状態を確認します。

```
Yamaha#show interface sa2  
Interface sa2  
Link is UP  
Hardware is AGGREGATE  
MRU 1522  
BPDU pass-through: Enabled  
EAP pass-through: Enabled  
Description:  
ifIndex 4502  
Vlan info :  
Switchport mode : access  
Ingress filter : enable  
Acceptable frame types : all  
Default Vlan : 1000  
Configured Vlans : 1000  
Interface counter:  
input packets : 2109  
bytes : 211698  
drops : 0  
broadcast-and-multicast-packets: 2109  
output packets : 24  
bytes : 2952  
drops : 0  
broadcast-and-multicast-packets: 24
```

8. [スイッチB] 論理インターフェースの状態を確認します。

```
Yamaha#show interface sa5  
Interface sa5  
Link is UP  
Hardware is AGGREGATE  
MRU 1522  
BPDU pass-through: Enabled  
EAP pass-through: Enabled  
Description:
```

```
ifIndex 4505
Vlan info :
  Switchport mode      : access
  Ingress filter       : enable
  Acceptable frame types : all
  Default Vlan         : 1000
  Configured Vlans     : 1000
Interface counter:
  input  packets        : 24
  bytes              : 2952
  drops              : 0
  broadcast-and-multicast-packets: 24
  output  packets       : 2109
  bytes              : 211698
  drops              : 0
  broadcast-and-multicast-packets: 2109
```

## 注意事項

特になし。

## 関連文書

- ・ [インターフェース基本設定](#)

# PoE制御

## 機能概要

**PoE (Power over Ethernet)** とは、Ethernet ケーブル (カテゴリ5e以上) を使って電力を供給する技術のことです。

本製品は、クラス4 受電機器へ給電可能な **IEEE 802.3at** に対応します。

IEEE 802.3atでは、

- ・ 電力供給側(給電機器) : PSE: Power Sourcing Equipment
- ・ 電力受電側(受電機器) : PD: Powered Device

と呼びます。

本製品は、給電方式として、ケーブルの信号線 (1,2,3,6) を使用する **Alternative A** を採用します。

## 用語の定義

特になし

## 機能詳細

### PoE 給電機能の有効/無効 制御

本製品のPoE 給電に対応しているポート (以下PoEポート) は、それぞれ以下のとおりです。

- ・ SWX2210P-10G : ポート 1-8
- ・ SWX2210P-18G : ポート 1-16
- ・ SWX2210P-28G : ポート 1-24

本製品では、工場出荷状態で、すべての PoEポートの給電機能が有効となっています。

ただしポートごとに給電機能を無効に設定することも可能です。

接続機器が通常のEthernet 機器の場合、給電を行わず **通常のEthernet ポート** として動作します。

### 給電クラスと同時給電可能なポートの最大数

本製品は、PoE 規格に準拠した給電機器として、**1ポートあたり最大30W** の電力供給が可能です。

接続されたPDの検出と電力クラスの識別を自動的に行い、給電を開始します。

IEEE 802.3at で規定される電力クラスと同時に給電可能なポートの最大数について、以下に示します。

Class	受電機器の電力 (MAX)	給電機器の電 力	同時給電可能 最大ポート数 (PoE供給可能電力上限)		
			SWX2210P- 10G(124W)	SWX2210P- 18G(247W)	SWX2210P- 28G(370W)
0	13.0 W	15.4W	8	16	24
1	3.84 W	4.0W	8	16	24
2	6.49 W	7.0W	8	16	24
3	13.0 W	15.4W	8	16	24
4	25.5 W	30.0W	4 (*)	8 (*)	12 (*)

- 
- (\*)：受電機器の電力使用量によって、記載しているポート数以上の同時給電が可能です。

## ガードバンド

ガードバンドとは、不意の給電停止を避けるために最大供給電力に対して設定するマージンのことです。給電可能電力量がガードバンド以下の場合、新たに接続されたPDに対しての給電を抑制します。このガードバンドの値を適切に設定することにより、後から接続されたPDによって他のPDへの給電が停止されてしまうのを防ぐことができます。本製品では、ガードバンドの値を**0～30W**の範囲で設定することができ、デフォルトは**7W**です。

## 給電優先度

本製品はPoEポートごとに給電優先度の設定が可能です。

優先度は高い順に **critical, high, low** となり、デフォルトは全ポート**low**の設定となります。同じ優先度が設定されているポート間では、ポート番号の小さい方が優先度が高く、ポート番号順(1 → 2 → 3 ...)に低くなります。PDからPower via MDI TLVを含むLLDPフレームを受信した場合、LLDPフレームを受信したPoEポートでは、給電優先度の設定に関わらずLLDPフレーム内で指定された給電優先度で動作します。

## PoE給電動作

本製品は電力使用量によって以下の処理を行います。

- システム全体の電力消費量がPoE供給可能電力上限を超えた場合  
優先度の低い順にPoEポートからの給電を停止し、電力消費量がPoE供給可能電力上限内に収まるようにします。  
このとき、電力供給を停止したポートのPoE STATE LEDが橙点灯し、STATUS LEDも橙点灯します。  
また、SYSLOGに "PortX.X over system power limit" を出力します。
- 給電可能電力量がガードバンド以下の場合  
既に給電を行っているPDへの給電は続行されますが、新たにPDを接続した場合には給電優先度に関わらずそのPDに対する給電は行われません。  
このとき、電力供給が行われなかったポートのPoE STATE LEDを橙点灯し、STATUS LEDも橙点灯します。
- 特定のPoEポートの電力消費量がポート単位のPoE供給可能電力上限を超えた場合  
該当するPoEポートの給電を停止します。他のPoEポートへの給電は継続します。  
このとき、電力供給を停止したポートのPoE STATE LEDを橙点滅し、STATUS LEDは橙点灯します。  
また、SYSLOGに、"PortX.X over load" を出力します。
- 電力使用量が上記以外（正常範囲内）の場合  
PDへの給電を継続します。  
このとき、給電しているPoEポートのPoE STATE LEDは緑色に点灯します。

また、PoEポートの状態あるいは給電可能電力量に変化があった場合、以下の処理を行います。

- 給電を開始した場合  
SYSLOGに、"PortX.X power on" を出力します。  
給電を開始したPoEポートのPoE STATE LEDを緑点灯します。
- 給電を停止した場合  
SYSLOGに、"PortX.X power off" を出力します。  
給電を停止したPoEポートのPoE STATE LEDを消灯します。
- 残りの給電可能電力量がガードバンド以下になった場合  
SYSLOGに、"guardband on" を出力します。

- ・残りの給電可能電力量がガードバンド以下の状態から回復した場合  
SYSLOGに、"guardband off" を出力します。

## LLDPによる給電設定

本製品は、PDからPower via MDI TLVを含むLLDPフレームを受信したとき、PoEポートの給電動作を自動的に変更します。

本機能はLLDPフレームが受信可能なPoEポートでのみ動作します。  
Power Via MDI TLVと変更される動作の対応は以下のとおりです。

Power Via MDI TLV (IEEE802.3)	変更される動作
Requested power priority	給電優先度
PD requested power value	PoEポートの電力割り当て

## 関連コマンド

関連コマンドについて、以下に示します。  
コマンドの詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
システム全体でのPoE給電機能の設定	power-inline enable
インターフェース単位でのPoE給電機能の設定	power-inline enable
PoEポートの説明文の設定	power-inline description
PoEポートの優先度の設定	power-inline priority
ガードバンドの設定	power-inline guardband
PoE給電情報の表示	show power-inline

## コマンド実行例

### PoEポートの給電設定

port1.8の給電機能を設定します。

```

Yamaha(config)#power-inline enable ①
Yamaha(config)#interface port1.8
Yamaha(config-if)#power-inline description AP1 ②
Yamaha(config-if)#power-inline priority critical ③
Yamaha(config-if)#power-inline enable ④
Yamaha(config-if)#exit
Yamaha(config)#exit

```

- ① システム全体のPoE給電機能を有効化 ※default設定の場合不要
- ② PoEポートの説明文としてAP1を設定
- ③ PoEポートの優先度を最高に設定
- ④ インターフェースのPoE給電機能を有効化 ※default設定の場合不要

---

## **注意事項**

特になし

## **関連文書**

特になし

# Layer 2機能

## フォワーディングデータベース

### 機能概要

フォワーディングデータベース(以降、FDB)は、宛先MACアドレスと送出ポートとVLANの組み合わせを管理するものです。  
本製品は、受信フレームの転送先ポートを決定する際に使用します。

1. 学習機能の有効／無効制御
2. 学習したFDBエントリの保持時間の調整
3. 学習したFDBエントリのクリア
4. FDBエントリの手動登録(スタティックエントリ)

### 用語の定義

#### FDB

Forwarding Data Base の略です。  
宛先MACアドレスと送出ポートと VLAN の組み合わせを管理するデータベースです。

#### FDBエントリー

FDBに登録するデータのことで、複数の要素で構成されます。

### 機能詳細

#### FDBエントリー

本製品は、FDBに対して下表に示す内容を一つのエントリーとして登録します。

管理要素	説明
MACアドレス	デバイスのMACアドレス、ユニキャストとマルチキャストがあります。
VLAN-ID (FID)	デバイスの所属するVLAN ID。1～4094の値となります。
転送先インターフェースID	デバイスが存在するインターフェース*。 (*:LANポート or スタティック論理インターフェース)
アクション	デバイス宛てフレームの処理方法。 処理方法には、破棄(discard)と転送(forward)があります。
登録種別	エントリの登録種別。以下の種別があります。 * dynamic … 自動学習により登録されたエントリー * static … コマンドにより手動で登録したエントリー

#### MACアドレス

FDBのキー項目の一つで、VLAN-IDとMACアドレスの二つを合わせてレコードキーになります。  
MACアドレスが、ユニキャストの時と、マルチキャストの時では、動作に違いがあります。

- ユニキャスト  
あるレコードキーに対して、転送先インターフェースIDは、一意に決まる必要があるので、重複は認められません。  
(同じ、VLAN-IDとMACアドレスの組み合わせは複数存在しない)
- マルチキャスト  
あるキーレコードに対しての、転送先インターフェースIDは、複数個存在しても構いません。  
その場合、複数の転送先インターフェースIDに、転送されます。

本製品は、自動学習／手動登録合わせて 最大8,192個のアドレス を登録できます。

すべての受信フレームをMACアドレス学習の対象とし、送信元MACアドレスを学習してFDBに登録します。  
(ただし、送信元MACアドレスがマルチキャストの場合は、これを不正なフレームとみなして破棄し、登録しません。)

自動学習で登録したMACアドレス情報は、エージングタイムアウトまで保持します。

#### VLAN-ID

MACアドレスの学習はVLAN単位に行い、FDBは MACアドレス と VLAN のペアで管理します。  
異なるVLANであれば、同一のMACアドレス情報も学習します。

#### 転送先インターフェースID

登録されるIDは下記となります。

- LANポート (port)
- スタティックインターフェース (sa)

#### アクション

キーレコードヒー一致した受信フレームに対してのアクションを定義します。  
MACアドレスが、ユニキャストの場合は、下記のアクションになります。

- forward … 転送先インターフェースIDに転送します。
- discard … 転送せず破棄します。

MACアドレスがマルチキャストの場合は、下記のアクションになります。

- forward … 転送先インターフェースIDに転送します。
- discard … 設定できません。  
(MACアドレスがマルチキャストの場合、discardは設定できません。)

#### 登録種別

- dynamic … 自動的に登録、削除が行われます。configファイルには、登録結果は残りません。
- static … 手動で登録、削除するため、configファイルに残ります。

#### MACアドレスの自動学習

MACアドレスの自動学習とは、受信フレームの送信元MACアドレスと受信ポートの情報に基づいてFDBエントリーを動的に作成し、登録していくことを指します。

この自動学習により登録されたエントリーを ダイナミックエントリー といいます。

個々のダイナミックエントリーに対して、タイマー（エージングタイム）による監視が行われます。

一定時間フレーム受信がなかったMACアドレスに対するエントリーは、FDBから削除されます(後述\*)。

---

これにより、電源断、移動などで無効になったデバイスのエントリーが、FDBに残らないようになっています。なお、時間内に再度受信があった場合は、監視タイマーがリセットされます。

以下に自動学習の制御仕様について示します。

1. MACアドレスの自動学習は、 **mac-address-table learning** コマンドを使用して、有効／無効の制御が可能です。  
初期状態では、有効となっています。
2. 自動学習が有効な状態から、無効に変更すると、 **学習したダイナミックエントリーはすべて削除** されます。  
なお、学習機能・無効の設定は、すべての受信フレームを全ポートにフラッディングしたい場合に有用です。
3. ダイナミックエントリーに対するエージングタイムの調整は、 **10~634秒** の指定を可能とし、 **mac-address-table ageing-time** コマンドで行います。  
初期状態では、300秒が設定されています。
4. 学習したダイナミックエントリーのクリアは、 **clear mac-address-table dynamic** コマンドで行います。  
クリアする単位として、全FDB内容を一括クリアする指定のほかに、VLAN番号を指定することで指定VLANとして学習した全MACアドレスをFDBからクリアします。  
また、ポート番号を指定することで指定ポートから学習したMACアドレスをFDBからクリアすることもできます。
5. 自動学習の状態を確認するには、 **show mac-address-table** コマンドを使用します。
6. **mac-address-table ageing-time** コマンドで設定した時間と、実際にダイナミックエントリーがMACアドレステーブルから削除されるまでの時間との間で、誤差が生じる場合があります。

## MACアドレスの手動設定

本製品は、受信フレームによる自動学習のほかに、ユーザーのコマンド操作でMACアドレスを設定することができます。

コマンド操作で登録したエントリーを **スタティックエントリー** といいます。

以下に手動設定についての仕様を示します。

1. スタティックエントリーの登録は、 **mac-address-table static** コマンドを使用します。
2. 手動で登録できるスタティックエントリーの数は 256個 です。
3. スタティックエントリーの登録を行うと、そのMACアドレスに対してダイナミックな学習は行いません。  
学習済みのエントリは、FDBから削除され、スタティックエントリーとして登録されます。
4. スタティックエントリーの削除は、 **no mac-address-table static** コマンド を使用します。
5. 受信フレームの宛先MACアドレスに対して転送(forward)か廃棄(discard)かを指定可能とします。
  - 転送指定を行う場合、転送先のLANポート、またはスタティック論理インターフェースを指定することができます。
  - 廃棄指定を行った場合、MACアドレスに対する受信フレームは、どのポートにも転送せずに廃棄します。
6. マルチキャストのMACアドレスを登録する場合、廃棄(discard)は指定できません。  
また下記の範囲にあるMACアドレスは登録できません。
  - 0180.c200.0000～0180.c200.000f
  - 0180.c200.0020～0180.c200.002f

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
MACアドレス学習機能の有効・無効設定	mac-address-table learning
ダイナミックエントリー エージングタイムの設定	mac-address-table ageing-time
ダイナミックエントリーの削除	clear mac-address-table dynamic
スタティックエントリーの登録	mac-address-table static
スタティックエントリーの削除	no mac-address-table static
MACアドレステーブルの参照	show mac-address-table

## コマンド実行例

### FDBの参照

```
Yamaha#show mac-address-table
VLAN  port      mac          fwd      type      timeout
  1  port1.2  00a0.de11.2233  forward  static      0
  1  port1.1  1803.731e.8c2b  forward  dynamic    300
  1  port1.1  782b.cbc.218d  forward  dynamic    300
```

### ダイナミックエントリーの削除

FDBに登録されているFDBエントリー ( MACアドレス00:a0:de:11:22:33 )を削除する

```
Yamaha#clear mac-address-table dynamic address 00a0.de11.2233
```

### ダイナミックエントリー エージング時間の変更

ダイナミックエントリーのエージング時間を 600秒 に変更する。

```
Yamaha(config)#mac-address-table ageing-time 600
```

### スタティックエントリーの登録

VLAN #10に所属するデバイス (MACアドレス 00:a0:de:11:22:33) 宛てフレームをLANポート2 (port1.2) に転送する。

```
Yamaha(config)#mac-address-table static 00a0.de11.2233 forward port1.2 vlan 10
```

VLAN #10に所属するデバイス (MACアドレス 00:a0:de:11:22:33) 宛てフレームを破棄する。  
インターフェース名の指定(例ではport1.2)は、動作に影響ありません。省略不可のため、LANポートを指定してください。

```
Yamaha(config)#mac-address-table static 00a0.de11.2233 discard port1.2 vlan 10
```

## スタティックエントリーの削除

VLAN #10に所属するデバイス (MACアドレス 00:a0:de:11:22:33)宛ての転送設定を削除する。

```
Yamaha(config)#no mac-address-table static 00a0.de11.2233 forward port1.2 vlan 10
```

## 注意事項

特になし

## 関連文書

特になし

# VLAN

## 機能概要

VLAN ( Virtual LAN ) は、物理的な接続構成と関係なく、仮想的にLANを構成することができる技術です。本製品でVLANを使用するとLANを複数の**ブロードキャストドメイン**に分割することができます。本製品でサポートするVLANについて、以下に示します。

VLANの種類	概要
ポートベースVLAN	LANポート単位で通信可能なグループを構成します。
タグVLAN	イーサネットフレームに付加した固定長のタグ情報で通信可能なグループを識別します。 1つのLANポートで複数の異なるVLANを通信させることができます。

## 用語の定義

### ブロードキャストドメイン

Ethernetなどのネットワークで、ブロードキャストフレームが届く範囲のこと。  
スイッチングハブなどのデータリンク層(MAC層)を中継する機器によって接続された端末同士が同じブロードキャストドメインに所属することになります。  
一般的にEthernetにおけるネットワークとはこのブロードキャストドメインのことを指します。

## 機能詳細

### VLAN IDの定義

本製品は、VLAN IDとして2~4094の範囲で最大255個定義することが可能です。(ID #1はデフォルトVLAN IDとして使用します。)

VLAN IDは、**vlan database** コマンドでVLANモード遷移後に **vlan** コマンドを使用して定義します。  
詳細はコマンドリファレンスを参照願います。

### LANポートに対するVLAN設定

本製品でVLANを利用するためには、使用するVLANを定義した後に、以下の設定を行う必要があります。

- LANポートのモードを設定する
- LANポートの所属VLANを設定する

1. 本製品のLANポートは、以下に示すどちらかのモードに設定します。
  - アクセスポート  
タグなしフレームを扱うポート。1つのVLANに所属することができます。
  - トランクポート  
タグなし/タグ付き両方のフレームを扱うポート。  
複数のVLANに所属することができ、主にスイッチ同士を接続する際に使用します。  
本製品では、IEEE 802.1Qのみをサポートします。(Cisco ISLについてはサポートしません。)
2. LANポートのモード設定は、**switchport mode** コマンドで行います。  
トランクポートに設定する際、指定したVLAN ID以外のフレームを扱うかどうかを 入力フィルタ(ingress-filter) で制御することができます。

- 
- 入力フィルタ有効時：指定したVLAN IDが設定されているフレームのみを扱います。

- 入力フィルタ無効時：全VLAN IDを扱います。

3. LANポートの設定モードの確認は、 **show interface switchport** コマンドで行います。

4. アクセスポートの所属VLANは、 **switchport access vlan** コマンドで設定します。

5. トランクポートの所属VLANは、 **switchport trunk allowed vlan** コマンドで設定します。

トランクポートは複数のVLANに所属できるため、以下に示す all 、 none 、 except 、 add 、 remove で設定を行います。

- add

指定したVLAN IDを追加します。

追加可能なVLAN IDは、 VLANモードで定義されているIDに限定されます。

- remove

指定したVLAN IDを削除します。

- all

VLANモードで定義した全てのVLAN IDを追加します。

本コマンド実行後、 VLANモードで追加したVLAN IDも追加の対象となります。

- none

どのVLANにも所属しません。

- except

指定したVLAN ID以外を追加します。

本コマンド実行後、 VLANモードで追加したVLAN IDも追加の対象となります。

6. トランクポートに対して、 タグなしフレームを扱うVLAN（ネイティブVLAN）を指定することができます。

7. LANポートの所属VLANの確認は、 **show vlan** コマンドで行います。

## デフォルトVLAN

デフォルトVLANとは、 本スイッチの初期状態から存在する VLAN #1 (vlan1) のことです。

デフォルトVLANは特殊なVLANであるため、 常に存在し、 削除することはできません。

なお、 以下の操作を行うと、 該当ポートは自動的にデフォルトVLANから削除されます。

- アクセスポートに対してデフォルトVLAN以外のVLAN を設定した
- トランクポートに対してデフォルトVLAN以外をネイティブVLANに設定した
- トランクポートに対してネイティブVLANをなし(none)にした

## ネイティブVLAN

ネイティブVLANとは、 トランクポートに設定したLANポートで、 受信したタグなしフレームを所属させるVLANのことです。

LANポートをトランクポートとして定義すると、 デフォルトVLAN（VLAN #1）がネイティブVLANとして設定されます。

特定のVLANをネイティブVLANとして定義する場合は、 **switchport trunk native vlan** コマンドを使用します。

該当LANポートでタグなしフレームを扱わないようにしたい場合は、 ネイティブVLANをなしに設定することも可能です。 (**switchport trunk native vlan** コマンドでnoneを指定)

## 関連コマンド

### 関連コマンド一覧

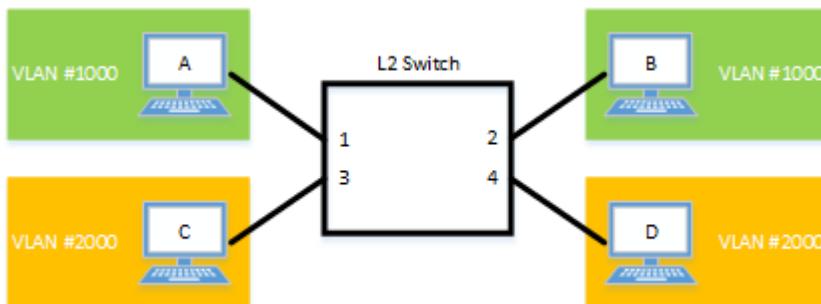
関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
VLANモードへの遷移	vlan database
VLANインターフェースの定義、定義済VLANの変更	vlan
アクセスポート(タグなしポート)の設定	switchport mode access
アクセスポート(タグなしポート)の所属VLANの設定	switchport access vlan
トランクポート(タグ付きポート)の設定	switchport mode trunk
トランクポート(タグ付きポート)の所属VLANの設定	switchport trunk allowed vlan
トランクポート(タグ付きポート)のネイティブVLANの設定	switchport trunk native vlan
VLAN情報の表示	show vlan

## コマンド実行例

### ポートベースVLAN の設定

ホストA～B間、ホストC～D間 の通信を可能にするために、本製品にポートベースVLANを設定します。



本製品のLANポートの設定は以下とします。

- LANポート #1/#2 : アクセスポートに設定し、VLAN #1000 に所属
- LANポート #3/#4 : アクセスポートに設定し、VLAN #2000 に所属

### ■設定手順

1. **vlan database** コマンドでVLANモードに移行し、**vlan** コマンドで2つのVLANを定義します。

```
Yamaha(config)# vlan database ①
Yamaha(config-vlan)# vlan 1000 ②
Yamaha(config-vlan)# vlan 2000 ③
Yamaha(config-if)# exit
```

① VLANモードに移行

- 
- ② VLAN #1000の作成
  - ③ VLAN #2000の作成
2. LANポート #1/#2をアクセスポートに設定し、VLAN #1000 に所属させます。

```
Yamaha(config)# interface port1.1 ①
Yamaha(config-if)# switchport mode access ②
Yamaha(config-if)# switchport access vlan 1000 ③
Yamaha(config-if)# interface port1.2 ④
Yamaha(config-if)# switchport mode access ⑤
Yamaha(config-if)# switchport access vlan 1000 ⑥
Yamaha(config-if)# exit
```

