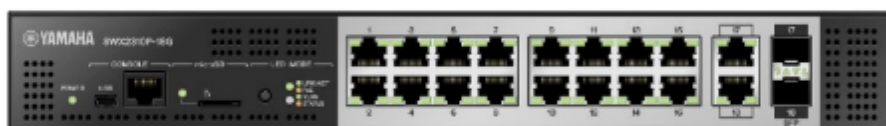


SWX2310P series

Technical Data



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
ログインパスワードを忘れてしまった場合の対処方法	8
関連コマンド	8
コマンド実行例	9
ユーザーを追加する	9
注意事項	9
関連文書	10
LED制御	11
機能概要	11
用語の定義	11
機能詳細	11
POWER LED	11
SD LED	12
ポートLED	12
スタックID表示 LED	19
関連コマンド	19
コマンド実行例	20
LAN/SFP ポートの状態確認	20
LAN/SFP ポート ループ検出状態の確認	20
初期LEDモードの設定	21
外部メモリの利用	22
機能概要	22
用語の定義	22
機能詳細	22
利用可能な外部メモリ	22
フォルダ構成	22
SDカードのマウント/アンマウント	23
SDカードブート(ファームウェア、コンフィグ)	23
SDカードブート自動適用(ファームウェア、コンフィグ)	24
ファームウェア更新	26
コンフィグファイルの保存・コピー	26
ログファイルの保存	26
技術サポート情報の保存	27

統計情報の保存	27
システム情報のバックアップ・リストア	27
関連コマンド一覧	28
コマンド実行例	28
SDカードのアンマウント	28
SDカードのマウント	28
ログファイルのバックアップ	28
技術サポート情報の保存	29
注意事項	29
関連文書	29
起動情報の管理	30
機能概要	30
関連コマンド	30
コマンド実行例	30
起動情報の表示	30
起動情報のクリア	31
注意事項	31
関連文書	31
筐体情報の表示	32
機能概要	32
機能詳細	32
コマンドによる筐体情報の表示	32
技術サポート情報のリモート取得	35
技術サポート情報の外部メモリへの保存	36
関連コマンド	36
コマンド実行例	36
製品情報の表示	36
稼働情報の表示	37
技術サポート情報の表示	37
注意事項	38
関連文書	38
システム自己診断	39
機能概要	39
用語の定義	39
機能詳細	39
診断	39
診断結果表示	40
オンデマンド診断結果削除	40
テスト詳細	40
Loading Test	40
RTC Test	41
Packet Processor Test	41
PHY Test	41
Thermal Test	41
Fan Test	41
Thermal Sensor Test	41
PoE Test	41

SFP Test	41
関連コマンド.....	41
コマンド実行例.....	42
システム自己診断結果の表示.....	42
オンデマンド診断の実行	43
オンデマンド診断結果の削除.....	43
注意事項	43
関連文書	43
ケーブル診断	44
機能概要	44
用語の定義	44
機能詳細	44
ケーブル診断方法	44
関連コマンド.....	44
コマンド実行例.....	45
ケーブル診断の実行.....	45
前回の診断結果の確認	45
注意事項	45
関連文書	45
コンフィグ管理	46
機能概要	46
用語の定義	46
機能詳細	46
ランニングコンフィグ	46
スタートアップコンフィグ	46
デフォルトコンフィグ	47
起動時のコンフィグファイルの決定.....	47
TFTPによるコンフィグファイルの制御.....	47
関連コマンド.....	48
コマンド実行例.....	49
スタートアップコンフィグの選択	49
ランニングコンフィグの保存.....	49
スタートアップコンフィグのコピー.....	49
スタートアップコンフィグの消去	50
注意事項	50
関連文書	50
リモートアクセス制御	51
機能概要	51
用語の定義	51
機能詳細	51
関連コマンド.....	52
コマンド実行例.....	53
TELNETサーバーに対するアクセス制御	53
SSHサーバーに対するアクセス制御.....	54
HTTPサーバーに対するアクセス制限	54
TFTPサーバーに対するアクセス制限.....	55
SNMPサーバーに対するアクセス制限	55

注意事項	55
関連文書	56
時刻管理	57
機能概要	57
用語の定義	57
機能詳細	57
日付・時刻の手動設定	57
日付・時刻の自動設定	57
タイムゾーンの設定	58
サマータイムの設定	58
関連コマンド	58
コマンド実行例	59
時刻の手動設定	59
時刻の自動設定	59
サマータイムの設定	59
注意事項	60
関連文書	60
SNMP	61
機能概要	61
用語の定義	61
機能詳細	61
SNMPv1	61
SNMPv2c	62
SNMPv3	62
SNMPサーバーへのアクセス制限	63
プライベートMIB	63
関連コマンド	64
コマンド実行例	64
SNMPv1 設定例	64
SNMPv2c 設定例	64
SNMPv3 設定例	65
注意事項	65
関連文書	66
RMON	67
機能概要	67
用語の定義	67
機能詳細	67
グループ共通	68
イーサネット統計情報グループ	68
履歴グループ	69
アラームグループ	70
イベントグループ	72
SNMPマネージャーのSetRequestによる設定	73
関連コマンド	73
コマンド実行例	74
イーサネット統計情報グループの設定	74
履歴グループの設定	74

アラーム・イベントグループの設定	75
注意事項	76
関連文書	76
sFlow	77
機能概要	77
用語の定義	78
機能詳細	78
関連コマンド	79
コマンド実行例	80
注意事項	80
関連文書	81
SYSLOG	82
機能概要	82
用語の定義	82
機能詳細	82
関連コマンド一覧	83
コマンド設定例	83
注意事項	84
関連文書	84
ファームウェア更新	85
機能概要	85
用語の定義	85
機能詳細	85
更新ファームウェア送付による更新	85
HTTPクライアントを使用した更新	86
SDカードを使用した更新	88
書き込み後の再起動	88
関連コマンド	89
コマンド実行例	89
HTTPクライアントを使用した更新	89
HTTPクライアントを使用した更新(プロキシ環境下)	90
SDカードを使用した更新	91
注意事項	92
関連文書	92
L2MS (Layer2 Management Service)	93
機能概要	93
用語の定義	93
機能詳細	94
対応機種	94
使用方法	94
L2MSのプロトコル	95
エージェントの監視	95
エージェントの占有	95
エージェントの操作	96
エージェントからの情報通知	99
接続端末の監視	100
関連コマンド	101

コマンド実行例	102
エージェントの監視設定	102
端末の管理機能の設定	102
L2MS制御フレームの送受信設定	103
イベント監視機能の設定	103
ゼロコンフィグ機能の使用の有無	104
注意事項	104
機器構成について	104
端末の監視について	104
他機能との併用について	105
SYSLOGメッセージ一覧	106
関連文書	116
メール通知	117
機能概要	117
用語の定義	117
機能詳細	117
動作	117
メールサーバーの設定	117
メールテンプレートの設定	118
メール通知に対応している機能	119
メール本文の例	122
関連コマンド	126
注意事項	127
関連文書	127
LLDP	128
機能概要	128
用語の定義	128
機能詳細	128
動作仕様	128
TLV一覧	130
サポートMIB	133
関連コマンド	133
コマンド実行例	134
LLDPフレームの送受信の設定	134
LLDP インターフェース状態の表示	135
LLDP 接続機器の情報の表示	135
注意事項	136
関連文書	136
LLDP自動設定(AP連携)	137
機能概要	137
用語の定義	137
LLDP	137
機能詳細	137
基本仕様	137
RADIUSサーバーの自動設定	137
ヤマハ無線APの死活監視	140
ヤマハ無線AP停止前のログ保存	141

関連コマンド	142
設定例	142
注意事項	142
関連文書	142
端末監視	144
機能概要	144
用語の定義	145
機能詳細	145
Ping (ICMP Echo request / reply) による監視	145
フレーム受信量による監視	145
LLDP による監視	146
関連コマンド	146
Web GUI による設定	146
端末監視 トップページ	146
監視端末の新規追加・変更	147
監視端末の状態確認	149
注意事項	149
関連文書	149
パフォーマンスの観測	150
機能概要	150
用語の定義	151
機能詳細	151
リソース・トラフィック使用量の観測	151
観測データのバックアップ	151
観測データのエクスポートデータ	152
関連コマンド	153
Web GUI による設定	153
リソース使用量の参照	154
トラフィック使用量の参照	154
消費電力量の参照	156
観測データのバックアップ・クリア・エクスポート	156
注意事項	159
関連文書	159
スケジュール機能	160
機能概要	160
用語の定義	160
機能詳細	160
時刻トリガー	161
イベントトリガー	162
アクション	162
関連コマンド	163
設定例	163
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	163
microSD挿入時に内部情報を取得	163
実行禁止コマンド	164
SYSLOG	165
注意事項	165

関連文書	166
Dante最適設定機能	167
機能概要	167
用語の定義	167
機能詳細	167
LLDPによる自動最適設定	170
Web GUIからの手動最適設定	171
関連コマンド	171
コマンド実行例	172
LLDPによる自動最適設定	172
注意事項	172
関連文書	173
ProAV設定	174
機能概要	174
用語の定義	174
ProAVプロファイル詳細	174
Danteプロファイル	174
NDIプロファイル	179
複数プロファイル併用時の設定	181
キッティングとトラブルシューティング	184
[キッティング] IPアドレスを意識せずに初期設定する	184
[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	188
[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	190
[トラブルシューティング] Dante機器の状態を確認する	192
注意事項	193
関連文書	193
商標名称について	193
ADECIAとのセキュリティ連携	194
機能概要	194
用語の定義	194
機能詳細	195
ADECIAコンポーネントの自動認識	195
スイッチの遠隔制御	195
スイッチからの状態通知	196
関連コマンド	197
セキュリティ連携の初期設定	197
注意事項	197
関連文書	197
スタック機能	198
機能概要	198
用語の定義	198
機能詳細	199
スタックの構成	199
メンバースイッチ間の接続	200
メインスイッチの選出とMACアドレスの付与	200
仮想スイッチに対する操作	201
スタック構成時のスイッチの状態	202

異常状態の検出と措置	202
関連コマンド	204
スタックの初期設定	204
必要機材の準備	204
メンバースイッチの設定	204
メンバースイッチの接続	207
メンバースイッチの交換	208
SDカードを使用した交換手順	208
SDカードを使用しない交換手順	209
ファームウェア更新	210
ファームウェアの平行更新	211
ファームウェアのシーケンシャル更新	212
注意事項	212
関連文書	214
初期設定一覧	215
インターフェース制御機能	219
インターフェース基本機能	219
機能概要	219
用語の定義	219
機能詳細	219
インターフェースの種類	219
インターフェース制御	219
LAN/SFPポートの初期状態	221
ポートミラーリング	221
フレームカウンター	221
SFPモジュールの受光レベル監視	223
送信キューの使用率監視	224
ifIndexの割り当て	224
関連コマンド	224
コマンド実行例	225
LANポートに対する基本設定	225
ポートミラーリング設定	226
LAN/SFPポートの情報表示	226
注意事項	227
関連文書	227
リンクアグリゲーション	228
機能概要	228
用語の定義	228
機能詳細	229
スタティック/LACP リンクアグリゲーション 共通仕様	229
スタティック リンクアグリゲーション	230
LACP リンクアグリゲーション	230
関連コマンド	232
コマンド実行例	232
スタティック論理インターフェースの設定	232
LACP 論理インターフェースの設定	235
注意事項	240

関連文書	240
ポート認証機能	241
機能概要	241
用語の定義	241
機能詳細	242
IEEE 802.1X認証	243
MAC認証	244
Web認証	245
認証機能の併用	249
ホストモード	251
ダイナミックVLAN	251
未認証・認証失敗ポートのVLAN	252
EAPパススルー機能	252
RADIUSサーバーに通知する属性値	252
関連コマンド	253
コマンド実行例	254
IEEE 802.1X認証の設定	254
MAC認証の設定	256
Web認証の設定	257
注意事項	259
関連文書	259
ポートセキュリティ機能	260
機能概要	260
用語の定義	260
機能詳細	260
アクセスする端末を制限	260
関連コマンド	261
コマンド実行例	261
アクセスする端末を制限	261
注意事項	262
関連文書	262
PoE制御	263
機能概要	263
用語の定義	263
機能詳細	263
PoE 給電機能の有効/無効 制御	263
給電クラスと同時給電可能なポートの最大数	263
ガードバンド	264
給電優先度	264
PoE給電動作	264
LLDP による給電設定	265
関連コマンド	265
コマンド実行例	265
PoEポートの給電設定	265
注意事項	266
関連文書	266
Layer 2機能	267

フォワーディングデータベース(FDB).....	267
機能概要.....	267
用語の定義.....	267
機能詳細.....	267
FDBエントリー.....	267
MACアドレスの自動学習.....	269
MACアドレスの手動設定.....	269
関連コマンド.....	270
コマンド実行例.....	270
FDBの参照.....	270
ダイナミックエントリーの削除.....	270
ダイナミックエントリー エージング時間の変更.....	271
スタティックエントリーの登録.....	271
スタティックエントリーの削除.....	271
注意事項.....	271
関連文書.....	271
VLAN.....	272
機能概要.....	272
用語の定義.....	272
機能詳細.....	272
VLAN IDの定義.....	272
LAN/SFPポートに対するVLAN設定.....	272
VLANに対するアクセス制御.....	273
デフォルトVLAN.....	274
ネイティブVLAN.....	274
プライベートVLAN.....	274
ボイスVLAN.....	275
関連コマンド.....	276
関連コマンド一覧.....	276
コマンド実行例.....	276
ポートベースVLAN の設定.....	276
タグVLAN の設定.....	278
プライベートVLAN の設定.....	279
ボイスVLAN の設定.....	282
注意事項.....	283
関連文書.....	283
マルチプルVLAN.....	284
機能概要.....	284
用語の定義.....	284
機能詳細.....	284
動作仕様.....	284
マルチプルVLANグループ間の通信例.....	285
VLAN間ルーティング可能な場合の通信例.....	285
関連コマンド.....	286
コマンド実行例.....	286
マルチプルVLANの設定例1.....	286
マルチプルVLANの設定例2.....	288

注意事項	291
関連文書	291
スパニングツリー	292
機能概要	292
用語の定義	292
機能詳細	293
関連コマンド	293
コマンド実行例	294
MSTP 設定例	294
注意事項	302
関連文書	302
独自ループ検出	303
機能概要	303
用語の定義	303
機能詳細	303
ループ検出 動作仕様	303
ループ検出例	305
関連コマンド	306
コマンド実行例	306
注意事項	308
関連文書	309
DHCPスヌーピング	310
機能概要	310
用語の定義	310
機能詳細	310
DHCPスヌーピングの有効化	311
バインディングデータベース	311
DHCPスヌーピングのポート種別	311
Option 82	312
DHCPパケットのレート制限	314
DHCPスヌーピングの統計情報	314
SYSLOGへの出力	314
関連コマンド	314
コマンド実行例	315
信頼するインターフェイスを指定	315
DHCPスヌーピングの有効化	315
注意事項	316
Layer 3機能	317
IPv4/IPv6共通設定	317
機能概要	317
用語の定義	317
機能詳細	317
DNS クライアントの設定	317
等コストマルチパスの設定	318
関連コマンド	318
コマンド実行例	319
DNSクライアントの設定	319

等コストマルチパス.....	320
注意事項.....	320
関連文書.....	320
IPv4基本設定.....	321
機能概要.....	321
用語の定義.....	321
機能詳細.....	321
IPv4アドレスの設定.....	321
Auto IP機能.....	321
ルート情報の設定.....	322
ARP テーブルの設定.....	323
MTUの設定.....	323
関連コマンド.....	324
コマンド実行例.....	325
IPv4ネットワーク環境の設定 (DHCP).....	325
注意事項.....	326
関連文書.....	326
IPv6基本設定.....	327
機能概要.....	327
用語の定義.....	327
機能詳細.....	327
IPv6アドレスの設定.....	327
ルート情報の設定.....	328
Neighbor キャッシュテーブルの設定.....	329
MTUの設定.....	330
DHCPv6-PDクライアントの設定.....	330
関連コマンド.....	331
コマンド実行例.....	331
IPv6ネットワーク環境の設定 (固定設定).....	331
IPv6ネットワーク環境の設定 (RAによる自動設定).....	332
IPv6ネットワーク環境の設定 (DHCPv6).....	333
IPv6ネットワーク環境の設定 (DHCPv6-PD).....	334
注意事項.....	335
関連文書.....	335
スタティックルーティング.....	336
機能概要.....	336
用語の定義.....	336
機能詳細.....	336
VLANインターフェースルート情報.....	336
スタティックルート情報.....	336
経路表の表示.....	337
ルート情報の優先度(管理距離).....	338
ルーティング機能の有効化.....	338
関連コマンド.....	338
注意事項.....	338
関連文書.....	339
IPマルチキャスト機能.....	340

IGMP Snooping	340
機能概要	340
用語の定義	341
機能詳細	342
関連コマンド	344
コマンド実行例	344
IGMP Snooping の設定(マルチキャストルーターあり)	344
IGMP Snooping の設定(マルチキャストルーターなし)	346
IGMP Snooping の設定(双方向でデータ配信する場合)	348
IGMP Snooping の設定(複数のマルチキャスト環境をVLANで分離する場合)	352
注意事項	355
関連文書	355
MLD Snooping	356
機能概要	356
用語の定義	356
機能詳細	357
関連コマンド	358
コマンド実行例	359
MLD Snooping の設定(マルチキャストルーターあり)	359
MLD Snooping の設定(マルチキャストルーターなし)	360
注意事項	363
関連文書	363
トラフィック制御機能	364
ACL	364
機能概要	364
用語の定義	364
機能詳細	365
アクセスリストの生成	365
インターフェースへの適用	365
LAN/SFPポートおよび論理インターフェースに対する設定	365
VLANインターフェースに対する設定	366
関連コマンド	366
コマンド実行例	367
IPv4アクセスリストの設定	367
IPv6アクセスリストの設定	373
MACアクセスリストの設定	377
注意事項	380
関連文書	380
QoS	381
機能概要	381
用語の定義	381
機能詳細	382
QoS の有効・無効制御	382
QoS 処理フロー	382
送信キューの割り当て	383
送信キューの割り当て(スイッチ本体から送信されるフレーム)	385
トラフィック分類	385

プレマーキング	386
メータリング・ポリシング・リマーキング	387
送信キューへの格納	390
スケジューリング	391
シェーピング	392
Web会議アプリケーション向け最適設定	392
別表1. 標準 PHB (RFC 推奨値)	393
関連コマンド	394
コマンド実行例	396
DSCP 値を使用した優先制御(SP)	396
アクセスリストを使用した優先制御(SP+WRR)	397
ポート優先トラストモードを使用した優先制御	401
アクセスリストを使用した帯域制御(ツインレート・個別ポリサー)	402
アクセスリストを使用した帯域制御(シングルレート・集約ポリサー)	404
注意事項	406
関連文書	406
商標名称について	406
フロー制御	407
機能概要	407
用語の定義	407
機能詳細	407
IEEE 802.3x フロー制御	407
バックプレッシャー	408
関連コマンド	409
コマンド実行例	409
注意事項	409
関連文書	409
ストーム制御	410
機能概要	410
用語の定義	410
機能詳細	410
関連コマンド	411
コマンド実行例	411
注意事項	411
関連文書	411
アプリケーション層機能	412
RADIUSサーバー	412
機能概要	412
用語の定義	413
機能詳細	414
ルート認証局	414
RADIUSクライアントの設定	415
ユーザーの登録	415
認証方式の制限	416
RADIUSサーバー機能の有効化	416
設定内容の動作への反映	416
クライアント証明書の発行	417

クライアント証明書の失効	418
証明書のメール送信.....	418
設定および証明書の確認	419
クライアント証明書の期限切れ事前メール通知.....	420
ユーザー情報のインポートとエクスポート	421
すべてのRADIUSサーバー関連情報のバックアップとリストア	421
ヤマハ無線アクセスポイント(WLXシリーズ)でバックアップしたRADIUSサーバー関連情報のリス トア.....	422
SYSLOGの出力情報.....	423
関連コマンド	423
設定例.....	424
RADIUSサーバー機能とポート認証機能を同時に利用する場合	424
ヤマハルーターのログインユーザーの認証でRADIUSサーバー機能を利用する場合.....	425
ヤマハ無線アクセスポイント(WLXシリーズ)のMAC認証でRADIUSサーバー機能を利用する場合.	426
証明書を使ってヤマハ無線アクセスポイント(WLXシリーズ)に接続するためにRADIUSサーバー機 能を利用する場合	428
注意事項	430
関連文書	432
その他の情報.....	433
SNMP MIBリファレンス.....	433

重要なお知らせ

ログインセキュリティ

機能概要

基本機能

本製品では、サイバーセキュリティ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いて適切なユーザー・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(管理パスワード)が初期設定から変更されていない場合、特権パスワード(管理パスワード)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(管理パスワード)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

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 (管理パスワード) を変更する
 - 特権パスワード (管理パスワード) 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。

ゲストユーザー

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(管理パスワード)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ゲストユーザーになります。

特権パスワード(管理パスワード)

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.2.02.23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(管理パスワード)の設定

enable password コマンドを使用して特権パスワード(管理パスワード)を設定します。
特権パスワード(管理パスワード)は、以下の用途で使います。

- ・ 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(管理パスワード)として **admin** が設定されていますが、特権パスワード(管理パスワード)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(管理パスワード)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。
- ・ 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。

	コンソール		Web GUI	
	管理ユーザー(権限有り)	ゲストユーザー(権限無し)	管理ユーザー(権限有り)	ゲストユーザー(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。

ゲスト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(管理パスワード)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

SWX2310P-28GT Rev.2.02.06 (Tue Mar 13 08:41:39 2018)
Copyright (c) 2015-2016 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}

SSH	Login access from SSH 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。

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 でログインした場合、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。

SWX2310P-18G

SWX2310P

初期管理ユーザー "admin" のパスワードを初期パスワードから変更してください。

新しいパスワードを入力してください。

パスワード強度

弱

中

強

最強

確認のため、再度新しいパスワードを入力してください。

保存

Yamaha Corporation

ログインパスワードを忘れてしまった場合の対処方法

シリアルコンソール を接続した状態で本製品を起動し、起動処理中に **I (大文字のアイ)** を入力することにより工場出荷状態で起動させることができます。

なお、SDカードブートを使用している場合は、本機能は動作しません。

```
BootROM - X.XX
Booting from SPI flash

SWX2310P-28GT BootROM Ver.1.00      ##### BootROM Verが表示されたらすぐに「I」を入力 #####

Initialize or not?(y/n) y

Loading config0 because can't read config in SD card.
Starting .....
Loading configuration ... Done!

SWX2310P-28GT Rev.2.02.06 (Tue Mar 13 08:41:39 2018)
Copyright (c) 2015-2016 Yamaha Corporation. All Rights Reserved.
```

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(管理パスワード)の設定	enable password

操作項目	操作コマンド
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

ユーザーを追加する

ユーザー **yamaha** に **管理者権限** 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:

SWX2310P-28GT Rev.2.02.06 (Tue Mar 13 08:41:39 2018)
Copyright (c) 2015-2016 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.2.02.23 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.2.02.23 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.2.02.23 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.2.02.23 より新しいファームウェアに更新する