- ① interface modelに移行
  - ② アクセスポートに設定
  - ③ VLAN IDの指定
  - ④ interface modelに移行
  - ⑤ アクセスポートに設定
  - ⑥ VLAN IDの指定
3. LANポート #3/#4をアクセスポートに設定し、VLAN #2000 に所属させます。

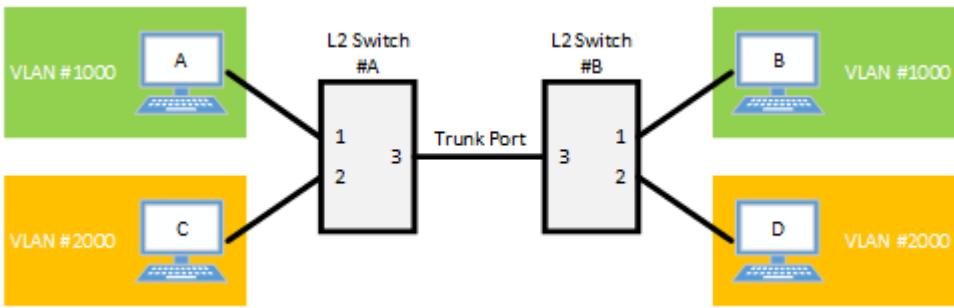
```
Yamaha(config)# interface port1.3
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 2000
Yamaha(config-if)# interface port1.4
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 2000
Yamaha(config-if)# exit
```

4. VLANの設定を確認します。

```
Yamaha#show vlan brief
(u)-Untagged, (t)-Tagged
VLAN ID  Name          State   Member ports
=====  ======  ======  ======
1        default      ACTIVE  port1.5(u) port1.6(u) port1.7(u)
                  port1.8(u) port1.9(u) port1.10(u)
1000    VLAN1000    ACTIVE  port1.1(u) port1.2(u)
2000    VLAN2000    ACTIVE  port1.3(u) port1.4(u)
```

## タグVLAN の設定

ホストA～B間、ホストC～D間の通信を可能にするために、本製品の#A～#B間にタグVLANを設定します。



本製品#A/#Bの LANポートの設定は以下とします。

- LANポート #1 : アクセスポートに設定し、VLAN #1000 に所属
- LANポート #2 : アクセスポートに設定し、VLAN #2000 に所属
- LANポート #3 : トランクポートに設定し、LAN #1000、VLAN #2000 に所属

1. [スイッチ#A/#B] VLAN を定義します。

```
Yamaha(config)#vlan database ①
Yamaha(config-vlan)#vlan 1000 ②
Yamaha(config-vlan)#vlan 2000 ③
```

- ① vlan mode に移行
- ② VLAN #1000の定義
- ③ VLAN #2000の定義

2. [スイッチ#A/#B] LANポート #1をアクセスポートに設定し、VLAN #1000 に所属させます。

```
Yamaha(config)#interface port1.1 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#exit
```

- ① interface mode に移行
- ② アクセスポートに設定
- ③ VLAN #1000に所属させる

3. [スイッチ#A/#B] LANポート #2をアクセスポートに設定し、VLAN #2000 に所属させます。

```
Yamaha(config)#interface port1.2 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 2000 ③
Yamaha(config-if)#exit
```

- ① interface modeに移行
- ② アクセスポートに設定
- ③ VLAN #2000に所属させる

4. [スイッチ#A/#B] LANポート #3をトランクポートに設定し、VLAN #1000 / #2000 を所属させます。

```
Yamaha(config)#interface port1.3 ①
Yamaha(config-if)#switchport mode trunk ②
Yamaha(config-if)#switchport trunk allowed vlan add 1000 ③
Yamaha(config-if)#switchport trunk allowed vlan add 2000 ④
Yamaha(config-if)#exit
```

- ① interface mode に移行
- ② トランクポートに設定
- ③ VLAN #1000を追加
- ④ VLAN #2000を追加

5. VLANの設定を確認します。

```
Yamaha#show vlan brief
(u)-Untagged, (t)-Tagged

VLAN ID Name          State Member ports
----- -----
1      default        ACTIVE port1.3(u) port1.4(u) port1.5(u)
                      port1.6(u) port1.7(u) port1.8(u)
                      port1.9(u) port1.10(u)
1000   VLAN1000       ACTIVE port1.1(u) port1.3(t)
2000   VLAN2000       ACTIVE port1.2(u) port1.3(t)
```

## 注意事項

特になし

## 関連文書

特になし

# マルチプルVLAN

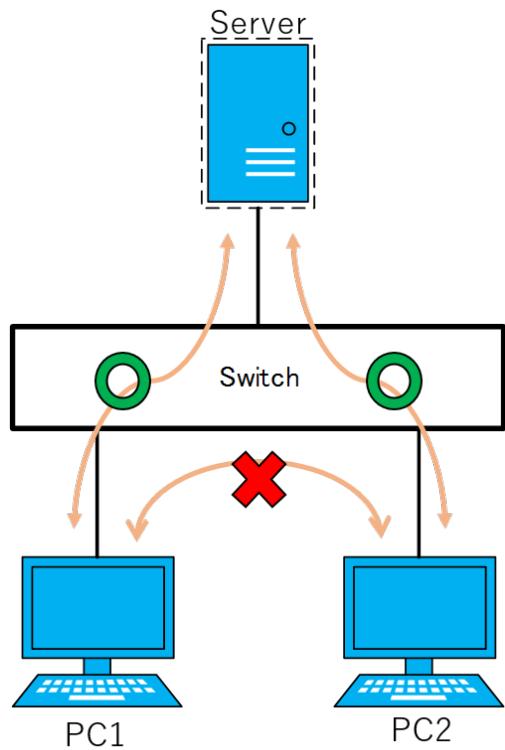
## 機能概要

マルチプルVLANでは、同じVLANに所属するポートを複数のグループに分けて、グループ間の通信を遮断することができます。

また、ポートを複数のグループに分けるだけでなく、ひとつのポートを複数のグループに参加させることもできます。

この機能により、図にあるような、各端末はサーバーにアクセスできるものの、端末間の通信は遮断したい、といった要望を簡単に実現できます。

- マルチプルVLANの利用例



## 用語の定義

特になし

## 機能詳細

### 基本動作仕様

マルチプルVLANでは、VLAN内にグループを作成できます。

マルチプルVLANグループは、**switchport multiple-vlan group** コマンドで設定します。

マルチプルVLANはLANインターフェース、リンクアグリゲーション論理インターフェースに設定可能です。トランクポートにマルチプルVLANグループを設定した場合、該当ポートの所属する全VLANに対して適用されます。

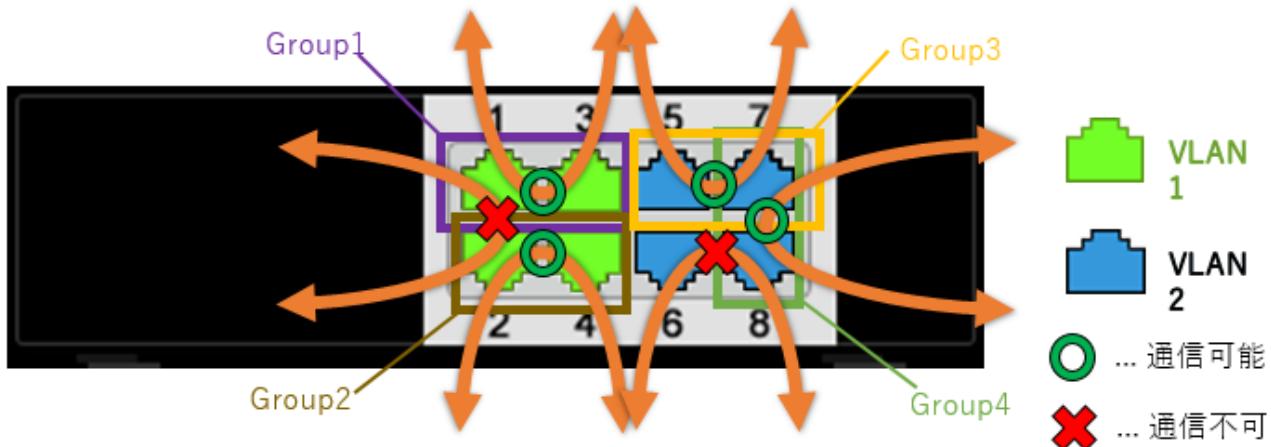
マルチキャストフレーム(\*1)にもマルチプルVLANグループ設定が適用されます。

最大グループ数は、製品のポート数と同じ数です。

(\*1) : 以下のフレームについては、マルチプルVLANグループが異なるポートにも転送されます。

- ・ L2MS制御フレーム
- ・ ヤマハ無線アクセスポイントで使用する制御フレーム
- ・ BPDU/パススルー有効時のBPDUフレーム

## マルチプルVLANグループ間の通信例



上図のようなマルチプルVLANグループ設定(Group #1 ~ #4)の場合、特定ポートA/B間の通信可否とその理由は以下の表のようになります。

ポート番号 A (グループ)	ポート番号 B (グループ)	通信可否	理由
port1.1 (Group 1)	port1.2 (Group 2)	不可	マルチプルVLANグループが違うため
port1.1 (Group 1)	port1.3 (Group 1)	可	マルチプルVLANグループ #1 に所属
port1.2 (Group 2)	port1.4 (Group 2)	可	マルチプルVLANグループ #2 に所属
port1.5 (Group 3)	port1.7 (Group 3,4)	可	マルチプルVLANグループ #3 に所属
port1.6 (Group なし)	port1.8 (Group 4)	不可	マルチプルVLANグループが違うため
port1.7 (Group 3,4)	port1.8 (Group 4)	可	マルチプルVLANグループ #4 に所属

※上記の例のport1.6はどのポートとも通信できませんが、他にどのグループにも属さないポートがある場合、どのグループにも属さないポート間で通信することは可能です。

## 関連コマンド

### 関連コマンド一覧

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

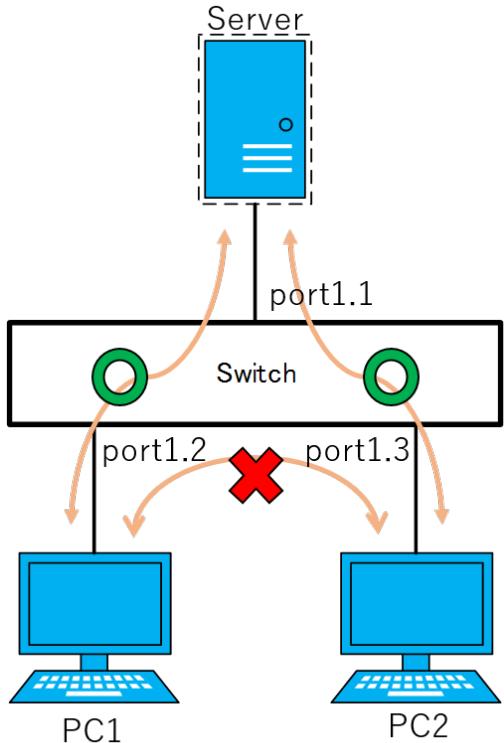
操作項目	操作コマンド
マルチプルVLANグループの設定	switchport multiple-vlan group

## コマンド実行例

### マルチプルVLAN の設定

VLAN #1 内で、PC1-Server間、PC2-Server間の通信は許可し、PC1-PC2間の通信は遮断します。

- マルチプルVLAN設定例



マルチプルVLANグループの設定は以下とします。

- port1.1 : マルチプルVLANグループ #1 , #2 に所属
- port1.2 : マルチプルVLANグループ #1 に所属
- port1.3 : マルチプルVLANグループ #2 に所属

1. port1.1をマルチプルVLANグループ #1 , #2 に所属させます。

```
Yamaha(config)# interface port1.1 ①  
Yamaha(config-if)# switchport multiple-vlan group 1 ②  
Yamaha(config-if)# switchport multiple-vlan group 2 ③  
Yamaha(config-if)# exit
```

① interface modeに移行

② マルチプルVLANグループ 1 に参加する

③ マルチプルVLANグループ 2 に参加する

2. port1.2をマルチプルVLANグループ #1 に所属させます。

```
Yamaha(config)# interface port1.2 ①  
Yamaha(config-if)# switchport multiple-vlan group 1 ②
```

```
Yamaha(config-if)# exit
```

- ① interface modeに移行
  - ② マルチプルVLANグループ 1 に参加する
3. port1.3をマルチプルVLANグループ #2 に所属させます。

```
Yamaha(config)# interface port1.3 ①
Yamaha(config-if)# switchport multiple-vlan group 2 ②
Yamaha(config-if)# exit
```

- ① interface modeに移行
- ② マルチプルVLANグループ 2 に参加する

## 注意事項

本機能の注意事項は以下のとおりです。

- ・ リンクアグリゲーション論理インターフェースに所属させるポートのマルチプルVLANグループは同一にする必要があります。
- ・ マルチプルVLANグループが適用されるのは、ポート間のフォワーディングのみです。自発のパケットはマルチプルVLANグループ設定の影響を受けません。
- ・ マルチプルVLANを設定していても、以下の影響で正しく通信できないことがあります。
  - ループ検出のブロック状態

## 関連文書

特になし

# 独自ループ検出

## 機能概要

本製品は、構成したネットワーク環境でループが発生していないかどうかを検出する独自の仕組みを提供します。

LANポートから独自のループ検出フレームを送信し、そのフレームが自身に戻ってくるかどうかを監視します。

送信フレームが自身に戻ってきた場合、該当ポートでループが発生していると判断します。

## 用語の定義

### LDF (Loop Detection Frame)

ループ検出のために使用するヤマハ独自のイーサーネットフレーム。

## 機能詳細

### ループ検出 動作仕様

本製品のループ検出仕様について、以下に示します。

1. 本製品のループ検出は、システム全体の有効・無効制御に加え、LANポートごとに有効・無効制御が行えます。  
LANポートでループ検出を機能させる場合は、システム全体の設定が**有効**になっている必要があります。
  - システム全体の設定は、グローバルコンフィギュレーションモードで **loop-detect** コマンドを使用します。
  - LANポートごとの設定は、該当ポートのインターフェースモードで **loop-detect** コマンドを使用します。
2. ループ検出機能の初期設定は、以下のようになっています。
  - システム全体の設定: 有効
  - LANポート設定: 有効
3. ループ検出機能が有効となっている本製品は、以下の動作を行います。
  - ループ検出フレーム(以降、LDF)を、リンクアップしているLANポートから**2秒間隔**で送信します。  
ただし、スタティック論理インターフェース、ミラーリング設定を行ったポート(ミラーポート)は、**ループ検出機能対象外**とします。
  - 送信したLDFを自身で受信した場合、ループが発生したと判断し、以下の動作を行います。

#### ■ Port Blocking

送信したLANポートの番号が受信時のポート番号より小さい場合、LDF以外のフレームを遮断します。

LDFは定期的に送信しますが、他機器からのLDFの転送は行いません。

BlockingしたLANポートは、5秒間、自分が送信したLDFを検出しなかった場合、ループが解消したと判断し、通常の通信を再開します。

**loop-detect blocking interval** コマンドでブロッキング持続時間が指定されている場合、ループ検出時点から指定時間が経過したタイミングでループが解消されているか確認を行います。

このとき、ループが解消されていれば Blocking 状態を解除しますが、ループが解消されていなければ、再度指定時間が経過するまで Blocking 状態を継続します。

#### ■ Port Detected

送信したLANポートの番号が受信時のポート番号より大きい場合、他のポートでブロックングを行っているため、通常の通信を継続します。

- ループを検出すると、本製品のLINK/ACT LED表示を 橙色で点滅 に、STATUS LED表示を 橙色で点灯 に変更し、以下のSYSLOGメッセージを出力します。

- [LOOP]: inf: Detected Loop! : port1.1 ①

① ループ検出開始から5秒周期で表示

- ループ解消後の通信再開と合わせて、本製品のポートランプ表示を復旧し、以下のSYSLOGメッセージを出力します。

- [LOOP]: inf: Recovered Loop! : port1.1

4. ループ検出状態(Detected, Blocking)は、**loop-detect reset** コマンドにより、強制的に解消することができます。

ループ検出中のポートでリンクダウンが発生した場合も同様に、検出状態は解消されます。

5. ループ検出機能の状態は、**show loop-detect** コマンドで確認できます。以下を表示します。

- システムの有効/無効状態の表示
- ループ検出状態の表示 (LANポート単位の状態)

6. ループ検出機能が無効な状態で、LANポートでLDFを受信すると、他の全ポートから受信フレームをそのまま転送します。

ただし、スタティック論理インターフェース、ミラーリング設定を行ったポート（ミラーポート）は、転送対象外とします。

7. 以下のような場合、本製品に接続されているハブで発生しているループを検出できないことがあります。

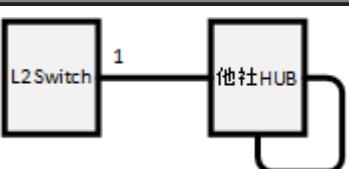
- 接続中のハブでループ検出が行われている
- 接続中のハブでループ検出フレームが転送されない

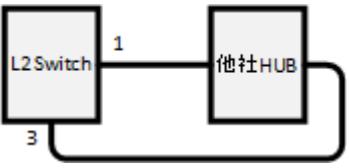
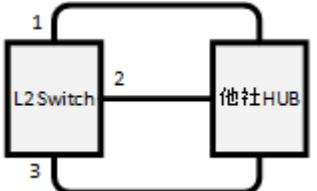
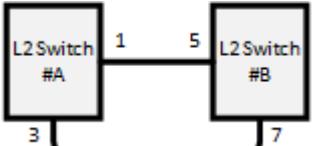
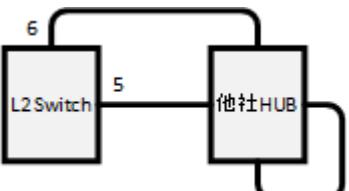
8. 異なるポートベースVLAN間、および異なるマルチプルVLAN間でループを発生させた場合、以下の動作となります。

条件	動作
異なるポートベースVLANに所属するポート間でループが発生	ブロッキングしない
異なるマルチプルVLANに所属するポート間でループが発生	ブロッキングする

### ループ検出例

以下に本製品におけるループ検出例を示します。

ループ検出ケース	構成例	ループ検出状況
1		自分が送信したLDFを受信することでループを検出します。 port1.1 : Blocking

ループ検出ケース	構成例	ループ検出状況
2		同一端末の複数ポートでループを検出した場合、大きい番号のポートをBlockingします。 port1.1 : Detected port1.3 : Blocking
3		複数のポートをBlockingすることで、ループを回避します。 Blocking Portの選択は、Case2と同じ規則となります。 port1.1 : Detected port1.2 : Blocking port1.3 : Blocking
4		複数組のループを検出した場合、各組で大きい番号のポートをBlockingします。 port1.1 : Detected, port1.2 : Blocking port1.3 : Detected, port1.4 : Blocking
5		スイッチ同士でループが起きた場合、どちらか一方でループが検出されます。 ○スイッチ#Aのport1.3で検出した場合 port1.1: Detected, port1.3: Blocking  ○スイッチ#Bのport1.7で検出した場合 port1.5: Detected, port1.7: Blocking
6		ケーブルが繋がっている6ポートのうち、ループ検出が一番早かった一つのポートをBlockingします。 ○スイッチ#Aのport1.2で検出した場合 port1.1: Detected, port1.2: Blocking  ○スイッチ#Bのport1.4で検出した場合 port1.3: Detected, port1.4: Blocking  ○スイッチ#Cのport1.6で検出した場合 port1.5: Detected, port1.6: Blocking
7		各ポートから送信したLDFが、各ポートに戻ってくるため、port1.5, port1.6ともにBlockingします。 port1.5 : Blocking port1.6 : Blocking

ループ検出ケース	構成例	ループ検出状況
8		<p>スイッチ#Bのport1.6をBlockingします。          タイミングによってはスイッチ#Aのport1.1もBlockingしますが、          スイッチ#Bのport1.6をBlockingすることで、スイッチ#Aのport1.1の          ループは解消されます。</p> <p>スイッチ#A port1.1 : Blocking          スイッチ#B port1.5 : Detected          スイッチ#B port1.6 : Blocking</p>

## 関連コマンド

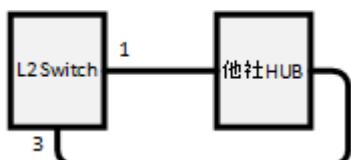
関連コマンドについて、以下に示します。  
 コマンドの詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
ループ検出機能の有効・無効設定(システム)	loop-detect enable/disable
ループ検出機能の有効・無効設定(LANポート)	loop-detect enable/disable
ループ検出によるポートブロッキングの持続時間の設定	loop-detect blocking interval
ループ検出状態のリセット	loop-detect reset
ループ検出 設定状態の参照	show loop-detect

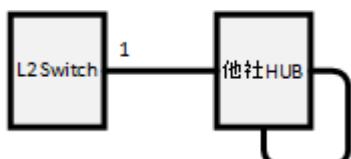
## コマンド実行例

ループ検出機能が有効になっていると、以下のような構成のとき、本製品上で発生しているループを検出します。

- [例1] 本製品内でループが発生



- [例2] 本製品に接続されている他社ハブでループが発生



LANポート #1 と #3 でループを検出するように設定します。

### ■設定手順

1. システム全体のループ検出機能を有効にします。

```
Yamaha(config)#loop-detect enable ①
```

- ① システム全体のループ検出機能を有効にする
2. LANポート #1 と #3 のループ検出機能を有効にします。

```
Yamaha(config)#interface port1.1  
Yamaha(config-if)#loop-detect enable ①  
(上記設定をLANポート #3 に対しても行います。)
```

- ① LANポートごとのループ検出機能を有効にする
- システム全体のループ検出機能を有効化、LANポートごとのループ検出機能の有効化とともに、初期値として設定されています。
3. ループ検出機能の設定を確認します。  
LANポート #1 と #3 でループ検出機能が有効(\*)になっていることが確認できます。

```
Yamaha>show loop-detect  
loop-detect: Enable  
  
port      loop-detect      status  
-----  
port1.1    enable(*)       Normal  
port1.2    enable(*)       Normal  
port1.3    enable(*)       Normal  
port1.4    enable(*)       Normal  
:          :              :
```

4. ループ検出が発生した場合、ループ検出機能の状態が確認できます。
- 例1の場合

```
Yamaha>show loop-detect  
loop-detect: Enable  
  
port      loop-detect      status  
-----  
port1.1    enable(*)       Detected ①  
port1.2    enable(*)       Normal  
port1.3    enable(*)       Blocking ②  
port1.4    enable(*)       Normal  
:          :              :
```

- ① LANポート #1 はDetected状態になる
- ② LANポート #3 はBlocking状態になる

- 例2の場合

```
Yamaha>show loop-detect  
loop-detect: Enable
```

port	loop-detect	status
port1.1	enable(*)	Blocking ①
port1.2	enable(*)	Normal
port1.3	enable(*)	Normal
port1.4	enable(*)	Normal
:	:	:

① LANポート #1 はBlocking状態になる

## 注意事項

特になし

## 関連文書

特になし

# パススルー

## 機能概要

パススルーは、通常のスイッチでは破棄されてしまう予約済み特殊MACアドレス宛てのフレームを破棄せずに転送する機能です。

本製品では、スパニングツリープロトコルで使用される BPDUフレーム および、IEEE 802.1X認証で使用される EAPフレーム のパススルーに対応しています。