Rev.2.02.23 以前のファームウェアでの設定

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

Rev.2.02.23 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。
 - 保守VLANと異なるネットワークセグメントからTELNET,SSH,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".
```

- 以下のコマンドを実行することはできません。また、Web GUIで同様の設定変更を行うことはできません。
 - ip address / no ip address
※ ただし、ip address dhcpのみ実行可能
 - auto-ip / no auto-ip
 - ipv6 / no ipv6
 - ipv6 address / no ipv6 address
 - management interface / no management interface

関連文書

- [リモートアクセス制御](#)

LED制御

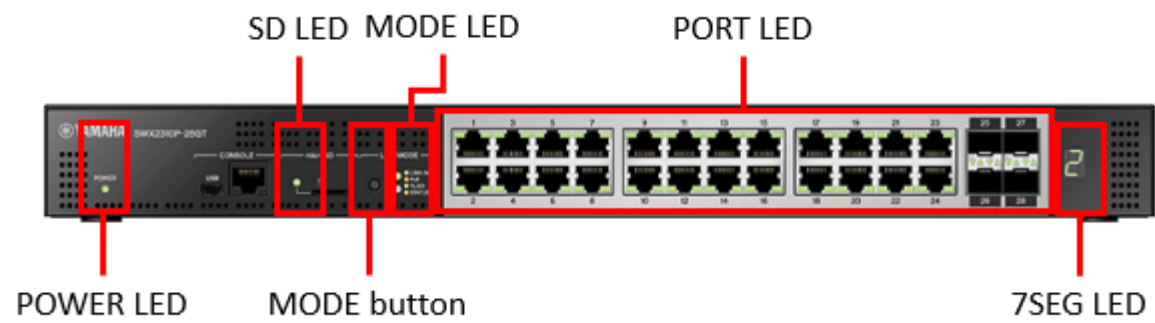
機能概要

本製品の本体にあるLED、ボタンは以下のとおりです。

- ・ LED、ボタンの種類

LEDの種類	説明
POWER LED	通電状態を表示します。
microSD LED	microSD カードの接続、使用状態を表示します。
ポートLED	LAN/SFPケーブルの接続、使用状態を表示します。
MODEボタン	LEDモードを切り替えます。
スタックID表示 LED (7SEG LED)	スタック番号を表示します。SWX2310P-28GTのみ搭載しています。

各LEDとボタンの配置を以下に示します。



用語の定義

ポートLEDの点灯凡例

以降の説明で使用するポートLEDの点灯は、以下で表します。

- ・ ポートLED点灯凡例



機能詳細

POWER LED

POWER LEDは、本製品の通電状態を表示します。
POWER LEDの点灯パターンとその状態は以下のとおりです。

- ・ POWER LEDの点灯パターンと状態

POWER LED 点灯パターン	状態
消灯	電源がOFFです。
緑色 点滅	電源がONで、システムを起動中です。
緑色 点灯	電源がONで、システムが正常に動作しています。
橙色 点灯	電源がONで、システムに異常が発生しています。

以下の異常を検知するとPOWER LEDが橙色で点灯します。
検知された異常の状態を確認して適切に対応してください。

- ・ファンの停止
本製品で発生した熱を排出するファンが停止しています。
すぐに使用を中止し、必ずご購入の販売店に修理や点検をご依頼ください。
- ・本製品内部温度の異常
本製品内部の温度が異常です。
本製品内部の温度が適正になるように、設置環境を見直して本製品を正しく設置してください。

show environment コマンドで、温度異常とファン異常を確認できます。

SD LED

SD LEDは、microSDカードの接続、使用状態を表示します。
SD LEDの点灯パターンとその状態は以下のとおりです。

- ・SD LEDの点灯パターンと状態

SD LED 点灯パターン	状態
消灯	microSDカードが挿入されていないか、アンマウント状態で使用できません。
緑色 点滅	microSDカードにアクセスしています。
緑色 点灯	microSDカードが挿入されており、使用できます。

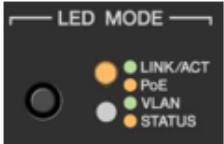
緑色点滅中は、microSDカードにアクセスしているため、microSDカードを取り出さないでください。

ポートLED

表示モードと表示モードの切り替え

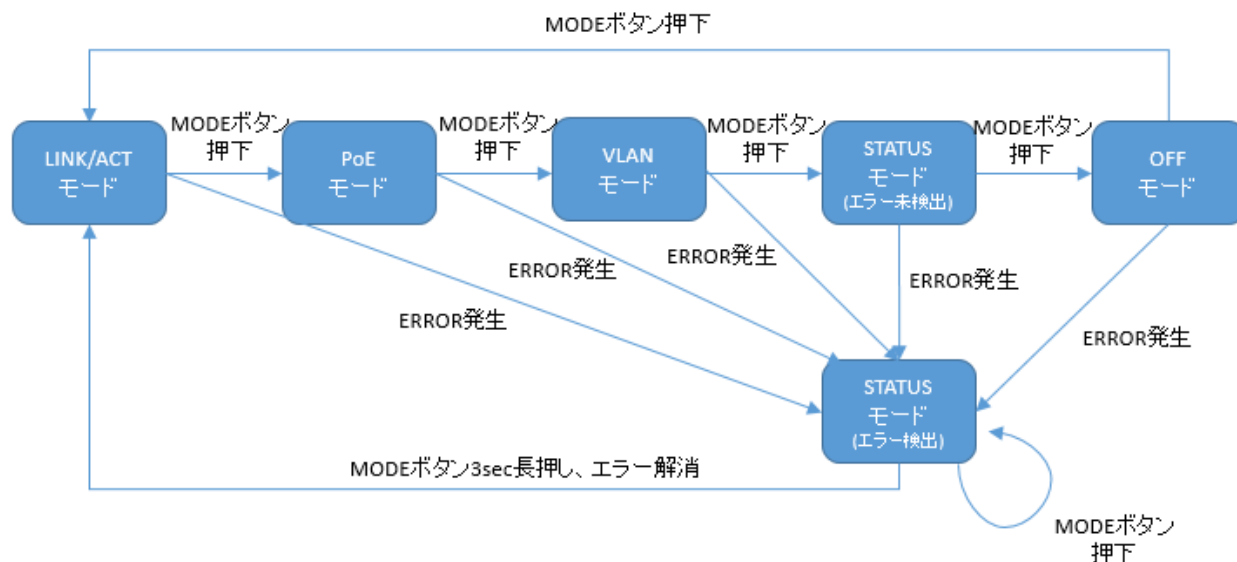
本製品は、以下に示す5つの表示モードを提供します。

モード名	MODE LED点灯状態	機能概要
LINK/ACT モード		LAN/SFPポートの左側LEDにリンク状態、右側LEDに接続速度を表示します。

モード名	MODE LED点灯状態	機能概要
PoE モード		PoE給電ポートの給電状態を表示します。
VLAN モード		LAN/SFPポートに設定されているVLAN IDを表示します。
STATUS モード		LAN/SFPポートのエラー状態を表示します。
OFF モード		LAN/SFPポート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、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)



システム起動後の表示モード、エラー解消後の表示モードは、初期LEDモードの設定に依存します。

以下の機能でエラーを検出すると、ポートLEDの表示が、自動的にSTATUSモードに切り替わります。

- ・ループ検出
- ・SFP受光レベル監視
- ・PoE給電

エラーを検出した状態でMODEボタンを押下しても、STATUSモードのままとなります。(全てのエラーが解消

するまで受け付けません。)

本状態でMODEボタンを3秒間長押しすると、全てのエラー状態がリセットされ、初期LEDモードの設定にしたがった表示に切り替わります。

(詳細は、**STATUS モード時のLED表示** を参照ください。)

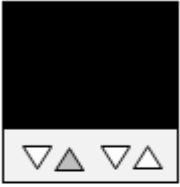
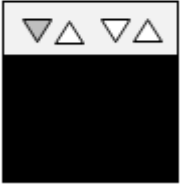
LINK/ACT モード時のLED表示

LINK/ACTモードでは、ポートLEDに以下を表示します。

- ・ LAN/SFP ポートのリンク状態
- ・ LAN/SFP ポートの接続速度

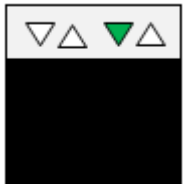
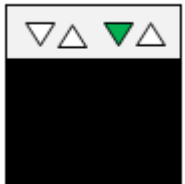
リンク状態のLED表示について、以下に示します。

- ・ LAN/SFP ポートのリンク状態 LED表示

	リンクダウン中	リンクアップ中	データ転送中
LANポート	  (消灯)	  (緑点灯)	  (緑点滅)
SFPポート	  (消灯)	  (緑点灯)	  (緑点滅)

接続速度のLED表示について、以下に示します。

- ・ LAN/SFP ポートの接続速度 LED表示

	10M Link	100M Link	1000M Link	10000M Link
LANポート	  (消灯)	  (橙点灯)	  (緑点灯)	(なし)
SFPポート	(なし)	(なし)	  (緑点灯)	  (緑点灯)

PoE モード時のLED表示

PoEモードでは、PoE給電可能ポート(以降、PoEポート)のポートLEDに給電状況を表示します。
 スタック構成時、PoEモードには変更できません。
 各モデルの給電ポートは以下のとおりです。

- ・モデル別給電ポート

モデル名	給電ポート
SWX2310P-10G	ポート #1-#8
SWX2310P-18G	ポート #1-#16
SWX2310P-28GT	ポート #1-#24

PoE モードのLED表示について、以下に示します。

- ・給電ポートのポートLED表示

	給電なし	給電中
LANポート		
		
	(消灯)	(緑点灯)

VLAN モード時のLED表示

VLANモードでは、ポートLEDにVLANの所属状況を表示します。

スタック構成時、VLANモードには変更できません。

ポートLEDの点灯状態について、以下に示します。

- VLAN モード時のポートLEDの点灯状態

LAN/SFPポートのVLAN 所属状況	ポートLEDの点灯状態
どのVLANにも所属していない	  (消灯)
1つのVLANに所属	VLAN ID の昇順 1st 2nd 3rd 4th 5th 6th 7th 以降   Type-1 Type-2 Type-3 Type-4 Type-5 Type-6 Type-7 VLAN IDのうち、若いIDから6つを特定の点灯パターンで表現します。 7番目以降のVLAN IDはすべて同じ点灯パターンとなります。
複数のVLANに所属	  (左右のポートLEDを 橙色 で点灯)

- デフォルトVLAN(VLAN #1)は、表示対象外とします。所属VLANとしてカウントしません。
- VLANの所属状況は、各LAN/SFPポートのリンク状態に依存しません。リンクダウン状態のポートも表

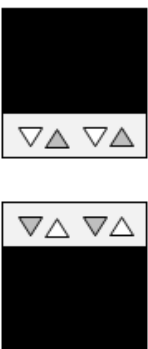
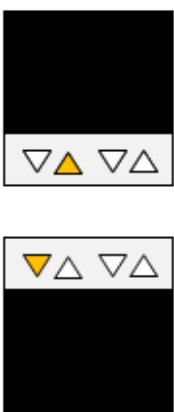
示対象となります。

- ・ 表示対象となるVLAN IDは、所属するLAN/SFPポートが存在するもののみにします。
VLAN IDのみが定義されているもの(所属LAN/SFPポートがない)については、表示対象外となります。

STATUS モード時のLED表示

STATUSモードでは、ポートLEDに本製品の以下の機能で発生したエラー状態を表示します。

- ・ ループ検出
- ・ SFP受光レベル監視
- ・ PoE給電
- ・ エラー発生中のポートLED表示

	正常状態	ループ検出 or SFP受光レベル異常	PDエラー	PoEシステムリミット	PoEポートリミット
LANポート	 (消灯)	 (左橙点滅)	 (左橙点灯)	 (右橙点滅)	 (右橙点灯)
SFPポート	 (消灯)	 (左橙点滅)	(なし)	(なし)	(なし)

本製品でエラーを検出すると、強制的にSTATUSモードに切り替わります。
それぞれの機能で以下の場合にエラーと判定します。

- ・ ループ検出
 - ループを検出し、ポートをブロックした
 - ループを検出し、ポートをshutdownした
- ・ SFP受光レベル監視
 - SFPの受光レベルが正常範囲より下回った

-
- SFPの受光レベルが正常範囲より上回った
 - PoE給電
 - ポートリミット(1ポートあたりの最大給電量)を越えたため給電を停止した
 - システムリミット(システム全体の最大給電量)を越えたため優先度の低いポートの給電を停止した
 - PDエラーを検出した

エラー要因については、 **show error port-led** コマンドで確認することができます。

エラー発生中のSTATUSモードでは、以下の状態になると、自動で **初期 LED モード** に切り替わります。

- 以下の全てのエラーが解消した
 - ループ検出によるブロック状態が解消した
 - ループ検出によるshutdown状態が解消した
 - ループ検出によってshutdownされてから監視時間が経過した
 - ループ検出によるshutdown状態で **no shutdown** コマンド実行後、リンクアップした
 - SFPの受光レベルが回復した
 - PoEポートのエラーが解消した
- MODEボタンの長押し(3秒間)を行い、エラー状態を強制的にリセット(クリア)した

OFFモードのLED表示

初期LEDモードがOFFモードのとき、ポートLEDはリンク状態に関係なくすべて消灯にします。

初期LEDモードがOFFモードでも、エラー発生時には自動的にSTATUSモードに移行し、エラーの発生状態を表示します。

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。

ただし、スタック構成時のLEDモード変更は不可能です。

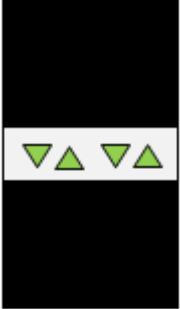
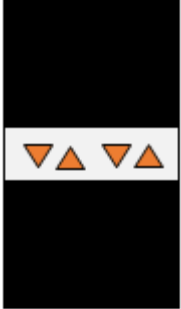
show led-mode コマンドにより初期 LED モード、現在表示中の LED モード を確認することができます。

エラー発生中の **STATUS モード** でエラーが解消されると、 設定した初期LED モードに遷移します。

その他のポートLED表示

LEDモードの状態に関係なく、起動時の初期化中、ファーム更新中は全ポートLEDは以下の表示となります。

- その他のポートLED表示

	ファームアップ中	初期化中
LANポート	  (緑点滅)	  (消灯)
SFPポート	 (緑点滅)	 (橙点灯)

スタックID表示 LED

SWX2310P-28GTに搭載されたスタックID表示 LED (7SEG LED)は、起動時のカウントダウン表示後に、スタック構成時のスタックIDを表示します。

スタック構成中でない場合は、'1' を表示します。

スタック構成中にエラーとなった場合、エラーを示す 'E' を表示します。

初期LEDモードがOFFモードの場合、スタックID表示 LED の表示も消灯します。

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願います。

操作項目	操作コマンド
LAN/SFP ポート 状態表示	show interface
ループ検出 設定状態の表示	show loop-detect
VLAN 情報の表示	show vlan brief
初期LEDモードの設定	led-mode default
LEDモードの表示	show led-mode
ポートのエラー状態の表示	show error port-led

コマンド実行例

LAN/SFP ポートの状態確認

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

```
Yamaha#show interface
show interface
Interface port1.1
  Link is UP
  Hardware is Ethernet
  HW addr: ac44.f23d.0b2c
  ifIndex 5001, MRU 1522
  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      : 317111
           bytes        : 31387581
           multicast packets: 317074
    output packets      : 162694
           bytes        : 220469213
           multicast packets: 162310
           broadcast packets: 149
           drop packets   : 0
  :
```

(全LAN/SFPポートの情報が表示される)

LAN/SFP ポート ループ検出状態の確認

LAN/SFPポートのループ検出状態を確認します。

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

loop-detect: Enable
```

port	loop-detect	port-blocking	status
port1.1	enable	enable	Normal
port1.2	enable	enable	Normal
port1.3	enable	enable	Normal
port1.4	enable	enable	Normal
port1.5	enable	enable	Normal
port1.6	enable	enable	Normal
port1.7	enable	enable	Normal
port1.8	enable	enable	Normal
port1.9	enable	enable	Normal
port1.10	enable	enable	Normal

(*) : Indicates that the feature is enabled.

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

外部メモリの利用

機能概要

本製品では、外部メモリを使った以下の機能を提供します。

- SDカードブート(ファームウェア、コンフィグ)
 - SDカード内のファームウェアファイル、コンフィグファイルを使用してシステムを起動できます。
- SDカードブート自動適用(ファームウェア、コンフィグ)
 - SDカードブートで使用したファームウェアやコンフィグを次回起動時にSDカードが無くても適用することができます。
- ファームウェア更新
 - SDカード内のファームウェアファイルを読み込んで本体のファームウェアを更新することができます。
- コンフィグファイルの保存・コピー
 - 現在システムで稼働中のrunning-configをSDカード内に保存したり、SDカードから本体Flash ROM、本体Flash ROMからSDカードへコンフィグファイルをコピーできます。
- ログファイルの保存
 - **save logging** コマンド実行時にSDカード内にログファイルをバックアップすることができます。
- 技術サポート情報の保存
 - 技術サポート情報(**show tech-support** コマンドの実行結果)をSDカード内に保存できます。
- 統計情報の保存
 - リソース情報、トラフィック情報の観測データを定期的にバックアップします。
 - 観測データの統計情報をCSVファイル形式で保存できます。
- システム情報のバックアップ・リストア
 - システム情報(コンフィグを含む)をSDカードにバックアップすることができます。
 - バックアップしたシステム情報を本体Flash ROMにリストアすることができます。

用語の定義

特になし

機能詳細

利用可能な外部メモリ

利用可能な外部メモリの条件は以下の通りです。

- カードタイプ: microSDカード/microSDHCカード
- ファイルフォーマット: FAT16/FAT32

フォルダ構成

SDカード内は以下のフォルダ構成である必要があります。

機種名	+- firmware	ファームウェアファイル保存フォルダ
	+- startup-config	スタートアップコンフィグ保存フォルダ
	+- log	SYSLOG保存フォルダ
	+- techsupport	技術サポート情報保存フォルダ
	+- data	システム共通フォルダ
	+- backup-system	システムバックアップフォルダ

SDカードのマウント/アンマウント

SDカードが起動時、または起動後に挿入された時、自動的にマウントされ、利用可能となります。

ファイルの欠損などを防止するため、SDカードを抜く時には事前に **umount sd** コマンドを実行するか、Web GUIからアンマウントを実行してください。

SDカードがアンマウント状態のとき、SDカードを利用することができません。

umount sd コマンド実行後に再度利用したい場合は、以下を実行する必要があります。

- ・一度SDカードを抜き差しする
- ・ **mount sd** コマンドを実行する
- ・ Web GUIからマウントを実行する

SDカードブート(ファームウェア、コンフィグ)

SDカード内に保存されたファームウェアファイルやコンフィグファイルを利用してシステムを起動することができます。

SDカードブートを利用するためには以下の条件を満たす必要があります。

- ・ ファームウェアファイルを利用したSDカードブート
 - システム起動時にSDカードが接続されている。
 - SDカード内に以下のファイルが存在する。
 - /swx2310p/firmware/swx2310p.bin
 - **boot prioritize sd enable** が設定されている。
※工場出荷状態では **boot prioritize sd enable** が設定されています。
- ・ コンフィグファイルを利用したSDカードブート
 - システム起動時にSDカードが接続されている。
 - SDカード内に以下のファイルが存在する。
 - /swx2310p/startup-config/config.txt
 - **startup-config select sd** が設定されている。
※工場出荷状態では **startup-config select sd** が設定されています。

なお、SDカードブート自動適用機能([SDカードブート自動適用](#))を利用することで、SDカードブートに使用したファイルを内蔵Flash ROMへ自動的に適用することもできます。

SDカードブートに成功したか否かは **show environment** コマンドで確認可能です。

- ・ファームウェアファイルを利用したSDカードブートの場合、"Startup Firmware"に"exec(SD)"と表示されます。
- ・コンフィグファイルを利用したSDカードブートの場合、"Startup Configuration"に"config(SD)"と表示されます。

コンフィグファイルを利用したSDカードブートの場合、 **write , copy running-config startup-config** コマンドを実行すると、SDカード内のコンフィグファイルを更新します。

コンフィグファイルを利用したSDカードブートに失敗した場合は、スタートアップコンフィグ #0 が読み込まれます。

また、以下のメッセージがコンソールとSYSLOGに表示されます。

```
Loading config0 because can't read config in SD card.
```

SDカードブート自動適用(ファームウェア、コンフィグ)

SDカードブートに使用したファームウェアやコンフィグを、内蔵Flash ROMに自動適用することができます。本機能を利用することで、新しく購入した機器(工場出荷状態)に、予め用意しておいたファームウェアとコンフィグを簡単に導入することができます。

自動適用のための事前準備

本機能を動作させるためには、以下の条件を満たす必要があります。

- ・以下いずれかのSDカードブートを可能な状態にする(詳細は[SDカードブート](#)を参照)
 - **boot prioritize sd enable** が設定されており、SDカードの適切なパスにファームウェアが存在する
 - **startup-config select sd** が設定されており、SDカードの適切なパスにコンフィグが存在する
- ・SDカードブート自動適用機能を有効にする
 - SDカードブート自動適用機能は、 **boot auto-apply enable** コマンドで有効にすることができます。
(※工場出荷時は有効)
 - **show environment** コマンドの「Boot auto-apply」の表示結果により、機能の有効/無効を確認することが可能です。
- ・SDカードブート自動適用するためのファイルを用意する
 - ファームウェアを自動適用させる場合
 - SDカード内のfirmwareフォルダに **auto-apply.txt** (空のテキストファイル)を用意する。

```
/swx2310p/firmware/auto-apply.txt
```

- コンフィグを自動適用させる場合
 - SDカード内のstartup-configフォルダに **auto-apply.txt** (空のテキストファイル)を用意する。

```
/swx2310p/startup-config/auto-apply.txt
```

自動適用の手順

SDカードブートの自動適用の手順は以下のようになります。

1. 事前準備([自動適用のための事前準備](#)を参照)
2. SDカードをセットし本製品を起動
3. SDカードブート完了後、指定ファイルを内蔵Flash ROMへ自動適用(ファームウェアの自動適用時、起動時間が通常より長くなります。)
4. 自動適用結果の保存([自動適用の結果](#)を参照)
5. SDカードを自動アンマウント
6. microSD LEDを自動消灯

自動適用の結果

自動適用の実行結果はSDカード内に保存されます。

ファイル名と配置パス	ログ
/swx2310p/startup-config/auto-apply-result.txt	シリアル : 日時 : 結果
/swx2310p/firmware/auto-apply-result.txt	シリアル : 日時 : 結果

コンフィグの適用先

コンフィグの適用先を任意のコンフィグIDへ変更したい場合は、作成した **auto-apply.txt** のファイル名を以下のように変更してください。

指定しない場合は、デフォルトのコンフィグID 0が適用先になります。

ファイル名と配置パス	コンフィグID
/swx2310p/startup-config/auto-apply.txt	0
/swx2310p/startup-config/auto-apply0.txt	0
/swx2310p/startup-config/auto-apply1.txt	1
/swx2310p/startup-config/auto-apply2.txt	2
/swx2310p/startup-config/auto-apply3.txt	3
/swx2310p/startup-config/auto-apply4.txt	4

注意事項

本機能を利用する際は、以下に注意してください。

- ・ 自動適用に成功すると本機能は自動で無効になります。
自動で無効になることを回避するためには、作成した **auto-apply.txt** 内の先頭に、以下のよう
に「keep」という文字列を記述する必要があります。

keep

- ・スタック機能が有効の場合、本機能は動作しません。
- ・SDカード内に **auto-apply.txt** が存在しない場合、本機能は動作しません。
- ・SDカードブートをしていない場合、**auto-apply.txt** が存在していても自動適用は失敗となります。[SDカードブート](#)を参考に、SDカード内のファイルおよびSDカードブート機能が有効になっていることを確認してください。
- ・自動適用に失敗した場合、本機能は自動で無効にはならず、SDカードのみアンマウントされます。
- ・自動適用機能を使用しない場合は、誤動作を防ぐために **auto-apply.txt** は必ず削除するようにしてください。

ファームウェア更新

SDカード内のファームウェアファイルを読み込んで本体のファームウェアを更新することができます。

本機能を利用するためには以下の条件があります。

- ・SDカード内に以下のファイルが存在する。
 - /swx2310p/firmware/swx2310p.bin

SDカードが挿入され上記ファイルが存在する場合、**firmware-update sd execute** コマンドを実行すると、SDカード内のファームウェアファイルを使ってFlash ROM内のファームウェアを更新します。

firmware-update sd execute コマンドを実行すると、ファームウェアファイルの読み込みが完了したときにSDカードのマウント状態を継続するかユーザーに確認します。SDカードは必要に応じてアンマウント後に抜いてください。

ファームウェア更新による自動再起動時にSDカードを挿したままの状態にすると、SDカード内のファームウェアファイルでシステムが起動されてしまうため、ご注意ください。

スタック構成中にメインスイッチから **firmware-update sd execute** コマンドを実行すると、メンバースイッチのファームウェアも更新することができます。

コンフィグファイルの保存・コピー

現在システムで稼働中のrunning-configをSDカード内に保存することができます。(**copy running-config startup-config** コマンド、 **write** コマンド)

SDカードから本体Flash ROM、本体Flash ROMからSDカードへコンフィグファイルをコピーできます。(**copy startup-config** コマンド)

SDカード内のstartup-configを消去、表示できます。(**erase startup-config** コマンド、 **show startup-config** コマンド)

SDカード内の以下のフォルダが対象となります。

- ・ /swx2310p/startup-config

ログファイルの保存

save logging コマンド実行時にSDカード内にログファイルをバックアップすることができます。

logging backup sd コマンドにより、SDカードへのSYSLOGバックアップを有効にすることが可能です。SDカードへのSYSLOGバックアップが有効なとき、 **save logging** コマンドを実行すると、SDカード内に以下

の保存日付入りログファイルが保存されます。

- /swx2310p/log/YYYYMMDD_log.txt ※YYYYMMDD=年月日

SDカード内のログファイルの表示、消去はできません。

技術サポート情報の保存

技術サポート情報(**show tech-support** コマンドの実行結果)をSDカード内に保存できます。

copy tech-support sd コマンドを実行すると、SDカード内に以下の保存日付入り技術サポート情報ファイルが保存されます。

- /swx2310p/techsupport/YYYYMMDDHHMMSS_techsupport.txt ※YYYYMMDD=年月日、HHMMSS=時分秒

SDカード内の技術サポート情報ファイルの表示、消去はできません。

スタック構成中にメインスイッチから **copy tech-support sd** コマンドを実行すると、メンバースイッチの技術サポート情報を含んだファイルが保存されます。

統計情報の保存

リソース情報、トラフィック情報の観測データを定期的にバックアップします。

SDカードへの統計情報のバックアップを有効にするには、WebGUIの[管理]-[保守]-[統計情報の管理]より設定する必要があります。

また、観測データの統計情報をWebGUIよりCSVファイル形式で保存できます。

システム情報のバックアップ・リストア

本体のシステム情報をSDカードにバックアップし、バックアップしたシステム情報を任意のスイッチに対してリストアすることができます。

本体にSDカードを接続した状態で **backup system** コマンドを実行すると、以下のフォルダにシステム情報のバックアップを作成します。

- /swx2310p/backup-system

バックアップ実行時に /swx2310p/firmware/ フォルダに swx2310p.bin ファイルが存在した場合、ファームウェアファイルとしてバックアップします。

システム情報のバックアップが格納されているSDカードを任意のスイッチに接続し、 **restore system** コマンドを実行するとバックアップしたシステム情報をリストアします。

ファームウェアファイルがバックアップされていた場合、そのファイルを使ってファームウェア更新も行います。

リストアが完了するとシステムを再起動します。

システム情報のバックアップには以下が含まれます。

- 本体に付随する設定
 - startup-config #0 - #4 とそれらに付随する情報
 - startup-config select コマンドの設定値
 - boot prioritize sd コマンドの設定値
- ファームウェアファイル
※バックアップ実行時、SDカードの指定フォルダにファームウェアファイルを保存していた場合に限る

そのため、故障による機器交換などを行う際、バックアップしたシステム情報をリストアするだけで交換前の機器と同じ動作を再現することができます。
バックアップされたシステム情報に対して、編集や削除などを行わないでください。

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願います。

操作項目	操作コマンド
SDカードのマウント	mount sd
SDカードのアンマウント	unmount sd
ログのSDカードバックアップの設定	logging backup sd
ログのバックアップ	save logging
技術サポート情報の保存	copy tech-support sd
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コピー	copy startup-config
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
システム情報のバックアップ	backup system
システム情報のリストア	restore system

コマンド実行例

SDカードのアンマウント

SDカードをアンマウントする。

```
Yamaha>unmount sd
```

SDカードのマウント

SDカードをマウントする。

```
Yamaha>mount sd
```

ログファイルのバックアップ

save logging コマンド実行時にSDカード内にも同時にログファイルをバックアップします。

```
Yamaha(config)#logging backup sd enable ①  
Yamaha(config)#exit
```

```
Yamaha#save logging ②
```

- ① ログのSDカードバックアップを有効にする
- ② ログをバックアップする

技術サポート情報の保存

技術サポート情報を保存します。

```
Yamaha#copy tech-support sd
```

注意事項

特になし

関連文書

- [コンフィグ管理](#)
- [SYSLOG](#)
- [ファームウェア更新](#)
- [パフォーマンスの観測](#)

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 * startup-config selectコマンドによる再起動 * boot prioritize sdコマンドによる再起動 * restore systemコマンドによる再起動 * stack enable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 * メモリ枯渇による再起動 * カーネルパニックによる再起動 * プロセスの異常終了による再起動

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。
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
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: SWX2310P Rev.2.02.02 (Tue Dec 5 11:37:39 2017)
Previous EXEC: SWX2310P Rev.2.02.02 (Tue Dec 5 11:37:39 2017)
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	2018/03/15	09:50:29	Restart by reload command
1	2018/03/14	20:24:40	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

本製品は、製品情報や稼働情報などを取得する仕組みとして、以下の機能を提供します。

- ・ コマンドによる筐体情報の表示
- ・ 技術サポート情報のリモート取得
- ・ 技術サポート情報の外部メモリへの保存

技術サポート情報 とは、本製品の製品情報や稼働情報のほか、コンフィグの内容やプロセスの稼働状況など、さまざまな解析情報が集約されたものです。
機器の情報をまとめて表示したい際にご活用いただけます。

機能詳細

コマンドによる筐体情報の表示

コンソールにコマンドを入力して筐体情報を表示します。
表示できる筐体情報には以下のものがあります。

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。また、SFPモジュールが挿入されている場合、モジュールの製品情報についても表示します。	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
プロセス一覧	システムの概要情報と実行中のプロセス一覧を表示します。	show process
メモリ使用状況	プロセスごとのメモリ使用状況を表示します。	show memory
ディスク使用状況	システムで使用しているディスクの使用状況を表示します。	show disk-usage
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表示します。スタック機能が有効なときは、メインスイッチの技術サポート情報に加えて、メンバースイッチの技術サポート情報も表示します。	show tech-support

製品情報の表示

show inventory コマンドにより、本体およびSFPモジュールの製品情報を表示します。製品情報には以下の情報が含まれます。

- ・ 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)

稼働情報の表示

show environment コマンドにより、システムの稼働状態を表示します。システムの稼働状態には以下の情報が含まれます。

- ・ ブートバージョン
- ・ 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
- ・ ファームウェアファイル
- ・ スタートアップコンフィグファイル
- ・ SDカードブート自動適用機能の設定
- ・ シリアルボーレート
- ・ 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

技術サポート情報の表示

show tech-support コマンドにより、技術サポート情報を表示します。技術サポート情報には、以下のコマンドの実行結果が含まれます。

スタック機能が有効なときは、スタックを構成しているすべての機器の技術サポート情報を表示します。ただし、メインスイッチとメンバースイッチで実行されるコマンドが異なります。詳細は以下のコマンド一覧を参照してください。

- ・ 実行されるコマンド一覧

コマンド	スタック無効	スタック有効	
		メインスイッチ	メンバースイッチ
show running-config	○	○	○
show startup-config	○	○	○
show stack	○ (※1)	○ (※1)	○ (※1)
show environment	○	○	○
show system-diagnostics	○	○	○
show clock detail	○	○	-

show disk-usage	○	○	○
show inventory	○	○	○
show boot all	○	○	○
show boot prioritize sd	○	○	○
show logging	○	○	○
show process	○	○	○
show memory	○	○	○
show users	○	○	○
show interface	○	○	-
show frame-counter	○	○	-
show vlan brief	○	○	-
show spanning-tree mst detail	○	○	-
show etherchannel status detail	○	○	-
show loop-detect	○	○	-
show mac-address-table	○	○	-
show l2ms detail	○	○	-
show qos queue-counters	○	○	-
show ddm status	○	○	○
show errdisable	○	○	-
show auth status	○	○	-
show auth supplicant	○	○	-
show power-inline	○	○	-
show error port-led	○	○	-
show ip interface brief	○	○	-
show ip forwarding	○	○	-
show ipv6 interface brief	○	○	-
show ipv6 forwarding	○	○	-
show ip route	○	○	-
show ip route database	○	○	-
show ipv6 route	○	○	-
show ipv6 route database	○	○	-
show arp	○	○	-
show ipv6 neighbors	○	○	-

show ip igmp snooping groups	○	○	-
show ip igmp snooping interface	○	○	-
show ipv6 mld snooping groups	○	○	-
show ipv6 mld snooping interface	○	○	-
show ip dhcp snooping binding	○	○	-
show ip dhcp snooping statistics	○	○	-
show radius-server local certificate status	○	○	-
show radius-server local nas	○	○	-
show radius-server local user	○	○	-
show radius-server local certificate list	○	○	-
show radius-server local certificate revoke	○	○	-
show sflow	○	○	-
show sflow sampling	○	○	-

※1 スタック対応モデルだけに含まれるコマンドです。

技術サポート情報のリモート取得

Web GUI、または、TFTPによるリモートアクセスで、本製品から **技術サポート情報(show tech-supportの出力結果)** を取得できます。

Web GUI

本製品のhttp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. 保守に使用するVLANを決めます。
2. 保守VLANにIPv4アドレスを設定します。設定には、ip address コマンドを使用します。
3. 保守VLANからhttpサーバーへのアクセスを許可します。management interfaceコマンド設定と違うVLANを指定する場合、http-server interface コマンドを使用して設定します。

以下の操作はWeb GUIへアクセスして実施してください。

- 技術サポート情報をWeb GUIへ表示する
 - 「TECHINFO」メニューの「ブラウザーで表示」ボタンを押すと、サブウィンドウに show tech-support コマンドの実行結果が表示されます。
 - 終了する場合は、Web ブラウザーの終了ボタンを押してください。
- 技術サポート情報をWeb GUIより取得する
 - 「TECHINFO」メニューの「テキストファイルで取得」ボタンを押すと、自動的にダウンロードが始まります。
 - 以下のファイル名で保存されます。
 - techinfo_YYYYMMDDhhmmss.txt ※YYYYMMDDHHMMSS … コマンド実行時の年月日時分秒

TFTP

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. 保守に使用するVLANを決めます。
2. 保守VLANにIPv4アドレスを設定します。設定には、ip address コマンドを使用します。
3. 保守VLANからtftpサーバーへのアクセスを許可します。management interfaceコマンド設定と違うVLANを指定する場合、tftp-server interface コマンドを使用して設定します。

なお、tftpクライアント使用时、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。

技術サポート情報の外部メモリへの保存

copy tech-support sd コマンドにより、本製品の **技術サポート情報(show tech-supportの出力結果)** をSDカードに保存することができます。

コマンド実行前に、SDカードを挿入しておく必要があります。

SDカード内には以下のファイル名で保存されます。

- ・ /swx2310p/techsupport/YYYYMMDDHHMMSS_techsupport.txt ※YYYYMMDDHHMMSS … コマンド実行時の年月日時分秒

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
製品情報の表示	show inventory
稼動情報の表示	show environment
プロセス一覧	show process
メモリ使用状況	show memory
ディスク使用状況	show disk-usage
技術サポート情報の表示	show tech-support
技術サポート情報の保存	copy tech-support sd

コマンド実行例

製品情報の表示

本体およびSFPモジュールの製品情報を表示します。

```
Yamaha>show inventory
NAME: L2 POE switch
DESCR: SWX2310P-10G
Vendor: Yamaha
PID: SWX2310P-10G
VID: 0000
SN: S00000000
```

```
NAME: SFP1
DESCR: 1000BASE-LX
Vendor: YAMAHA
PID: YSFP-G-LX
VID: 0000
SN: 000000000000
```

```
NAME: SFP2
DESCR: 1000BASE-SX
Vendor: YAMAHA
PID: YSFP-G-SX
VID: 0000
SN: 000000000000
```

稼働情報の表示

システムの稼働状態を表示します。

```
Yamaha>show environment
SWX2310P-10G BootROM Ver.1.00
SWX2310P Rev.2.02.02 (Tue Dec 5 11:37:39 2017)
main=SWX2310P-10G ver=00 serial=S000000000 MAC-Address=00a0.de00.0000
CPU: 7%(5sec) 8%(1min) 8%(5min) Memory: 18% used
Fan status: Normal
Fan speed: FAN1=4444RPM FAN2=4444RPM FAN3=4444RPM
Startup firmware: exec0
Startup Configuration file: config0
Auto-apply: Enable
Serial Baudrate: 9600
Boot time: 2018/01/01 11:13:44 +09:00
Current time: 2018/01/02 16:19:43 +09:00
Elapsed time from boot: 1days 05:06:04
Temperature status: Normal
Temperature: 28 degree C

Yamaha>
```

技術サポート情報の表示

技術サポート情報を表示します。

```
Yamaha#show tech-support
#
# Information for Yamaha Technical Support
#

*** show running-config ***
!
! - Running Configuration -
! Current Time: Fri Jan 1 00:00:00 JST 2021
!
dns-client enable
```

```
!  
vlan database  
  vlan 2 name VLAN0002  
  vlan 3 name VLAN0003  
!  
interface port1.1  
  switchport  
  switchport mode access  
...  
  
*** show startup-config ***  
...  
  
*** show stack ***  
...  
  
*** show environment ***  
...  
  
*** show disk-usage ***  
...  
...  
...  
  
#  
# End of Information for Yamaha Technical Support  
#
```

注意事項

特になし

関連文書

特になし

システム自己診断

機能概要

本製品は、システムの自己診断機能を提供します。

システム自己診断機能では次のような異常を検出できます。

- ・ 起動処理異常
- ・ ハードウェアコンポーネント異常
 - インターフェース（イーサネットポート）
 - RTC
 - SFP
 - ファン
 - PoEコントローラー
 - 温度センサー
- ・ 温度異常

用語の定義

RTC (Real-Time Clock)

時刻を管理するデバイス。

PoEコントローラー

PoE（Power over Ethernet）を制御するためのデバイス。

PSE (Power Sourcing Equipment)

給電機器。本ページではPoEコントローラーと同義。

パケットプロセッサ

パケットを処理するためのデバイス。

機能詳細

診断

システム自己診断機能は、診断を実行するタイミングによってブートアップ診断、オンデマンド診断、ヘルスマニタリング診断に分類できます。
各診断の特徴を以下に示します。

- ・ ブートアップ診断
 - システム起動時に自動的に実行する
 - 起動処理異常、ハードウェアコンポーネント異常（RTCなど）を検出する
- ・ オンデマンド診断
 - **system-diagnostics on-demand execute** コマンドにより、ユーザーが任意のタイミングで実行できる

- ・ ハードウェアコンポーネント異常（インターフェース）を検出する
- ・ 診断中は全ポートシャットダウンし、終了時にはシステムを再起動する
- ・ ヘルスモニタリング診断
 - ・ システム稼働中にバックグラウンドで常時実行している
 - ・ ハードウェアコンポーネント異常（ファン異常など）、温度異常を検出する
 - ・ ヘルスモニタリング診断の結果はGUIやLEDでも表示する（LEDで表示するのは一部のテストのみ）

各診断では複数のテストを実行します。各診断で実行するテスト項目を以下に示します。
各テスト項目の詳細は [テスト詳細](#) を参照してください。

テスト項目	ブートアップ診断	オンデマンド診断	ヘルスモニタリング診断
Loading Test	○		
RTC Test	○		
Packet Processor Test	○		
PHY Test		○	
Thermal Test			○
Fan Test			○
Thermal Sensor Test			○
PoE Test			○
SFP Test			○

診断結果表示

診断結果は **show system-diagnostics** コマンドで確認できます。
オンデマンド診断は実行後に自動でシステムを再起動しますが、再起動後に診断結果を確認できます。

オンデマンド診断結果削除

オンデマンド診断結果を削除したい場合は **clear system-diagnostics on-demand** コマンドで削除できます。

テスト詳細

各テスト項目の詳細を以下に示します。

Loading Test

ソフトウェアモジュールのロード状態を検証します。
すべてのモジュールのロードに成功した場合はPass、一つでもロードに失敗した場合はFailとします。

show system-diagnostics コマンドではロードに失敗したモジュールの情報は表示しません。
ロードに失敗したモジュールを特定したい場合は **show logging** コマンドで下記のログを探してください。
※ XXXX 部分にはモジュール名が入ります。

```
[ HAMON]:err: An unexpected error has occurred. (XXXX daemon)
```

RTC Test

RTCのレジスタへのアクセスを検証します。

RTCから時刻を2回取得し、時刻が変化していたらPass、同じならFailとします。

また、RTCの時刻取得（レジスタ読み込み）に失敗した場合もFailとします。

Packet Processor Test

パケットプロセッサのレジスタへのアクセスを検証します。

パケットプロセッサのレジスタに対して書き込んだ値と読み込んだ値が一致したらPass、不一致ならFailとします。

また、レジスタアクセスに失敗した場合もFailとします。

PHY Test

PHYのレジスタへのアクセスを検証します。

PHYのレジスタに対して書き込んだ値と読み込んだ値が一致したらPass、不一致ならFailとします。

また、レジスタアクセスに失敗した場合もFailとします。

Thermal Test

CPU、PHY、SFPモジュール、温度センサー（筐体）、PSEの温度を監視します。

温度がしきい値を超えたときに警告します。

Fan Test

ファンの回転数を監視します。

ファンの回転が停止したとき、回転速度が上がったときに警告します。

Thermal Sensor Test

温度センサーを監視します。

温度センサーの異常を検出したときに警告します。

PoE Test

PoEの給電状態を監視します。

PoE給電制御で異常が発生したときに警告します。

SFP Test

SFPモジュールの受光レベルを監視します。

受光レベルが一定範囲外になったときに警告します。

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願います。

操作項目	操作コマンド
システム自己診断結果の表示	show system-diagnostics
オンデマンド診断実行	system-diagnostics on-demand execute
オンデマンド診断結果の削除	clear system-diagnostics on-demand

コマンド実行例

システム自己診断結果の表示

1. システム自己診断結果を確認します。

```

Yamaha#show system-diagnostics
Test results: (P = Pass, F = Fail, U = Untested, N = Normal, W = Warning)

- Bootup
  Loading Test: Pass

  RTC Test: Pass

  Packet Processor Test: Pass

- On-demand
Last on-demand diagnostics information:
Date       : 2021/07/07 09:00:00 +09:00
BootROM    : Ver.1.01
Firmware   : Rev.2.02.23

PHY Test:
Port   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16
-----
      P   P   P   P   P   P   P   P   P   P   P   P   P   P   P   P

Port  17  18
-----
      P   P

- Health monitoring
  Thermal Test:
    CPU: Normal, PHY: Normal, SFP: Normal, TS: Normal, PSE: Normal

  Fan Test: Normal

  Thermal Sensor Test: Normal

PoE Test:
Port   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16
-----
      N   N   N   N   N   N   N   N   N   N   N   N   N   N   N   N

SFP Test:
Port  17  18
-----

```


オンデマンド診断の実行

1. オンデマンド診断を実行します。

```
Yamaha#system-diagnostics on-demand execute
The system will be rebooted after diagnostics. Continue ? (y/n) y
on-demand diagnostics completed (pass). reboot immediately...
```

オンデマンド診断結果の削除

1. オンデマンド診断結果を削除します。

```
Yamaha#clear system-diagnostics on-demand
```

注意事項

- ・ オンデマンド診断の実行時には自動的にすべてのポートをシャットダウンし、再起動を行います。システム運用中に実行する際には十分にご注意ください。
- ・ オンデマンド診断はスタックの状態が Standalone もしくは Disable の場合にのみ実行可能です。スタックを構成している状態でオンデマンド診断を実行したい場合は、一度メンバースイッチ間の接続を切り離してください。
- ・ オンデマンド診断を Telnet や Web Console など、リモートで実行する場合、診断時にすべてのポートをシャットダウンするため再起動前の簡易結果表示ができません。診断結果は再起動後に **show system-diagnostics** コマンドでご確認ください。

関連文書

特になし

ケーブル診断

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。

cable-diagnostics tdr execute interface コマンドでケーブル診断を実行すると、診断が開始されます。
診断終了後、**show cable-diagnostics tdr** コマンドを実行すると、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。 * OK: 電氣的に接続されています。 * 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。 * Short: 短絡（ショート）が発生しています。 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。

前回実行したケーブル診断実行結果は **show 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 cable-diagnostics tdr 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	cable-diagnostics tdr execute interface
ケーブル診断結果の表示	show cable-diagnostics tdr
ケーブル診断結果のクリア	clear cable-diagnostics tdr

スマートスイッチで実装されている以下コマンドも上記コマンドと同様に使用することができます。

- test cable-diagnostics tdr interface
- show test cable-diagnostics tdr
- clear test cable-diagnostics tdr

コマンド実行例

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
% To check result, enter "show cable-diagnostics tdr"
```

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 Tue May 31 18:12:13 2022
Port      Pair  Status  Fault distance
-----
port1.1   1     OK      -
           2     OK      -
           3     Open    15 m
           4     Open    15 m
```

注意事項

- 本機能は簡易的な診断であり、専用機器ほど精密に診断することはできないため予めご了承ください。
- 診断可能なケーブルは10m以上です。10m未満の場合正しく診断できない場合があります。
- ケーブル診断を実行すると一時的に通信断が発生します。
- 診断対象ポートに **shutdown** コマンドが設定されていたり、ループ検知などによりシャットダウンしていると診断できません。
- 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とき、正しく診断できない場合があります。
- 診断対象ポートでPoE給電をしていると正しく診断できません。
- スタック構成時メンバースイッチからのコマンド実行はできません。

関連文書

- 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上の5つのコンフィグとSDカード上の1つのコンフィグを管理する。 startup-config select コマンドで選択したROM上のコンフィグ、またはSDカード上のコンフィグが、システム起動時に読み込まれる。 SDカード上の1つのコンフィグは"/swx2310p/startup-config"フォルダで管理する。	参照 / 消去 / コピー
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内もしくはSDカード内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。

本製品では、Flash ROM上の5つのスタートアップコンフィグとSDカード上の1つのスタートアップコンフィグを管理できます。
本体 Flash ROM 内の startup-config は、0 - 4 の ID で、SDカード内のコンフィグは sd というキーワードで管理します。

本体Flash ROM内の5種類のコンフィグからどのコンフィグを使用するかは、ユーザーが **startup-config select** コマンドで設定します。

- ・デフォルトは **sd** を使用します。
- ・ **startup-config select** コマンド実行時、再起動するか否かをユーザーが選択します。再起動しない場合、コマンド設定に変更はありません。
再起動を選択した場合、ユーザーがコマンド設定したIDのstartup-configで起動します。

Rev.2.02.09以前のファームウェアからRev.2.02.10以降のファームウェアに更新する場合、**startup-config select 0** が設定されていると、自動的に **startup-config select sd** に変更されます。
そのため、CONFIGを保存したmicroSDカードを挿入して運用している場合、SDカードブートが行われてしまうため、注意が必要です。
Rev.2.02.10以降のファームウェアでstartup-config selectコマンドを実行した後、Rev.2.02.09以前のファームウェアにリビジョンダウンした場合はその限りではありません。

各コンフィグには 管理をしやすくするために、**startup-config description** コマンドで **Description (説明文)** を付加することができます。

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。
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、**copy startup-config** コマンドでコピーができます。

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める流れは以下のとおりです。

1. **startup-config select** コマンド設定値を参照し、使用する startup-config を決定する。
startup-config select コマンドで **sd** が設定されていて、startup-configが保存されているSDカードが挿入されていなかった場合、startup-config #0 が選択される。
2. 決定した 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。
startup-config select コマンド設定値にしたがって決定した startup-config がROM上に存在しない場合、default-config をRAM上に展開する。

SDカード内のコンフィグを使用した起動に失敗した場合、以下のメッセージがコンソールとSYSLOGに表示されます。

```
Loading config0 because can't read config in SD card.
```

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、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、VLAN に対して 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。

また、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。
管理パスワードが初期設定の状態では、コンフィグファイルの取得および設定を受け付けることはできません。前もって管理パスワードを変更する必要があります。
なお、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。

対象CONFIG	対象ファイル	リモートパス	取得(GET)	設定(PUT)	自動再起動
running-config	CONFIGファイル (.txt)	config	○	○	-
startup-config # 0	CONFIGファイル (.txt)	config0	○	○	-
	すべての設定 (.zip)	config0-all	○	○	-
startup-config # 1	CONFIGファイル (.txt)	config1	○	○	-
	すべての設定 (.zip)	config1-all	○	○	-
startup-config # 2	CONFIGファイル (.txt)	config2	○	○	-
	すべての設定 (.zip)	config2-all	○	○	-
startup-config # 3	CONFIGファイル (.txt)	config3	○	○	-
	すべての設定 (.zip)	config3-all	○	○	-
startup-config # 4	CONFIGファイル (.txt)	config4	○	○	-
	すべての設定 (.zip)	config4-all	○	○	-
startup-config # SD	CONFIGファイル (.txt)	configs	○	○	-
	すべての設定 (.zip)	configs-all	○	○	-

設定ファイルを適用後、自動的にシステムを再起動させたい場合は、以下のリモートパスを指定します。
現在稼働しているコンフィグが適用対象となります。

対象CONFIG	対象ファイル	リモートパス	取得(GET)	設定(PUT)	自動再起動
現在稼働している startup-config	CONFIGファイル (.txt)	reconfig	-	○	○

設定ファイルを適用(PUT)するとき、対象CONFIG、および、対象ファイルの種別が正しいことを確認してください。

誤ったファイルを指定すると正しく反映できません。
running-configの場合は、設定ファイルの先頭に以下を追記する必要があります。

```
!  
! Switch Configuration  
!
```

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願います。

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コピー	copy startup-config
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
スタートアップコンフィグの選択	startup-config select
スタートアップコンフィグの説明文の設定	startup-config description

コマンド実行例

スタートアップコンフィグの選択

startup-config #1を選択して再起動する。

```
Yamaha#startup-config description 1 TEST ①
Yamaha#startup-config select 1 ②
reboot system? (y/n): y ③
```

① startup-config #1に"TEST"と説明文を設定

② startup-config #1を選択

③ 再起動する

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
Succeeded to write configuration
Yamaha#
```

スタートアップコンフィグのコピー

startup-config #2 を SDカードへコピーする。