BPDU パススルーを有効にすると、本製品を スパニングツリープロトコル を使用しているスイッチ間に設置することができます。

EAP パススルーを有効にすると、本製品を IEEE 802.1X 認証の認証スイッチと PC の間に設置することができます。

## 用語の定義

### BPDU (Bridge Protocol Data Unit)

スパニングツリープロトコルにおいて、ループ回避のために対応機器間のやりとりで使用されるメッセージ。

### EAP (Extended authentication protocol)

PPPを拡張して各種の認証方式を使用できるようにした認証プロトコル。RFC3748で規定されています。  
IEEE 802.1X 認証では、このプロトコルの使用をサポートしています。

## 機能詳細

### BPDU/パススルー 動作仕様

BPDU/パススルーの仕様を以下に示します。

1. BPDU/パススルーを有効にすることで、受け取ったBPDUフレームを破棄せずに転送することができます。  
BPDU/パススルーが無効の場合、受け取ったBPDUフレームは破棄され、転送されません。
2. BPDUフレームは **タグVLAN**、**ポートベースVLAN**、**マルチプルVLAN**の設定に関係なく、**受け取ったポート以外のすべてのポートに転送**されます。
3. **pass-through bpdu** コマンドまたはWeb GUIの[詳細設定]-[パススルー]より、BPDU/パススルーの有効/無効を切り替えることができます。  
初期設定では有効になっています。
4. BPDU/パススルーの設定は、システム単位（全ポート共通）の設定となります。

### EAP/パススルー 動作仕様

EAP/パススルーの仕様を以下に示します。

1. EAP/パススルーを有効にすることで、受け取ったEAPフレームを破棄せずに転送することができます。  
EAP/パススルーが無効の場合、受け取ったEAPフレームは破棄され、転送されません。
2. EAPフレームは **通常のマルチキャストフレームと同様に**、**タグVLAN**、**ポートベースVLAN**、**マルチプルVLAN**の設定に従って転送されます。
3. **pass-through eap** コマンドまたはWeb GUIの[詳細設定]-[パススルー]より、EAP/パススルーの有効/無効を切り替えることができます。  
初期設定では有効になっています。

- 
- EAP/パススルーの設定は、システム単位（全ポート共通）の設定となります。

## 関連コマンド

関連コマンドについて、以下に示します。

コマンドの詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
BPDU/パススルーの有効・無効設定	pass-through bpdu
EAP/パススルーの有効・無効設定	pass-through eap

## コマンド実行例

本製品を スパニングツリープロトコル を使用しているスイッチ間に設置するために、BPDU/パススルーを有効化する。

- BPDU/パススルーを有効にします。

```
Yamaha(config)#pass-through bpdu enable ①
```

① BPDU/パススルーを有効にする

本製品を IEEE 802.1X 認証の認証スイッチと PC の間に設置するために、EAP/パススルーを有効化する。

- EAP/パススルーを有効にします。

```
Yamaha(config)#pass-through eap enable ①
```

① EAP/パススルーを有効にする

## 注意事項

特になし

## 関連文書

特になし

# Layer 3機能

## IPv4/IPv6共通設定

### 機能概要

本製品は、主に保守（スイッチの設定操作）を行うために以下に示す **IPv4/IPv6ネットワーク共通の環境設定**に対応します。

1. DNS クライアントの設定

### 用語の定義

特になし

### 機能詳細

#### DNS クライアントの設定

本製品は、**DNS (Domain Name System)クライアント** に対応します。  
NTPサーバー、Syslogサーバーなどに **FQDN (Fully Qualified Domain Name)** が設定されている場合にDNSサーバーに問い合わせを行うことでIPv4/IPv6アドレスを取得します。

本製品は、DNSクライアントの制御機能として、以下を提供します。

- DNS サーバーのIPアドレス設定
- デフォルトドメイン名の設定
- 検索ドメインリストの設定

なお、DNS サーバーへの問い合わせは、初期状態で **有効** となっており、**dns-client enable/disable** コマンドで設定を変更することができます。

#### DNS サーバーのIPアドレス設定

DNS サーバーのIPアドレスは、以下の方法で **最大3件** まで設定することができます。

- **dns-client name-server** コマンドによる手動設定
  - IPv4/IPv6アドレスを設定することができます。
- DHCPによる自動設定

本製品では、**コマンドで設定した情報を必ず優先的に扱います。**  
設定されているDNS サーバーは、**show dns-client** コマンドで確認します。

#### デフォルトドメインの設定

デフォルトドメインは、以下の方法で **1件のみ** 設定することができます。設定可能な最大文字数は **256文字** です。

- **dns-client domain-name** コマンドによる手動設定
- DHCPによる自動設定

本製品では、DNS サーバー のIPアドレスと同様、**コマンドで設定した情報を優先的に扱います。**

設定されているデフォルトドメインは、**show dns-client** コマンドで確認します。  
なお、デフォルトドメイン名の利用は、検索ドメインリストに登録がない場合に限定されます。

### 検索ドメインリストの設定

本製品は、DNS問い合わせ時に使用するドメイン名を、検索ドメインリストで管理します。  
ドメイン名は、検索ドメインリストに以下の方法で **最大6件** まで設定することができます。

- **dns-client domain-list** コマンドによる手動設定

設定されている検索ドメインリストは、**show dns-client** コマンドで確認します。  
なお、検索ドメインリストは、**登録するすべてのドメイン名の文字数の合計を255文字以内に収める必要があります。**

## 関連コマンド

関連コマンドについて、以下に示します。  
コマンドの詳細は、コマンドリファレンスを参照してください。

機能種別	操作項目	操作コマンド
DNS クライアントの設定	DNS クライアントの設定	dns-client enable/disable
	DNS サーバーアドレスの設定	dns-client name-server
	デフォルトドメインの設定	dns-client domain-name
	検索ドメインリストの設定	dns-client domain-list
	DNSクライアント情報の表示	show dns-client

## コマンド実行例

### DNSクライアントの設定

本製品にDNSクライアントの設定をして、DNS問い合わせを行う環境を整備します。

- DNS問い合わせ先のサーバーのIPアドレスを 192.168.100.1 と 192.168.100.2 とします。
- DNS問い合わせ時に使用するデフォルトドメインを example.com とします。

#### ■設定手順

1. DNSへの問い合わせ機能を有効にします。

```
Yamaha(config)#dns-client enable
```

- 初期値として設定されているため特に設定する必要はありません。

2. DNSサーバーを設定します。

```
Yamaha(config)#dns-client name-server 192.168.100.1
Yamaha(config)#dns-client name-server 192.168.100.2
```

---

3. デフォルトドメインを設定します。

```
Yamaha(config)#dns-client domain-name example.com
```

4. 設定したDNSクライアント情報を確認します。

```
Yamaha#show dns-client

DNS client is enabled
Default domain  : example.com
Domain list    :
Name Servers   : 192.168.100.1 192.168.100.2

* - Values assigned by DHCP Client.
```

## 注意事項

特になし

## 関連文書

特になし

# IPv4基本設定

## 機能概要

本製品は、主に保守（スイッチの設定操作）を行うために以下に示す **IPv4ネットワークの環境設定** に対応します。

1. IPv4 アドレスの設定
2. ルート情報の設定
3. ARP テーブルの設定

## 用語の定義

### IPv4 リンクローカルアドレス

同一のセグメント内でのみ有効なアドレスで **169.254.0.0/16 ~ 169.254.255.255/16** の範囲のアドレス。

## 機能詳細

### IPv4アドレスの設定

本製品は、**VLANインターフェース** に対して、**IPv4アドレスとサブネットマスク** を設定することができます。

設定方法としては、**固定設定**、**DHCPによる自動設定** に対応します。

- IPv4アドレスの固定/自動設定は、**ip address** コマンドで行います。
- IPv4アドレスを設定しない状態にすることはできません。
- DHCPによる自動設定を指定した際の動作は、以下となります。
  - Discover/Requestメッセージに HostNameオプション（オプションコード12）を付加することができます。
  - DHCPサーバーに対して要求するリース期間は、**72時間固定** となっています。（実際にリースされる期間はDHCPサーバーの設定に依存します。）
  - 自動設定されている状態で **ip address** コマンドを実行し固定設定に変更すると、取得していたIPv4アドレスの解放メッセージをDHCPサーバーに送ります。
  - DHCPサーバーより取得した情報は、**show dhcp lease** コマンドで確認します。
- IPv4アドレスは**1つのVLANインターフェースにのみ** 設定することができます。  
IPv4アドレスが設定された状態で別のVLANインターフェースにIPv4アドレスを設定すると、古いほうのVLANのIPv4アドレスは削除されます。  
VLANインターフェースに割り振られているIPv4アドレスは、**show ip interface** コマンドで確認します。
- 初期状態では、**デフォルトVLAN (VLAN #1)** に固定で **192.168.100.240/24** を設定しています。

### Auto IP機能

本製品は、IPv4アドレスの設定機能として、MACアドレスをベースにIPv4リンクローカルアドレスを自動生成する Auto IP 機能を提供します。

Auto IP機能は、DHCPサーバーからIPv4アドレスが割り当たらない場合にのみ機能します。（前提として、IPv4アドレス設定がDHCPに設定されていること。）

自動生成したIPv4リンクローカルアドレスは、ARPによりネットワーク上で重複していないか確認します。  
アドレスが重複していないことを確認できた場合に生成アドレスの使用を開始します。

---

なお、Auto IPによりIPv4リンクローカルアドレスが決定した後に、DHCPサーバーからIPv4アドレスが割り当てられた場合、IPv4リンクローカルアドレスを破棄して、DHCPサーバーからのアドレスを使用します。

- Auto IP機能は、**IPv4アドレスが設定されているVLANインターフェイスのみ有効**です。初期状態では**デフォルトVLAN (VLAN #1)**が有効となっています。

## ルート情報の設定

本製品は、Syslogメッセージの送信、NTPによる時刻合わせなどのIPv4ホストとして自発的にIPv4/パケット送信する際、ルーティングテーブルを参照します。

本製品では、以下の機能を使用して、ルーティングテーブルを操作します。

- VLANインターフェースのルート情報の設定
- デフォルトゲートウェイの設定
- ルート情報の表示

### VLANインターフェースのルート情報

本製品は、VLANインターフェースに対してIPv4アドレスを設定すると、ネットワークアドレスとVLAN IDの対応を

ルート情報として自動で設定します。

### デフォルトゲートウェイの設定

本製品は、ルーティングテーブルに設定されていないネットワークアドレスに対してIPv4/パケットを送信する先を

デフォルトゲートウェイとして設定することができます。

- デフォルトゲートウェイの設定は、**ip route** コマンドで行います。
- デフォルトゲートウェイの表示は、**show ip route** コマンドで行います。

### ルート情報の表示

- 本製品はルート情報としてFIB (Forwarding Information Base : IP転送表)を持ちます。  
FIBは、IP/パケットの転送判断時に参照するデータベースです。  
**show ip route** コマンドで、FIBを確認することができます。

## ARP テーブルの設定

本製品は、IPv4/パケットを送信する際、ARP (Address Resolution Protocol)を利用して、IPv4アドレスからMACアドレスを取得します。

IPv4アドレスとMACアドレスの対応は、以下の仕様でARPテーブルに保存されます。

- ARPテーブルで保存する**ARPエントリー**は、以下の情報を管理します。
  - IPv4アドレス
  - MACアドレス
  - VLANインターフェース
- ARPテーブルのエントリー数は、**最大512エントリー**までが動作保証範囲です。
- ARPテーブルに保存された動的エントリーは、初期状態で**300秒**保持する設定になっています。  
エントリーの保持時間の変更は、**arp-ageing-timeout** コマンドで行います。
- ARPテーブルに保存された動的エントリーは、保持時間に関係なく**clear arp-cache** コマンドでクリア

することができます。

- ARP テーブルの確認は、**show arp** コマンドで行います。

## 関連コマンド

関連コマンドについて、以下に示します。

コマンドの詳細は、コマンドリファレンスを参照してください。

機能種別	操作項目	操作コマンド
IPv4 アドレスの設定	IPv4アドレスの設定	ip address
	IPv4アドレスの表示	show ip interface
	DHCPクライアントによる動的IPv4アドレスの設定	ip address dhcp
	DHCPクライアントの状態の表示	show dhcp lease
ルート情報の設定	デフォルトゲートウェイの設定	ip route
	デフォルトゲートウェイの表示	show ip route
ARP テーブルの設定	ARP テーブルの表示	show arp
	動的エントリーの保持時間の設定	arp-ageing-timeout
	動的エントリーのクリア	clear arp-cache

## コマンド実行例

### IPv4ネットワーク環境の設定 (DHCP)

本製品にIPv4アドレスを設定して、リモート端末からアクセスを行う環境を整備します。

- IPv4アドレスは、デフォルトVLAN (VLAN #1) に対して DHCP にて自動で設定します。

- 現在設定されているIPv4アドレスを確認します。  
初期状態のままであれば、固定IPv4アドレス (192.168.100.240/24) が設定されています。

```
Yamaha#show ip interface brief
Interface          IP-Address           Status        Protocol
vlan1              192.168.100.240/24    up            up
```

- デフォルトVLAN (VLAN #1) に対して DHCP を設定します。

※IPアドレスの変更により、本製品へのアクセスができなくなる可能性があります。変更の際は十分にご注意ください。

```
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ip address dhcp
Do you really want to change IP address? [y/N]:y
```

- DHCPサーバーから払い出されたIPアドレスにTELNETでアクセスし、ログインします。

```
Username:*****
Password:*****  
  
SWX2210P-10G Rev.1.03.03 (Thu Jan 16 13:20:45 2020)  
Copyright (c) 2018-2020 Yamaha Corporation. All Rights Reserved.  
  
Yamaha>enable  
Password:*****  
Yamaha#
```

4. ログイン後、DHCPサーバーより払い出された情報を確認します。

```
Yamaha#show dhcp lease  
Interface    vlan1  
-----  
IP Address:          192.168.1.9  
Expires:            2019/10/13 18:47:32  
Renew:              2019/10/12 18:47:32  
Rebind:             2019/10/13 12:47:33  
Server:  
Options:  
    subnet-mask        255.255.255.0  
    default-gateway    192.168.1.1  
    dhcp-lease-time    172800  
    domain-name-servers 192.168.1.1  
    dhcp-server-identifier 192.168.1.1  
    domain-name        domain.test
```

## 注意事項

IPv4アドレスの設定を変更すると、リモートアクセス制御に関する以下のコマンドがすべて削除されます。  
IPv4アドレス変更の際は十分にご注意ください。

- telnet-server access
- http-server access
- tftp-server access
- snmp-server access

## 関連文書

- [L2スイッチング機能 : VLAN](#)
- [リモートアクセス機能 : リモートアクセス制御](#)
- [Yamaha RTpro: ARPって何？](#)

# IPv6基本設定

## 機能概要

本製品は、主に保守（スイッチの設定操作）を行うために以下に示す **IPv6ネットワークの環境設定** に対応します。

1. IPv6 アドレスの設定
2. ルート情報の設定
3. Neighbor キャッシュテーブルの設定

## 用語の定義

### RA (Router Advertisement : ルータ広告)

IPv6ネットワークで、ルータが所属するネットワークの機器に対して、アドレス情報やネットワーク設定などを自動設定する仕組み。

### IPv6 アドレス

IPv6アドレスは、128ビットを16進数で表記します。以下のように、16bitごとに「:」で8つのフィールドに区切れます。

- 2001:02f8:0000:0000:1111:2222:0000:4444

以下のルールで表記の省略が可能です。

- 各フィールドの先頭が0の場合、0を省略可
- 0が4個のフィールドは0の記述を1個に省略可
- 0のみが連続する複数のフィールドは **全体で1箇所だけ** 「::」で省略可

上記のアドレスにこのルールを当てはめると以下のようになります。

- 2001:2f8::1111:2222:0:4444

### IPv6 リンクローカルアドレス

同一のセグメント内でのみ有効なアドレスで、以下の範囲のアドレス。

- [開始] FE80:0000:0000:0000:0000:0000:0000:0000
- [終了] FE80:0000:0000:0000:FFFF:FFFF:FFFF:FFFF

## 機能詳細

### IPv6アドレスの設定

本製品は、**VLANインターフェース** に対して、**IPv6アドレスとプレフィックス長** を設定することができます。

設定方法としては、**固定設定**、**RA (ルータ広告)による自動設定** に対応します。

- IPv6アドレスを設定するには、該当VLANインターフェイスで、IPv6機能を有効にする必要があります。
  - IPv6機能の設定は、**ipv6 enable** コマンドで行います。

- IPv6機能を有効にすると、IPv6リンクローカルアドレスが自動的に割り当てられます。
- IPv6アドレスの固定/自動設定は、**ipv6 address** コマンドで行います。
- IPv6アドレスは**1つのVLANインターフェースにのみグローバルアドレスとリンクローカルアドレスを1つずつ** 設定することができます。  
IPv6アドレスが設定された状態で別のVLANインターフェースにIPv6アドレスを設定すると、古いほうのVLANのIPv6アドレスは削除されます。  
1つのVLANインターフェースに設定できるIPv6アドレスは、**固定設定または自動設定のどちらか** となります。  
VLANインターフェースに割り振られているIPv6アドレスは、**show ipv6 interface** コマンドで確認します。

## ルート情報の設定

本製品は、Syslogメッセージの送信、NTPによる時刻合わせなどのIPv6ホストとして自発的にIPv6パケット送信する際、ルーティングテーブルを参照します。

本製品では、以下の機能を使用して、ルーティングテーブルを操作します。

- VLANインターフェースのルート情報の設定
- デフォルトゲートウェイの設定
- ルート情報の表示

### VLANインターフェースのルート情報

本製品は、VLANインターフェースに対してIPv6アドレスを設定すると、ネットワークアドレスとVLAN ID の対応をルート情報として自動で設定します。

VLANインターフェースに対して設定したIPv6アドレスを解放すると、上記設定を削除します。

### デフォルトゲートウェイの設定

本製品は、ルーティングテーブルに設定されていないネットワークアドレスに対してIPv6パケットを送信する先をデフォルトゲートウェイとして設定することができます。

- デフォルトゲートウェイの設定は、**ipv6 route** コマンドで行います。
- デフォルトゲートウェイの表示は、**show ipv6 route** コマンドで行います。

### ルート情報の表示

- 本製品はルート情報としてFIB (Forwarding Information Base : IP転送表)を持ちます。  
FIBは、IPパケットの転送判断時に参照するデータベースです。  
**show ipv6 route** コマンドで、FIBを確認することができます。

## Neighbor キャッシュテーブルの設定

本製品は、IPv6パケットを送信する際、Neighbor Discovery (近隣検索)プロトコルを利用して、IPv6アドレスからMACアドレスを取得します。

IPv6アドレスとMACアドレスの対応は、以下の仕様でNeighbor キャッシュテーブルに保存されます。

- Neighbor キャッシュテーブルで保存する **Neighbor キャッシュエントリー** は、以下の情報を管理します。
  - IPv6アドレス
  - MACアドレス

## ◦ VLAN インターフェース

- Neighbor キャッシュテーブルには、**最大10エントリー** 保存されます。  
エントリーが最大に達した状態で新たなNeighborが見つかった場合、一番古いNeighborが削除され、新しいNeighborが登録されます。
- Neighbor キャッシュテーブルに保存された動的エントリーは、**clear ipv6 neighbors** コマンドでクリアすることができます。
- Neighbor キャッシュテーブルの確認は、**show ipv6 neighbor** コマンドで行います。

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

機能種別	操作項目	操作コマンド
IPv6 アドレスの設定	IPv6アドレスの有効／無効設定	ipv6 enable/disable
	IPv6アドレスの設定	ipv6 address
	IPv6アドレスの表示	show ipv6 interface
	IPv6アドレスのRA設定	ipv6 address autoconfig
ルート情報の設定	デフォルトゲートウェイの設定	ipv6 route
	デフォルトゲートウェイの表示	show ipv6 route
	ルート情報の表示	show ipv6 route
Neighbor キャッシュの設定	Neighbor キャッシュテーブルの表示	show ipv6 neighbors
	Neighbor キャッシュテーブルの消去	clear ipv6 neighbors

## コマンド実行例

### IPv6ネットワーク環境の設定 (固定設定)

本製品にIPv6アドレスを手動設定して、リモート端末からアクセスを行う環境を整備します。

- IPv6アドレスは、デフォルトVLAN (VLAN #1) に対して手動で設定します。

1. デフォルトVLAN (VLAN #1) に対して 2001:db8:1::2/64 を設定します。

```
Yamaha#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Yamaha(config)#interface vlan1  
Yamaha(config-if)#ipv6 enable ①  
Yamaha(config-if)#ipv6 address 2001:db8:1::2/64 ②
```

① IPv6を有効にする

② IPv6アドレスを設定する

2. 設定したIPv6アドレス情報を確認します。

```

Yamaha(config-if)#end
Yamaha#show ipv6 interface brief
Interface      IP-Address           Status
Protocol
vlan1          2001:db8:1::2/64      up
                  fe80::2a0:deff:fe:2/64

```

### IPv6ネットワーク環境の設定 (RAによる自動設定)

本製品にIPv6アドレスを自動設定して、リモート端末からアクセスを行う環境を整備します。

- IPv6アドレスは、デフォルトVLAN (VLAN #1) に対して RA にて自動で設定します。

  - デフォルトVLAN (VLAN #1) に対して RA を設定します。

```

Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#interface vlan1
Yamaha(config-if)#ipv6 enable ①
Yamaha(config-if)#ipv6 address autoconfig ②

```

① IPv6を有効にする

② RAを設定する

- RA により取得したIPv6アドレス情報を確認します。

```

Yamaha(config-if)#end
Yamaha#show ipv6 interface brief
Interface      IP-Address           Status
Protocol
vlan1          2001:db8::2a0:deff:fe:2/64      up
                  fe80::2a0:deff:fe:2/64

```

### 注意事項

IPv6アドレスの設定を変更すると、リモートアクセス制御に関する以下のコマンドがすべて削除されます。IPv6アドレス変更の際は十分にご注意ください。

- telnet-server access
- http-server access
- tftp-server access
- snmp-server access

### 関連文書

- [L2スイッチング機能 : VLAN](#)
- [リモートアクセス機能 : リモートアクセス制御](#)