```
Yamaha#copy startup-config 2 sd ①
Succeeded to copy configuration
Yamaha#show startup-config sd ②
!
! Last Modified: Tue Mar 13 17:34:02 JST 2018
!
dns-client enable
!
interface port1.1
switchport
switchport mode access
```

```
no shutdown
!  
...
```

- ① startup-config #2 を SDカードへコピー
- ② SDカードのstartup-configを表示

スタートアップコンフィグの消去

SDカードのstartup-configを消去する。

```
Yamaha#erase startup-config sd ①  
Succeeded to erase configuration  
Yamaha#
```

- ① SDカード内のstartup-configを消去

注意事項

特になし

関連文書

- ・ [外部メモリの利用](#)

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
- SSHサーバー
- HTTP サーバー／HTTPS 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4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先の限定
- 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対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	アクセス先の限定	アクセス元の限定
TELNET サーバー	○	○	○	○
SSH サーバー	○	○	○	○
HTTP サーバー HTTPS 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先の限定は、 **VLANインターフェース** に対して行います。
3. 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** と **アクセスの許可/拒否** を指定することができます。
4. 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	アクセス先の限定	アクセス元の限定
TELNET サーバー	起動	23	デフォルト保守VLAN (VLAN #1)のみ許可	全て許可
SSH サーバー	停止	22	デフォルト保守VLAN (VLAN #1)のみ許可	全て許可
HTTP サーバー	起動	80	デフォルト保守VLAN (VLAN #1)のみ許可	全て許可
HTTPS サーバー	停止	443		
TFTP サーバー	停止	69	デフォルト保守VLAN (VLAN #1)のみ許可	全て許可
SNMP サーバー	起動	161	全て許可	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願います。

ネットワークサービス	操作項目	操作コマンド
共通	保守VLAN	management interface
TELNETサーバー	起動停止	telnet-server
	受付ポート番号変更	telnet-server enable (引数でポート番号を指定)
	アクセス制御	telnet-server interface
	IPアドレスアクセス制御	telnet-server access
	設定の表示	show telnet-server
SSHサーバー	起動停止	ssh-server
	受付ポート番号変更	ssh-server enable (引数でポート番号を指定)
	アクセス制御	ssh-server interface
	IPアドレスアクセス制御	ssh-server access
	クライアント生存確認	ssh-server client alive
	設定の表示	show ssh-server
	ホスト鍵の作成	ssh-server host key generate
	ホスト鍵のクリア	clear ssh-server host key
	公開鍵の表示	show ssh-server host key

ネットワークサービス	操作項目	操作コマンド
HTTPサーバー	HTTPサーバー起動停止	http-server
	HTTPサーバー受付ポート番号変更	http-server enable (引数でポート番号を指定)
	HTTPSサーバー起動停止	http-server secure
	HTTPSサーバー受付ポート番号変更	http-server secure enable (引数でポート番号を指定)
	アクセス制御	http-server interface
	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	tftp-server
	アクセス制御	tftp-server interface
SNMPサーバー	IPアドレスおよびコミュニティ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。

保守VLANを **VLAN #1000** に変更しアクセスを許可します。保守VLAN以外からのアクセスは拒否します。

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)#management interface vlan1000 ②
Yamaha(config)#telnet-server access permit 192.168.100.1 ③
Yamaha(config)#end
Yamaha#show telnet-server ④
Service:Enable
Port:1024
Management interface(vlan):1000
Interface(vlan):None
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 保守VLANとしてVLAN #1000 のアクセスを許可する
- 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

SSHサーバーに対するアクセス制御

SSHサーバーに対するアクセス制限を実現します。

SSHサーバーホスト鍵の作成を行います。

ユーザー名とパスワードの登録をします。

SSHクライアントからは登録したユーザーとパスワードのみログイン可能です。

SSHサーバーの受付ポートを1024に変更します。

保守VLANを **VLAN #1000** に変更、 **VLAN #2** のアクセスを許可します。

これにより保守VLAN **VLAN #1000** と、 **VLAN #2** からのみアクセスを許可します。

ssh-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#ssh-server host key generate ①
Yamaha#show ssh-server host key ②
ssh-dss (省略)
ssh-rsa (省略)
Yamaha#
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#username user1 password pw1 ③
Yamaha(config)#ssh-server enable 1024 ④
Yamaha(config)#management interface vlan1000 ⑤
Yamaha(config)#ssh-server interface vlan2 ⑥
Yamaha(config)#end
Yamaha#show ssh-server ⑦
Service:Enable
Port:1024
Hostkey:Generated
Client alive :Disable
Management interface(vlan):1000
Interface(vlan):2
Access:None
Yamaha#
```

- ① ホスト鍵を作成する
- ② 鍵の内容を確認
- ③ ユーザー名とパスワードを登録する
- ④ 受付ポートを1024に変更し、SSHサーバーを再起動する
- ⑤ 保守VLANとして #1000 のアクセスを許可する
- ⑥ VLAN #2 のアクセスを許可する
- ⑦ 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に変更し、 **VLAN #2** のアクセスを許可します。

これによりデフォルト保守VLAN **VLAN #1** と、 **VLAN #2** からのみアクセスを許可します。

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 interface vlan2 ②
Yamaha(config)#http-server access permit 192.168.100.1 ③
Yamaha(config)#end
Yamaha#show http-server ④
HTTP :Enable(8000)
HTTPS:Disable
Management interface(vlan):1
Interface(vlan):2
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 VLAN #2 のアクセスを許可する
- 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、**VLAN #10** のアクセスを許可します。
デフォルト保守VLAN **VLAN #1** と、**VLAN #10** からのみアクセスを許可します。

```
Yamaha(config)#tftp-server enable 2048 ①
Yamaha(config)#tftp-server interface vlan10 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 VLAN #10 の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

注意事項

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。

- ・ 保守VLANと異なるネットワークセグメントからTELNET,SSH,HTTP,HTTPSで本製品にアクセスすることはできません。

TFTPクライアントからTFTPサーバーにアクセスする場合、以下の制限があります。

- ・ 特権パスワード(管理パスワード)が初期設定の状態ではアクセスを受け付けることはできません。前もっ

て特権パスワード(管理パスワード)を変更する必要があります。

- アクセス先VLANのIPv4プライマリアドレスとIPv4セカンダリアドレスが同じセグメントの場合、IPv4セカンダリアドレスにはアクセスできません。
- IPv6アドレスでアクセスする場合、アクセス先VLANで最後に設定されたIPv6アドレスにのみアクセスできます。
本製品を再起動した場合は、内部的にアドレスが再設定されるため、コンフィグの並び順で一番下にあるIPv6アドレスにのみアクセスできます。
- 経路的にTFTPクライアントから最も近いVLANのIPアドレスへのみアクセスできます。
例えば、VLAN 1に属するTFTPクライアントから本製品のVLAN 2のIPアドレスにはアクセスできません。

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
- ・ サマータイム(DST : Daylight Saving Time)を設定する機能

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、インターバル更新周期として **1時間** が設定されています。

ただし、システム起動後、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、1分周期でタイムサーバーに対して問合せを行います。

なお、タイムサーバーとの同期は、サンプリング数(サーバーからの応答回数)が1回、タイムアウト1秒で動作します。

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。

サマータイムの設定

clock summer-time コマンドで、ユーザーがサマータイム(DST : Daylight Saving Time)を設定することができます。

指定するパラメーターは以下のとおりです。

- ・ タイムゾーン名
サマータイムが施行されているときに表示するタイムゾーンの名前です。
- ・ サマータイムの開始時刻と終了時刻
時刻の指定方法は以下の2つから選択します。
 - 繰り返し (recurring)
毎年同じ期間を繰り返すように、月の週と曜日を指定します。
 - 日付指定 (date)
実際の日付を指定します。
- ・ オフセット
サマータイムの間に追加する時間(分)です。
指定可能な範囲は 1 ～ 1440 分です。指定がなければ **60 分** となります。

サマータイムは重複設定できません。

サマータイムの設定内容は、show clock detail コマンドで確認できます。

関連コマンド

関連コマンドについて、以下に示します。

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
時刻の手動設定	clock set
タイムゾーンの設定	clock timezone
サマータイムの設定(繰り返し)	clock summer-time recurring
サマータイムの設定(日付指定)	clock summer-time date
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 **2014.01.21 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 Jan 21 2014 ②
Yamaha#show clock ③
15:50:59 JST Tue Jan 21 2014
```

- 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 +9:00 Mon Dec 12 2016
Yamaha#show ntpdate ⑥
NTP server 1 : 192.168.100.1
NTP server 2 : ntp.nict.jp
adjust time : Mon Dec 12 10:03:15 2016 + interval 24 hours
sync server : 192.168.100.1
```

- 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

サマータイムの設定

繰り返し

サマータイムが毎年 3 月の第二日曜の 2 時に始まり、11 月の第一日曜の 2 時に終わるように設定します。

```
Yamaha#configure terminal
Yamaha(config)#clock summer-time JDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00 ①
Yamaha(config)#exit
Yamaha#show clock detail ②
Fri Jan 1 00:00:20 JST 2021

Summer Time
Type : Recurring
Offset : 60 (min)
From : Sun Mar 14 02:00:00 JST 2021 ③
To : Sun Nov 7 02:00:00 JDT 2021
```

- ① サマータイムの設定
- ② サマータイムの設定確認
- ③ 次(または現在施行中)のサマータイム期間の実際の日付を表示

日付指定

サマータイムが 2021 年 3 月 14 日の 2 時に始まり、2021 年 11 月 7 日の 2 時に終わるように設定します。

```
Yamaha#configure terminal
Yamaha(config)#clock summer-time JDT date Mar 14 2021 2:00 Nov 7 2021 2:00 ①
Yamaha(config)#exit
Yamaha#show clock detail ②
Fri Jan 1 00:02:54 JST 2021

Summer Time
Type : Date
Offset : 60 (min)
From : Sun Mar 14 02:00:00 JST 2021
To : Sun Nov 7 02:00:00 JDT 2021
```

- ① サマータイムの設定
- ② サマータイムの設定確認

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SNMPv2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、上述の通り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ルーター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可能です。

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。

snmp-server startup-trap-delay コマンドで、起動時に送信するトラップの送信タイミングを設定可能です。

SNMPv2c

SNMPv1と同様に、コミュニティ名によりSNMPマネージャ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可能です。
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-server startup-trap-delay コマンドで、起動時に送信するトラップの送信タイミングを設定可能です。

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、リプレイ攻撃などから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
ユーザが所属するグループの設定のパラメータでセキュリティのレベルを指定することができます。
セキュリティレベルは認証・暗号化の組み合わせで以下のように分類できます。
 - noAuthNoPriv : 認証・暗号化を行わない
 - AuthNoPriv : 認証のみ行う
 - 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でメッセージが改竄されていないことと送信者がユーザ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-MD5-96と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DES-CBCとAES128-CFBをサポートします。

snmp-server user コマンドで、ユーザ名と所属するグループ名、ユーザ認証方式、暗号化方式、パスワードを設定することができます。

グループ設定で指定したセキュリティレベルに応じて、必要な認証と暗号化の設定を行います。

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。

- グループ

VACMでは、後述のアクセスポリシーをユーザ毎ではなくグループ毎に定義します。

snmp-server user コマンドのgroupオプションでユーザが所属するグループを設定します。ここで指定したグループ毎にアクセス可能なMIBビューを設定します。

- MIBビュー

SNMPv3では、グループ毎にアクセスできるMIBオブジェクトの集合を定義できます。このときMIBオブジェクトの集合をMIBビューと呼び、MIBビューは、オブジェクトIDのツリーを表すビューサブツリーを集約することで表現されます。

snmp-server view コマンドでMIBビューの設定を行います。ビューサブツリー毎にMIBビューに含めるか除外するかを選択できます。

- アクセスポリシー

VACMでは、グループ毎に読み込み、書き込みが許可されるMIBビューを設定します。

snmp-server group コマンドでグループ名、セキュリティレベル、MIBビューを設定します。

MIBビューは **snmp-server view** コマンドで設定されているMIBビューとなります。

- ・ 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-server startup-trap-delay コマンドで、起動時に送信するトラップの送信タイミングを設定可能です。

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	snmp-server host
システム起動時に通知メッセージを送信するまでの待機時間の設定	snmp-server startup-trap-delay
送信する通知メッセージタイプの設定	snmp-server enable trap
システムコンタクトの設定	snmp-server contact
システムロケーションの設定	snmp-server location
SNMPコミュニティの設定	snmp-server community
SNMPビューの設定	snmp-server view
SNMPグループの設定	snmp-server group
SNMPユーザーの設定	snmp-server user
SNMPサーバーのアクセス設定	snmp-server access
SNMPコミュニティの情報の表示	show snmp community
SNMPビューの設定内容の表示	show snmp view
SNMPグループの設定内容の表示	show snmp group
SNMPユーザーの設定内容の表示	show snmp user

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 permit 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。

3. コミュニティー名"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 permit 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。

1. internetノード(1.3.6.1)以下を表すビューを "most" とします。
2. mib-2ノード(1.3.6.1.2.1)以下を表すビューを "standard" とします。
3. ユーザーグループ "admins" を作成し、"admins" グループに所属するユーザーに mostビュー へのフルアクセス権を与えます。
4. ユーザーグループ "users" を作成し、"users" グループの所属するユーザーに standardビュー への読み出しアクセス権を与えます。
5. "admins" グループに所属するユーザー "admin1" を作成します。
認証アルゴリズムに "HMAC-SHA-96" を採用し、パスワードを "passwd1234" とします。
暗号化アルゴリズムに "AES128-CFB" を採用し、暗号パスワードを "passwd1234" とします。
6. "users" グループに所属するユーザー "user1" を作成します。
認証アルゴリズムに "HMAC-SHA-96" を採用し、パスワードを "passwd5678" とします。
7. 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。
8. 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 view most 1.3.6.1 include ... 1
Yamaha(config)# snmp-server view standard 1.3.6.1.2.1 include ... 2
Yamaha(config)# snmp-server group admins priv read most write most ... 3
Yamaha(config)# snmp-server group users auth read standard ... 4
Yamaha(config)# snmp-server user admin1 admins auth sha passwd1234 priv aes passwd1234 ... 5
Yamaha(config)# snmp-server user user1 users auth sha passwd5678 ... 6
Yamaha(config)# snmp-server host 192.168.10.13 traps version 3 priv admin1 ... 7
Yamaha(config)# snmp-server host 192.168.20.13 informs version 3 priv admin1 ... 8
```

注意事項

- ・ご使用のSNMPマネージャが対応する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。
- ・SNMPv3に関連する以下の機能には対応していません。
 - プロキシ機能
 - snmpV2サブツリー (1.3.6.1.6) 以降のMIBオブジェクトへのアクセス。また、SNMP経由によるSNMPv3関連の設定変更はサポートしていません。
- ・コミュニティ名、ユーザー名、パスワード、グループ名の文字列の仕様は以下の通りです。
 - "" または " で囲まれていたときに、""、" 内の文字列が使用されます。
 - "" または " の外側に文字列があるケースはサポートしていません。
 - "" または " で囲まれていたときは、両端の ""、" は文字列の文字数に含まれません。

-
- グループ名は、**snmp-server user** コマンドで使用する文字列に適用されます。
 - **snmp-server group** コマンドで使用する文字列には適用されません。
 - \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。
 - **snmp-server access** コマンドによる、SNMPサーバーに対するアクセスの制限は、SNMPv1, SNMPv2c のアクセスのみ適用されます。SNMPv3 のアクセスには適用されません。

関連文書

- [Yamaha RTpro SNMP](#)
- [Yamaha RTpro Private MIB](#)
- [SNMP MIBリファレンス](#)

RMON

機能概要

RMON (Remote network MONitoring) 機能の設定を行うことにより、インターフェース毎の通信量やエラーの発生状況などを監視、記録することができます。

RMON機能の設定および、RMON機能で取得したデータはMIBとして保持しているため、SNMPマネージャーから取得、変更することができます。

本製品のRMON機能は、RFC2819で定義されている以下のグループに対応しています。

- ・ イーサネット統計情報グループ
- ・ 履歴グループ
- ・ アラーム・グループ
- ・ イベント・グループ

用語の定義

RMON MIB

RFC2819で定義されている、RMON機能用のMIB。

イーサネット統計情報グループ

RMON MIB のグループ1として定義されているMIBグループ。

イーサネットの統計情報をモニターするためのテーブルを持ちます。

テーブルの情報には、パケット数や、エラー数等のカウンターがあります。

本製品で対象となるMIBは、etherStatsTableです。

履歴グループ

RMON MIB のグループ2として定義されているMIBグループ。

設定した間隔で、イーサネット統計情報グループと同様の情報を測定し、測定した情報の履歴を保存するためのテーブルを持ちます。

本製品で対象となるMIBは、historyControlTableと、etherHistoryTable です。

アラームグループ

RMON MIB のグループ3として定義されているMIBグループ。

設定した間隔で、イーサネット統計情報グループの統計情報をしきい値と比較します。

サンプリングした値がしきい値を超えた場合、イベントグループで定義したイベントが発生します。

本製品で対象となるMIBは、alarmTable です。

イベントグループ

RMON MIB のグループ9として定義されているMIBグループ。

アラームグループの条件に合致したときの対応する動作です。

本製品で対象となるMIBは、eventTable です。

機能詳細

RMON機能の動作仕様について以下に示します。

グループ共通

グループで共通の仕様について以下に示します。

1. 本製品でRMON機能を有効にするには、システム全体のRMON機能を有効にする必要があります。
 - **rmon** コマンドで設定を行います。
 - 初期設定は有効となっています。
 - プライベートMIB `ysrmonSetting(1.3.6.1.4.1.1182.3.7.1)`を用いて設定することも可能です。

イーサネット統計情報グループ

イーサネット統計情報グループの動作仕様について以下に示します。

1. インターフェースに対して、**rmon statistics** コマンドで設定を行います。
2. **rmon statistics** コマンドを設定した時点から、統計情報の収集が行われ、RMON MIBの `etherStatsTable` が取得できるようになります。
3. 物理インターフェースに設定が可能です。
4. 同一インターフェースに対する、**rmon statistics** コマンドの設定数の上限は8です。
5. **rmon statistics** コマンドを削除した場合、収集した統計情報も削除されます。
6. **rmon statistics** コマンドを上書きした場合は、これまで収集した統計情報を削除したうえで、再度収集を開始します。
7. システム全体でRMON機能を無効にした場合、統計情報の収集が中断されます。
その後、システム全体のRMON機能を有効にした場合、これまで収集した統計情報を削除したうえで、再度収集を開始します。
8. イーサネット統計情報グループで、対応しているOIDは以下の通りです。

```
rmon(1.3.6.1.2.1.16)
+- statistics(1.3.6.1.2.1.16.1)
  +- etherStatsTable(1.3.6.1.2.1.16.1.1)
    + etherStatsEntry(1.3.6.1.2.1.16.1.1.1) { etherStatsIndex }
      +- etherStatsIndex(1.3.6.1.2.1.16.1.1.1.1)      (read-only)
      +- etherStatsDataSource(1.3.6.1.2.1.16.1.1.1.2) (read-create)
        | 監視対象のインターフェース
      +- etherStatsDropEvents(1.3.6.1.2.1.16.1.1.1.3) (read-only)
        | ドロップパケット数
      +- etherStatsOctets(1.3.6.1.2.1.16.1.1.1.4)      (read-only)
        | 受信オクテット数
      +- etherStatsPkts(1.3.6.1.2.1.16.1.1.1.5)        (read-only)
        | 受信パケット数
      +- etherStatsBroadcastPkts(1.3.6.1.2.1.16.1.1.1.6) (read-only)
        | ブロードキャストパケット受信数
      +- etherStatsMulticastPkts(1.3.6.1.2.1.16.1.1.1.7) (read-only)
        | マルチキャストパケット受信数
      +- etherStatsCRCAlignErrors(1.3.6.1.2.1.16.1.1.1.8) (read-only)
        | FCSエラーパケット受信数
      +- etherStatsUndersizePkts(1.3.6.1.2.1.16.1.1.1.9) (read-only)
        | アンダーサイズパケット受信数(64オクテット未満のパケット)
      +- etherStatsOversizePkts(1.3.6.1.2.1.16.1.1.1.10) (read-only)
        | オーバーサイズパケット受信数(1518オクテットを超えるパケット)
      +- etherStatsFragments(1.3.6.1.2.1.16.1.1.1.11)   (read-only)
        | フラグメントパケット受信数
```

```

|(64オクテット未満でFCSが異常であるパケット)
+- etherStatsJabbers(1.3.6.1.2.1.16.1.1.12)      (read-only)
|ジャバークラッシュ受信数
|(1518オクテットを超えるFCSが異常であるパケット)
+- etherStatsCollisions(1.3.6.1.2.1.16.1.1.13)   (read-only)
|コリジョン数
+- etherStatsOwner(1.3.6.1.2.1.16.1.1.20)        (read-create)
|オーナー名
+- etherStatsStatus(1.3.6.1.2.1.16.1.1.21)       (read-create)
統計グループの状態

```

履歴グループ

履歴グループの動作仕様について以下に示します。

1. インターフェースに対して、**rmon history** コマンドで設定を行います。
2. **rmon history** コマンドを設定した時点から、設定した間隔で履歴情報の収集が行われ、RMON MIBの etherHistoryTable が取得できるようになります。
3. 物理インターフェースに設定が可能です。
4. 同一インターフェースに対する、**rmon history** コマンドの設定数の上限は8です。
5. **rmon history** コマンドを削除した場合、収集した履歴情報も削除されます。
6. **rmon history** コマンドを上書きした場合は、これまで収集した履歴情報を削除したうえで、再度収集を開始します。
7. システム全体でRMON機能を無効にした場合、履歴情報の収集が中断されます。
その後、システム全体のRMON機能を有効にした場合、これまで収集した履歴情報を削除したうえで、再度収集を開始します。
8. 履歴グループで、対応しているOIDは以下の通りです。

```

rmon(1.3.6.1.2.1.16)
+- history(1.3.6.1.2.1.16.2)
  +- historyControlTable(1.3.6.1.2.1.16.2.1)
    |+ historyControlEntry(1.3.6.1.2.1.16.2.1.1) { historyControlIndex }
    |+ historyControlIndex(1.3.6.1.2.1.16.2.1.1.1)      (read-only)
    |+ historyControlDataSource(1.3.6.1.2.1.16.2.1.1.2) (read-create)
    ||監視対象のインターフェース
    |+ historyControlBucketsRequested(1.3.6.1.2.1.16.2.1.1.3)(read-create)
    ||履歴グループの履歴保持要求数
    |+ historyControlBucketsGranted(1.3.6.1.2.1.16.2.1.1.4) (read-only)
    ||履歴グループの履歴保持数
    |+ historyControlInterval(1.3.6.1.2.1.16.2.1.1.5)      (read-create)
    ||履歴グループの履歴保存間隔
    |+ historyControlOwner(1.3.6.1.2.1.16.2.1.1.6)          (read-create)
    ||オーナー名
    |+ historyControlStatus(1.3.6.1.2.1.16.2.1.1.7)         (read-create)
    |履歴グループの状態
    |
  +- etherHistoryTable(1.3.6.1.2.1.16.2.2)
    + etherHistoryEntry(1.3.6.1.2.1.16.2.2.1) { etherHistoryIndex,
etherHistorySampleIndex }
      +- etherHistoryIndex(1.3.6.1.2.1.16.2.2.1.1)      (read-only)
      +- etherHistorySampleIndex(1.3.6.1.2.1.16.2.2.1.2) (read-only)

```

```

+- etherHistoryIntervalStart(1.3.6.1.2.1.16.2.2.1.3) (read-only)
|履歴グループの履歴保存間隔
+- etherHistoryDropEvents(1.3.6.1.2.1.16.2.2.1.4) (read-only)
|ドロップパケット数
+- etherHistoryOctets(1.3.6.1.2.1.16.2.2.1.5) (read-only)
|受信オクテット数
+- etherHistoryPkts(1.3.6.1.2.1.16.2.2.1.6) (read-only)
|受信パケット数
+- etherHistoryBroadcastPkts(1.3.6.1.2.1.16.2.2.1.7) (read-only)
|ブロードキャストパケット受信数
+- etherHistoryMulticastPkts(1.3.6.1.2.1.16.2.2.1.8) (read-only)
|マルチキャストパケット受信数
+- etherHistoryCRCAlignErrors(1.3.6.1.2.1.16.2.2.1.9)(read-only)
|FCSエラーパケット受信数
+- etherHistoryUndersizePkts(1.3.6.1.2.1.16.2.2.1.10)(read-only)
|アンダーサイズパケット受信数(64オクテット未満のパケット)
+- etherHistoryOversizePkts(1.3.6.1.2.1.16.2.2.1.11) (read-only)
|オーバーサイズパケット受信数(1518オクテットを超えるパケット)
+- etherHistoryFragments(1.3.6.1.2.1.16.2.2.1.12) (read-only)
|フラグメントパケット受信数
|(64オクテット未満でFCSが異常であるパケット)
+- etherHistoryJabbers(1.3.6.1.2.1.16.2.2.1.13) (read-only)
|ジャバーパケット受信数
|(1518オクテットを超えるFCSが異常であるパケット)
+- etherHistoryCollisions(1.3.6.1.2.1.16.2.2.1.14) (read-only)
|コリジョン数
+- etherHistoryUtilization(1.3.6.1.2.1.16.2.2.1.15) (read-only)
ネットワーク使用率推定値