# IPマルチキャスト機能

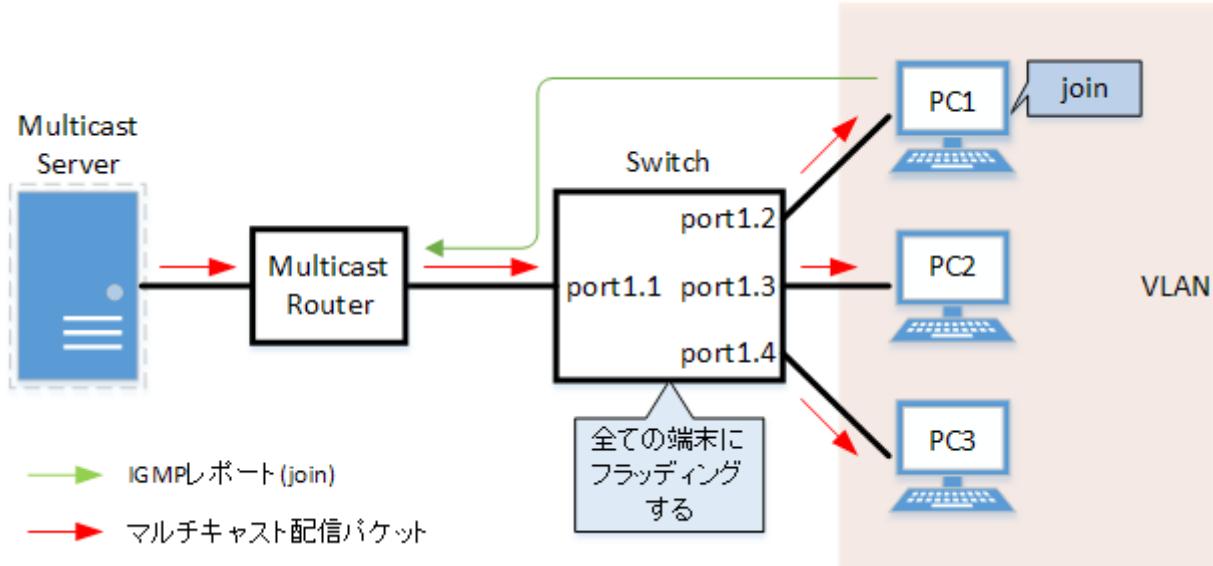
## IGMP Snooping

### 機能概要

IGMP Snoopingは、VLAN環境において余分なマルチキャストのフラッディングを制御することで、ネットワークの帯域幅の消費を抑える機能です。

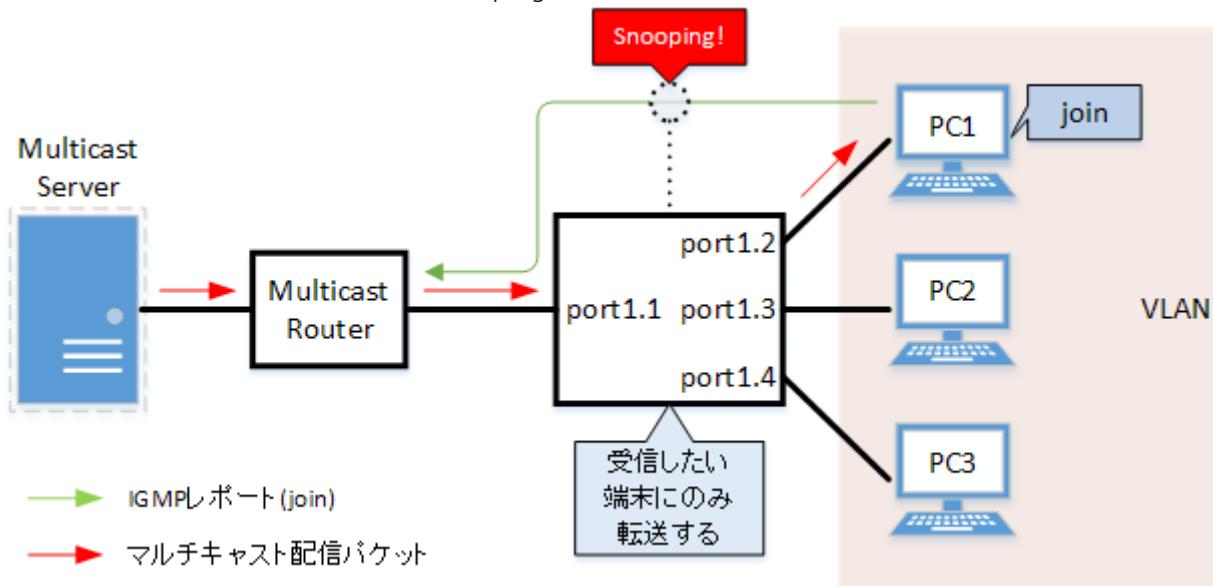
L2スイッチでは、マルチキャストパケットはVLAN単位で配信されるため、VLAN内に1つでもマルチキャストパケットを受信したい端末が存在すると、同一VLAN内のすべてのポートにパケットが配信されてしまいます。

- マルチキャスト配信時の動作(IGMP Snoopingなし)



IGMP Snooping機能を使用すると、受信端末とマルチキャストルーター間で交換されるIGMPメッセージを監視(Snooping)することで、マルチキャストパケットを受信したい端末が接続されたポートのみに該当グループのパケットを配信することができます。

- マルチキャスト配信時の動作(IGMP Snoopingあり)



## 用語の定義

### IGMP (Internet Group Management Protocol)

マルチキャストグループを制御するためのプロトコル。

マルチキャストルーターはLAN上のどのホストがマルチキャストグループのメンバーであるか判断でき、ホストは自分がどのマルチキャストグループのメンバーかを伝えることができます。

3つのバージョンがあり、 [IGMPv1 \(RFC1112\)](#)、 [IGMPv2 \(RFC2236\)](#)、 [IGMPv3 \(RFC3376\)](#) で規定されます。

### マルチキャストルーターポート

マルチキャストルーターが接続されているLAN/SFPポートのこと。

IGMPジェネラルクエリーを受信したLAN/SFPポートをマルチキャストルーターポートとして自動で学習します。

### IGMPレポート抑制機能

マルチキャストルーターとホスト間で行われる通信負荷をスイッチで抑制する機能。

抑制するために本製品がまとめるメッセージは、以下となります。

- ・マルチキャストルーターから送られる IGMPジェネラルクエリー に対してホストが応答するIGMPレポート
- ・ホストから通知されるIGMP leaveメッセージ

レポート抑制機能は、IGMPv1/v2/v3に対して動作します。

### Fast Leave (高速脱退) 機能

IGMPv2/v3 離脱メッセージを受信したLAN/SFPポートを即座にマルチキャスト受信ポートから外す(転送に必要なFDBエントリーを削除する)機能。

本来、IGMPv2/v3の離脱処理では、離脱メッセージを受信した際、そのポートにグループスペシフィッククエリーを送信し、レシーバーの存在確認が行われますが、高速脱退機能が **有効** な場合、本動作を行いません。

このため、高速脱退機能は **LAN/SFPポート配下に1つのレシーバーが接続されている場合にのみ効果的な機能** です。

なお、高速脱退機能はIGMPv2のLeaveメッセージおよびIGMPv3の離脱メッセージ受信時のみ動作します。

高速脱退機能が **有効** かつ **auto-assignment** オプションが指定されている場合、LAN/SFPポート配下にスイッチが接続されているポートでは、離脱メッセージを受信した際のレシーバーの存在確認を行います。

**auto-assignment** オプションを使用することで、スイッチをカスケード接続する構成でも高速脱退機能を使用することができます。

### IGMP クエリー送信機能 (IGMP Querier)

IGMP ジェネラルクエリー、スペシフィッククエリーを送信する機能。

マルチキャストルーターがいない環境でIGMP Snoopingを機能させる場合に使用します。

### マルチキャストルーターポートへのデータ転送抑制機能

マルチキャストルーターポートへ転送するマルチキャストデータを抑制する機能。

本来、マルチキャストルーターポートには、本製品が学習済みであるすべてのマルチキャストグループのデータが転送されますが、本機能が **有効** な場合、マルチキャストルーターポートでIGMPレポートを受信して学習済みとなったマルチキャストグループのデータのみ転送します。

スイッチ間に不要なマルチキャストデータが流れることで帯域が逼迫する場合は、本機能を **有効** にし、 **I2-unknown-mcast discard** コマンドと併用することで軽減できます。

## IGMPレポート転送機能

IGMP Join/Leaveメッセージを、LAN/SFPポート配下にスイッチが接続されているポートに転送する機能。本機能を有効にすることで、スイッチがカスケード接続されている構成において、非クエリラーのスイッチに対してIGMP Join/Leaveメッセージが転送されるようになります。  
複数のマルチキャストデータが流れる環境で **マルチキャストルーターポートへのデータ転送抑制機能** を使用する場合、本機能を **有効** にすることを推奨します。

## **機能詳細**

IGMP Snoopingの動作仕様について以下に示します。

1. 本製品は、**IGMP v1/v2/v3** に対応したSnooping機能を提供します。  
本製品で機能させる上位バージョンを **ip igmp snooping version** コマンドで設定できます。  
バージョン設定は **VLANインターフェース** に対して行い、初期設定は **v3** となっています。  
設定バージョンと受信フレームのバージョンの違いによる動作は以下となります。
  - 設定したバージョンよりも上位バージョンのIGMPクエリーを受信した場合、設定バージョンに下げてクエリーを転送します。
  - 設定したバージョンよりも上位バージョンのIGMPレポートを受信した場合、該当レポートを転送せずに破棄します。
  - 設定したバージョンよりも下位バージョンのIGMPクエリーおよびレポートを受信した場合、受信したバージョンのまま転送します。
2. IGMP Snoopingの**有効 / 無効** 設定は、**VLANインターフェース** に対して行います。  
初期値は**無効**です。
3. IGMP Snoopingの機能として、以下の6つに対応します。
  - マルチキャストルーターポートの設定
  - IGMPレポート抑制
  - Fast-leave(高速脱退)
  - IGMPクエリー送信
  - マルチキャストルーターポートへのデータ転送抑制
  - IGMPレポート転送
4. IGMP Snoopingが**有効**に設定されているVLANインターフェースでは、**マルチキャストルーターポートを自動で学習**しますが、**ip igmp snooping mrouter interface** コマンドで静的に設定することもできます。  
なお、VLANインターフェースに設定されているマルチキャストルーターポートは、**show ip igmp snooping mrouter** コマンドで確認します。
5. **IGMPレポート抑制機能**は、VLANインターフェースに対して **ip igmp snooping report-suppression** コマンドで設定します。  
初期値は**有効**です。  
レポート抑制機能により、IGMPレポート、IGMP leaveメッセージを送信する場合、送信元IPv4アドレスには、VLANインターフェースに割り振られているIPv4アドレスを使用します。  
(割り振られていない場合は、0.0.0.0を設定して送信します。)
6. **Fast-Leave(高速脱退)機能**は、VLANインターフェースに対して **ip igmp snooping fast-leave** コマンドで設定します。  
初期値は**無効**です。  
高速脱退機能が**有効**かつ**auto-assignment**オプションが指定されている場合、LAN/SFPポート配下にスイッチが接続されている場合に、そのポートでは自動的に高速脱退機能が**無効**になります。  
LAN/SFPポート配下にスイッチが接続されているか否かの判定には、当該ポートで受信したLLDPフレー

ムの基本管理TLV「System Capabilities」に「Bridge」が含まれているか否かで判定します。そのため、**auto-assignment** オプションを使用する際は、本製品と対向スイッチの両方でLLDPの送受信を有効にしてください。なお、本製品でLLDPを有効にした場合、基本管理TLVは常に送信されます。

7. マルチキャストルーターが存在しない環境でIGMP Snoopingを使用するために、**IGMP クエリー送信機能**に対応します。

IGMP クエリー送信機能は、以下の2つのパラメータで制御します。

- IGMP クエリー送信機能の 有効 / 無効
  - VLANインターフェースに対して、**ip igmp snooping querier** コマンドで行います。
  - 初期値は **無効** です。
- IGMP クエリーの送信間隔
  - **ip igmp snooping query-interval** コマンドで行います。
  - 送信間隔は、20 ~ 18,000秒 の範囲で設定可能とし、初期値は **125秒** となっています。

8. VLAN内に複数の機器がクエリーを送信する場合、VLAN内で最も小さいIPv4アドレスを持つ機器がクエリー送信を行います。

本製品は、自身のIPv4アドレスより小さなIPv4アドレスを持つ機器からのクエリーを受信した場合、クエリー送信機能を停止します。

なお、クエリー送信時に設定する送信元IPv4アドレスは、VLANインターフェースに割り振られているIPv4アドレスを使用しますが、割り振られていない場合は、他のVLANインターフェースに割り振られているIPv4アドレスを使用します。

9. 本製品では、受信したIGMP/パケットのTTL値が不正（1以外）だった場合、破棄をしないで強制的に"1"に変更する機能を提供します。

本機能を "**TTLチェック機能**" と定義し、VLANインターフェースに対して **ip igmp snooping check ttl** コマンドで設定を行うことができます。

**TTLチェック機能** の初期値は **有効(TTL不正値のパケットを破棄)** です。

10. 本製品では、受信したIGMPv2/IGMPv3/パケットにRA（Router Alert）オプションが含まれていない場合、破棄をしないでIPヘッダーにRAオプションを付与して転送する機能を提供します。

本機能を "**RAチェック機能**" と定義し、VLANインターフェースに対して **ip igmp snooping check ra** コマンドで設定を行うことができます。

**RAチェック機能** の初期値は **無効(RAオプションが含まれないパケットを転送)** です。

11. 本製品では、受信したIGMPv3/パケットのToS（Type of field）値が不正（0xc0以外）だった場合、破棄をしないで強制的に"0xc0"に変更する機能を提供します。

本機能を "**ToSチェック機能**" と定義し、VLANインターフェースに対して **ip igmp snooping check tos** コマンドで設定を行うことができます。

**ToSチェック機能** の初期値は **無効(ToS不正値のパケットを転送)** です。

12. **マルチキャストルーターポートへのデータ転送抑制機能** は、VLANインターフェースに対して **ip igmp snooping mrouter-port data-suppression** コマンドで設定します。

初期値は **無効** です。

13. **IGMPレポートの転送機能** は、VLANインターフェースに対して **ip igmp snooping report-forward** コマンドで設定します。

初期値は **無効** です。

本機能が **有効** のとき、LAN/SFPポート配下にスイッチが接続されている場合に、そのポートに対してIGMP Join/Leaveメッセージを転送します。

LAN/SFPポート配下にスイッチが接続されているか否かの判定には、当該ポートで受信したLLDPフレームの基本管理TLV「System Capabilities」に「Bridge」が含まれているか否かで判定します。

そのため、本機能を使用する際は、本製品と対向スイッチの両方でLLDPの送受信も有効にしてください。なお、本製品でLLDPを有効にした場合、基本管理TLVは常に送信されます。

## 関連コマンド

関連コマンドについて、以下に示します。

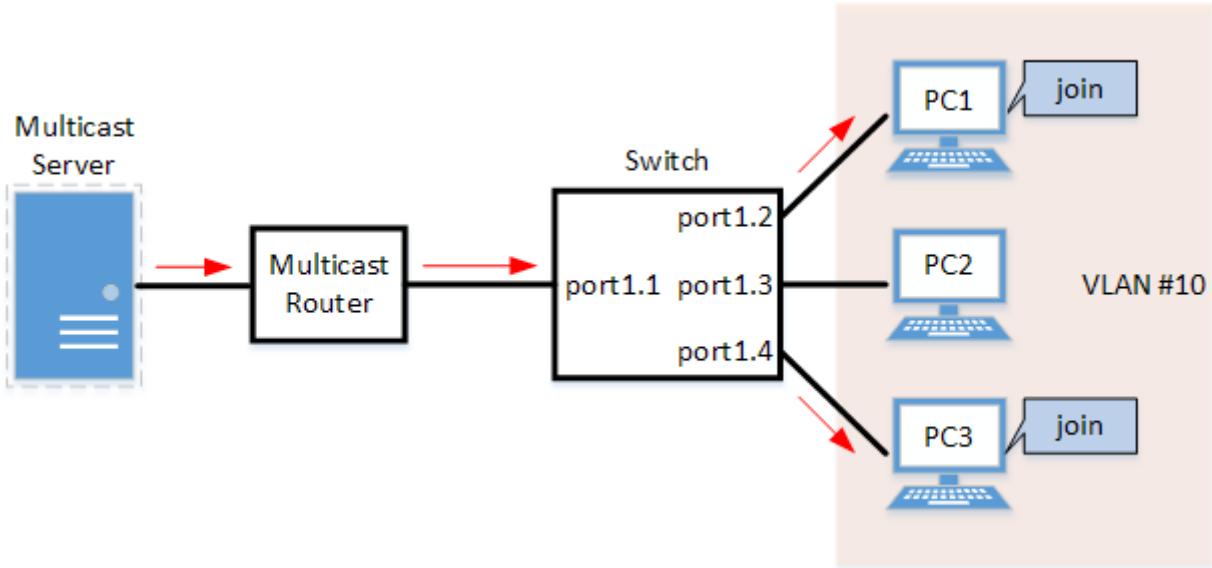
コマンドの詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
IGMPスヌーピングの有効／無効設定	ip igmp snooping
IGMPスヌーピング高速脱退の設定	ip igmp snooping fast-leave
マルチキャストルーターポートの設定	ip igmp snooping mrouter interface
クエリー送信機能の設定	ip igmp snooping querier
IGMPクエリー送信間隔の設定	ip igmp snooping query-interval
IGMPスヌーピングTTLチェックの設定	ip igmp snooping check ttl
IGMPスヌーピングRAチェックの設定	ip igmp snooping check ra
IGMPスヌーピングToSチェックの設定	ip igmp snooping check tos
IGMPバージョンの設定	ip igmp snooping version
IGMPレポート抑制機能の設定	ip igmp snooping report-suppression
マルチキャストルーターポートへのデータ転送抑制機能の設定	ip igmp snooping mrouter-port data-suppression
IGMPレポート転送機能の設定	ip igmp snooping report-forward
システムにおける未知のマルチキャストフレームの処理方法の設定	I2-unknown-mcast
システムにおけるリンクローカルマルチキャストアドレスの転送設定	I2-unknown-mcast forward link-local
VLANインターフェースにおける未知のマルチキャストフレームの処理方法の設定	I2-unknown-mcast
VLANインターフェースにおけるマルチキャストフレームの転送設定	I2-mcast flood
マルチキャストルーターポートの情報の表示	show ip igmp snooping mrouter
IGMPマルチキャスト受信者の情報を表示	show ip igmp snooping groups
インターフェースのIGMP関連情報を表示	show ip igmp snooping interface
IGMPグループメンバーシップのエンタリー削除	clear ip igmp snooping

## コマンド実行例

### IGMP Snooping の設定(マルチキャストルーターあり)

マルチキャストルーターがある環境でIGMP Snooping機能を有効にして、マルチキャストグループに参加しているPC1、PC3にのみデータが配信されるようにします。



- ・ LANポート #1 ~ #4 は、 アクセスポートに設定し、VLAN #10 に所属させます。
- ・ マルチキャストルーターがあるため、IGMP クエリー送信機能は無効のままでします。
- ・ マルチキャストルーターポートの学習は、自動学習のみとします。(静的な設定は行わない。)
- ・ Fast-Leave(高速脱退)機能を有効にします。

1. VLAN #10 を定義して、IGMP Snoopingの設定を行います。

```

Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#no ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping fast-leave ④

```

① VLAN #10 の定義

② VLAN #10 のIGMP Snoopingを有効にする

③ VLAN #10 のIGMP クエリー送信機能を無効にする

④ VLAN #10 のIGMP Fast-leave機能を有効にする

　　◦ IGMP クエリー送信機能の無効化は、初期値として設定されているため特に設定する必要はありません。

2. LANポート #1 ~ #4 を アクセスポートに設定し、VLAN #10 に所属させます。

```

Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①

```

① 上記設定をLANポート #2 ~ #4に対しても行います。

3. マルチキャストルーターポートの情報を確認します。(LANポート #1 につながっている)

```

Yamaha#show ip igmp snooping mrouter vlan10
VLAN      Interface          IP-address      Expires
10        port1.1(dynamic)    192.168.100.216  00:00:49

```

4. マルチキャスト受信者の情報を確認します。

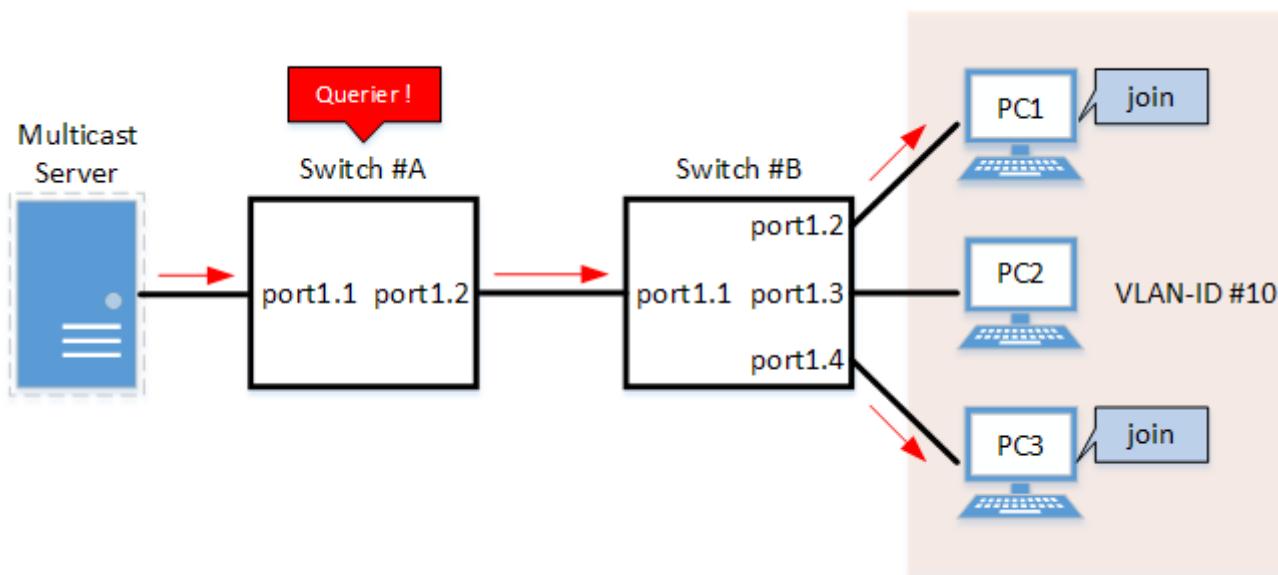
```

Yamaha#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan  Group/Source Address   Interface   Flags  Uptime   Expires  Last Reporter
Version
10    239.0.0.1             port1.2     R      00:00:13  00:00:41  192.168.100.2
V3
10    239.0.0.1             port1.4     R      00:00:02  00:00:48  192.168.100.4
V3

```

### IGMP Snooping の設定(マルチキャストルーターなし)

マルチキャストルーターがない環境でIGMP Snooping機能を有効にして、マルチキャストグループに参加しているPC1、PC3にのみデータが配信されるようにします。



- スイッチ#A
  - LANポート #1 ~ #2 は、**アクセスポート**に設定し、**VLAN #10** に**所属**させます。
  - **IGMP クエリー送信機能を 有効** にします。  
IGMPクエリーの送信間隔を **20秒** とします。
- スイッチ#B
  - LANポート #1 ~ #4 は、**アクセスポート**に設定し、**VLAN #10** に**所属**させます。
  - **マルチキャストルーターポート** の学習は、**自動学習** のみとします。(静的な設定は行わない。)
  - **Fast-Leave(高速脱退)機能を有効** にします。
  - IGMPパケットに不正なTTL値を設定する端末があるため、**TTLチェック機能を無効** にします。

1. [スイッチ#A] VLAN #10 を定義して、IGMP Snoopingの設定を行います。

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping query-interval 20 ④
```

- ① VLAN #10 の定義
- ② VLAN #10 のIGMP Snoopingを有効にする
- ③ VLAN #10 のIGMP クエリー送信機能を有効にする
- ④ VLAN #10 のIGMP クエリーの送信間隔を20秒にする

2. [スイッチ#A] LANポート #1 ~ #2 を アクセスポートに設定し、VLAN #10 に所属させます。

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

- ① 上記設定をLANポート #2に対しても行います。

3. [スイッチ#B] VLAN #10 を定義して、IGMP Snoopingの設定を行います。

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#no ip igmp snooping querier ③
Yamaha(config-if)#no ip igmp snooping check ttl ④
Yamaha(config-if)#ip igmp snooping fast-leave ⑤
```

- ① VLAN #10 の定義
- ② VLAN #10 のIGMP Snoopingを有効にする
- ③ VLAN #10 のIGMP クエリー送信機能を無効にする
- ④ VLAN #10 のTTLチェック機能を無効にする
- ⑤ VLAN #10 のIGMP Fast-leave機能を有効にする
  - IGMP クエリー送信機能の無効化は、初期値として設定されているため特に設定する必要はありません。