```

アラームグループ

アラームグループの動作仕様について以下に示します。

1. **rmon alarm** コマンドで設定を行います。
2. **rmon alarm** コマンドを設定した時点から、設定した間隔でサンプリングが行われます。
3. **rmon alarm** コマンドを上書きした場合は、これまでのサンプリングデータを削除したうえで、再度サンプリングを開始します。
4. システム全体でRMON機能を無効にした場合、サンプリングが中断されます。
その後、システム全体のRMON機能を有効にした場合、これまでのサンプリングデータを削除したうえで、再度サンプリングを開始します。
5. アラームグループの監視対象は、etherStatsEntry(.1.3.6.1.2.1.16.1.1.1)のMIBオブジェクトのうち、カウンタ型を持つMIBオブジェクトのみ指定可能です。
6. **rmon alarm** コマンドで使用しているイーサネット統計情報グループが削除された場合、**rmon alarm** コマンドも削除されます。
7. **rmon alarm** コマンドで使用しているイベントグループが削除された場合、**rmon alarm** コマンドも削除されます。
8. アラームグループで、対応しているOIDは以下の通りです。

```

rmon(1.3.6.1.2.1.16)
+- alarm(1.3.6.1.2.1.16.3)
  +- alarmTable(1.3.6.1.2.1.16.3.1)

```

```

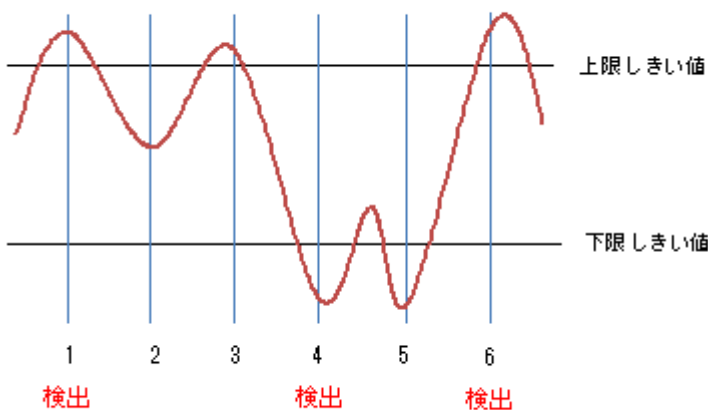
+ alarmEntry(1.3.6.1.2.1.16.3.1.1) { alarmIndex }
  +- alarmIndex(1.3.6.1.2.1.16.3.1.1.1)          (read-only)
  +- alarmInterval(1.3.6.1.2.1.16.3.1.1.2)        (read-create)
  | サンプル間隔
  +- alarmVariable(1.3.6.1.2.1.16.3.1.1.3)         (read-create)
  | 監視対象MIBオブジェクト
  +- alarmSampleType(1.3.6.1.2.1.16.3.1.1.4)       (read-create)
  | サンプル種別
  +- alarmValue(1.3.6.1.2.1.16.3.1.1.5)           (read-only)
  | 測定値
  +- alarmStartupAlarm(1.3.6.1.2.1.16.3.1.1.6)     (read-create)
  | アラームの最初の判定で使用するしきい値
  +- alarmRisingThreshold(1.3.6.1.2.1.16.3.1.1.7)  (read-create)
  | 上限しきい値
  +- alarmFallingThreshold(1.3.6.1.2.1.16.3.1.1.8) (read-create)
  | 下限しきい値
  +- alarmRisingEventIndex(1.3.6.1.2.1.16.3.1.1.9) (read-create)
  | 上限を超えたときのイベントインデックス
  +- alarmFallingEventIndex(1.3.6.1.2.1.16.3.1.1.10) (read-create)
  | 下限を超えたときのイベントインデックス
  +- alarmOwner(1.3.6.1.2.1.16.3.1.1.11)          (read-create)
  | オーナー名
  +- alarmStatus(1.3.6.1.2.1.16.3.1.1.12)         (read-create)
  | アラームグループの状態

```

アラームの検出は、上限しきい値、下限しきい値で決まります。しきい値を超えた場合に、設定したイベントが実行されます。

アラームを検出した場合、反対側のしきい値を超えるまで、再度アラームを検出することはありません。

以下のケースを例に説明します。



- 1 では、上限しきい値を超えたため、アラームを検出します。
また、一番最初の判定で使用するしきい値は、STARTUP にて指定可能です。
上記の例では、STARTUPの設定値が「1」（上限しきい値のみ使用する(risingAlarm))または、「3」（上限しきい値、下限しきい値の両方を使用する(risingOrFallingAlarm))に設定されているものとします。
- 2 では、アラームを検出しません。
- 3 では、上限しきい値を超えていますが、それまでに反対側の下限しきい値を超えていないため、アラームを検出しません。

- ・ 4 では、下限しきい値を超えており、それまでに上限しきい値を超えていたため、アラームを検出します。
- ・ 5 では、下限しきい値を超えていますが、それまでに反対側の上限しきい値を超えていないため、アラームを検出しません。
- ・ 6 では、上限しきい値を超えており、それまでに下限しきい値を超えていたため、アラームを検出します。

イベントグループ

イベントグループの動作仕様について以下に示します。

1. **rmon event** コマンドで設定を行います。
2. イベントグループで指定できる動作は以下の通りです。
 - ログへの記録
 - SNMPトラップの送信
 - ログに記録と、SNMPトラップ送信の両方
3. トラップの送信を指定した場合、SNMPトラップを送信するために、以下のSNMPコマンドの設定が必要です。
 - **snmp-server host**
 - **snmp-server enable trap rmon**
4. トラップの送信を指定した場合、以下の動作になります。
 - SNMPv1、SNMPv2c
 - **rmon event** コマンドで指定したコミュニティ名と、**snmp-server host** コマンドで指定したコミュニティ名が一致しているホストのみにトラップが送信されます。
 - SNMPv3
 - **rmon event** コマンドで指定したコミュニティ名と、**snmp-server host** コマンドで指定したユーザー名が一致しているホストのみにトラップが送信されます。
5. イベントグループで、対応しているOIDは以下の通りです。

```
rmon(1.3.6.1.2.1.16)
+- event(1.3.6.1.2.1.16.9)
  +- eventTable(1.3.6.1.2.1.16.9.1)
    + eventEntry(1.3.6.1.2.1.16.9.1.1) { eventIndex }
      +- eventIndex(1.3.6.1.2.1.16.9.1.1.1)      (read-only)
      +- eventDescription(1.3.6.1.2.1.16.9.1.1.2) (read-create)
        | イベントの説明
      +- eventType(1.3.6.1.2.1.16.9.1.1.3)      (read-create)
        | イベントの種別
      +- eventCommunity(1.3.6.1.2.1.16.9.1.1.4) (read-create)
        | コミュニティー名
      +- eventLastTimeSent(1.3.6.1.2.1.16.9.1.1.5) (read-only)
        | イベント実行時間
      +- eventOwner(1.3.6.1.2.1.16.9.1.1.6)      (read-create)
        | オーナー名
      +- eventStatus(1.3.6.1.2.1.16.9.1.1.7)      (read-create)
        | イベントグループの状態
```

SNMPマネージャーのSetRequestによる設定

SNMPマネージャーのSetRequestでも、各グループのコマンドと同等の内容を設定可能です。
SNMPマネージャーから設定を行う手順について、以下に示します。

イーサネット統計情報(etherStatsTable)グループを、port1.1 に、インデックス1番で新規に設定する方法を例に説明します。

他のグループについても、対応するMIBに対して同様の操作で設定が可能です。

1. SNMPで、MIBの書き込みが可能となる設定にします。
詳細は、[SNMP](#)を参照願います。
2. etherStatsStatus.1に、「2」(createRequest)を設定します。
etherStatsStatus.1の「.1」はetherStatsTableのインデックスです。
3. etherStatsDataSource.1に、監視対象のインターフェースifIndex.5001指定します。
ifIndex.5001はport1.1を指します。
4. ownerの設定は任意ですが、設定する場合は、etherStatsOwner.1に文字列を設定します。
5. etherStatsStatus に、「1」(valid)を設定します。

上記の手順を行った場合、port1.1に以下のコマンドが設定されます。
ownerの設定には、「RMON」を設定したものとします。

```
rmon statistics 1 owner RMON
```

SNMPマネージャーから、システム全体のRMON機能を無効に設定する方法を以下に示します。

1. SNMPで、MIBの書き込みが可能となる設定にします。
詳細は、[SNMP](#)を参照願います。
2. ysrmonSetting(1.3.6.1.4.1.1182.3.7.1)に、「2」(disabled)を設定します。

上記の手順を行った場合、以下のコマンドが設定されます。

```
rmon disable
```

有効に設定する場合は、ysrmonSetting(1.3.6.1.4.1.1182.3.7.1)に、「1」(enabled)を設定します。

関連コマンド

関連コマンドについて、以下に示します。
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
RMON機能の設定	rmon
RMONイーサネット統計情報グループの設定	rmon statistics
RMON履歴グループの設定	rmon history
RMONイベントグループの設定	rmon event
RMONアラームグループの設定	rmon alarm

操作項目	操作コマンド
RMON機能の状態表示	show rmon
RMONイーサネット統計情報グループの状態表示	show rmon statistics
RMON履歴グループの状態表示	show rmon history
RMONイベントグループの状態表示	show rmon event
RMONアラームグループの状態表示	show rmon alarm
RMONイーサネット統計情報グループのカウンターのクリア	rmon clear counters

コマンド実行例

イーサネット統計情報グループの設定

port1.1のイーサネット統計情報グループの設定を行い、SNMPマネージャーから、イーサネット統計情報グループのMIBを取得します。

■設定手順

1. port1.1のイーサネット統計情報グループの設定を有効にします。
イーサネット統計情報グループのインデックスは"1"です。

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

① イーサネット統計情報グループの設定を有効にする

2. SNMPマネージャーから、イーサネット統計情報グループのMIBを取得できるように、SNMPの設定を行います。
ここでは、SNMPv1または、SNMPv2cで、"private"アクセスします。

```
Yamaha(config)#snmp-server community private rw ①
```

① 読み書き可能なコミュニティ名を "private" にする

3. SNMPマネージャーから、コミュニティ名"private"で、etherStatsTable(.1.3.6.1.2.1.16.1.1)を取得できるようになります。

履歴グループの設定

port1.1の履歴グループの設定を行い、SNMPマネージャーから、履歴グループのMIBを取得します。

■設定手順

1. port1.1の履歴グループの設定を有効にします。
履歴グループのインデックスは"1"です。

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


① 履歴グループの設定を有効にする

2. SNMPマネージャーから、履歴グループのMIBを取得できるように、SNMPの設定を行います。
ここでは、SNMPv1または、SNMPv2cで、"private"アクセスします。

```
Yamaha(config)#snmp-server community private rw ①
```

① 読み書き可能なコミュニティ名を "private" にする

3. SNMPマネージャーから、コミュニティ名"private"で、etherHistoryTable(.1.3.6.1.2.1.16.2.2)を取得できるようになります。

アラーム・イベントグループの設定

アラームグループにより、イーサネット統計情報グループの統計情報の値を監視します。
監視する条件は以下の通りです。

- ・ 監視するMIBは、port1.1の etherStatsPkts(.1.3.6.1.2.1.16.1.1.1.5)
- ・ サンプリング間隔は、180秒
- ・ サンプリング種別は、delta
- ・ 上限しきい値の値は2000
- ・ 下限しきい値の値は1000

上記の監視条件に一致した場合、以下のイベントグループを実行します。

- ・ ログに記録し、SNMPトラップを送信する
- ・ コミュニティ名は"RMON"

■ 設定手順

1. SNMPトラップ送信のために必要な設定を行います。

```
Yamaha(config)#snmp-server host 192.168.100.3 traps version 2c RMON ①  
Yamaha(config)#snmp-server enable trap rmon ②
```

① トラップの送信先を設定する

② RMON機能のトラップの送信を有効にする

2. イベントグループの設定を行います。
イベントグループのインデックスは"1"です。

```
Yamaha(config)#rmon event 1 log-trap RMON ①
```

① イベントグループの設定を有効にする

3. アラームグループの監視対象MIBオブジェクトの設定のため、port1.1のイーサネット統計情報グループの設定を有効にします。
イーサネット統計情報グループのインデックスは"1"です。

```
Yamaha(config)#interface port1.1
```

```
Yamaha(config-if)#rmon statistics 1 ①
```

① イーサネット統計情報グループの設定を有効にする

4. 記載した条件で、アラームグループの設定を行います。
アラームグループのインデックスは"1"です。

```
Yamaha(config)#rmon alarm 1 etherStatsPkts.1 interval 180 delta rising-threshold 3000  
event 1 falling-threshold 2000 event 1 ①
```

① アラームグループを有効にする

注意事項

特になし

関連文書

- ・ [保守・運用機能 : SNMP](#)

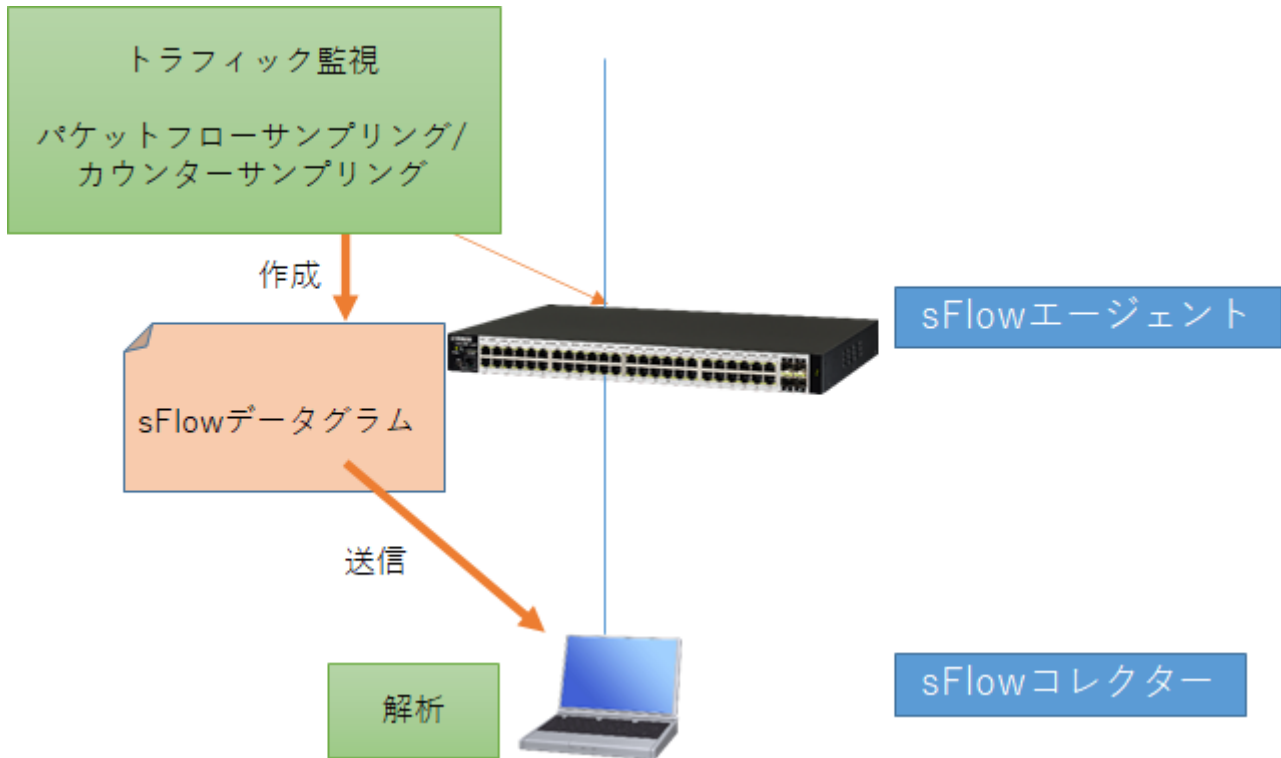
sFlow

機能概要

sFlowはトラフィックを監視する技術です。

sFlowでは、トラフィックに流れる全パケットではなく、特定の割合のパケットをサンプリングすることで、トラフィック情報を統計的に監視することができます。

sFlowは、sFlowエージェントと、sFlowコレクターによって構成されます。



- sFlowエージェント
 - サンプリングでトラフィックを監視し、sFlowの情報を作成する。
 - sFlowの情報を格納したsFlowデータグラムをsFlowコレクターに送信する。
- sFlowコレクター
 - sFlowエージェントから、sFlowの情報を格納したsFlowデータグラムを受け取る。
 - 上記データグラムから、sFlowの情報を収集、解析する。

sFlowエージェントが行う、sFlowのサンプリングには、以下の2種類があります。
以下の両方、または、どちらかの情報がsFlowデータグラムに格納されます。

- パケットフローサンプリング
 - インターフェースで送受信したすべてのパケットのうち、特定の割合をサンプルとして取得する。
- カウンターサンプリング
 - インターフェースのカウンターを定期的にサンプリングする。

本製品は、sFlowエージェントとして動作します。
sFlowコレクターは、別途用意する必要があります。

本製品は、sFlow Version 5 (https://sflow.org/sflow_version_5.txt) に対応しています。

用語の定義

sFlowエージェント

サンプリングでトラフィックを監視し、sFlowの情報を作成後、sFlowの情報をsFlowコレクターに送信する機器。
本製品は、sFlowエージェントとして動作する。

sFlowコレクター

sFlowエージェントから、sFlowの情報を受け取り、情報の収集、解析を行う機器。

パケットフローサンプリング

インターフェースで送受信したすべてのパケットのうち、特定の割合をサンプルとして取得するサンプリング方法。

カウンターサンプリング

インターフェースのカウンターを定期的に取得するサンプリング方法。

sFlowデータグラム

sFlowエージェントがサンプリングによって取得した情報を格納した、UDPのパケット。
sFlowエージェントから、sFlowコレクターに送信される。

機能詳細

sFlow機能の動作仕様について、以下に示します。

1. sFlow機能を有効にする場合は、**sflow enable** コマンドで設定を行います。
 - 初期設定は、**sflow disable** (無効) となっています。
2. **sflow agent** コマンドで、sFlowエージェントの以下の設定を行います。
 - IPアドレス
 - IPv4アドレス
 - IPv6アドレス
 - 本コマンドで設定したIPアドレスはsFlowデータグラムのsFlowヘッダーに使用されます。
 - 初期設定は、設定なしとなっています。
3. **sflow collector** コマンドで、sFlowコレクターの以下の設定を行います。
 - IPアドレス
 - IPv4アドレス
 - IPv6アドレス
 - UDPポート番号
 - 初期値は、6343 です。
 - 本コマンドで設定した、IPアドレス、UDPポート番号宛てに、sFlowデータグラムが送信されます。
 - 初期設定は、設定なしとなっています。
 - 本製品では、sFlowコレクターを1台だけ設定できます。

- 本コマンドが設定されていない場合、サンプリングは開始されません。

4. パケットフローサンプリングの動作は以下の通りです。

- 物理ポートに対して、**sflow sampling-rate** コマンドで、サンプリングレートを設定することで、対象のポートにて、パケットフローサンプリングが行われます。
 - 初期設定は、設定なしとなっています。
- サンプリングレートは、指定したパケットのうちの、1パケットをサンプリングする比率を指定します。
 - 例えば、サンプリングレートを 1000 とした場合、対象のポートで 1000 パケットを送信または、受信したときの1パケットがサンプリングされます。
- 送信と、受信のサンプリングは別々に行われます。
- ポートごとに独立してサンプリングが行われます。
- **sflow max-header-size** コマンドで、パケットフローサンプリングを行う際の、サンプリングするイーサネットフレームのヘッダーサイズの最大値を設定を行います。
 - 初期値は、128です。
- **sflow sampling-rate** コマンドで、サンプリングレートを設定した場合、以下の動作となります。
 - 設定する前のサンプリングレートを用いたサンプリングが終了した後に、新しいサンプリングレートが適用されます。

5. カウンターサンプリングの動作は以下の通りです。

- 物理ポートに対して、**sflow polling-interval** コマンドで、ポーリング間隔を設定することで、対象のポートにて、カウンターサンプリングが行われます。
 - 初期設定は、設定なしとなっています。
- ポーリング間隔は、カウンターを取得する秒数を指定します。
 - 例えば、ポーリング間隔が30の場合、対象ポートのカウンター情報が30秒に1回サンプリングされます。
- ポートごとに独立してサンプリングが行われます。

6. 本製品から送信される、sFlowデータグラムは以下の通りです。

- **sflow collector max-datagram-size** コマンドで、sFlowデータグラムの最大サイズの設定を行います。
- パケットフローサンプリングのsFlowデータグラムには、sFlow Version 5 の以下が格納されます。
 - Raw Packet Header(enterprise = 0, format = 1)
- カウンターサンプリングのsFlowデータグラムには、sFlow Version 5 の以下が格納されます。
 - Generic Interface Counters(enterprise = 0, format = 1)
 - Ethernet Interface Counters(enterprise = 0, format = 2)
 - 使用できないカウンターには、カウンターの最大値が格納されます。(32ビットカウンターであれば、0xFFFFFFFF)

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
sFlow機能の設定	sflow
sFlowエージェントの設定	sflow agent
sFlowコレクターの設定	sflow collector
sFlow データグラムの最大サイズの設定	sflow collector max-datagram-size
パケットフローサンプリングのサンプリングレートの設定	sflow sampling-rate
パケットフローサンプリングのイーサネットフレームの最大ヘッダーサイズの設定	sflow max-header-size
カウンターサンプリングのポーリング間隔の設定	sflow polling-interval
sFlowの状態の表示	show sflow
sFlowのサンプリング情報の表示	show sflow sampling

コマンド実行例

port1.1でsFlowのパケットフローサンプリングと、カウンターサンプリングを実施します。

1. sflowエージェントのIPアドレスを設定します。

```
Yamaha(config)#sflow agent 192.168.100.240
```

2. sFlowコレクターのIPアドレスを設定します。

```
Yamaha(config)#sflow collector 192.168.100.2
```

3. 対象ポートのパケットフローサンプリングのサンプリングレートを設定します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#sflow sampling-rate 1000
```

4. 対象ポートのカウンターサンプリングのポーリング間隔を設定します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#sflow polling-interval 30
```

5. sFlowを有効にします。

```
Yamaha(config)#sflow enable
```

注意事項

- ・ sFlow MIBには対応していません。

-
- スタック構成にて、スタックメイン、スタックメンバー間で、show sflow sampling コマンドのサンプリング情報は同期されません。
 - 通信量が多い環境で **sflow sampling-rate** コマンドが小さい値に設定されている場合、以下となる可能性があります。この場合 **sflow sampling-rate** コマンドの値の見直しを検討してください。
 - **show environment** コマンドで表示されるCPU使用率が高くなります。
 - **show sflow** コマンドで表示される「sFlow Drop Sampling Count」がカウントされます。
 - この値がカウントされている場合、パケットフローサンプリングでサンプリングされたパケットが、高負荷のため処理できずにドロップされています。（※サンプリングはドロップされますが、パケット自体がドロップされるわけではありません）
 - サンプリング対象のポート数、他の機能の動作有無によって変わるため、一概に推奨値を示すことはできませんが、目安として、全ポート使用した場合でも、sFlowでのドロップが発生する可能性が低い **sflow sampling-rate** コマンドの値を以下に示します。
 - 1Gのインタフェースを使用する場合 … 2000 (1/2000)
 - 10Gのインタフェースを使用する場合 … 10000 (1/10000)

関連文書

特になし

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、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。