4. [スイッチ#B] LANポート #1 ~ #4 を アクセスポートに設定し、VLAN #10 に所属させます。

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

- ① 上記設定をLANポート #2 ~ #4に対しても行います。

5. [スイッチ#B] マルチキャストルーターポートの情報を確認します。(LANポート #1 につながっている)

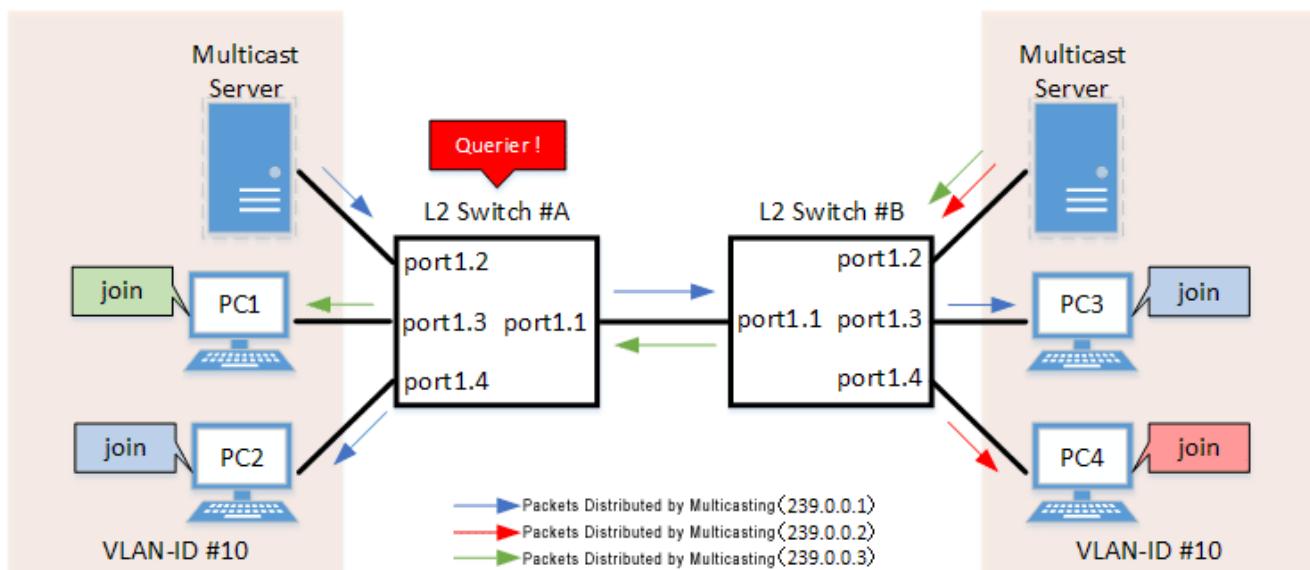
```
Yamaha#show ip igmp snooping mrouter vlan10
VLAN      Interface          IP-address   Expires
10        port1.1(dynamic)    192.168.100.216 00:00:49
```

6. [スイッチ#B] マルチキャスト受信者の情報を確認します。

```
Yamaha#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan  Group/Source Address  Interface  Flags  Uptime  Expires  Last Reporter
Version
10    239.0.0.1            port1.2    R      00:00:13  00:00:41  192.168.100.2
V3
10    239.0.0.1            port1.4    R      00:00:02  00:00:48  192.168.100.4
V3
```

#### IGMP Snooping の設定(双方向でデータ配信する場合)

スイッチを 2 つ使用した構成で、どちらのスイッチにもマルチキャストサーバーと PC が接続されています。各 PC は参加するマルチキャストグループを頻繁に切り替えますが、途切れる時間ができるだけ短くなるようにします。



- スイッチ#A
  - LANポート #1 ~ #4 は、**アクセスポート**に設定し、**VLAN #10** に**所属** させます。
  - **IGMP クエリー送信機能を 有効** にします。  
IGMPクエリーの送信間隔を **20秒** とします。
  - **Fast-Leave(高速脱退)機能を有効** にし、対向スイッチ配下に複数のマルチキャスト受信者が接続されている場合に存在確認を行うため、**LLDPの送受信を有効かつauto-assignmentオプションを有効** にします。
  - **IGMPレポート抑制機能を無効** にします。
  - マルチキャストサーバーやデータ配信の数が増えた場合にポートの帯域が逼迫する可能性がある

ので、最低限のものだけ転送するように **マルチキャストルーターポートへのデータ転送抑制機能を有効** にします。

また、**未知のマルチキャストフレームを破棄** するようにします。

- 非エンドスイッチへIGMPレポートを転送するため、**LLDPの送受信を有効かつIGMPレポート転送機能を有効** にします。

- スイッチ#B

- LANポート #1～#4は、**アクセスポートに設定し、VLAN #10に所属**させます。
- **マルチキャストルーターポート** の学習は、**自動学習**のみとします。(静的な設定は行わない。)
- **Fast-Leave(高速脱退)機能を有効**にし、対向スイッチ配下に複数のマルチキャスト受信者が接続されている場合に存在確認を行うため、**LLDPの送受信を有効かつauto-assignmentオプションを有効**にします。
- **IGMPレポート抑制機能を無効**にします。
- マルチキャストサーバーやデータ配信の数が増えた場合にポートの帯域が逼迫する可能性があるので、最低限のものだけ転送するように **マルチキャストルーターポートへのデータ転送抑制機能]]を有効**にします。

また、**未知のマルチキャストフレームを破棄**するようにします。

1. [スイッチ#A] VLAN #10を定義して、IGMP Snoopingの設定を行います。

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping query-interval 20 ④
Yamaha(config-if)#ip igmp snooping fast-leave auto-assignment ⑤
Yamaha(config-if)#ip igmp snooping report-suppression disable ⑥
Yamaha(config-if)#ip igmp snooping mrouter-port data-suppression enable ⑦
Yamaha(config-if)#ip igmp snooping report-forward enable ⑧
```

① VLAN #10の定義

② VLAN #10のIGMP Snoopingを有効にする

③ VLAN #10のIGMP クエリー送信機能を有効にする

④ VLAN #10のIGMP クエリーの送信間隔を20秒にする

⑤ VLAN #10のFast-Leave機能とauto-assignmentオプションを有効にする

⑥ VLAN #10のレポート抑制機能を無効にする

⑦ VLAN #10のマルチキャストルーターポートへのデータ転送抑制機能を有効にする

⑧ VLAN #10のレポート転送機能を有効にする

2. [スイッチ#A] LANポート #1～#4を アクセスポートに設定し、VLAN #10に所属させます。

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

- 
- ① 上記設定をLANポート #2～#4に対しても行います。
3. [スイッチ#A] 未知のマルチキャストフレームを破棄するようにします。

```
Yamaha(config)#l2-unknown-mcast discard
```

4. [スイッチ#A] LANポート #1でLLDPの送受信を有効にします。

```
Yamaha(config)# lldp run
Yamaha(config)# interface port1.1
Yamaha(config-if)# lldp-agent
Yamaha(lldp-agent)# set lldp enable txrx
```

5. [スイッチ#B] VLAN #10 を定義して、IGMP Snoopingの設定を行います。

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ip igmp snooping enable ②
Yamaha(config-if)#no ip igmp snooping querier ③
Yamaha(config-if)#ip igmp snooping fast-leave ④
Yamaha(config-if)#ip igmp snooping report-suppression disable ⑤
Yamaha(config-if)#ip igmp snooping mrouter-port data-suppression enable ⑥
Yamaha(config-if)#ip igmp snooping report-forward enable ⑦
```

- ① VLAN #10 の定義
- ② VLAN #10 のIGMP Snoopingを有効にする
- ③ VLAN #10 のIGMP クエリー送信機能を無効にする
- ④ VLAN #10 のFast-Leave機能とauto-assignmentオプションを有効にする
- ⑤ VLAN #10 のレポート抑制機能を無効にする
- ⑥ VLAN #10 のマルチキャストルーターポートへのデータ転送抑制機能を有効にする
- ⑦ VLAN #10 のレポート転送機能を有効にする
- IGMP クエリー送信機能の無効化は、初期値として設定されているため特に設定する必要はありません。

6. [スイッチ#B] LANポート #1～#4 をアクセスポートに設定し、VLAN #10 に所属させます。

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

- ① 上記設定をLANポート #2～#4に対しても行います。
7. [スイッチ#B] 未知のマルチキャストフレームを破棄するようにします。

```
Yamaha(config)#l2-unknown-mcast discard
```

8. [スイッチ#B] LANポート #1でLLDPの送受信を有効にします。

```
Yamaha(config)# lldp run
Yamaha(config)# interface port1.1
Yamaha(config-if)# lldp-agent
Yamaha(lldp-agent)# set lldp enable txrx
```

9. [スイッチ#A] マルチキャスト受信者の情報を確認します。

```
Yamaha#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan  Group/Source Address  Interface   Flags  Uptime   Expires  Last Reporter
Version
10    239.0.0.1           port1.1     R       00:00:02  00:00:48 192.168.100.3
V3
10    239.0.0.2           port1.1     R       00:00:02  00:00:48 192.168.100.4
V3
10    239.0.0.3           port1.3     R       00:00:04  00:00:46 192.168.100.1
V3
10    239.0.0.1           port1.4     R       00:00:03  00:00:47 192.168.100.2
V3
```

10. [スイッチ#B] マルチキャストルーターポートの情報を確認します。(LANポート #1 につながっている)

```
Yamaha#show ip igmp snooping mrouter vlan10
VLAN  Interface          IP-address  Expires
10    port1.1(dynamic)    192.168.100.240  00:00:25
```

11. [スイッチ#B] マルチキャスト受信者の情報を確認します。

```
Yamaha#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan  Group/Source Address  Interface   Flags  Uptime   Expires  Last Reporter
Version
10    239.0.0.1           port1.1     R       00:00:03  00:00:47 192.168.100.2
V3
10    239.0.0.3           port1.1     R       00:00:04  00:00:46 192.168.100.1
V3
10    239.0.0.1           port1.3     R       00:00:02  00:00:48 192.168.100.3
V3
10    239.0.0.2           port1.4     R       00:00:02  00:00:48 192.168.100.4
V3
```

---

## 注意事項

未知のマルチキャストフレームの処理を変更したい場合は、 **l2-known-mcast** コマンドで行ってください。

## 関連文書

- [VLAN](#)

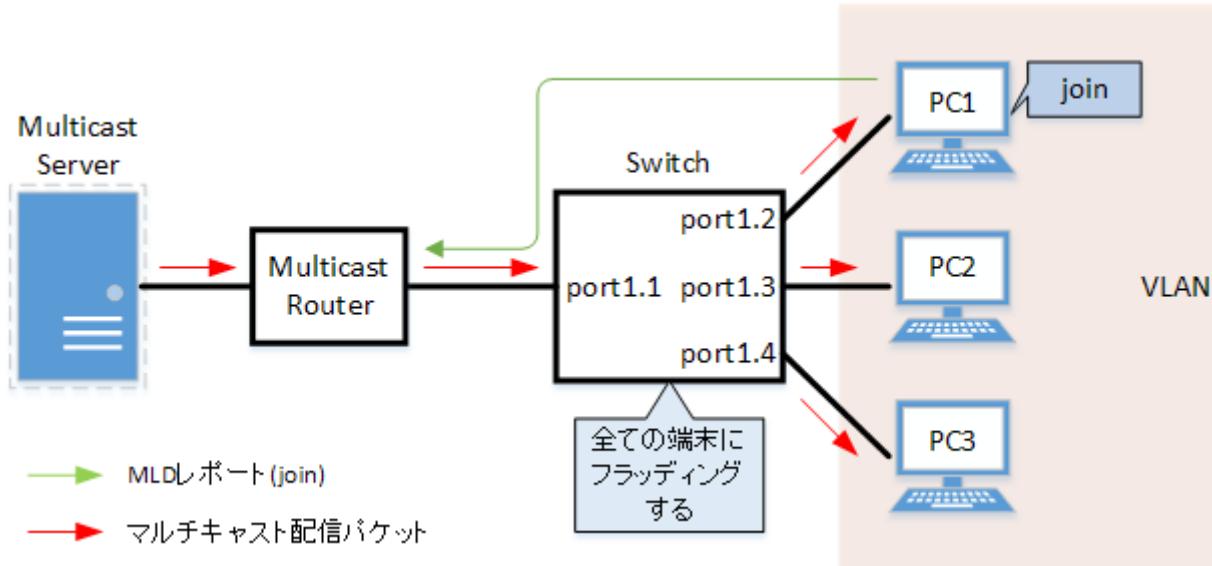
# MLD Snooping

## 機能概要

MLD Snoopingは、IPv6のVLAN環境において余分なマルチキャストのフラッディングを制御することで、ネットワークの帯域幅の消費を抑える機能です。

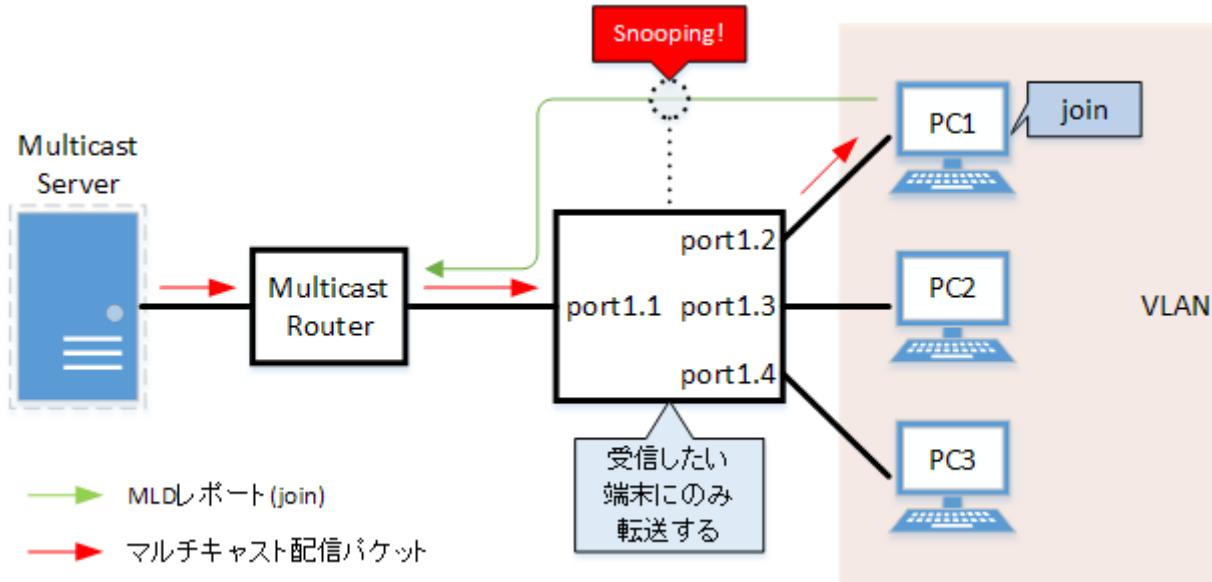
L2スイッチでは、マルチキャストパケットはVLAN単位で配信されるため、VLAN内に1つでもマルチキャストパケットを受信したい端末が存在すると、同一VLAN内のすべてのポートにパケットが配信されてしまいます。

- マルチキャスト配信時の動作(MLD Snoopingなし)



MLD Snooping機能を使用すると、受信端末とマルチキャストルーター間で交換されるMLDメッセージを監視(Snooping)することで、マルチキャストパケットを受信したい端末が接続されたポートのみに該当グループのパケットを配信することができます。

- マルチキャスト配信時の動作(MLD Snoopingあり)



## 用語の定義

### MLD (Multicast Listener Discovery)

IPv6でマルチキャストグループを制御するためのプロトコル(ICMPv6のサブプロトコル)。

---

マルチキャストルーターはLAN上のどのホストがマルチキャストグループのメンバーであるか判断でき、ホストは自分がどのマルチキャストグループのメンバーかを伝えることができます。  
2つのバージョンがあり、 **MLDv1 (RFC2710)**、 **MLDv2 (RFC3810)** で規定されます。

## マルチキャストルーターポート

マルチキャストルーターが接続されているLAN/SFPポートのこと。  
MLDジェネラルクエリーを受信したLAN/SFPポートをマルチキャストルーターポートとして自動で学習します。

## MLDレポート抑制機能

マルチキャストルーターとホスト間で行われる通信負荷をL2スイッチで抑制する機能。  
抑制するために本製品がまとめるメッセージは、以下となります。

- ・マルチキャストルーターから送られる MLDジェネラルクエリー に対してホストが応答するMLDレポート
- ・ホストから通知されるMLD DoneメッセージおよびMLDレポート(離脱)

レポート抑制機能は、MLDv1/v2に対して動作します。

## MLD Fast Leave (高速脱退) 機能

MLDv1 DoneメッセージおよびMLDv2のReport(離脱)メッセージを受信したLAN/SFPポートを即座にマルチキャスト受信ポートから外す(転送に必要なFDBエントリーを削除する)機能。

本来、MLDの離脱処理では、MLDv1 DoneメッセージおよびMLDv2 Report(離脱)メッセージを受信した際、グループスペシフィッククエリーを送信し、レシーバーの存在確認が行われますが、高速脱退機能が **有効** な場合、本動作を行いません。

このため、高速脱退機能は **LAN/SFPポート配下に1つのレシーバーが接続されている場合にのみ効果的な機能** です。

## MLD クエリー送信機能 (MLD Querier)

MLD ジェネラルクエリー、スペシフィッククエリーを送信する機能。  
マルチキャストルーターがない環境でMLD Snoopingを機能させる場合に使用します。

## **機能詳細**

MLD Snoopingの動作仕様について以下に示します。

1. 本製品は、 **MLD v1/v2** に対応したSnooping機能を提供します。  
本製品で機能させる上位バージョンを **ipv6 mld snooping version** コマンド で設定できます。  
バージョン設定は **VLANインターフェース** に対して行い、初期設定は **v2** となっています。  
設定バージョンと受信フレームのバージョンの違いによる動作は以下となります。
  - ・ 設定したバージョンよりも上位バージョンのMLDクエリーを受信した場合、設定バージョンに下げてクエリーを転送します。
  - ・ 設定したバージョンよりも上位バージョンのMLDレポートを受信した場合、該当レポートを転送せずに破棄します。
2. MLD Snoopingの **有効 / 無効** 設定は、 **VLANインターフェース** に対して行います。  
デフォルトVLAN (VLAN #1)に対する初期設定、VLAN生成後の初期設定どちらも **無効** となっています。
3. MLD Snoopingの機能として、以下の4つに対応します。
  - ・ マルチキャストルーターポートの設定

- MLDレポート抑制
- MLD Fast-leave(高速脱退)
- MLDクエリー送信

4. MLD Snoopingが**有効**に設定されているVLANインターフェースでは、**マルチキャストルーターポートを自動で学習**しますが、**ipv6 mld snooping mrouter interface** コマンドで静的に設定することもできます。  
なお、VLANインターフェースに設定されているマルチキャストルーターポートは、**show ipv6 mld snooping mrouter** コマンドで確認します。
5. **MLDレポート抑制機能**は、VLANインターフェースに対して**ipv6 mld snooping report-suppression** コマンドで設定します。  
初期値は**有効**です。  
レポート抑制機能により、MLDレポート、MLD leaveメッセージを送信する場合、送信元IPv6アドレスには、VLANインターフェースに割り振られているIPv6リンクローカルアドレスを使用します。  
(割り振られていない場合は、::を設定して送信します。)
6. **MLD Fast-Leave(高速脱退)機能**は、VLANインターフェースに対して**ipv6 mld snooping fast-leave** コマンドで設定します。  
デフォルトVLAN (VLAN #1)に対する初期設定、VLAN生成後の初期設定どちらも**無効**となっています。
7. マルチキャストルーターが存在しない環境でMLD Snoopingを使用するために、**MLD クエリー送信機能**に対応します。  
MLD クエリー送信機能は、以下の2つのパラメータで制御します。
  - MLD クエリー送信機能の**有効 / 無効**
    - VLANインターフェースに対して、**ipv6 mld snooping querier** コマンドで行います。
    - デフォルトVLAN (VLAN #1)に対する初期設定、VLAN生成後の初期設定どちらも**無効**となっています。
  - MLD クエリーの送信間隔
    - **ipv6 mld snooping query-interval** コマンドで行います。
    - 送信間隔は、20 ~ 18,000秒の範囲で設定可能とし、初期値は**125秒**となっています。
8. VLAN内に複数の機器がクエリーを送信する場合、VLAN内で最も小さいIPv6アドレスを持つ機器がクエリー送信を行います。  
本製品は、自身のIPv6アドレスより小さなIPv6アドレスを持つ機器からのクエリーを受信した場合、クエリー送信機能を停止します。  
なお、クエリー送信時に設定する送信元IPv6アドレスは、VLANインターフェースに割り振られているIPv6リンクローカルアドレスを使用しますが、割り振られていない場合は、他のVLANインターフェースに割り振られているIPv6リンクローカルアドレスを使用します。  
(すべてのVLANインターフェースにIPv6リンクローカルアドレスが割り当てられていない場合は、送信されません。)
9. 本製品では、受信したMLD/パケットのHop Limitが不正（1以外）である場合、MLD/パケットを破棄します。
10. 本製品では、受信したMLD/パケットにRouter Alertオプションが含まれていない場合、MLD/パケットを破棄します。

## 関連コマンド

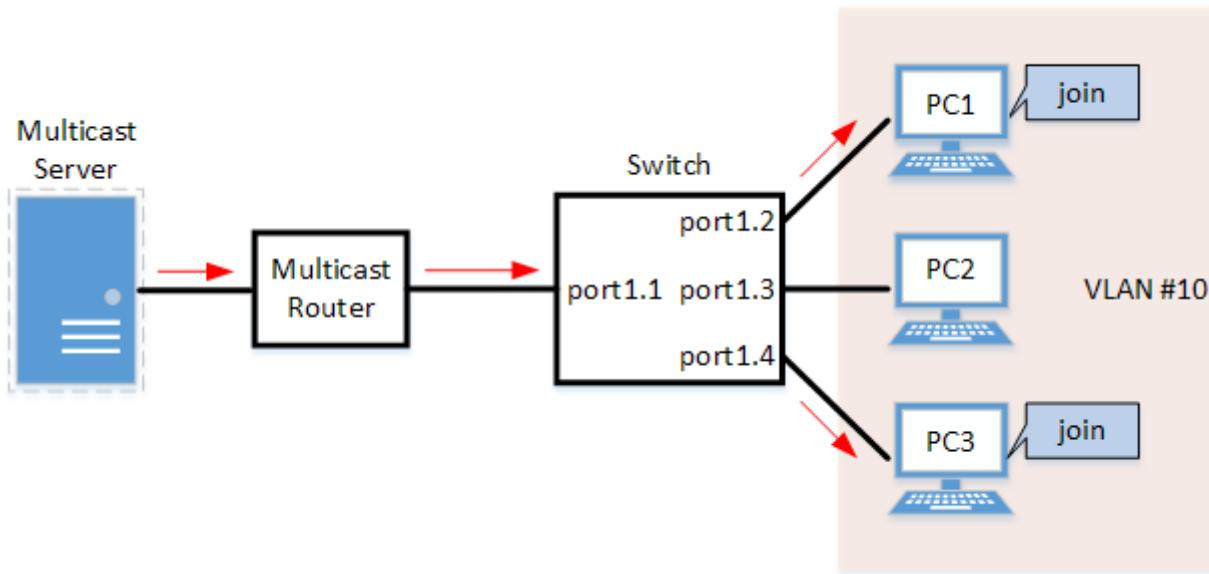
関連コマンドについて、以下に示します。  
コマンドの詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
MLDスヌーピングの有効／無効設定	ipv6 mld snooping
MLDスヌーピング高速脱退の設定	ipv6 mld snooping fast-leave
マルチキャストルーターポートの設定	ipv6 mld snooping mrouter interface
クエリー送信機能の設定	ipv6 mld snooping querier
MLDクエリー送信間隔の設定	ipv6 mld snooping query-interval
MLDバージョンの設定	ipv6 mld snooping version
MLDレポート抑制機能の設定	ipv6 mld snooping report-suppression
マルチキャストルーターポートの情報の表示	show ipv6 mld snooping mrouter
MLDマルチキャスト受信者の情報を表示	show ipv6 mld snooping groups
インターフェースのMLD関連情報を表示	show ipv6 mld snooping interface
MLDグループメンバーシップのエントリー削除	clear ipv6 mld snooping

## コマンド実行例

### MLD Snooping の設定(マルチキャストルーターあり)

マルチキャストルーターがある環境でMLD Snooping機能を有効にして、マルチキャストグループに参加しているPC1、PC3にのみデータが配信されるようにします。



- ・ LANポート #1 ~ #4 は、 **アクセスポートに設定し、VLAN #10 に所属** させます。
- ・ マルチキャストルーターがあるため、 **MLD クエリー送信機能は 無効** のまとします。
- ・ マルチキャストルーターポート の学習は、 **自動学習** のみとします。(静的な設定は行わない。)
- ・ **MLD Fast-Leave(高速脱退)機能を有効** にします。

### ■設定手順

1. VLAN #10 を定義して、MLD Snoopingの設定を行います。

```

Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ipv6 enable ②
Yamaha(config-if)#ipv6 mld snooping ③
Yamaha(config-if)#no ipv6 mld snooping querier ④
Yamaha(config-if)#ipv6 mld snooping fast-leave ⑤

```

① VLAN #10 の定義

② VLAN #10 のIPv6機能を有効にする

③ VLAN #10 のMLD Snoopingを有効にする

④ VLAN #10 のMLD クエリー送信機能を無効にする

⑤ VLAN #10 のMLD Fast-leave機能を有効にする

- MLD クエリー送信機能の無効化は、初期値として設定されているため特に設定する必要はありません。

2. LANポート #1 ~ #4 を アクセスポートに設定し、VLAN #10 に所属させます。

```

Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①

```

① 上記設定をLANポート #2 ~ #4に対しても行います。

3. マルチキャストルーターポートの情報を確認します。(LANポート #1 につながっている)

```

Yamaha#show ipv6 mld snooping mrouter vlan10
VLAN      Interface          IP-address      Expires
10        port1.1(dynamic)   fe80::2a0:deff:feae:b879    00:00:43

```

4. マルチキャスト受信者の情報を確認します。

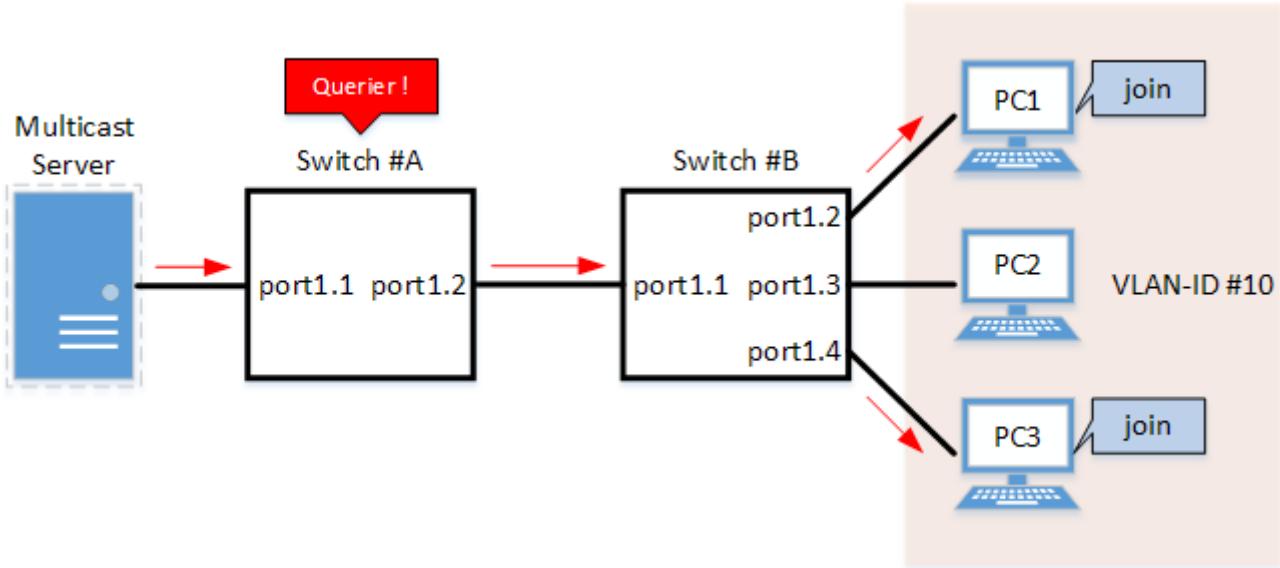
```

Yamaha#show ipv6 mld snooping groups
MLD Connected Group Membership
Vlan  Group Address          Interface      Uptime      Expires
Last Reporter
10    ff15::1                port1.2       00:00:13  00:00:41
fe80::a00:27ff:fe8b:87e2
10    ff15::1                port1.4       00:00:02  00:00:48
fe80::a00:27ff:fe8b:87e4

```

### MLD Snooping の設定(マルチキャストルーターなし)

マルチキャストルーターがない環境でMLD Snooping機能を有効にして、マルチキャストグループに参加しているPC1、PC3にのみデータが配信されるようにします。



- スイッチ#A
  - LANポート #1 ~ #2 は、 アクセスポートに設定し、VLAN #10 に所属させます。
  - MLD クエリー送信機能を 有効 にします。  
MLDクエリーの送信間隔を 20秒 とします。
- スイッチ#B
  - LANポート #1 ~ #4 は、 アクセスポートに設定し、VLAN #10 に所属させます。
  - マルチキャストルーターポート の学習は、 自動学習 のみとします。(静的な設定は行わない。)
  - MLD Fast-Leave(高速脱退)機能を有効 にします。

1. [スイッチ#A] VLAN #10 を定義して、MLD Snoopingの設定を行います。

```

Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ipv6 enable ②
Yamaha(config-if)#ipv6 mld snooping ③
Yamaha(config-if)#ipv6 mld snooping querier ④
Yamaha(config-if)#ipv6 mld snooping query-interval 20 ⑤

```

- ① VLAN #10 の定義
- ② VLAN #10 のIPv6機能を有効にする
- ③ VLAN #10 のMLD Snoopingを有効にする
- ④ VLAN #10 のMLD クエリー送信機能を有効にする
- ⑤ VLAN #10 のMLD クエリーの送信間隔を20秒にする

2. [スイッチ#A] LANポート #1 ~ #2 を アクセスポートに設定し、VLAN #10 に所属させます。

```

Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10

```

①

① 上記設定をLANポート #2に対しても行います。

3. [スイッチ#B] VLAN #10 を定義して、MLD Snoopingの設定を行います。

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan10
Yamaha(config-if)#ipv6 enable ②
Yamaha(config-if)#ipv6 mld snooping ③
Yamaha(config-if)#no ipv6 mld snooping querier ④
Yamaha(config-if)#ipv6 mld snooping fast-leave ⑤
```

① VLAN #10 の定義

② VLAN #10 のIPv6機能を有効にする

③ VLAN #10 のMLD Snoopingを有効にする

④ VLAN #10 のMLD クエリー送信機能を無効する

⑤ VLAN #10 のMLD Fast-leave機能を有効にする

。 MLD クエリー送信機能の無効化は、初期値として設定されているため特に設定する必要はありません。

4. [スイッチ#B] LANポート #1 ~ #4 をアクセスポートに設定し、VLAN #10 に所属させます。

```
Yamaha(config)# interface port1.1
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① 上記設定をLANポート #2 ~ #4に対しても行います。

5. [スイッチ#B] マルチキャストルーターポートの情報を確認します。(LANポート #1 につながっている)

```
Yamaha#show ipv6 mld snooping mrouter vlan10
VLAN      Interface          IP-address      Expires
10        port1.1(dynamic)   fe80::2a0:deff:feae:b879    00:00:43
```

6. [スイッチ#B] マルチキャスト受信者の情報を確認します。

```
Yamaha#show ipv6 mld snooping groups
MLD Connected Group Membership
Vlan      Group Address          Interface      Uptime      Expires
Last Reporter
10        ff15::1                port1.2        00:00:13 00:00:41
fe80::a00:27ff:fe8b:87e2
10        ff15::1                port1.4        00:00:02 00:00:48
fe80::a00:27ff:fe8b:87e4
```

---

## 注意事項

未知のマルチキャストフレームの処理を変更したい場合は、 **l2-known-mcast** コマンドで行ってください。

## 関連文書

- [VLAN](#)
- [IPv6基本設定](#)

# トラフィック制御機能

## ACL

### 機能概要

アクセスリスト(ACL)とは、フレームの許可・拒否を決めるための条件文のことです。インターフェースに対してアクセスリストを適用すると、許可したフレームと条件に一致しないフレームは転送し、拒否したフレームのみ破棄します。これにより、特定のフレームのみを転送対象とすることができるため、主にセキュリティを確保するために使用されます。本製品では、アクセスリストとして下表に示す3種類をサポートします。

- ・ アクセスリストの種類

アクセスリストの種類	判断基準	アクセスリストID	用途
IPv4 アクセスリスト	送信元IPv4アドレス	1～2000	特定のホスト、ネットワークからのアクセスをフィルタリングします。
IPv6 アクセスリスト	送信元IPv6アドレス	3001～4000	特定のホスト、ネットワークからのアクセスをフィルタリングします。
MAC アクセスリスト	送信元MACアドレス	2001～3000	特定のデバイスからのアクセスをフィルタリングします。

### 用語の定義

#### ACL

Access Control List の略。

#### ワイルドカードマスク

指定したIPv4アドレス、MACアドレスのどこを読み取るかを指定した情報です。ACLの条件で **IPv4アドレス、MACアドレスの範囲を指定する際に使用** します。

- ・ ワイルドカードマスクのビットが "0" の場合 : 該当ビットをチェックします
- ・ ワイルドカードマスクのビットが "1" の場合 : 該当ビットをチェックしません

ワイルドカードマスクを使用した設定例を以下に示します。(下線部分がワイルドカードマスク)

- ・ サブネット **192.168.1.0/24** に対して条件を指定する場合 : **192.168.1.0 0.0.0.255** (10進で指定)
- ・ ベンダーコード **00-A0-DE---\*** に対して条件を指定する場合: **00A0.DE00.0000 0000.00FF.FFFF** (16進で指定)

## 機能詳細

### アクセスリストの生成

アクセスリストは、IPv4アクセスリスト、IPv6アクセスリスト、MACアクセスリストのそれぞれで **最大28個** 生成することができます。

アクセスリストは、1つのリストに対して制御条件を **最大128件** 登録することができます。  
登録した制御条件を満たさなかった場合、通常どおり転送処理されます。

### インターフェースへの適用

本製品のインターフェースに対するアクセスリストの適用状況は、下表のようになっています。  
なお、インターフェースに対して適用可能なアクセスリストは **1つ** です。

アクセスリストの種類	LANポート		VLANインターフェース		論理インターフェース	
	in	out	in	out	in	out
IPv4アクセスリスト	○	×	×	×	×	×
IPv6アクセスリスト	○	×	×	×	×	×
MACアクセスリスト	○	×	×	×	×	×

インターフェースに適用できるアクセスリストの数は、アクセスリストに登録されている制御条件の数に依存します。

システム全体で使用可能な制御条件の数は **IPv4とMACの合計で最大896件、IPv6で最大384件** です。  
インターフェースにアクセスリストを適用させると "アクセスリストに登録されている制御条件の数だけ" リソースを消費します。

### LANポートに対する設定

LANポートにアクセスリストを適用させる場合の手順について、以下に示します。

1. フィルタリング条件を決め、アクセスリストを生成します。
  - 必要に応じて、名前を付けてください。
2. アクセスリストを確認します。
3. LANポートにアクセスリストを適用します。
4. 適用したアクセスリストを確認します。

以下に操作コマンドの一覧を示します。

- アクセスリスト操作コマンド

アクセスリストの種類	アクセスリストの生成	アクセスリストの確認	アクセスリストの適用	適用アクセスリストの確認
IPv4アクセスリスト	<b>access-list</b>	<b>show access-list</b>	<b>access-group</b>	<b>show access-group</b>
IPv6アクセスリスト	<b>access-list</b>	<b>show access-list</b>	<b>access-group</b>	<b>show access-group</b>
MACアクセスリスト	<b>access-list</b>	<b>show access-list</b>	<b>access-group</b>	<b>show access-group</b>

## 関連コマンド

関連コマンドについて、以下に示します。

コマンドの詳細は、コマンドリファレンスを参照願います。

操作項目	操作コマンド
IPv4アクセリストの生成	access-list
IPv4アクセリストのコメント追加	access-list description
IPv4アクセリストの適用	access-group
IPv6アクセリストの生成	access-list
IPv6アクセリストのコメント追加	access-list description
IPv6アクセリストの適用	access-group
MACアクセリストの生成	access-list
MACアクセリストのコメント追加	access-list description
MACアクセリストの適用	access-group
生成したアクセリストの表示	show access-list
インターフェースに適用したアクセリストの表示	show access-group

## コマンド実行例

### IPv4アクセリストの設定

#### ■ホスト指定

LANポート #1 に対して、ホスト: **192.168.1.1** からのアクセスのみ許可するように設定します。  
使用するアクセリストのIDは、**#123** とし、アクセリストの名前を **IPV4-ACL-EX** を追加します。

1. アクセリスト **#123** を生成し、確認します。

```
Yamaha(config)#access-list 123 permit host 192.168.1.1 ①
Yamaha(config)#access-list 123 deny any
Yamaha(config)#access-list 123 description IPV4-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ③
IPv4 access list 123
  10 permit host 192.168.1.1
  20 deny any
Yamaha#
```

- ① アクセリストの生成
- ② アクセリストに名前を付ける
- ③ アクセリストの確認

2. LANポート #1 に アクセリスト #123 を適用します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 123 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv4 access group 123 in
```

① アクセスリストの適用

② アクセスリストの設定確認

## ■ネットワーク指定

LANポート #1 に対して、ネットワーク: **192.168.1.0/24** からのアクセスのみ許可するように設定します。使用するアクセスリストのIDは、 **#123** とし、アクセスリストの名前を **IPV4-ACL-EX** を追加します。

1. アクセスリスト #123 を生成し、確認します。

```
Yamaha(config)#access-list 123 permit 192.168.1.0 0.0.0.255 ①
Yamaha(config)#access-list 123 deny any
Yamaha(config)#access-list 123 description IPV4-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show ip access-list ③
IPv4 access list 123
  10 permit 192.168.1.0/24
  20 deny any
Yamaha#
```

① アクセスリストの生成

② アクセスリストに名前を付ける

③ ACLの確認

2. LANポート #1 に アクセスリスト #123 を適用します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 123 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv4 access group 123 in
```

① アクセスリストの適用

② アクセスリストの設定確認

## IPv6アクセスリストの設定

### ■ホスト指定

LANポート #1 に対して、ホスト: **2001:db8::1** からのアクセスのみ許可するように設定します。使用するアクセスリストのIDは、 **#3001** とし、アクセスリストの名前を **IPV6-ACL-EX** とします。

---

1. アクセスリスト #3001 を生成し、確認します。

```
Yamaha(config)#access-list 3001 permit 2001:db8::1/128 ①
Yamaha(config)#access-list 3001 deny any
Yamaha(config)#access-list 3001 description IPV6-ACL-EX ②
Yamaha(config)#end

Yamaha# show access-list 3001 ③
IPv6 access list 3001
 10 permit 2001:db8::1/128
 20 deny any
```

① アクセスリストの生成

② アクセスリストに名前を付ける

③ アクセスリストの確認

2. LANポート #1 に アクセスリスト #3001 を適用します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 3000 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv6 access group 3001 in
```

① アクセスリストの適用

② アクセスリストの設定確認

### ■ネットワーク指定

LANポート #1 に対して、ネットワーク: **2001:db8::/64** からのアクセスのみ許可するように設定します。  
使用するアクセスリストのIDは、**#3001** とし、アクセスリストの名前を **IPV6-ACL-EX** とします。

1. アクセスリスト #3001 を生成し、確認します。

```
Yamaha(config)#access-list 3001 permit 2001:db8::/64 ①
Yamaha(config)#access-list 3001 deny any
Yamaha(config)#access-list 3001 description IPV6-ACL-EX ②
Yamaha(config)#end

Yamaha# show access-list 3001 ③
IPv6 access list 3001
 10 permit 2001:db8::/64
 20 deny any
```

① アクセスリストの生成

② アクセスリストに名前を付ける

③ アクセスリストの確認

2. LANポート #1 に アクセスリスト #3001 を適用します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 3001 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : IPv6 access group 3001 in
```

① アクセスリストの適用

② アクセスリストの設定確認

## MACアクセスリストの設定

### ■ホスト指定

LANポート #1 に対して、ホスト: **00-A0-DE-12-34-56** からのアクセスのみ拒否し、それ以外を許可します。

使用するアクセスリストのIDは、**#2001** とし、アクセスリストの名前を **MAC-ACL-EX** を追加します。

1. アクセスリスト **#2001** を生成し、確認します。

```
Yamaha(config)#access-list 2001 deny host 00a0.de12.3456 ①
Yamaha(config)#access-list 2001 description MAC-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 2001 ③
MAC access list 2001
 10 deny host 00A0.DE12.3456
```

① アクセスリストの生成

② アクセスリストの名前の設定

③ アクセスリストの確認

2. LANポート #1 に アクセスリスト #2001 を適用します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 2001 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : MAC access group 2001 in
```

① アクセスリストの適用

② アクセスリストの設定確認

### ■ベンダー指定

LANポート #1 に対して、ベンダーコード: **00-A0-DE---\*** (00-A0-DE-00-00-00 ~ 00-A0-DE-FF-FF-FF) からのアクセスのみ拒否し、それ以外を許可します。

使用するアクセスリストのIDは、**#2001** とし、アクセスリストの名前を **MAC-ACL-EX** を追加します。

1. アクセスリスト **#2001** を生成し、確認します。

```
Yamaha(config)#access-list 2001 deny 00a0.de00.0000 0000.00ff.ffff ①
Yamaha(config)#access-list 2001 description MAC-ACL-EX ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 2001 ③
MAC access list 2001
10 deny 00A0.DE00.0000 0000.00FF.FFFF
```

① アクセスリストの生成

② アクセスリストの名前の設定

③ アクセスリストの確認

2. LANポート #1 に アクセスリスト #2001 を適用します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 2001 in ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show access-group ②
Interface port1.1 : MAC access group 2001 in
```

① アクセスリストの適用

② アクセスリストの設定確認

## 注意事項

- 論理インターフェースに所属しているLANポートにアクセスリストが適用されている場合、論理インターフェースの最若番の所属ポートに適用されている設定が、他の所属ポートにも適用されます。

## 関連文書

- [L2スイッチング機能: VLAN](#)

# **QoS**

## **機能概要**

QoS ( Quality of Service ) とは、ネットワーク上で、ある特定の通信のための帯域を予約し、一定の通信速度を保証する技術です。

アプリケーションデータを分類・グループ化し、IPヘッダ内の DSCP や、IEEE802.1Q タグ内の CoS を参照してグループ毎の優先度に従い、データを転送します。

## **用語の定義**

### **CoS (IEEE 802.1p Class of Service)**

VLANタグヘッダ内にある3ビットのフィールドで優先度を表現し、0～7の値をとる。  
802.1p ユーザープライオリティとも呼ぶ。

### **IP Precedence**

IPヘッダの TOS フィールド内にある 3 ビットのフィールドで優先度を表現し、0～7 の値をとる。  
フレームを受信した機器に対して、該当フレームのトラフィッククラスを示すために使われる。

### **DSCP (Diffserv Code Point)**

IP ヘッダの TOS フィールド内にある 6 ビットのフィールドで優先度を表現し、0～63 の値をとる。  
DSCP は IP Precedence と同じ TOS フィールドを使用しているため、IP-Precedence と互換性がある。  
フレームを受信した機器に対して、該当フレームのトラフィッククラスを示すために使われる。

### **デフォルト CoS**

タグなしフレームに対して内部処理のために付与する CoS 値のこと。

### **送信キュー**

本製品は、ポート毎に 8 個の送信キューをもつ。送信キューには、ID 0～7 が割り振られており、IDの数値が大きいほど、優先度が高いキューとなる。

### **トラストモード**

送信キューID の決定を何に基づいて(信頼して)行うかを表す。

本製品では、受信フレームの CoS 値または DSCP 値を使用して、送信キューの振り分けをすることができる。  
LAN/SFP ポート単位で設定が可能で、初期状態(QoS を有効化したとき)は CoS に設定されている。

### **送信キューID変換テーブル**

CoS 値や DSCP 値から、送信キューID を決定するための変換テーブル。

CoS - 送信キューID変換テーブルと DSCP - 送信キューID変換テーブルの 2 種類があり、それぞれのトラストモードで使用される。

マッピングは、ユーザーが自由に変更することができる。

### **ポート優先度**

受信ポート毎に設定された優先度。トラストモードが"ポート優先"の場合、そのポートで受信したフレームは、ポート優先度の設定に基づいて送信キューへ格納される。

## 機能詳細

### QoS の有効・無効制御

本製品の QoS 制御は、工場出荷時、**無効** となっています。

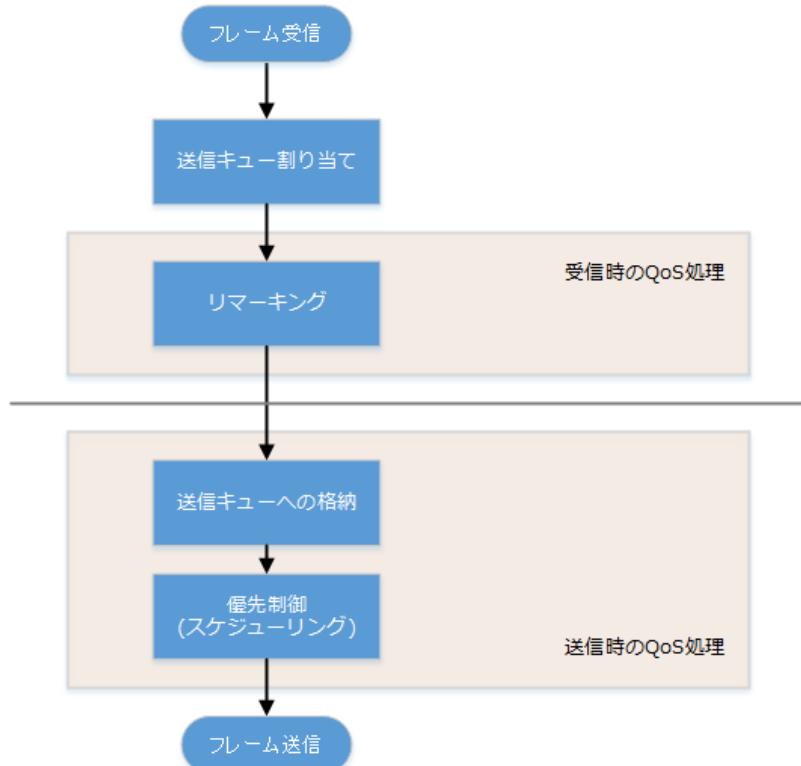
QoS 制御の有効化は、**qos enable** コマンドで行います。無効化する場合は、**no qos** コマンドで行います。