手動バックアップ時にSDカードに同時にバックアップすることも可能です。

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10000件蓄積可能とします。
Flash ROMへのバックアップは、以下の手段によって行うことができます。
 - システム起動から1時間ごとに行う自動バックアップ
 - **save logging** コマンドによる手動バックアップ
 - **write** コマンドの実行に成功した際に行われるバックアップ
2. 蓄積したログは、**show logging** コマンドにより参照することが可能です。
また、**clear logging** コマンドにより削除することが可能です。
なお、**show logging** コマンドは、RAMの情報を表示します。
本製品のログ情報は、RAMと Flash ROMの情報は、必ず一致していることが前提となります。
（システム起動時、Flash ROMのログ情報をRAMに展開し、サービスを開始します。また、バックアップ実行後、RAMのログ情報は、消去しません。）
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）
通知するログのファシリティ値は、**logging facility** コマンドで設定可能です。工場出荷時は、local0(16)が設定されています。
通知するログのフォーマットは、**logging format** コマンドでヘッダー部（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"
```

4. 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のみを有効にします。
5. **logging backup sd** コマンドにより、SDカードへのSYSLOGバックアップを有効にすることが可能です。
SDカードへのSYSLOGバックアップが有効なとき、**save logging** コマンドを実行すると、SDカード内に日付入りログファイルが保存されます。

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願います。

機能名	コマンド名
ログの出力レベル設定	logging trap
ログのコンソール出力設定	logging stdout
ログの通知先 (SYSLOGサーバ) 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
ログのSDカードバックアップの設定	logging backup sd
ログのファシリティ値の設定	logging facility

コマンド設定例

1. Debugレベルのログ出力を有効して、ファシリティ値10でSYSLOGサーバー (192.168.1.100) にログ出力を開始します。
さらにInformationalレベルのログをコンソールに出力します。

```
Yamaha(config)# logging trap debug ①  
Yamaha(config)# logging facility 10 ②  
Yamaha(config)# logging host 192.168.1.100 ③  
Yamaha(config)# logging stdout info ④
```

- ① Debugレベルのログ出力を有効にする
- ② ファシリティ値を10に設定する

③ SYSLOGサーバーの登録

④ Informationalレベルのログをコンソールに出力する

2. SYSLOGサーバーへの通知を終了します。

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

3. 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
2018/03/08 20:42:46: [ SESSION]:inf: Login succeeded as (noname) for HTTP: 192.168.1.40
2018/03/09 10:06:42: [      NSM]:inf: Interface port1.11 changed state to down
2018/03/09 10:09:48: [ SESSION]:inf: Logout timer expired as (noname) from HTTP:
192.168.1.40
2018/03/09 16:19:36: [      NSM]:inf: Interface port1.17 changed state to up
:
```

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3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
3. SDカードに置かれた更新ファームウェアを本製品に適用する機能

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。
ファームウェア更新中は、LED表示モードの設定に関係なく、**全ポートLEDを緑色で点滅**します

スタック構成時は、スタックメインとスタックメンバー同時に更新ファームウェアの書き込みをします。
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。
再起動の指定方法については [書き込み後の再起動](#) を参照ください。

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. 保守に使用するVLANを決めます。
2. 保守VLANにIPv4アドレスを設定します。設定には、**ip address** コマンドを使用します。
3. 保守VLANからtftpサーバーへのアクセスを許可します。設定には、**tftp-server interface** コマンド、もしくは **management interface** コマンドを使用します。
4. 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。

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。
- ・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。
ただし、管理パスワードが初期設定の状態ではファームウェア更新を受け付けることはできません。前

もって管理パスワードを変更する必要があります。

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3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

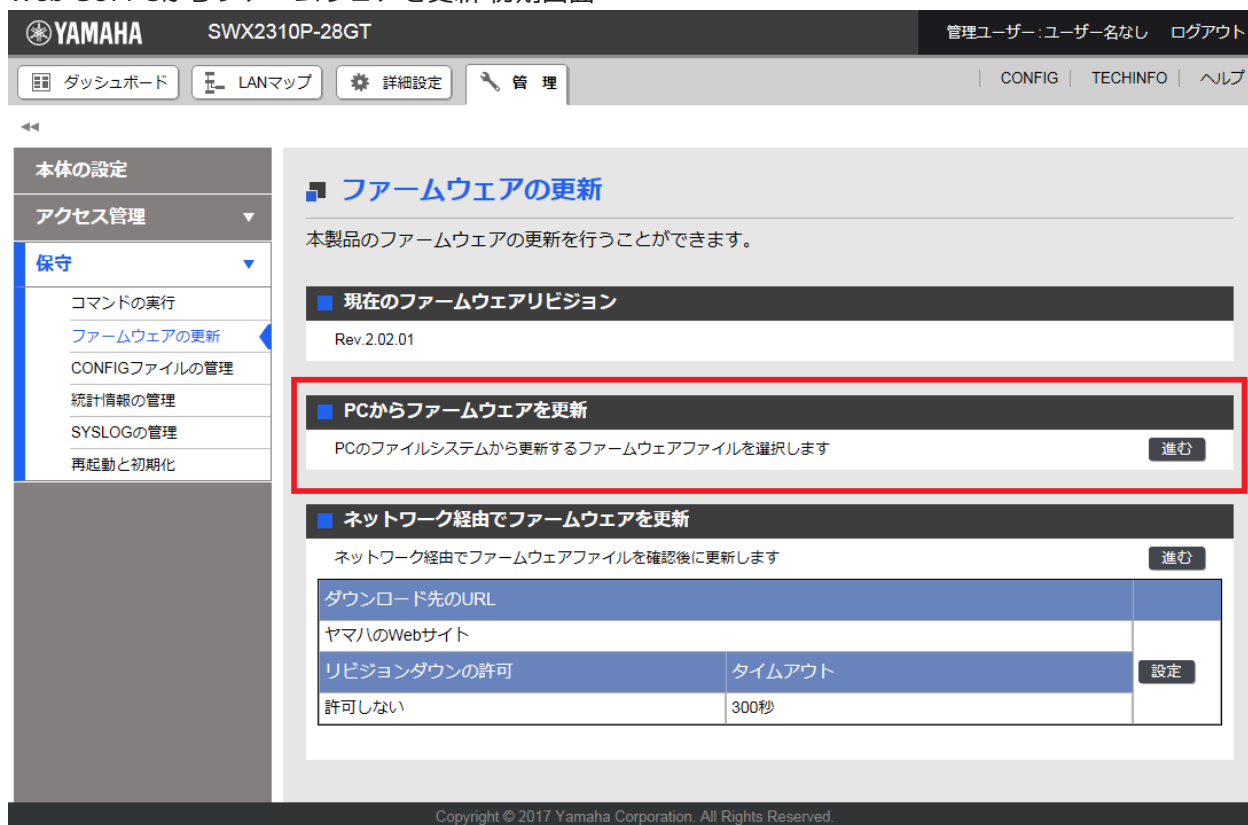
送付した更新ファームウェアに問題がなければ、更新ファームウェアの書き込みを行います。

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、リビジョンダウン許可中に限り、現バージョン以前のものを書き込むことを許可します。

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。

スタックが有効の場合、本機能は利用できません。

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。

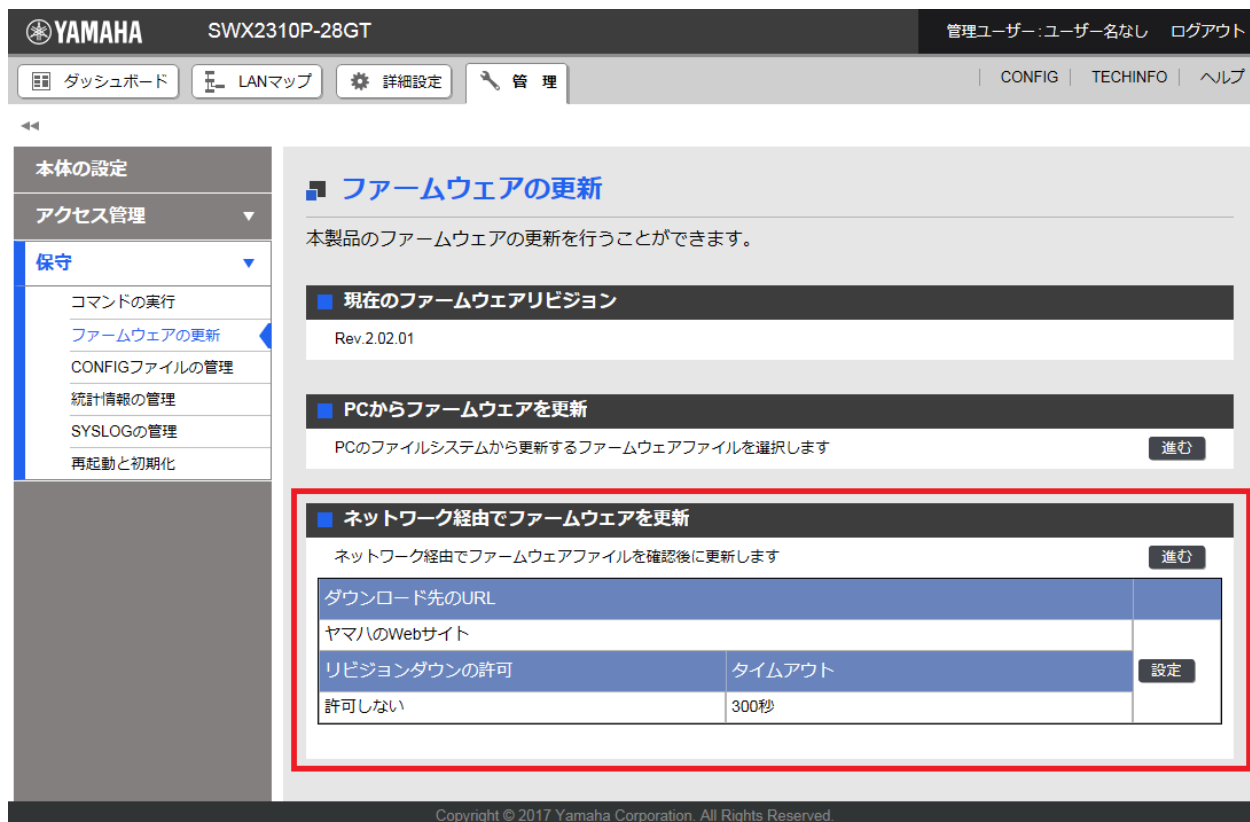
設定パラメータ	説 明
ダウンロード先のURL	ファームウェアのダウンロード先URLを設定します。URLは最大255文字まで設定することができます。 入力形式は“http://サーバーのIPv4/IPv6アドレスあるいはホスト名/パス名”という形式となります。 IPv6アドレスの場合は“[IPv6アドレス]”のように“[]”で囲う必要があります。 サーバーのポート番号が 80 以外の場合は、“http://サーバーの IP アドレスあるいは ホスト名:ポート番号/パス名”という形式で、URL の中に指定する必要があります。 初期値は、以下に設定されています。 http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2310p.bin
プロキシサーバーのURL	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。 初期設定では、プロキシサーバーの設定はありません。 入力形式は“プロキシサーバーのIPv4/IPv6アドレスあるいは http://ホスト名/パス名 ポート番号”という形式となります。 IPv6アドレスの場合は“[IPv6アドレス]”のように“[]”で囲う必要があります。
リビジョンダウンの許可	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。 初期設定では、“許可しない”に設定されています。 なお、現在と同じバージョンの書き込みは許可しません。
タイムアウト	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。 * 新旧ファームウェアのバージョンチェック * 指定URLからのダウンロード 監視タイマーは、100秒 ~ 86,400秒 で指定可能で、初期設定は 300秒 に設定されています。

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**" を参照願います。

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



SDカードを使用した更新

本体に挿入したSDカード内に置かれたファームウェアを更新ファームウェアとして適用させます。本更新は、CLI (Command-line interface) から **firmware-update sd execute** コマンドを使用して行います。

スタック構成の場合は、スタックメインからのみコマンドが使用できます。

ファーム更新確認の入力後はSDカードを抜いても更新を継続します。コマンド実行時にSDカードのアンマウントを行うには、SDカードのマウント状態継続の確認で "N" を入力するか、コマンドで "sd-unmount" オプションを指定してください。

SDカードを本体に挿入したままの状態再起動した際は **boot prioritize sd** コマンドの指定に従いSDカード内のファームウェアから起動されます。

- SDカード内のファイルパス
/swx2310p/firmware/swx2310p.bin

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、自動で再起動します。

firmware-update execute コマンドや、**firmware-update sd execute** コマンドに "no-reboot" オプションが指定されている場合は再起動しません。

no-reboot オプションが指定されておらず、**firmware-update reload-time** コマンドが設定されていた場合、再起動時刻設定に従い再起動します。

次回起動時のリビジョンは **show firmware-update** コマンドで確認することができます。

スタック構成時は **firmware-update reload-method** コマンドにより、ファームウェア更新方法を選択できます。

- 構成中のメンバースイッチを同時に更新する方法
- ネットワークサービスの停止なしに更新する方法

ファームウェア更新方法の動作概要については [スタック 公開技術資料のファームウェア更新](#) を参照ください。

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願います。

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
プロキシサーバーの設定	firmware-update http-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
SDカードからのファームウェア更新の実行	firmware-update sd execute
ファームウェア更新の再起動時刻の設定	firmware-update reload-time
スタック構成時のファームウェア更新の再起動方法の設定	firmware-update reload-method

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/swx2310p.bin> に変更します。
- リビジョンダウンは、**無効** のままとします。
- タイムアウト値は、**300秒** のままとします。
- 再起動時刻の設定を行わず、**更新直後の再起動** とします。

- 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/swx3210p.bin ①
Yamaha(config)#exit
Yamaha#show firmware-update ②
url:http://192.168.100.1/swx2310p.bin
http-proxy: -
timeout: 300 (seconds)
revision-down: Disable
firmware revision for next boot: -
reload-time: -
reload-method: Normal
```

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

- 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.2.02.01
New Revision:      Rev.2.02.03
Downloading...
Update to this firmware? (y/n)y ②
Updating...
Finish
```

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.2.02.01
New Revision:      Rev.2.02.03
Downloading... ①
^CCanceled the firmware download
```

- ① Ctrl-C を入力

HTTPクライアントを使用した更新(プロキシ環境下)

プロキシサーバーを指定し、ファームウェア更新を行います。

- ・ダウンロードのURLは **初期設定** のままとします。
- ・プロキシサーバーの設定は **<http://192.168.100.1:8080>** とします。
- ・リビジョンダウンは、**無効** のままとします。
- ・タイムアウト値は、**300秒** のままとします。
- ・再起動時刻の設定を行わず、**更新直後の再起動** とします。

1. HTTPプロキシを設定し、ファームウェア更新の設定を確認します。

```
Yamaha(config)#firmware-update http-proxy http://192.168.100.1 8080 ①
Yamaha(config)#exit
Yamaha#show firmware-update ②
url: http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx3220.bin
http-proxy: http://192.168.100.1:8080
timeout: 300 (seconds)
revision-down: Disable
firmware revision for next boot: -
reload-time: -
reload-method: Normal
```

- ① HTTPプロキシの設定

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.2.02.01
New Revision:     Rev.2.02.03
Downloading...
Update to this firmware? (y/n)y ②
Updating...
Finish
```

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

SDカードを使用した更新

本体に挿入したSDカード内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。
2台スタック構成での実行例です。

- ・再起動時刻を、**23:30** に変更します。
- ・再起動方法を、スタックメイン・メンバー **順次再起動** に変更します。

1. 再起動時刻と再起動方法を変更します。

```
Yamaha(config)#firmware-update reload-time 23 30 ①
Yamaha(config)#firmware-update reload-method sequential ②
Yamaha(config)#exit
```

- ① 再起動時刻の設定
- ② 再起動方法の設定

2. スタックメインにSDカードを挿入しファームウェア更新を実行します。

```
Yamaha#firmware-update sd execute ①
Update the firmware.
Current Revision: Rev.2.02.01
New Revision:     Rev.2.02.03

Update to this firmware? (y/n)y ②
Continue without unmounting the SD card? (y/n)n ③
Unmounted the SD card. Pull out the SD card.
Updating...
Finish
Yamaha#
(指定した再起動時刻にリブートします)
```

① ファームウェア更新の実行

② yを入力

③ nを入力

3. スタックメンバーは、スタックメインと同時にファーム更新、スタックメイン再起動後にリブートします。
スタックメンバーのコンソールには次のログが表示されます。

```
(スタックメインのENTER入力後、ファームウェアを受け取り更新開始します)
Receiving exec file...
Testing received file...
Writing to Nonvolatile memory...
Done.
```

(スタックメインの再起動を待ちリブートします)

4. 更新ファームウェアのバージョン確認後に、"n" を入力することで中断することができます。

```
Yamaha#firmware-update sd execute ①
Update the firmware.
Current Revision: Rev.2.02.01
New Revision:     Rev.2.02.03

Update to this firmware? (y/n)n ②
Yamaha#
```

① ファームウェア更新の実行

② nを入力

注意事項

ファームウェア更新中に再起動や電源OFFをすると、更新が中断され更新操作前のファームウェアで起動します。

関連文書

- ・ [保守運用機能 :LED制御](#)

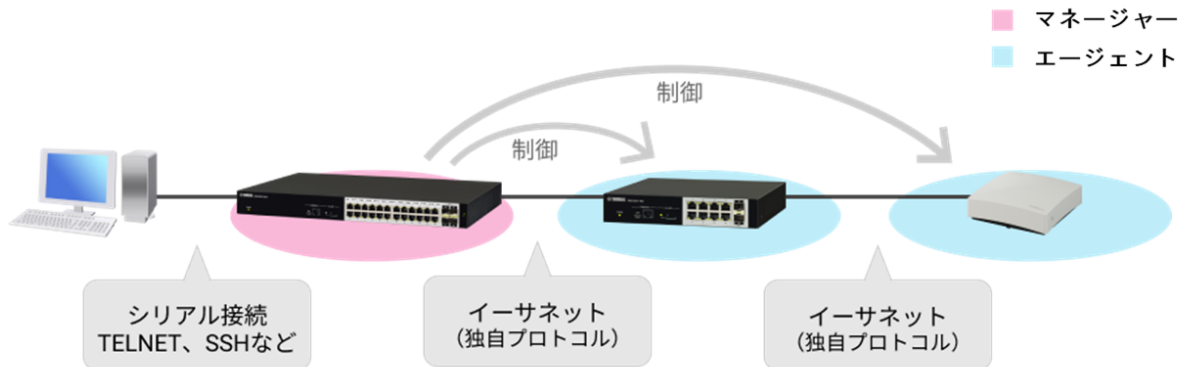
L2MS (Layer2 Management Service)

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L2MSマネージャーと、L2MSマネージャー（以下マネージャーと略す）から制御される複数台のL2MSエージェント（以下エージェントと略す）で構成されます。本機器は、マネージャー、エージェントどちらになることも可能です。

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



PCからマネージャーにはシリアル接続やTELNET、HTTP/HTTPSでログインします。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(L2MS)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SSH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(L2MS)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。
イーサネット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。
- ・ 複数の対応機器を同時制御
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。

L2MSで用いられる独自プロトコル通信は、ヤマハルーターやSWXシリーズ、WLXシリーズなどが対応しているスイッチ制御機能に用いられている通信と同じプロトコルです。従って、マネージャーからSWXシリーズやWLXシリーズを管理することができます。

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

本機器は、L2MSのマネージャー、エージェントどちらになることも可能です。

マネージャーとして動作させる場合、1台のマネージャーで **最大128台** のエージェントを制御することができます。

エージェントとして管理できる機種は以下の通りです。

前述のとおり、スイッチ制御機能(エージェント)に対応している機器も制御することができます。

- SWX2100シリーズ (SWX2100-8G、SWX2100-16G、SWX2100-24G、SWX2100-5PoE、SWX2100-10PoE)
- SWX2110シリーズ (SWX2110-5G、SWX2110-8G、SWX2110-16G)
- SWX2110Pシリーズ (SWX2110P-8G)
- SWX2200シリーズ (SWX2200-8G、SWX2200-24G、SWX2200-8PoE)
- SWX2210シリーズ (SWX2210-8G、SWX2210-16G、SWX2210-24G)
- SWX2210Pシリーズ (SWX2210P-10G、SWX2210P-18G、SWX2210P-28G)
- SWX2220シリーズ (SWX2220-10NT、SWX2220-18NT、SWX2220-26NT)
- SWX2221Pシリーズ (SWX2221P-10NT)
- SWX2220Pシリーズ (SWX2220P-18NT、SWX2220P-26NT)
- SWX2300シリーズ (SWX2300-8G、SWX2300-16G、SWX2300-24G)
- SWX2310シリーズ (SWX2310-10G、SWX2310-18GT、SWX2310-28GT、SWX2310-52GT)
- SWX2310Pシリーズ (SWX2310P-10G、SWX2310P-18G、SWX2310P-28GT)
- SWX2320シリーズ (SWX2320-16MT)
- SWX2322Pシリーズ (SWX2322P-16MT)
- SWX3100シリーズ (SWX3100-10G、SWX3100-18GT)
- SWX3200シリーズ (SWX3200-28GT、SWX3200-52GT)
- SWX3220シリーズ (SWX3220-16MT、SWX3220-16TMs)
- WLXシリーズ
(WLX202、WLX212、WLX222、WLX302、WLX313、WLX322、WLX323、WLX402、WLX413)

エージェントとして動作させる場合、ヤマハルーターもしくはヤマハスイッチのマネージャーから管理されます。

ヤマハルーターの対応機種については、[ヤマハルーターのスイッチ制御機能](#) を参照してください。

使用方法

L2MS動作および役割を、**l2ms** コマンドによって設定します。

- L2MSマネージャーの場合
エージェントとして動作するSWXシリーズや、WLXシリーズ を管理します。
terminal-watch enable コマンドを設定すると、定期的にネットワーク内に存在するPCなどの端末情報の取得し、監視を行います。

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

```
Yamaha(config-l2ms)#l2ms role manager
Yamaha(config-l2ms)#terminal-watch enable
```

- ・ L2MSエージェントの場合
マネージャーとして動作する ヤマハルーターもしくはヤマハスイッチから 管理されます。

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#l2ms enable
Yamaha(config-l2ms)#l2ms role agent
```

show l2ms コマンドで現在の動作や役割を確認することができます。

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, 0xe813

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。

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。

探索フレームの送信時間間隔は、**agent-watch interval** コマンドで設定します。
設定値を大きくすると、送信頻度は減りますが、エージェントを接続してからマネージャーが認識するまでの時間は長くなります。
設定値を小さくした場合はその逆となり、送信頻度は増えますが、エージェントを接続してからマネージャーが認識するまでの時間は短くなります。

マネージャーが探索フレームを一定回数送信してもエージェントから応答フレームを受信しない場合、当該のエージェントはダウンしたと判断します。

回数は **agent-watch down-count** コマンドで設定します。
また、エージェントを接続しているイーサネットケーブルを抜いた場合は当コマンドの設定よりも早いタイミングでエージェントがダウンしたと判断することがあります。

使用するネットワーク環境に合わせて **agent-watch interval** および **agent-watch down-count** コマンドに適切な値を設定してください。

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。

- ・ 探索フレームを30秒間受信しなかった場合
- ・ マネージャーを再起動した場合
- ・ マネージャーで **l2ms reset** コマンドを実行した場合

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。

エージェントを操作するためには、Web GUIのLANマップを使用します。
マネージャーのWeb GUIにログインしたのち、LANマップにて対象のエージェントを選択して操作してください。

LANマップでの詳しい操作方法は、Web GUIのヘルプページを参照してください。

本機器(マネージャー)からコマンドを用いてエージェントを操作することはできませんので、ご注意ください。

LANマップから可能な各エージェントに対する操作について説明します。

SWX2100シリーズに対する操作

エージェントに対して、以下の操作を行うことができます。

- ・ 機器、および、ポートの状態表示
- ・ ポートの給電状態の表示および操作(PoE対応モデルのみ)
- ・ スイッチの設定表示・保守（機能の設定表示、ファームウェアの更新、再起動など）

SWX2110/SWX2110Pシリーズに対する操作

エージェントに対して、以下の操作を行うことができます。

- ・ 機器、および、ポートの状態表示
- ・ ポートの給電状態の表示、および、操作(PoE対応モデルのみ)
- ・ スイッチの設定・保守（機能の設定変更、ファームウェアの更新、再起動など）
- ・ ポートの設定（タグVLANなど）
- ・ コンフィグの保存と復元

SWX2200シリーズに対する操作

エージェントに対して、以下の操作を行うことができます。

- ・ 機器、および、ポートの状態表示
- ・ ポートの給電状態の表示、および、操作(PoE対応モデルのみ)
- ・ スイッチの設定・保守（機能の設定変更、ファームウェアの更新、再起動など）
- ・ マネージャー内への設定の保存、マネージャーが保持している設定との同期

マネージャーからSWX2200の設定を行うと、設定内容がマネージャーとSWX2200の両方に保存されます。

設定は、マネージャーのCONFIGファイルとは別のファイルとして保存されますが、 **startup-config select**

コマンドによって、CONFIGと共に切り替えることが可能です。

SWX2200がマネージャーに管理されている場合は、マネージャーとSWX2200が保持している設定内容が常に同期しています。

設定の同期については「3.6.7. 設定の同期」を参照してください。

マネージャーが管理しているSWX2200に対する設定状態は **show l2ms agent-config** コマンドで確認できます。

SWX2210/SWX2210P/SWX2220/SWX2221P/SWX2220Pシリーズに対する操作

エージェントに対して、以下の操作を行うことができます。

- ・ 機器、および、ポートの状態表示
- ・ ポートの給電状態の表示、および、操作(PoE対応モデルのみ)
- ・ スイッチの設定・保守（機能の設定変更、再起動など）
- ・ ポートの設定（タグVLAN、マルチプルVLANなど）
- ・ リンクアグリゲーションの設定
- ・ IPアドレスの設定変更
- ・ コンフィグの保存と復元
- ・ HTTP Proxy機能を使用した、エージェントのGUIへのログイン
- ・ このスイッチを探す（SWX2220/SWX2221P/SWX2220Pのみ）

HTTP Proxy機能を有効にすることで、マネージャーのLANマップからエージェントのGUIにログインすることができます。

エージェントにログインする際にユーザー名およびパスワードの入力が不要となります。

SWX2210/SWX2210P/SWX2220/SWX2221P/SWX2220Pシリーズは、工場出荷状態で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。

詳しくは「3.6.8. HTTP Proxy機能およびIPアドレスの設定について」を参照してください。

※SWX2210は、Rev.1.02.10 以降のファームウェアで対応しています。

※SWX2210Pは、Rev.1.03.08 以降のファームウェアで対応しています。

SWX2300/SWX2310/SWX2310P/SWX2320/SWX2322P/SWX3100/SWX3200/SWX3220シリーズに対する操作

エージェントに対して、以下の操作を行うことができます。

- ・ 機器、および、ポートの状態を表示
- ・ ポートの給電状態の表示、および、操作(PoE対応モデルのみ)
- ・ IPアドレスの設定変更
- ・ コンフィグの保存と復元
※SWX2300のコンフィグの保存と復元は、Rev.2.00.14 以降のファームウェアで対応しています。
- ・ HTTP Proxy機能を使用した、エージェントのGUIへのログイン

HTTP Proxy機能を有効にすることで、マネージャーのLANマップからエージェントのGUIにログインすることができます。

エージェントにログインする際にユーザー名およびパスワードの入力が不要となります。

SWX2300/SWX2310/SWX2310P/SWX2320/SWX2322P/SWX3100/SWX3200/SWX3220シリーズは、工場出荷状態で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。

詳しくは「3.6.8. HTTP Proxy機能およびIPアドレスの設定について」を参照してください。

WLXシリーズに対する操作

エージェントに対して、以下の操作を行うことができます。

- ・ 機器、LANポート、および無線モジュールの状態を表示
- ・ IPアドレスの設定変更
- ・ コンフィグの保存と復元
- ・ HTTP Proxy機能を使用した、エージェントのGUIへのログイン

HTTP Proxy機能を有効にすることで、マネージャーのLANマップからエージェントのGUIにログインすることができます。

エージェントにログインする際にユーザー名およびパスワードの入力が不要となります。

WLXシリーズは、工場出荷状態で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。

詳しくは「3.6.8. HTTP Proxy機能およびIPアドレスの設定について」を参照してください。

設定の同期

マネージャーでSWX2200を管理している場合、マネージャーとSWX2200が保持している設定内容は常に同期しています。

同期はマネージャーからSWX2200への一方向であり、SWX2200は常にマネージャーが保持している設定で動作します。

マネージャーがSWX2200を管理し始める場合、最初にマネージャーとSWX2200の設定内容が一致しているかどうかを調べます。

一致していない場合は以下の処理が行われます。

1. SWX2200の全設定を初期値に戻す
2. マネージャーが保持している機能の設定値を、SWX2200に転送する

マネージャーは配下のSWX2200の設定内容を定期的に監視しており、マネージャーが保持している設定との不整合を検出した場合に同期処理を行います。

同期処理には時間を要することがあります (数十秒～数分)。

同期処理中のSWX2200に対しては他の操作を行うことができません。

設定を行おうとするとエラーとなり、設定はマネージャーおよびSWX2200に反映されません。

HTTP Proxy機能およびIPアドレスの設定について

SWX2300/SWX2310/SWX2310P/SWX2320/SWX2322P/SWX3100/SWX3200/SWX3220シリーズ、および、WLXシリーズについて以下の動作を行います。

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。ただし、エージェントに **http-server enable** を設定する必要があります。

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。

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LANマップに出力されます。
SYSLOGに出力されるメッセージの詳細は「7. SYSLOGメッセージ一覧」を参照してください。

各エージェントが通知する情報は以下のとおりです。

- 各エージェントがマネージャーに通知する情報

エージェント	通知する情報
SWX2100シリーズ	ポートのリンクアップ/ダウン ループの検出 SFP受光レベルの異常(SWX2100-24G) ポート単位の給電機能の状態(PoE対応モデルのみ) 機器単位の給電機能の異常(PoE対応モデルのみ)
SWX2110シリーズ SWX2110Pシリーズ	ポートのリンクアップ/ダウン ループの検出 ポート単位の給電機能の状態(PoE対応モデルのみ) 機器単位の給電機能の異常(PoE対応モデルのみ)
SWX2200シリーズ SWX2210シリーズ SWX2210Pシリーズ SWX2220シリーズ SWX2221Pシリーズ SWX2220Pシリーズ	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(SWX2200-24G、SWX2200-8PoE、SWX2210P、SWX2220-18NT/26NT、SWX2221P、SWX2220P) ポート単位の給電機能の状態(PoE対応モデルのみ) 機器単位の給電機能の異常(PoE対応モデルのみ) 温度の異常(SWX2220-18NT/26NT、SWX2221P、SWX2220P) 端末監視の状態(SWX2220、SWX2221P、SWX2220P) L2MSマネージャーの重複(SWX2220、SWX2221P、SWX2220P)
SWX2300シリーズ	ポートのリンクアップ/ダウン ループの検出 SFP受光レベルの異常 送信キュー使用率の異常

エージェント	通知する情報
SWX2310シリーズ	ポートのリンクアップ/ダウン
SWX2310Pシリーズ	スタックポートのリンクアップ/ダウン(スタック対応モデルのみ)
SWX2320シリーズ	ループの検出
SWX2322Pシリーズ	SFP受光レベルの異常
SWX3100シリーズ	送信キュー使用率の異常
SWX3200シリーズ	ポート単位の給電機能の状態(PoE対応モデルのみ)
SWX3220シリーズ	機器単位の給電機能の異常(PoE対応モデルのみ)
SWX3220Pシリーズ	温度の異常(SWX2310-52GT、SWX2310P、SWX3200、SWX2320、SWX2322P、SWX3220)
SWX3220Pシリーズ	ファンの異常(SWX2310-52GT、SWX2310P、SWX3200、SWX2320、SWX2322P、SWX3220)
SWX3220Pシリーズ	電源の異常(SWX3200)
SWX3220Pシリーズ	温度センサーの異常(SWX2310P)
SWX3220Pシリーズ	端末監視の状態(稼働/ダウン)
SWX3220Pシリーズ	L2MSマネージャーの重複
WLXシリーズ	無線機能の設定変更

接続端末の監視

マネージャーに **terminal-watch enable** コマンドを設定すると接続端末の監視機能が有効になり、マネージャー、およびエージェントに接続されている端末の情報を管理することができます。マネージャーが管理する接続端末の情報は以下のとおりです。

- ・ マネージャーおよびエージェントがヤマハスイッチの場合
 - 端末のMACアドレス
 - 端末が接続されているマネージャーまたはエージェントのポート番号
 - 端末を検出した日時
- ・ エージェントがヤマハ無線APの場合
 - 端末のMACアドレス
 - 端末が接続されているSSID
 - 端末が接続されている周波数(2.4GHz, 5GHz)
 - 端末を検出した日時

これらの情報は、**show l2ms detail** コマンドで参照することができます。

本機能による端末の推奨管理台数は、ネットワーク構成に関わらず、**200台まで**です。ネットワーク内に推奨管理台数を超える端末が存在する場合、Web GUIのLANマップの動作が重くなったり、応答しなくなることがありますので、ご注意ください。

マネージャーはネットワークの変化に応じて、接続されている端末の検索や管理している端末情報の削除を行います。

マネージャーが接続されている端末の検索を行うタイミングおよび検索対象は以下のとおりです。検索の結果、新しい端末の情報が見つかった場合に端末が検出されたと判断します。

- ・ 端末の検索を行うタイミングと検索を行う対象

タイミング	対象
マネージャーのポートがリンクアップした	マネージャーの当該ポート
新しいエージェントを検出した	検出したエージェントの全ポート
管理しているエージェントからポートのリンクアップが通知された	エージェントの当該ポート
terminal-watch interval コマンドで設定した時間が経過した	マネージャー、および全てのエージェント

また、マネージャーが端末がネットワークからいなくなったと判断して、管理している端末情報を削除するタイミングおよび削除対象は以下のとおりです。

- 端末の情報を削除するタイミングと削除対象となる端末

タイミング	対象
マネージャーのポートがリンクダウンした	マネージャーの当該ポートに接続されていた端末
エージェントのダウンを検出した	当該エージェントに接続されていた全ての端末
管理しているエージェントからポートのリンクダウンが通知された	エージェントの当該ポートに接続されていた端末
接続端末を検索した結果、前回まで検出されていた端末が見つからなかった	見つからなかった端末

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願います。

- L2MS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機能の役割の設定	l2ms role
エージェントの監視時間間隔の設定	agent-watch interval
エージェントのダウン検出を判断する回数の設定	agent-watch down-count
端末の管理機能の設定	terminal-watch enable
端末情報の取得時間間隔の設定	terminal-watch interval
無線AP配下の端末情報の取得時間間隔の設定	wireless-terminal-watch interval
イベント監視機能の設定	event-watch enable
イベント情報の取得時間間隔の設定	event-watch interval

操作項目	操作コマンド
L2MS制御フレームの送受信設定	l2ms filter enable
エージェントのゼロコンフィグ機能を使用するか否かの設定	config-auto-set enable
エージェントの管理のリセット	l2ms reset
L2MSの情報の表示	show l2ms
L2MSのエージェントコンフィグ情報の表示	show l2ms agent-config
スナップショット機能の設定	snapshot enable
スナップショットの比較対象に端末を含めるか否かの設定	snapshot trap terminal
スナップショットの作成	snapshot save
スナップショットの削除	snapshot delete
LANマップのログ出力の設定	logging event lan-map

コマンド実行例

エージェントの監視設定

エージェントの監視時間間隔を設定します。

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#agent-watch interval 8
```

エージェントのダウン検出を判断する回数を設定します。

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#agent-watch down-count 7
```

端末の管理機能の設定

端末の監視機能を有効にします。

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#terminal-watch enable
```

端末情報の取得時間間隔を設定します。

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#terminal-watch interval 3600
```

マネージャーが取得した端末情報を表示します。

```
Yamaha>show l2ms detail
Role : Manager
```

```

[Manager]
Number of Terminals : 0

[Agent]
Number of Agents : 2
[ac44.f230.00a5]
Model name : SWX2100-24G
Device name : SWX2100-24G_Z5301050WX
Route : port2.1
LinkUp : 1, 3, 9
Uplink : 1
Downlink : 3
Config : None
Appear time : Tue Mar 13 18:43:18 2018
Number of Terminals : 1
[bcae.c5a4.7fb3]
Port : 9
Appear time : Wed Mar 14 14:01:18 2018

[00a0.deae.b8bf]
Model name : SWX2300-24G
Device name : SWX2300-24G_S4L000401
Route : port2.1-3
LinkUp : 1
Uplink : 1
Downlink : None
Config : None
Appear time : Tue Mar 13 18:43:18 2018
Number of Terminals : 0

```

L2MS制御フレームの送受信設定

port1.5で、L2MSの制御フレームを送受信しないように設定します。

```

Yamaha(config)#interface port1.5
Yamaha(config-if)#l2ms filter enable

```

イベント監視機能の設定

イベント監視機能を無効にします。

```

Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#event-watch disable

```

イベント情報の取得時間間隔を設定します。

```

Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#event-watch interval 60

```

ゼロコンフィグ機能の使用の有無

マネージャーがエージェントに対してゼロコンフィグ機能を行うか設定します。
この設定は、マネージャーにする必要があります。

ゼロコンフィグ機能を無効にします。