QoS 制御コマンドのほとんどは、QoS が有効化されていないと実行することができません。

また、QoS 機能の状態は、**show qos** コマンドで確認することができます。

### QoS 処理フロー

QoS の処理フローは以下のようになります。



### 送信キューの割り当て

本製品はフレームを受信すると、フレーム内の **CoS 値** や **DSCP 値**、受信ポートの **ポート優先度** に基づいて、送信キューID の初期値を決定します。

フレームの CoS 値、DSCP 値のうち、何に基づいて送信キューを決定するかは、ポートの **トラストモード** によって決まります。

**トラストモード** は、**qos trust** コマンドで変更することができ、初期設定(QoS 有効化時)は **CoS** に設定されています。

送信キューの割り当ては、**トラストモード** 毎に以下のルールで行われます。

- トラストモードが "CoS" の場合
  - 受信フレームが VLAN タグ付きフレームの場合、タグ内の CoS 値を使用して、送信キューID を決定します。
  - 受信フレームが VLAN タグ無しフレームの場合、本製品で管理する **デフォルト CoS** を使用して、送信キューID を決定します。  
初期設定(QoS 有効化時)、**デフォルト CoS** は **0** に設定されています。**qos cos** コマンドで変更することができます。

- CoS値から送信キューIDへの変換は、CoS-送信キューID変換テーブルによって行われます。本テーブルはシステムで一つ保有し、初期設定(QoS 有効化時)では、以下が設定されています。**qos cos-queue** コマンドで変更することができます。

CoS 値	送信キューID	Traffic Type
0	2	Best Effort
1	0	Background
2	1	Standard(spare)
3	3	Excellent Effort(Business Critical)
4	4	Controlled Load(Streaming Multimedia)
5	5	Video(Interactive Media) less than 100 msec latency and jitter
6	6	Voice(Interactive Media) less than 10 msec latency and jitter
7	7	Network Control(Reserved Traffic)

#### ・ トラストモードが "DSCP" の場合

- IPヘッダ内の DSCP 値を使用して、送信キューID を決定します。
- DSCP値から送信キューIDへの変換は、DSCP-送信キューID変換テーブルによって行われます。本テーブルはシステムで一つ保有し、初期設定(QoS 有効化時)では、以下が設定されています。**qos dscp-queue** コマンドで変更することができます。

DSCP 値	送信キューID	Traffic Type
0 - 7	2	Best Effort
8 - 15	0	Background
16 - 23	1	Standard(spare)
24 - 31	3	Excellent Effort(Business Critical)
32 - 39	4	Controlled Load(Streaming Multimedia)
40 - 47	5	Video(Interactive Media) less than 100 msec latency and jitter
48 - 55	6	Voice(Interactive Media) less than 10 msec latency and jitter
56 - 63	7	Network Control(Reserved Traffic)

#### ・ トラストモードが "ポート優先" の場合

- ポート優先度** に従って送信キューID を決定します。
- 初期設定(QoS 有効化時)では、**ポート優先度** は 2 に設定されています。設定は **qos port-priority-queue** コマンドで変更することができます。

## リマーキング

受信したフレームのCoS値またはDSCP値の書き換えを、ポート毎に行います。

特定のポートで受信したフレームの優先度を制御するために使用します。

リマーキングは送信キュー再割り当ての前に実行されるため、本製品の優先制御においてもリマーキング後のCoS値またはDSCP値が使用されます。

トラストモードが "ポート優先" の場合は、リマーキングによって送信キューIDを変更することはできません。

## 送信キューへの格納

一連のQoS処理によって最終的に決定した送信キューへ、フレームを格納します。

本製品では、送信キュー混雑状況を解消するために、フレームを選択し、破棄する仕組みを提供します。

- ・ **テールドロップ**  
本製品では、送信キューの溢れ対策として、**テールドロップ**方式を採用します。  
テールドロップによって破棄されたフレームは、フレームカウンターによってカウントされます。
- ・ テールドロップのしきい値を変更することはできません。
- ・ 各ポートはパケットバッファを共有しており、各ポートの送信キューが使用できるパケットバッファの割合はパケットバッファの使用状況によって変動します。
- ・ **show qos queue-counters**コマンドにより、各送信キューがどれだけパケットバッファを使用しているか確認することができます。
- ・ 送信キューの使用状況は、**show qos queue-counters**コマンドで確認することができます。
- ・ テールドロップによって破棄されたパケット数は**show interface**, **show frame-counter**コマンドで確認することができます。

## スケジューリング

スケジューリングにより、送信キューに格納されたフレームをどのような規則で送出するかを決定します。

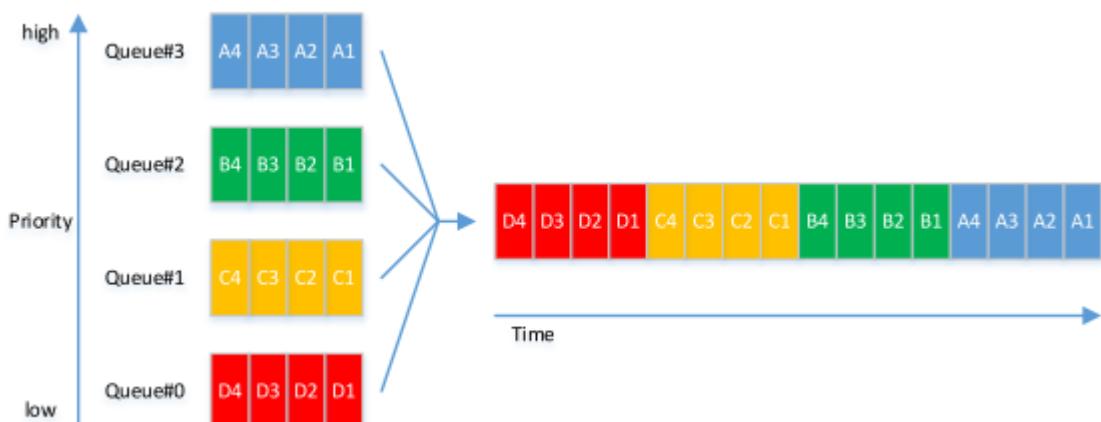
輻輳制御の仕組みと合わせて、スケジューリングを適切に制御することによって、QoSを保証するのに役立ちます。(不適切なスケジューリングはQoSを劣化させます。)

本製品は、送信キューのスケジューリング方式として、**絶対優先方式(SP)**と**重み付きラウンドロビン方式(WRR)**の2種類をサポートします。

- ・ **絶対優先方式 (SP : Strict Priority)**

キューの優先度の高いものから優先的に送信します。

優先度の高いキューにフレームが格納されている場合には、それより優先度の低いキューからは全く送信することができなくなります。



- ・ **重み付きラウンドロビン方式 (WRR : Weighted Round Robin)**

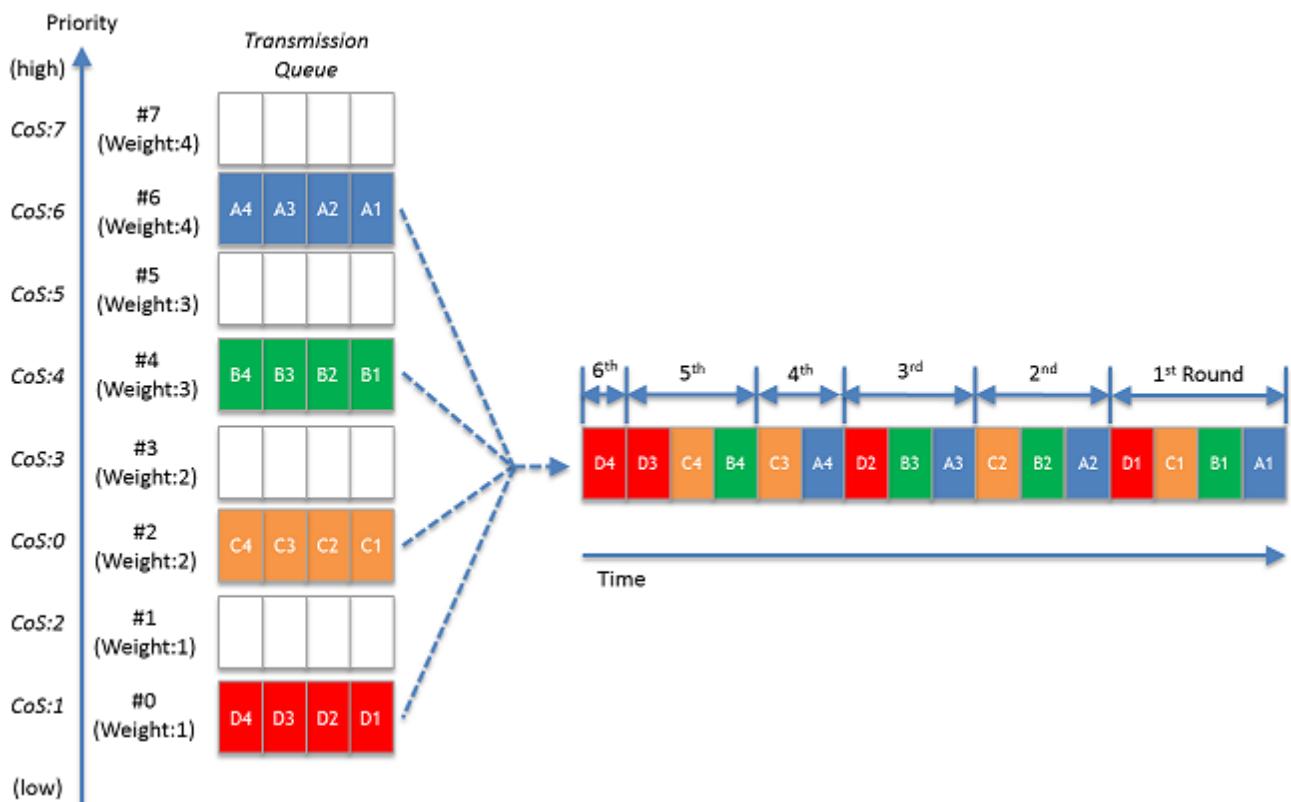
各キューに**重み**が設定され、その比率によってフレームを送信します。

優先度の低いキューからも、ある一定の割合にて送信することができます。

**重み**は以下の表に従って決定されます。

- ・ 各送信キューの重み

送信キューID	Weight	Ratio
7 (highest priority)	4	20%
6	4	20%
5	3	15%
4	3	15%
3	2	10%
2	2	10%
1	1	5%
0 (lowest priority)	1	5%



送信キューに対するスケジューリングの設定は、インターフェース単位ではなく、システムで一つの設定となります。

スケジューリングの設定は、 **qos scheduling** コマンドを使用します。

初期設定(QoS 有効化時)では、スケジューリング設定は **WRR** となっています。

### Web会議アプリケーション向け最適設定

Web GUIから、Web会議アプリケーション向けのQoS設定を簡単に行うことができます。

使用するWeb会議アプリケーションを選択するだけの簡単な操作で、「Zoom Meetings」や「Microsoft Teams」といったWeb会議アプリケーションの通信を優先させることができます。

- Web 会議アプリケーション向け最適設定ページ

Web会議アプリケーション向け最適設定では以下の設定を行います。

- ・ QoS を有効にします。
- ・ すべてのポートのトラストモードを DSCP に設定します。
- ・ 最適化対象の Web 会議アプリケーションで使用する DSCP 値を、優先度の高い送信キューに割り当てます。Web会議アプリケーションで使用するDSCP値は以下のとあります。Web会議アプリケーションの設定により、Web会議アプリケーションで使用するDSCP値をデフォルト値から変更している場合は、**qos dscp-queue** コマンドでDSCP値と送信キューの紐づけを変更してください。
  - Zoom Meetings
    - 56 (Audio)
    - 40 (Video/Screen sharing)
  - Microsoft Teams
    - 46 (Audio)
    - 34 (Video)
    - 18 (Application/Screen sharing)
- ・ 最適化対象の Web 会議アプリケーションで使用しない DSCP 値を、最も優先度の低い送信キューに割り当てます。
- ・ すべての送信キューのスケジューリングを絶対優先方式に設定します。

本Web会議アプリケーション向け最適設定機能は、スイッチ単体のQoS設定を行う機能です。QoSの効果を最大限に活かすには、ルーターを含むネットワーク全体で一貫したQoS設定を行う必要があります。また、Web会議アプリケーションのDSCP値をデフォルトから変更している場合は、別途、DSCPの送信キュー割り当ての設定を変更してください。

**別表1. 標準 PHB (RFC 推奨値)**

PHB	DSCP値	RFC
Default	0	RFC2474

PHB		DSCP値	RFC
CS (Class Selector)	CS0	0	RFC2474
	CS1	8	
	CS2	16	
	CS3	24	
	CS4	32	
	CS5	40	
	CS6	48	
	CS7	56	
AF (Assured Forwarding)	AF11	10	RFC2597
	AF12	12	
	AF13	14	
	AF21	18	
	AF22	20	
	AF23	22	
	AF31	26	
	AF32	28	
	AF33	30	
	AF41	34	
	AF42	36	
	AF43	38	
EF (Expedited Forwarding)	46		RFC2598

## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
QoS の有効・無効制御	qos enable
デフォルト CoS の設定	qos cos
トラストモードの変更	qos trust
CoS - 送信キューID 変換テーブルの設定	qos cos-queue
DSCP - 送信キューID 変換テーブルの設定	qos dscp-queue
ポート優先度の設定	qos port-priority-queue

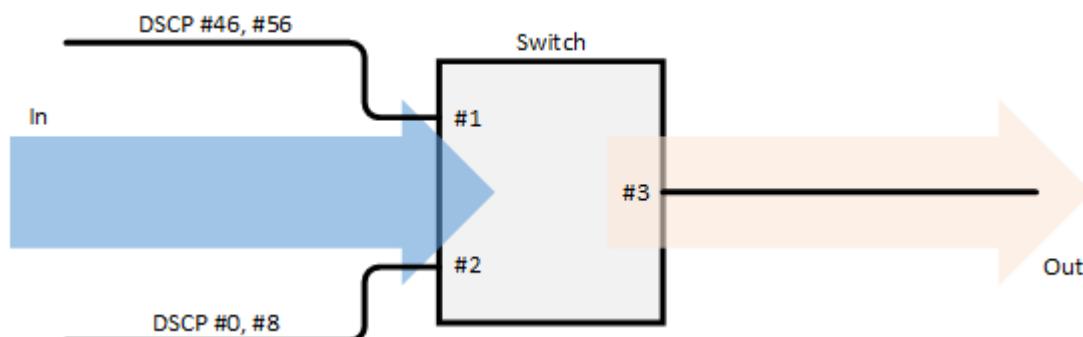
操作項目	操作コマンド
スケジューリング方式の設定	qos scheduling
QoS 機能の設定状態の表示	show qos
LAN/SFPポートの QoS 情報の表示	show qos interface
送信キュー使用率の表示	show qos queue-counters
リマーキングの設定	remark

## コマンド実行例

### DSCP 値を使用した優先制御(SP)

フレームの DSCP 値に基づき送信キューを振り分け、優先制御(SP)を行います。  
SP 優先制御により、LANポート#3 からは DSCP 値の大きなフレームが優先的に処理されるようにします。

- DSCP 優先制御 設定例



1. QoS の有効化と受信ポート ( LAN ポート #1, #2 ) のトラストモードの設定をする。

```

Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust dscp ③
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ④
Yamaha(config-if)#qos trust dscp ⑤
Yamaha(config-if)#exit

```

- ① QoS を有効にする
- ② LAN ポート #1 に対する設定
- ③ トラストモードを DSCP に変更
- ④ LAN ポート #2 に対する設定
- ⑤ トラストモードを DSCP に変更

2. スケジューリング方式を設定する。

```

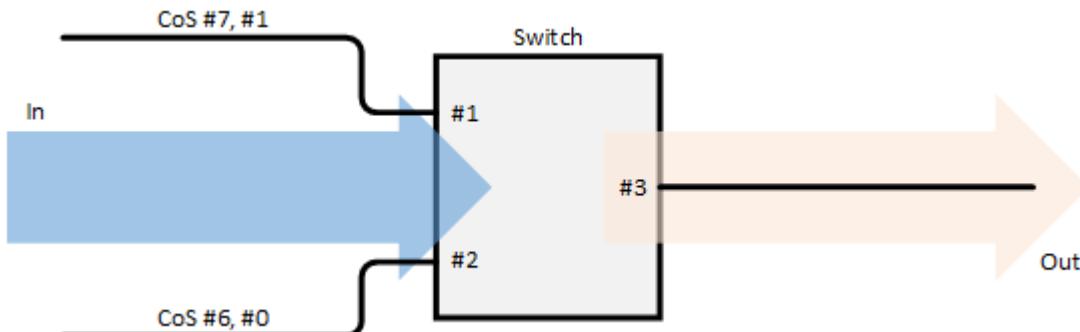
Yamaha(config)# qos scheduling sp

```

## CoS 値を使用した優先制御(WRR)

フレームの CoS 値に基づき送信キューを振り分け、優先制御(WRR)を行います。

- CoS 値を使用した優先制御 設定例



1. QoS の有効化と受信ポート ( LAN ポート #1, #2 ) のトラストモードの設定をする。

```
Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust cos ③
Yamaha(config-if)#qos cos 2 ④
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ⑤
Yamaha(config-if)#qos trust cos ⑥
Yamaha(config-if)#qos cos 2 ⑦
Yamaha(config-if)#exit
```

- ① QoS を有効にする
- ② LAN ポート #1 に対する設定
- ③ トラストモードを CoS に変更
- ④ タグ無しのフレームをCoS値 2 で受信したものとして扱う
- ⑤ LAN ポート #2 に対する設定
- ⑥ トラストモードを CoS に変更
- ⑦ タグ無しのフレームをCoS値 2 で受信したものとして扱う

2. スケジューリング方式を設定する。

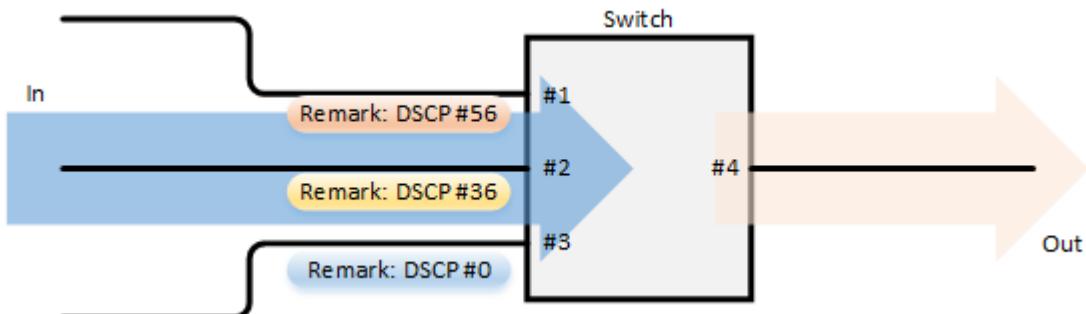
```
Yamaha(config)# qos scheduling wrr
```

## 受信ポート毎に付与したDSCP値に基づく優先制御

受信ポート毎にDSCP値を付与し、そのDSCP値に基づいて送信キューを再度割り当てます。  
以下の例の場合、LAN ポート #1で受信したフレームは最も優先度の高い送信キュー(ID: 7, 重み20%)に格納され、

LAN ポート #2で受信したフレームは次に優先度の高い送信キュー(ID: 5, 重み15%)に格納、  
LAN ポート #3で受信したフレームは3つのLANポートのうち最も優先度の低い送信キュー(ID: 2, 重み10%)に格納されます。

- 受信ポート毎に付与したDSCP値に基づく優先制御 設定例



- 受信ポートごとのリマーキングの設定
    - LAN ポート #1 (port1.1) で受信したフレームをDSCP値 **56** に設定する。
    - LAN ポート #2 (port1.2) で受信したフレームをDSCP値 **36** に設定する。
    - LAN ポート #3 (port1.3) で受信したフレームをDSCP値 **0** に設定する。
1. QoS の有効化および受信ポート( LAN ポート #1, #2, #3 ) のトラストモードとリマーキングの設定をする

```

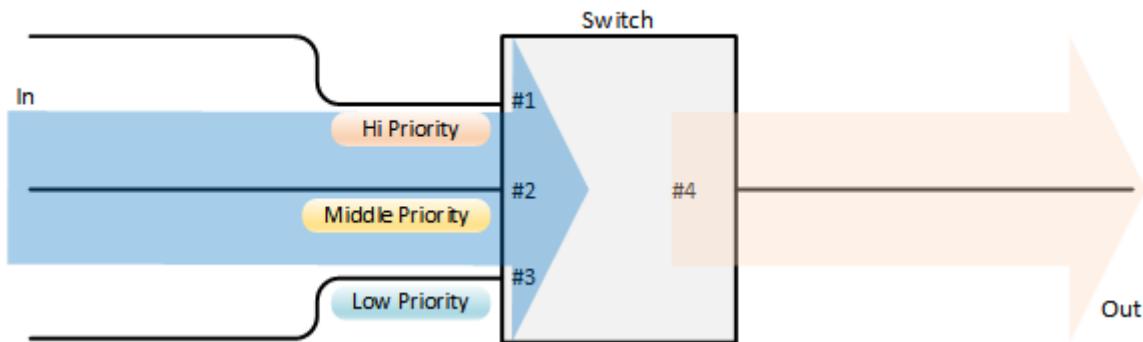
Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust dscp ③
Yamaha(config-if)#remark dscp 56 ④
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ⑤
Yamaha(config-if)#qos trust dscp ⑥
Yamaha(config-if)#remark dscp 36 ⑦
Yamaha(config-if)#exit
Yamaha(config)#interface port1.3 ... ⑧
Yamaha(config-if)#qos trust dscp ⑨
Yamaha(config-if)#remark dscp 0 ⑩
Yamaha(config-if)#exit
  
```

- ① QoS を有効にする
- ② LAN ポート #1 に対する設定
- ③ トラストモードを "DSCP" に変更
- ④ LAN ポート #1 で受信したフレームのDSCP値を 56 に設定
- ⑤ LAN ポート #2 に対する設定
- ⑥ トラストモードを "DSCP" に変更
- ⑦ LAN ポート #1 で受信したフレームのDSCP値を 36 に設定
- ⑧ LAN ポート #3 に対する設定
- ⑨ トラストモードを "DSCP" に変更
- ⑩ LAN ポート #1 で受信したフレームのDSCP値を 0 に設定

### ポート優先トラストモードを使用した優先制御

受信ポート毎に指定したポート優先度に基づいて、送信キューを決定します。

- ポート優先度による優先制御 設定例



- 受信ポートごとの優先度の設定
  - LAN ポート #1 (port1.1) の優先度を **6** に設定する。
  - LAN ポート #2 (port1.2) の優先度を **4** に設定する。
  - LAN ポート #3 (port1.3) の優先度を **2** に設定する。

### 1. QoS の有効化と受信ポート( LAN ポート #1, #2, #3 )のトラストモードの設定をする

```

Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust port-priority ③
Yamaha(config-if)#qos port-priority-queue 6 ④
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ⑤
Yamaha(config-if)#qos trust port-priority ⑥
Yamaha(config-if)#qos port-priority-queue 4 ⑦
Yamaha(config-if)#exit
Yamaha(config)#interface port1.3 ⑧
Yamaha(config-if)#qos trust port-priority ⑨
Yamaha(config-if)#qos port-priority-queue 2 ⑩
Yamaha(config-if)#exit
  
```

- ① QoS を有効にする
- ② LAN ポート #1 に対する設定
- ③ トラストモードを "ポート優先" に変更
- ④ ポート優先度を 6 に設定
- ⑤ LAN ポート #2 に対する設定
- ⑥ トラストモードを "ポート優先" に変更
- ⑦ ポート優先度を 4 に設定
- ⑧ LAN ポート #3 に対する設定
- ⑨ トラストモードを "ポート優先" に変更
- ⑩ ポート優先度を 2 に設定

## 注意事項

- 論理インターフェースに所属している LAN/SFP ポートに QoS の設定が適用されている場合、論理インターフェースの最若番の所属ポートに適用されている設定が、他の所属ポートにも適用されます。

---

## 関連文書

特になし

### 商標名称について

- Zoom はZoom Video Communications, Inc の米国及びその他の国における登録商標または商標です。
- Microsoft Teams は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

# フロー制御

## 機能概要

スイッチングハブは、受信したフレームを一度メモリに蓄積してから中継処理を行います。多くのフレームが同時に送られてきたことで中継処理が間に合わない状態(輻輳状態)になり、蓄積可能なメモリ容量を超えてしまうと、中継対象のフレームが破棄されてしまいます。本製品は、このような輻輳状態を防ぐ機能として、以下の2つを提供します。

- ・ポートが全二重で動作している場合：IEEE 802.3x フロー制御を有効にすることができます。
- ・ポートが半二重で動作している場合：バックプレッシャー機能が常に有効になります。

## 用語の定義

### ビット時間

10BASE のネットワークでは **10Mbps** であるため、1 ビット時間 = 100nsec となる。同様に、100BASE では 10nsec、1000BASE では 1nsec となる。

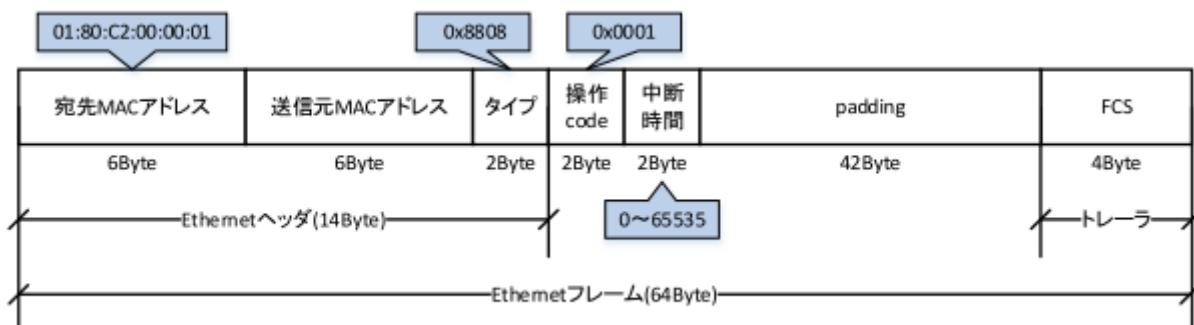
### ジャム信号

データの送信と受信を行なうことができない半二重通信では、データの衝突が発生する可能性がある。送信側の端末は、データ送信中に衝突の発生を監視しており、衝突を検出すると、送信を停止してジャム信号を送信する。ジャム信号送信後はランダムな待ち時間待機し、再度送信処理を行う。なお、IEEE では、ジャム信号について定義されていないが「101010101010101010101010101010」のように、1 と 0 が交互に 32 個並んだビット列になっていることが多い。

## 機能詳細

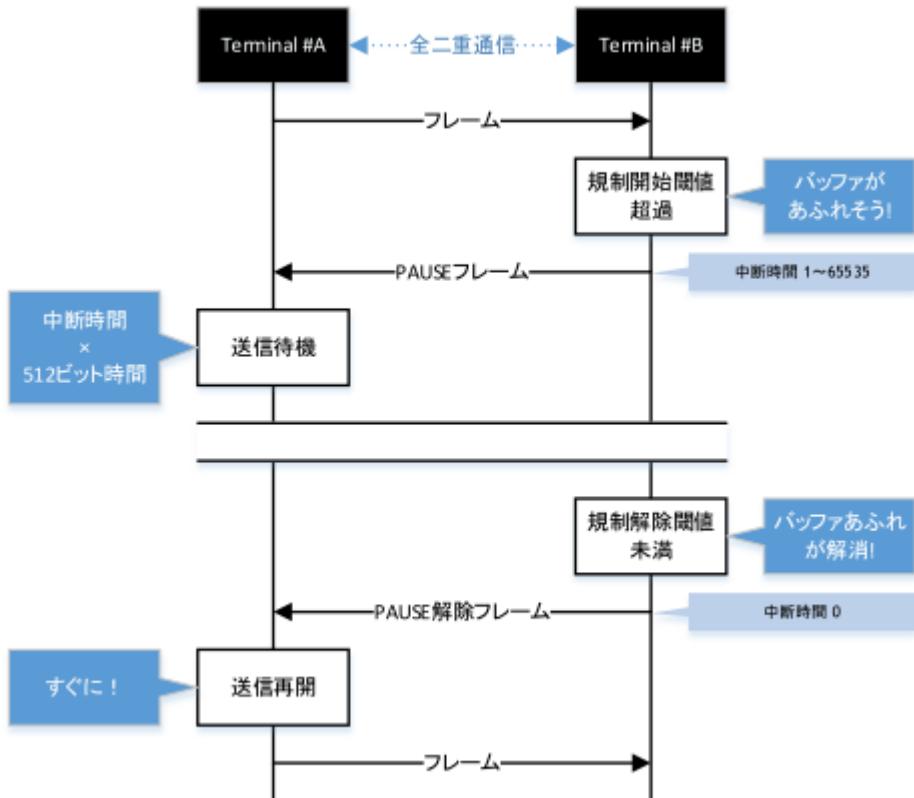
### IEEE 802.3x フロー制御

全二重通信の場合、IEEE802.3x オプションの MAC 制御プロトコルを使用することができます。フロー制御には、下図の **MAC 制御フレーム** が使われます。



フロー制御では、規制開始閾値と規制解除閾値をもとに、以下の動作を行います。

- ・フロー制御 処理フロー



本製品は、MAC 制御フレーム送信側、受信側のどちらにもなることができ、それぞれ以下の動作を行います。

- MAC 制御フレーム送信時の処理
  - パケットバッファにフレームが蓄積され、規制開始しきい値を超えたとき、中断時間 65535 の PAUSE フレームを送信します。
  - パケットバッファの溢れが解消され、規制解除しきい値を下回ったとき、中断時間 0 の PAUSE フレームを送信します。
- MAC 制御フレーム受信時の処理
  - 中断時刻 1 ~ 65535 の PAUSE フレームを受信すると、対応した **ビット時間** が経過する、または、中断時刻 0 の PAUSE フレームを受信する、のいずれかを満たすまで、送信処理を中断します。

フロー制御(MAC 制御フレームの送受信)の有効・無効の設定は **flowcontrol** コマンドを使用します。

システムと送受信LANポート単位で設定可能で、工場出荷時は無効となっています。

各ポートでフロー制御を有効にする際は、システムでフロー制御を有効にする必要があります。

システムでフロー制御を有効にした際に **テールドロップ機能が無効化** されます。

パケットバッファはポート間で共有されており、規制開始しきい値、規制解除しきい値は、パケットバッファ使用状況に応じて動的に変化します。(変更することはできません)

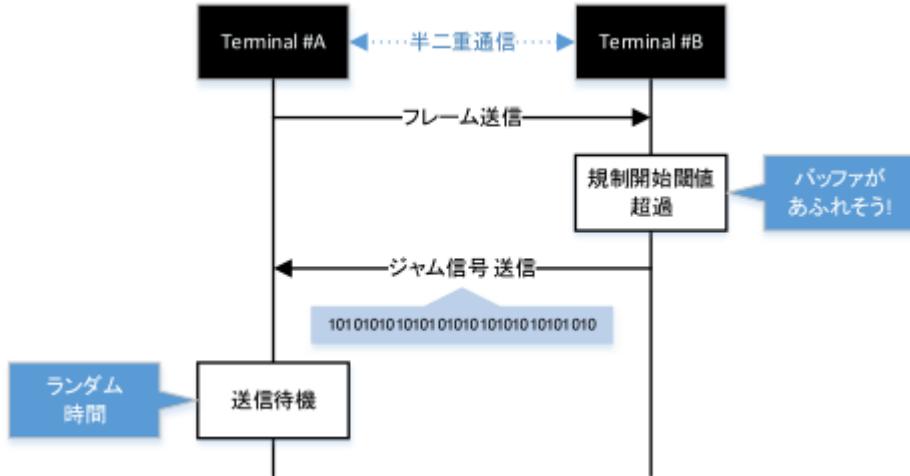
## バックプレッシャー

本製品は、LANポートの受信バッファがあふれそうになると、**ジャム信号** を送信します。

これにより送り手は、CSMA/CD に従い、ランダムな時間を待機してから再度フレームを送信するようになります。

LANポートが **半二重** で動作している場合、**バックプレッシャー機能は常に有効** になります。

- バックプレッシャー 処理フロー



## 関連コマンド

関連コマンドについて、以下に示します。  
詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
フロー制御(IEEE 802.3x PAUSEの送受信)の設定(システム)	flowcontrol
フロー制御(IEEE 802.3x PAUSEの送受信)の設定(インターフェース)	flowcontrol
フロー制御の動作状態の表示	show flowcontrol

## コマンド実行例

LAN ポート #1 のフロー制御を有効にする。  
機能を有効にした後、フロー制御の動作状況を確認する。

```

Yamaha(config)#flowcontrol enable
Yamaha(config)#interface port1.1
Yamaha(config-if)#flowcontrol both
Yamaha(config-if)#end
Yamaha#show flowcontrol port1.1
Port      FlowControl      RxPause TxPause
-----  -----
port1.1    Both            0       64

```

## 注意事項

特になし

## 関連文書

特になし

# ストーム制御

## 機能概要

本製品は、L2ループやDoS攻撃への対策の一つとして、**ストーム制御** 機能を提供します。LANポートごとにブロードキャスト、マルチキャスト、宛先不明ユニキャスト(dlf)宛てフレームを監視し、あらかじめ設定しておいた閾値を超えるとフレームを破棄します。これにより、LANポートにおいて上記フレームによる帯域占有を防ぎます。

## 用語の定義

### ブロードキャストストーム／マルチキャストストーム

ブロードキャストやマルチキャスト宛てフレームが転送され続けてしまうこと。  
スイッチは、ブロードキャストやマルチキャストを受信ポート以外の全ポートにフラッディングします。  
それを受信したスイッチは、同様に受信したポート以外の全ポートにフラッディングします。  
この動作が繰り返されることで、以下のような症状に陥ります。

- ・ ブロードキャスト／マルチキャストフレームで帯域が占有される
- ・ スイッチのCPU負荷が上昇し、正常動作が困難になる
- ・ スイッチに接続されている端末が通信不能に陥る

### ユニキャストストーム

宛先不明ユニキャスト(dlf: Destination Lookup Failure)宛てフレームが転送され続けてしまうこと。  
ARPテーブルに受信デバイスのMACアドレスが登録されていない場合、スイッチは、受信ポート以外の全ポートにフラッディングします。  
これにより、ブロードキャスト／マルチキャストストームと同様の症状に陥ります。

## 機能詳細

ストーム制御の動作仕様について、以下に示します。

1. LANポートに対してストーム制御機能を有効にすることができます。  
初期状態では、**全ポート無効** になっています。
2. 本製品におけるストーム制御は、ブロードキャストフレーム、マルチキャストフレーム、宛先不明ユニキャストフレームの受信をLANポートの帯域に対しどの程度許容するかを百分率で指定します。  
(百分率は、小数点以下第2位まで指定可能とし、100%指定は、ストーム機能を無効にしたことと同じになります。)  
帯域許容率はフレームに共通となり、どのフレームに適用させるかを選択することができます。  
本設定は、**storm-control** コマンドで行います。
3. 許可した帯域を上回るフレームを受信した場合、超過分のフレームは破棄されます。
4. LANポートに設定したストーム制御の情報は、**show storm-control** コマンドで確認することができます。

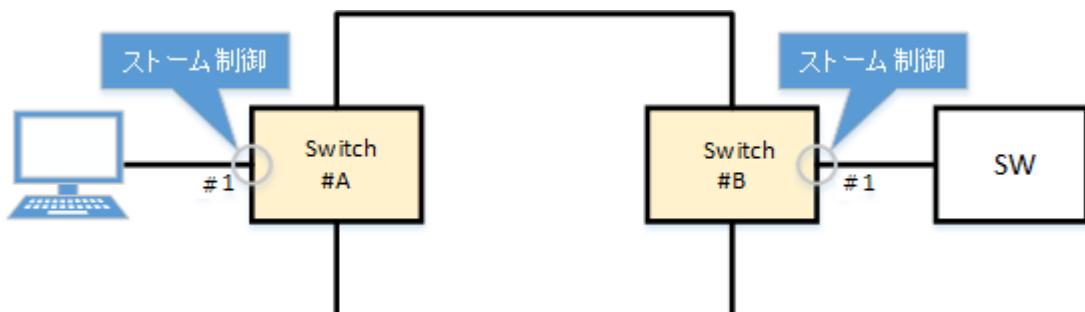
## 関連コマンド

関連コマンドについて、以下に示します。  
コマンドの詳細は、コマンドリファレンスを参照してください。

操作項目	操作コマンド
ストーム制御の設定	storm-control
ストーム制御 受信上限値の表示	show storm-control

## コマンド実行例

LANポート1で受信可能なL2ブロードキャストパケットをポート帯域の30%までに制限します。



```

Yamaha(config)#interface port1.1
Yamaha(config-if)#storm-control broadcast level 30 ①
Yamaha(config-if)#end
Yamaha#
Yamaha#show storm-control
Port      BcastLevel    McastLevel    UcastLevel
port1.1    30.00%       100.00%       100.00%
port1.2    100.00%      100.00%       100.00%
port1.3    100.00%      100.00%       100.00%
port1.4    100.00%      100.00%       100.00%
port1.5    100.00%      100.00%       100.00%
port1.6    100.00%      100.00%       100.00%
port1.7    100.00%      100.00%       100.00%
port1.8    100.00%      100.00%       100.00%
port1.9    100.00%      100.00%       100.00%
port1.10   100.00%      100.00%       100.00%

```

① broadcastを帯域の30%までに制限

## 注意事項

特になし

## 関連文書

- Layer 2機能：独自ループ検出

---

# その他の情報

## SNMP MIBリファレンス

詳細は、本文書のHTML版の「SNMP MIBリファレンス」章をご覧ください。

## コマンドリファレンス

[https://manual.yamaha.com/network/rt/swx2210p/cmdref\\_swx2210p\\_ja.html](https://manual.yamaha.com/network/rt/swx2210p/cmdref_swx2210p_ja.html)

# 本製品で使われるオープンソースソフトウェアのライセンスについて

## オープンソースソフトウェア一覧

本製品が利用しているオープンソースソフトウェアとそのライセンスについて、下表に示します。

- ・ オープンソースソフトウェアとライセンス

オープンソースソフトウェア	ライセンス
u-boot	GPLv2
OpenLLDP	GPLv2
OpenSSL	OpenSSL
Wide-DHCPv6	3-clause BSD
crypt-md5.c	2-clause BSD
ExplorerCanvas	Apache 2.0
jqCanvas	MIT
jqPlot	MIT/GPL2
jQuery	MIT
jQuery Datepicker plugin	MIT
jQuery File Upload Plugin	MIT
jQuery Iframe Transport Plugin	MIT
jQuery XDomainRequest Transport Plugin	MIT
jQuery Migrate	MIT
jQuery UI	MIT
jQuery UI Touch Punch	MIT/GPL2
jQuery UI Widget	MIT
jQuery UI Ympicker	MIT/GPL2
PowerTip	MIT

- ・ GPL/LGPLライセンス適用ソフトウェアについて

本製品には、GNU General Public License (GPL) または GNU Lesser General Public License (LGPL) に基づきライセンスされるソフトウェアが含まれています。

お客様は、当該ソフトウェアのソースコードを入手し、GPL または LGPL に従い、複製、頒布及び改変することができます。

本製品のソースコードのうち GPL または LGPL に基づいてライセンス供与された部分については、弊社より提供(最終出荷日より5年間)することができます。

弊社(または弊社認定の関係者)以外の第三者による、この製品のソフトウェアに対する変更や追加、削除などによって発生したいかなる損害に対しても、弊社は一切責任を負いません。

弊社より提供されたソースコードの再利用は保証されておりません。ソースコードに関して弊社は一切

責任を負いません。

- GPL/LGPLライセンス以外のソフトウェアについて

本製品は著作権者から提示されたライセンス条件に従ってオープンソフトウェアを利用しています。  
ソースコードに関して弊社は一切責任を負いません。

## ライセンス条文一覧

### GPLv2

#### GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,  
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA  
Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

#### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we

want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE  
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any

associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### END OF TERMS AND CONDITIONS

#### How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>  
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author  
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.  
This is free software, and you are welcome to redistribute it  
under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your

school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989  
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

## OpenSSL

### LICENSE ISSUES

---

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.  
See below for the actual license texts.

#### OpenSSL License

---

```
/*
 * Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
```

```
* permission of the OpenSSL Project.  
*  
* 6. Redistributions of any form whatsoever must retain the following  
* acknowledgment:  
* "This product includes software developed by the OpenSSL Project  
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"  
*  
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY  
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE  
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR  
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR  
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,  
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT  
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;  
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)  
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,  
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)  
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED  
* OF THE POSSIBILITY OF SUCH DAMAGE.  
* ======  
*  
* This product includes cryptographic software written by Eric Young  
* (eay@cryptsoft.com). This product includes software written by Tim  
* Hudson (tjh@cryptsoft.com).  
*  
*/
```

#### Original SSLeay License

---

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)  
 * All rights reserved.  
 *  
 * This package is an SSL implementation written  
 * by Eric Young (eay@cryptsoft.com).  
 * The implementation was written so as to conform with Netscapes SSL.  
 *  
 * This library is free for commercial and non-commercial use as long as  
 * the following conditions are aheared to. The following conditions  
 * apply to all code found in this distribution, be it the RC4, RSA,  
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation  
 * included with this distribution is covered by the same copyright terms  
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).  
 *  
 * Copyright remains Eric Young's, and as such any Copyright notices in  
 * the code are not to be removed.  
 * If this package is used in a product, Eric Young should be given attribution  
 * as the author of the parts of the library used.  
 * This can be in the form of a textual message at program startup or  
 * in documentation (online or textual) provided with the package.  
 *  
 * Redistribution and use in source and binary forms, with or without  
 * modification, are permitted provided that the following conditions  
 * are met:  
 * 1. Redistributions of source code must retain the copyright  
 * notice, this list of conditions and the following disclaimer.
```

```

* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*    Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the routines from the library
*    being used are not cryptographic related :).
* 4. If you include any Windows specific code (or a derivative thereof) from
*    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.

*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

```

## Wide-DHCPv6

\$KAME: COPYRIGHT,v 1.2 2004/07/29 19:02:18 jinmei Exp \$

Copyright (C) 1998-2004 WIDE Project.  
All rights reserved.

Redistribution and use in source and binary forms, with or without  
modification, are permitted provided that the following conditions  
are met:

1. Redistributions of source code must retain the above copyright  
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright  
notice, this list of conditions and the following disclaimer in the  
documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors  
may be used to endorse or promote products derived from this software  
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND  
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE  
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE  
ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE

FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## crypt-md5.c

```
* Copyright (c) 2003 Poul-Henning Kamp
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*   1. Redistributions of source code must retain the above copyright
*      notice, this list of conditions and the following disclaimer.
*   2. Redistributions in binary form must reproduce the above copyright
*      notice, this list of conditions and the following disclaimer in the
*      documentation and/or other materials provided with the distribution.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
```

## ExplorerCanvas

Copyright 2006 Google Inc.

Licensed under the Apache License, Version 2.0 (the "License");  
you may not use this file except in compliance with the License.  
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software  
distributed under the License is distributed on an "AS IS" BASIS,  
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.  
See the License for the specific language governing permissions and  
limitations under the License.

## jqCanvas

### The MIT License

Copyright (c) 2008 David Kwast <david \*dot\* kwast \*at\* gmail>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## jqPlot

### Title: jqPlot Charts

Pure JavaScript plotting plugin for jQuery.

### About: Version

version: 1.0.4  
revision: 1121

### About: Copyright & License

Copyright (c) 2009-2012 Chris Leonello  
jqPlot is currently available for use in all personal or commercial projects under both the MIT and GPL version 2.0 licenses. This means that you can choose the license that best suits your project and use it accordingly.

See <GPL Version 2> and <MIT License> contained within this distribution for further information.

The author would appreciate an email letting him know of any substantial use of jqPlot. You can reach the author at: chris at jqplot dot com or see <http://www.jqplot.com/info.php>. This is, of course, not required.

If you are feeling kind and generous, consider supporting the project by making a donation at: <http://www.jqplot.com/donate.php>.

sprintf functions contained in jqplot.strftime.js by Ash Searle:

```
version 2007.04.27
author Ash Searle
http://hexmen.com/blog/2007/03/printf-sprintf/
http://hexmen.com/js/sprintf.js
The author (Ash Searle) has placed this code in the public domain:
"This code is unrestricted: you are free to use it however you like."
```

## jQuery

jQuery JavaScript Library v1.9.1  
<http://jquery.com/>

Includes Sizzle.js  
<http://sizzlejs.com/>

Copyright 2005, 2012 jQuery Foundation, Inc. and other contributors  
Released under the MIT license  
<http://jquery.org/license>

Date: 2013-2-4

## jQuery DateTimePicker plugin

Copyright (c) 2013 <http://xdsoft.net>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## jQuery File Upload Plugin / jQuery Iframe Transport Plugin / jQuery XDomainRequest Transport Plugin

MIT License

Copyright © 2010 Sebastian Tschan, <https://blueimp.net>

Permission is hereby granted, free of charge, to any person obtaining a copy

of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## jQuery Migrate

Copyright jQuery Foundation and other contributors, <https://jquery.org/>

This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at <https://github.com/jquery/jquery-migrate>

The following license applies to all parts of this software except as documented below:

====

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

All files located in the node\_modules and external directories are externally maintained libraries used by this software which have their own licenses; we recommend you read them, as their terms may differ from

the terms above.

## jQuery UI

Copyright jQuery Foundation and other contributors, <https://jquery.org/>

This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at <https://github.com/jquery/jquery-ui>

The following license applies to all parts of this software except as documented below:

====

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CC0. Sample code is defined as all source code contained within the demos directory.

CC0: <http://creativecommons.org/publicdomain/zero/1.0/>

====

All files located in the node\_modules and external directories are externally maintained libraries used by this software which have their own licenses; we recommend you read them, as their terms may differ from the terms above.

## jQuery UI Touch Punch

jQuery UI Touch Punch 0.2.3

Copyright 2011–2014, Dave Furrero

Dual licensed under the MIT or GPL Version 2 licenses.

Depends:

jquery.ui.widget.js  
jquery.ui.mouse.js

## jQuery UI Ympicker

jQuery UI Ympicker 1.8.21

Copyright 2012, AUTHORS.txt (<http://jqueryui.com/about>)

Dual licensed under the MIT or GPL Version 2 licenses.

<http://jquery.org/license>

<http://docs.jquery.com/UI/Ympicker>

Depends:

jquery.ui.core.js

## PowerTip

Copyright (c) 2018 Steven Benner (<http://stevenbenner.com/>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

© 2025 Yamaha Corporation

Published 03/2025

YJ-A0