```
Yamaha(config)#l2ms configuration
Yamaha(config-l2ms)#l2ms enable
Yamaha(config-l2ms)#l2ms role manager
Yamaha(config-l2ms)#config-auto-set disable
```

注意事項

機器構成について

エージェントの管理台数は **最大128台** です。

エージェントを直列に接続して使用する場合、接続可能なエージェントの最大台数は **マネージャーから数えて8台まで** です。

エージェントをマネージャーから数えて9台以上直列に接続することはできません。

また、直列に接続するエージェントの台数がマネージャーから数えて8台までであれば、最大管理台数で定められた台数を制御できます。

エージェントをマネージャーから数えて9台以上直列に接続した場合、L2MSの通信が遅延してエージェントの認識や制御が正しく行えず、以下のような不具合が起こることがあります。

- ・ 同期処理が正しく動作しないことがあります
- ・ GUIからエージェントの設定を変更した場合に、正しく実行できないことがあります

また、マネージャーとエージェントの間に他社製スイッチを挟み込むなど、L2MSの通信経路上に他社製スイッチが存在すると、エージェントを正しく制御できないことがあります。

他社製スイッチを含めてネットワークを構成する際は、事前に動作確認を行ってください。

端末の監視について

ネットワーク内に推奨管理台数は、 **最大200台** です。

推奨管理台数を超える端末が存在する場合、Web GUIのLANマップの動作が重くなったり、応答しなくなることがあります。

必要に応じて、端末の管理機能を無効（terminal-watch disableコマンド）にしてください。

端末の検索は、対象機器のFDB (MACアドレステーブル)に登録されている情報を用いて行われます。

このため、検索を行うタイミングによっては、端末が接続されているのに検出されなかったり、端末がネットワークからいなくなったのに検出されたりすることがあります。

マネージャーのポートやヤマハスイッチのポートのリンクダウンが検知された場合、FDB (MACアドレステーブル)に端末が登録されていても、当該ポートに接続されている端末の情報は、全て削除されます。

エージェントがポートに接続されてから、L2MSによってエージェントと認識されるまでに数秒かかる場合があります。

この間、当該エージェントを一つの端末として扱われます。

マネージャーがエージェントとして管理していないヤマハネットワーク機器は、端末として扱われます。

terminal-watch interval コマンドで設定した時間の経過による端末の検索では、マネージャー、および全てのエージェントに対して端末の検索を行うため、ネットワークの構成によっては端末の検索が完了するまでに20分～30分程かかる場合があります。

なお、端末の検索が完了するまでの間に他の処理が実行できなくなることはありません。

L2MS対応機器に他社製L2スイッチが接続されている場合、他社製L2スイッチに接続されている端末はL2MS対応機器に接続されている端末として検出されます。

ただし、他社製L2スイッチに端末とヤマハスイッチが並列に接続されている場合、他社製L2スイッチに接続されている端末を検出することはできません。

他機能との併用について

VLANとの併用

VLANを使用する場合、L2MSの通信が行われるポートはアクセスポートに設定するか、もしくはネイティブVLANが設定されたトランクポートに設定してください。

ネイティブVLANが設定されていないトランクポートでは、L2MSの通信を行うことができません。

ミラーリングとの併用

ミラーリング機能を使用すると、モニターポートで送受信されたL2MSの通信もコピーされます。

このため、ミラーポートにマネージャーやエージェントを接続するとL2MSが正しく動作しないことがありますので、接続しないでください。

ACLとの併用

L2MSの通信はACLの制御対象にはなりません。

ACLでは、許可リストに設定されていないフレームは破棄されます(暗黙の拒否)が、L2MSの通信は制御対象にならないため、破棄されずに転送されます。

STP、ループ検出機能との併用

STPまたは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。

STPによるリンクの切替えが行われると、マネージャーがトポロジを正しく認識できず、エージェントが発見できなかったり、エージェントを発見したときの経路に誤りが生じることがあります。

そのような場合は、STPによるリンクの切替えが完了したのち、**l2ms reset** コマンドを実行して、エージェントの管理をリセットしてください。

複数のMSTインスタンスが動作している場合、L2MSの制御フレームはCIST(インスタンス #0)によって形成される論理経路(ツリー)で送受信されます。

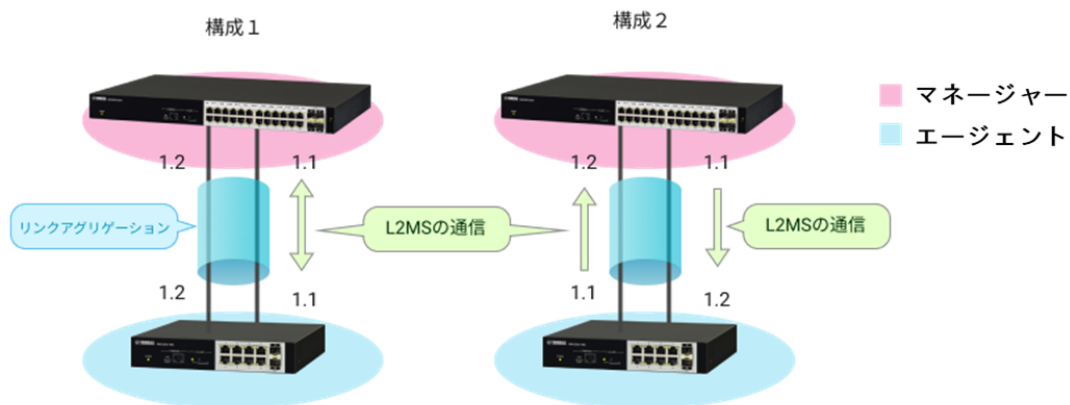
リンクアグリゲーションとの併用

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みなされます。

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。



スタック機能との併用

1台で運用していても、**L2MSは機能します。**

スタック機能が有効でも、メンバースイッチとネゴシエーションがとれない場合、状態はStandaloneとなり、1台で運用することになります。
この場合でも、L2MSは機能します。

- ・ L2MSマネージャーの場合、L2MSエージェントを検出することができます。
- ・ L2MSエージェントの場合、L2MSマネージャーから検出されます。
ただし、Standaloneのスイッチの配下に接続した機器のみが検出され、ダウンしたと思われるもう一方のスイッチに接続した機器は検出されません。

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。

マネージャーとして動作しているときに表示されるSYSLOGには、さらに"**route (addr):**"というプレフィックスが付加されます。

_route* は経路、**addr** はエージェントのMACアドレス("xxxx.xxxx.xxxx" 全て小文字で表示)となります。

- ・ 本体起動時、動作モード変更時に表示されるSYSLOG

分類	出力レベル	メッセージ	意味
動作モード	informational	Start L2MS(Manager)	マネージャーとしてL2MSが起動しました。
		Start L2MS(Agent)	エージェントとしてL2MSが起動しました。
		L2MS is disabled	L2MSは無効に設定されているため、起動しませんでした。
		L2MS mode change mode_from to mode_to	動作モードが mode_from から mode_to に変更されました。

- ・ マネージャーとして動作しているときに表示されるSYSLOG

分類	出力レベル	メッセージ	意味
エージェントの管理	informational	Find agent	エージェントを認識しました。
		Detect down	エージェントがダウンしました。
同期処理	informational	Sync start	エージェントの同期処理を開始しました。
		Sync done	エージェントの同期処理が完了しました。
		Sync failed	エージェントの同期処理に失敗しました。
	debug	Can't get param of sync	同期処理を行うために必要なエージェントの情報を取得できませんでした。
コンフィグ管理	informational	Received config (file)	マネージャーはエージェントからコンフィグファイル(file)を取得し保存しました。
		Sent config (file)	マネージャーはエージェントへコンフィグファイル(file)を送信しました。
		Removed config (file)	コンフィグファイル(file)を削除しました。
端末の管理	debug	Update device info	エージェントに接続されている端末情報を更新しました。
		Fail to update device info	エージェントに接続されている端末情報の更新に失敗しました。
端末情報DB管理	debug	_path* : Format Version: Not found.	端末情報DBファイル path にフォーマットバージョンの記載がありません。
		_path* : Format Version: Illegal value.	端末情報DBファイル path のフォーマットバージョンに不正な値が記載されています。
		_path* : Device Information: Illegal value. (line)	端末情報DBファイル path のデバイス情報に不正な値が記載されています。(_line* 行)
		_path* : Device Information: Duplicate device. (line)	端末情報DBファイル path のデバイス情報に重複したデバイスが記載されています。(_line* 行)
		_path* : Character Code: Not Shift_JIS.	端末情報DBファイル path の文字コードがShift JISで記載されていません。
マネージャーの重複	informational	L2MS manager duplication detected. (addr, port *X_)	L2MSマネージャーの重複を検出しました。(MACアドレス, 重複検出したポート番号)
		L2MS manager duplication resolved. (addr, port *X_)	L2MSマネージャーの重複が解消しました。(MACアドレス, 重複検出したポート番号)

- ・ マネージャーとして動作し、 **logging event lan-map** コマンドが設定されている場合に表示されるSYSLOG
メッセージには、 "[LANMAP]" というプレフィックスが付与されます。

分類	出力レベル	メッセージ	意味
スナップショット機能	informational	SnapShot: Not found. [Device_Name: " *device_name_", MAC_Address: *addr_]	見つからないヤマハスイッチがあります。
		SnapShot: Not found. [MAC_Address: *addr_]	見つからない端末があります。
		SnapShot: Unknown. [Device_Name: " *device_name_", MAC_Address: *addr_]	登録されていないヤマハスイッチがあります。
		SnapShot: Unknown. [MAC_Address: *addr_]	登録されていない端末があります。
		SnapShot: Route difference. [Device_Name: " *device_name_", Route: *route_(UpLink: *uplink_port_), Route(SnapShot): *route_snapshot_(UpLink: *uplink_port_snapshot_), MAC_Address: *addr_]	接続ポートの異なるヤマハスイッチがあります。 正しい経路は route_snapshot_ 、 アップリンクポートは *uplink_port_snapshot です。
		SnapShot: Route difference. [Route: *route_, Route(SnapShot): *route_snapshot_, MAC_Address: *addr_]	接続ポートの異なる端末があります。 正しい経路は route_snapshot です。
		SnapShot: Status recovered. [Device_Name: " *device_name_", MAC_Address: *addr_] / SnapShot: Status recovered. [MAC_Address: *addr_] (split row)	ヤマハスイッチの状態がスナップショットファイルと一致しました。 端末の状態がスナップショットファイルと一致しました。

- ・ マネージャーが受け取るエージェントからの情報通知には以下があります。

分類	出力レベル	メッセージ	意味
リンク状態	informational	port N link up(10-hdx)	エージェントのポート N が10Mbps半二重でリンクアップしました。
		port N link up(10-fdx)	エージェントのポート N が10Mbps全二重でリンクアップしました。
		port N link up(100-hdx)	エージェントのポート N が100Mbps全二重でリンクアップしました。
		port N link up(100-fdx)	エージェントのポート N が100Mbps全二重でリンクアップしました。
		port N link up(1000-fdx)	エージェントのポート N が1Gbps全二重でリンクアップしました。
		port N link up(2500-fdx)	エージェントのポート N が2.5Gbps全二重でリンクアップしました。
		port N link up(5000-fdx)	エージェントのポート N が5Gbps全二重でリンクアップしました。
		port N link up(10000-fdx)	エージェントのポート N が10Gbps全二重でリンクアップしました。
		port N link down	エージェントのポート N がリンクダウンしました。
		stack port(port * N) link up	エージェントのスタックポート(ポート * N)がリンクアップしました。
		stack port(port * N) link down	エージェントのスタックポート(ポート * N)がリンクダウンしました。
ループ検出	informational	port N loop detect	エージェントのポート N でループが発生しています。
		sa N loop detect	エージェントのスタティック論理インターフェース # N でループが発生しています。
		po N loop detect	エージェントのLACP論理インターフェース # N でループが発生しています。
無線機能	informational	Airlink setting changed	エージェントの無線機能が設定変更されました。
PoE	informational	port N PoE state(supply-class0)	エージェントのポート N でclass0の機器に給電を開始しました。
		port N PoE state(supply-class1)	エージェントのポート N でclass1の機器に給電を開始しました。
		port N PoE state(supply-class2)	エージェントのポート N でclass2の機器に給電を開始しました。
		port N PoE state(supply-class3)	エージェントのポート N でclass3の機器に給電を開始しました。
		port N PoE state(supply-class4)	エージェントのポート N でclass4の機器に給電を開始しました。

分類	出力レベル	メッセージ	意味
PoE	informational	port N PoE state(supply-class5)	エージェントのポート N でclass5の機器に給電を開始しました。
		port N PoE state(supply-class6)	エージェントのポート N でclass6の機器に給電を開始しました。
		port N PoE state(supply-class7)	エージェントのポート N でclass7の機器に給電を開始しました。
		port N PoE state(supply-class8)	エージェントのポート N でclass8の機器に給電を開始しました。
		port N PoE state(terminate)	エージェントのポート N の給電が停止しました。
		port N PoE state(overcurrent)	エージェントのポート N で過電流が生じたため、給電が停止しました。
		port N PoE state(forced-terminate)	エージェントのポート N でClass4(30W)給電によりClass3(15.4W)を給電していたポートの給電が停止しました。
		port N PoE state(over-supply)	エージェントのポート N で供給電力が最大給電能力を超えたため、給電が停止しました。
		port N PoE state(over-temperature)	エージェントのポート N で温度異常が発生したため、給電が停止しました。
		port N PoE state(fanlock)	エージェントのポート N でファンが停止したため、給電が停止しました。
		port N PoE state(power-failure)	エージェントのポート N で電源が故障したため、給電が停止しました。
		port N PoE state(class-failure)	エージェントのポート N で電力クラス設定より大きなクラスを認識したため、給電が停止しています。
		PoE state(over-guardband)	エージェントの供給電力量がガードバンドの範囲に入りました。
		port N PoE state(pd-failure)	エージェントのポート N で受電側の異常を認識したため、給電が停止しました。
		port N PoE state(guardband-restrict)	エージェントのポート N でガードバンドを超える給電を認識したため、給電が停止しました。
		PoE state error(over-supply)	エージェントの供給電力が最大給電能力を超えています。
		PoE state error(stop-supply)	エージェントの給電が停止しています。
		PoE state error(power-failure)	エージェントの電源に異常が発生しています。

分類	出力レベル	メッセージ	意味
PoE	informational	PoE state error(over-temperature, stop) Stack N PoE state error(over-temperature, stop)	エージェントの温度異常により給電を強制停止しました。 エージェント(スタックID: *N_)の温度異常により給電を強制停止しました。
		PoE state error(over-temperature, normal) Stack N PoE state error(over-temperature, normal)	エージェントの温度異常による給電強制停止を解除しました。 エージェント(スタックID: *N_)の温度異常による給電強制停止を解除しました。
		PoE state error(fanlock, stop) Stack N PoE state error(fanlock, stop)	エージェントのファン停止により給電を強制停止しました。 エージェント(スタックID: *N_)のファン停止により給電を強制停止しました。
		PoE state error(fanlock, normal) Stack N PoE state error(fanlock, normal)	エージェントのファン停止による給電強制停止を解除しました。 エージェント(スタックID: *N_)のファン停止による給電強制停止を解除しました。
		PoE state error(power-failure, stop) Stack N PoE state error(power-failure, stop)	エージェントの電源異常により給電を強制停止しました。 エージェント(スタックID: *N_)の電源異常により給電を強制停止しました。
SFP受光レベル	informational	port N SFP RX power(low)	エージェントのポート N のSFP受光レベルが下限閾値を下回っています。
		port N SFP RX power(high)	エージェントのポート N のSFP受光レベルが上限閾値を超えています。
		port N SFP RX power(normal)	エージェントのポート N のSFP受光レベルが正常に戻りました。
送信キューの使用率	informational	port N queue Q usage rate(busy)	エージェントのポート N の送信負荷が高くなっています。(QoS送信キュー: *Q_)
		port N queue Q usage rate(full)	エージェントのポート N の送信負荷が上限に達しました。(QoS送信キュー: *Q_)
		port N queue Q usage rate(recovered)	エージェントのポート N の送信負荷が正常に戻りました。(QoS送信キュー: *Q_)

分類	出力レベル	メッセージ	意味
端末監視	informational	ping: *ip-address_(description) state(DOWN)	ping疎通による監視で *ip-address_(description)はダウンしました。
		ping: *ip-address_(description) state(UP)	ping疎通による監視で *ip-address_(description)は稼働中になりました。
		ping: *ip-address_(description) state(IDLE)	ip-address(description)は、ping疎通による監視を行っていません。
		Frame Counter: *port_(description) state(DOWN)	フレーム受信量による監視で *port_(description)はダウンしました。
		Frame Counter: *port_(description) state(UP)	フレーム受信量による監視で *port_(description)は稼働中になりました。
		Frame Counter: *port_(description) state(IDLE)	port(description)は、フレーム受信量による監視を行っていません。
		LLDP: *port_(description) state(DOWN)	LLDPフレームによる監視で *port_(description)はダウンしました。
		LLDP: *port_(description) state(UP)	LLDPフレームによる監視で *port_(description)は稼働中になりました。
		LLDP: *port_(description) state(IDLE)	port(description)は、LLDPフレームによる監視を行っていません。
電源	informational	Power voltage(high) Stack N Power voltage(high)	エージェントの電源電圧が上限閾値を超えました。 エージェント(スタックID: *N_)の電源電圧が上限閾値を超えました。
		Power current(high) Stack N Power current(high)	エージェントの電源で過電流が発生しました。 エージェントスタックID: *N_)の電源で過電流が発生しました。
ファン	informational	Fan lock	エージェントのファンが停止しています。
		FAN control(high) Stack N FAN control(high)	エージェントのファン回転速度が上がりました。 エージェント(スタックID: *N_)のファン回転速度が上がりました。
		FAN control(low) Stack N FAN control(low)	エージェントのファン回転速度が下がりました。 エージェント(スタックID: *N_)のファン回転速度が下がりました。
		FAN X (stop) Stack N FAN X (stop)	エージェントのファン(FAN *X_)が停止しています。 エージェント(スタックID: *N_)のファン(FAN *X_)が停止しています。
		FAN X (normal) Stack N FAN X (normal)	エージェントのファン(FAN *X_)が復旧しました。 エージェント(スタックID: *N_)のファン(FAN *X_)が復旧しました。

分類	出力レベル	メッセージ	意味
温度	informational	CPU temperature(high) Stack N CPU temperature(high)	エージェントのCPU温度が閾値を超えています。 エージェント(スタックID: *N_)のCPU温度が閾値を超えています。
		CPU temperature(normal) Stack N CPU temperature(normal)	エージェントのCPU温度が正常に戻りました。 エージェント(スタックID: *N_)のCPU温度が正常に戻りました。
		CPU temperature error(alarm) Stack N CPU temperature error(alarm)	エージェントのCPUで温度異常が発生しました。 エージェント(スタックID: *N_)のCPUで温度異常が発生しました。
		CPU temperature error(normal) Stack N CPU temperature error(normal)	エージェントのCPUで温度異常が解消されました。 エージェント(スタックID: *N_)のCPUで温度異常が解消されました。
		PHY temperature(high) Stack N PHY temperature(high)	エージェントのPHY温度が閾値を超えています。 エージェント(スタックID: *N_)のPHY温度が閾値を超えています。
		PHY temperature(normal) Stack N PHY temperature(normal)	エージェントのPHY温度が正常に戻りました。 エージェント(スタックID: *N_)のPHY温度が正常に戻りました。
		PHY temperature error(alarm) Stack N PHY temperature error(alarm)	エージェントのPHYで温度異常が発生しました。 エージェント(スタックID: *N_)のPHYで温度異常が発生しました。
		PHY temperature error(normal) Stack N PHY temperature error(normal)	エージェントのPHYで温度異常が解消されました。 エージェント(スタックID: *N_)のPHYで温度異常が解消されました。
		SFP temperature(high) Stack N SFP temperature(high)	エージェントのSFPモジュール温度が閾値を超えています。 エージェント(スタックID: *N_)のSFPモジュール温度が閾値を超えています。
		SFP temperature(normal) Stack N SFP temperature(normal)	エージェントのSFPモジュール温度が正常に戻りました。 エージェント(スタックID: *N_)のSFPモジュール温度が正常に戻りました。
		SFP temperature error(alarm) Stack N SFP temperature error(alarm)	エージェントのSFPモジュールで温度異常が発生しました。 エージェント(スタックID: *N_)のSFPモジュールで温度異常が発生しました。
		SFP temperature error(normal) Stack N SFP temperature error(normal)	エージェントのSFPモジュールで温度異常が解消されました。 エージェント(スタックID: *N_)のSFPモジュールで温度異常が解消されました。

分類	出力レベル	メッセージ	意味
温度	informational	Unit temperature(high) Stack N Unit temperature(high)	endif::[]エージェントの本体温度が閾値を超えています。 エージェント(スタックID: *N_)の本体温度が閾値を超えています。
		Unit temperature(normal) Stack N Unit temperature(normal)	エージェントの本体温度が正常に戻りました。 エージェント(スタックID: *N_)の本体温度が正常に戻りました。
		Unit temperature error(alarm) Stack N Unit temperature error(alarm)	エージェントの本体で温度異常が発生しました。 エージェント(スタックID: *N_)の本体で温度異常が発生しました。
		Unit temperature error(normal) Stack N Unit temperature error(normal)	エージェントの本体で温度異常が解消されました。 エージェント(スタックID: *N_)の本体で温度異常が解消されました。
		PSE temperature(high) Stack N PSE temperature(high)	エージェントのPSE温度が閾値を超えています。 エージェント(スタックID: *N_)のPSE温度が閾値を超えています。
		PSE temperature(normal) Stack N PSE temperature(normal)	エージェントのPSE温度が正常に戻りました。 エージェント(スタックID: *N_)のPSE温度が正常に戻りました。
		PSE temperature error(alarm) Stack N PSE temperature error(alarm)	エージェントのPSEで温度異常が発生しました。 エージェント(スタックID: *N_)のPSEで温度異常が発生しました。
		PSE temperature error(normal) Stack N PSE temperature error(normal)	エージェントのPSEで温度異常が解消されました。 エージェント(スタックID: *N_)のPSEで温度異常が解消されました。
		MAC temperature(high) Stack N MAC temperature(high)	エージェントのMAC温度が閾値を超えています。 エージェント(スタックID: *N_)のMAC温度が閾値を超えています。
		MAC temperature(normal) Stack N MAC temperature(normal)	エージェントのMAC温度が正常に戻りました。 エージェント(スタックID: *N_)のMAC温度が正常に戻りました。
		MAC temperature error(alarm) Stack N MAC temperature error(alarm)	エージェントのMACで温度異常が発生しました。 エージェント(スタックID: *N_)のMACで温度異常が発生しました。
		MAC temperature error(normal) Stack N MAC temperature error(normal)	エージェントのMACで温度異常が解消されました。 エージェント(スタックID: *N_)のMACで温度異常が解消されました。

分類	出力レベル	メッセージ	意味
温度	informa tional	Thermal sensor(alarm) Stack N Thermal sensor(alarm)	エージェントの温度センサーで異常が発生しました。 エージェント(スタックID: *N_)の温度センサーで異常 が発生しました。
コンフィグ 管理	informa tional	Executing a config ... progress % (file)	エージェントでコンフィグファイル(file)の設定を復元 中。進捗率 progress %
		Finished executing a config (file)	エージェントでコンフィグファイル(file)の復元が完了 しました。
		line: errmsg (file)	エージェントでコンフィグファイル(file)の復元中に、 line 行が errmsg エラーになりました。
マネージャ ーの重複	informa tional	l2ms-manager- duplication(occur). (addr, port *X_)	エージェントでL2MSマネージャーの重複を検出しまし た。(MACアドレス, 重複検出したポート番号)
		l2ms-manager- duplication(stop). (addr, port *X_)	エージェントでL2MSマネージャーの重複が解消しまし た。(MACアドレス, 重複検出したポート番号)
機能	informa tional	unsupported function(function)	エージェントは該当のプロトコルに未対応のファーム ウェアです。 _function* には以下が入ります。 Setting info Status l2ms info SFP RX power Qos queue rate Qos queue rate2 Terminal monitoring System monitoring ※Find agent後、初回だけ出力されます。2回目以降の ログ出力は抑制されます。 尚、一旦Detect down した際はこれらはリセットされ ます。

- ・ エージェントとして動作しているときに表示されるSYSLOG

分類	出力レベル	メッセージ	意味
エージェン トの管理	informa tional	Start management by manager(addr)	マネージャーに管理されました。
		Release from manager(addr)	マネージャーの管理から外れました。
再起動	informa tional	Restart by manager request.	マネージャーの要求により再起動します。

分類	出力レベル	メッセージ	意味
コンフィグ管理	informational	Sent config to manager (addr)	マネージャーへコンフィグファイルを送信しました。
		Received config from manager (addr)	マネージャーからコンフィグファイルを受信しました。
		Restart for update settings.	受信したコンフィグファイルを更新するために、再起動します。
マネージャーの重複	informational	L2MS manager duplication detected. (addr, port *X_)	L2MSマネージャーの重複を検出しました。(MACアドレス, 重複検出したポート番号)
		L2MS manager duplication resolved. (addr, port *X_)	L2MSマネージャーの重複が解消しました。(MACアドレス, 重複検出したポート番号)

関連文書

- [ヤマハルーターのスイッチ制御機能](#)

メール通知

機能概要

メール通知機能は、L2MS機能や端末監視機能によって検知した情報を、Eメールで通知する機能です。以下を設定しておくことで各機能で検知した情報を通知できます。

- ・ メール送信時に使用するメールサーバーの設定
- ・ メールテンプレートの設定

用語の定義

メールテンプレート

メールを送信する際に必要な以下の情報をまとめた定義

- ・ 使用するメールサーバー
- ・ 送信元メールアドレス
- ・ 宛先メールアドレス
- ・ メールの件名
- ・ 通知内容
- ・ 送信待機時間

機能詳細

動作

メールサーバーの設定とメールテンプレートの設定を正しく行った状態で、メール通知に対応している機能の通知イベントが発生すると、メール通知機能は送信待機状態になります。

送信待機状態になったメール通知機能は、メールテンプレートごとに設定されたメール送信待機時間が経過するまで待機します。

メール送信待機時間が経過するとメール通知機能は、待機している間に発生した通知イベントをまとめて1通のメールとして各宛先に送信します。

メールサーバーの設定

Web GUI の[詳細設定]-[メール通知]の **登録されているメールサーバーの一覧** より設定できます。

新規 ボタン、または既存の設定の **設定** ボタンを押下することで **メールサーバーの設定** に遷移します。

メールサーバーの設定 では、以下を設定します。

- ・ アカウント識別名
メールサーバーの設定を識別するための名称。省略可能。
- ・ SMTPサーバーアドレス
- ・ SMTPサーバーのポート番号
- ・ SMTPの暗号化
SMTP over SSLによる暗号化、またはSTARTTLSによる暗号化を選択できます
- ・ SMTP認証
SMTP認証を行う場合、ユーザー名とパスワードを入力します

■ メール通知

メールサーバーの設定

各項目を入力してください。入力が完了したら、「確認」ボタンを押してください。

■ 設定に必要な情報入力	
識別番号	1
アカウント識別名	※省略可
SMTPサーバーアドレス	
SMTPサーバーのポート番号	☐ サブミッションポート (587番ポート) 25
SMTPの暗号化	暗号化しない
SMTP認証	認証する ユーザー名: パスワード:
戻る 確認	

メールテンプレートの設定

Web GUI の[詳細設定]-[メール通知]の **メール通知の設定一覧** より設定できます。

新規 ボタン、または既存の設定の **設定** ボタンを押下することで **メール通知の設定** に遷移します。

メール通知の設定 では、以下を設定します。

- ・ 送信元 (From)
- ・ 宛先 (To)
- ・ 件名
既定の件名を使う にチェックを入れると、メールの件名が **Notification from 機器名** になります。
- ・ 通知内容
LANマップの異常検知 では、種別を細かく指定でき、指定した種別だけが通知されるように設定できます。
- ・ メール送信待機時間

メール通知の設定

各項目を入力してください。入力が完了したら、「確認」ボタンを押してください。

■ 設定に必要な情報入力	
識別番号	1
送信元 (From)	SMTPサーバー: 1: yamaha.example.com ▼ メールアドレス:
宛先 (To)	メールアドレス1: メールアドレス2: ※省略可 メールアドレス3: ※省略可 メールアドレス4: ※省略可
件名	☒ 既定の件名を使う
通知内容	☐ LANマップの異常検知 ☐ 端末監視の状態通知 ☐ スタック機能の異常検知
メール送信待機時間	通知イベントが発生してから、一定時間送信を待機します。 待機中に他の通知イベントが発生した場合、それらの通知内容も一通のメールにまとめて送信します。 イベントが発生してから 30 秒待機した後に送信 ※1 - 3600 秒
戻る 確認	

メール通知に対応している機能

以下がメール通知に対応している機能です。

- ・ LANマップ
以下の通知イベントがメール通知の対象となります。

分類	種類	イベント	説明
本体異常	ファン異常	Fan Lock	ファンが停止した
		Fan speed	ファン回転速度が上がった
		Fan stop	特定のファンが停止した
	電源異常	Power voltage	電源電圧が上限閾値を超えた
		Power supply	電源で過電流が発生した
	温度異常	CPU temperature CPU temperature error PHY temperature PHY temperature error SFP temperature SFP module temperature error	ヤマハスイッチの温度(CPU 温度、PHY 温度、SFP モジュール温度、本体温度、PSE 温度、MAC 温度)が閾値を超えた
		Unit temperature Unit temperature error PSE temperature PSE temperature error MAC temperature MAC temperature error	ヤマハスイッチの温度が正常に戻った
		Thermal Sensor invalid	ヤマハスイッチの温度センサーで異常が発生した
	ループ発生	Loop Detect	ポートでループが発生した
			ポートで発生したループが解消された
SFP受光レベル異常	SFP受光レベルの異常	SFP RX Power	SFP受光レベルの閾値を超えた
			SFP受光レベルが正常範囲内に収まった
送信キュー監視	送信キュー使用率の異常	Queue Usage Rate	送信キュー使用率が上昇した
			送信キュー使用率が上限に達した
			送信キュー使用率が正常な値に戻った

分類	種類	イベント	説明
PoE給電	温度異常	Over Temperature	温度異常が発生したため、給電が停止した
	最大給電能力超過	Over Supply	供給電力が最大供給能力を超えた
	電源異常	Power Failure	給電の電源が故障した
	給電Class異常による給電停止	Class Failure	給電ポートで給電Class設定より大きなClassを認識したため、給電が停止した
	Class4給電による給電停止	Forced Terminate	給電ポートでClass4（30W）給電により、Class3（15.4W）を給電していたポートの給電が停止した
	過電流による給電停止	Over Current	給電ポートで過電流が生じたため、給電が停止した
	給電能力超過による給電停止	PoE state error(over-supply)	供給電力が最大供給能力を超えた
			最大給電能力の超過が解消された
	温度異常による給電停止	PoE state error(over-temperature)	温度異常が発生したため、給電が停止した
			温度異常による給電停止が解消された
	ファン停止による給電停止	PoE state error(fanlock)	ファンが停止したため、給電が停止した
			ファン停止による給電停止が解消された
	電源異常による給電停止	PoE state error(power-failure)	PoE 電源異常が発生したため、給電が停止した
スナップショット	不正機器の接続	Illegal Equipment(SnapShot)	スナップショットに登録されていない機器が検出された
			不正機器の接続が解消された
	接続ポートの不一致	Port Mismatch(SnapShot)	接続ポートがスナップショットと異なる機器が検出された
			接続ポートの不一致が解消された
	機器の消失	Disappearance Equipment(SnapShot)	スナップショットに登録されている機器が接続されていない
			機器の消失が解消された
L2MSマネージャーの重複	L2MSマネージャーの重複	L2MS manager duplication	L2MSマネージャーの重複を検出した

- 端末監視機能
以下の通知イベントがメール通知の対象となります。

分類	種類	説明
Ping監視	アップ検知	端末のアップを検知した
	ダウン検知	端末のダウンを検知した

(Detected: 2017/06/13 10:15:42	Recovered: 2017/06/13 10:17:24)
SWX2310P-10G	SWX2310P-10G_S4K000398
00a0.deae.b89c	1.6
port1.7(UpLink:1.5)	
Full(Queue:2)	

[Fan Lock]

Type	Device_Name
MAC_Address	
Route	

```
(Detected: 2017/06/13 10:28:43 Recovered: ----/--/-- --:--:--)  
SWX2200-8PoE SWX2200-8PoE_S45000345  
00a0.de83.4146  
port1.5(UpLink:2)
```

```
(Detected: 2017/06/13 10:42:13   Recovered: 2017/06/13 10:42:22)
SWX2200-24G                               SWX2200-24G_X00000344
00a0.de2a.dbbb
port1.1(UpLink:23)
```

```
<<<<<<<<<<<<<<<<<<      Terminal Monitoring Information      >>>>>>>>>>>>>>>>>>
```

[via Ping]

Date	Status	IP Address	Description
2017/06/13 Thu 10:42:56	UP	192.168.100.155	IP_Camera_1
2017/06/13 Thu 10:51:00	DOWN	192.168.100.155	IP_Camera_1
2017/06/13 Thu 10:54:02	UP	192.168.100.10	Wireless_AP_1
2017/06/13 Thu 11:29:27	UP	192.168.100.155	IP_Camera_1
2017/06/13 Thu 11:30:31	DOWN	192.168.100.10	Wireless AP 1

[via Bandwidth Usage]

Date	Status	Interface	Description
2017/06/13 Thu 10:45:43	UP	port1.4	IP_Camera_2
2017/06/13 Thu 10:45:56	UP	port1.6	Note_PC_1
2017/06/13 Thu 10:50:00	DOWN	port1.6	Note_PC_1
2017/06/13 Thu 10:53:27	DOWN	port1.4	IP_Camera_2

[via LLDP]

Date	Status	Interface	Description
2017/06/13 Thu 10:53:56	UP	port1.3	Note_PC_2
2017/06/13 Thu 11:11:54	DOWN	port1.3	Note_PC_2
2017/06/13 Thu 11:14:24	UP	port1.3	Note_PC_2

[illegible]

Date	Information

```

2017/06/13 Thu 10:53:44 The stack port changed state to down. (port1.27)
2017/06/13 Thu 10:53:46 Promoted to a main. (Old main ID : 1)
2017/06/13 Thu 10:59:10 Occurred the heartbeat error. (ID : 1)

```

LANマップの通知内容

- ・ イベントごとの通知内容

LANマップの通知では、イベントの種類によりメール本文に記載される内容が異なります。
イベントごとの通知内容を以下に示します。

イベント	Type Device_Name MAC_Address	Comment	Stack_ID	Err_Port	Fan_number	Route	Route(SnapShot)	Status
Fan Lock	○	×	×	×	×	○	×	×
Fan speed		×	○	×	×	○	×	×
Fan stop		×	○	×	○	○	×	×
Power voltage Power supply		×	○	×	×	○	×	×
CPU temperature CPU temperature error PHY temperature PHY temperature error SFP temperature SFP module temperature error Unit temperature Unit temperature error PSE temperature PSE temperature error MAC temperature MAC temperature error Thermal Sensor invalid		×	○	×	×	○	×	×
Loop Detect		×	×	○	×	○	×	×
SFP RX Power		×	×	○	×	○	×	○

イベント	Type Device_Name MAC_Address	Comment	Stack_ID	Err_Port	Fan_number	Route	Route(SnapShot)	State
Queue Usage Rate	○	×	×	○	×	○	×	○
Over Temperature Over Supply Power Failure		×	×	×	×	○	×	×
Class Failure Forced Terminate Over Current		×	×	○	×	○	×	×
PoE state error(over-supply) PoE state error(over-temperature) PoE state error(fanlock) PoE state error(power-failure)		×	○	×	×	○	×	×
Illegal Equipment(SnapShot)		○	×	×	×	○	×	×
Port Mismatch(SnapShot)		○	×	×	×	○	○	×
Disappearance Equipment(SnapShot)		○	×	×	×	×	○	×
L2MS manager duplication		○	×	○	×	○	×	×

- ・ 通知内容の詳細
通知内容に含まれる各種情報の詳細を以下に示します。

通知内容	記載例	説明
Detected	Detected: 2021/10/01 8:25:40	異常が発生した日時が記載されます。
Recovered	Recovered: 2021/10/01 10:09:40	異常が解消された日時が記載されます。
Type	SWX2310P-28GT	モデル名が記載されます。
Device_Name	SWX2310P-28GT_XXXXXXXXXX	機器名が記載されます。
MAC_Address	ac44.f2xx.xxxx	MACアドレスが記載されます。

通知内容	記載例	説明
Comment	スナップショット : Comment	LANマップの機器一覧で設定したコメントが記載されます。
	L2MSマネージャーの重複 : ac44.f2xx.xxxx	重複しているL2MSマネージャーのMACアドレスが記載されます。
Stack_ID	1	スタックIDが記載されます。
Err_Port	1.5	異常が発生したポートの番号が記載されます。
Fan_number	1	異常が発生したファンの番号が記載されます。
Route	port1.20(UpLink:1.2)	対象機器の経路情報が記載されます。
Route(Snap Shot)	port1.20(UpLink:1.2)	対象機器のスナップショット上での経路情報が記載されます。
State	SFP受光レベル異常 : Low	SFP受光レベルに応じて、Low / High のいずれかが記載されます。
	送信キュー監視 : Full(Queue:2)	送信キューの使用状況に応じて、Busy / Full のいずれかと送信キュー番号が記載されます。

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願います。

操作項目	操作コマンド
SMTP メールサーバーの設定	mail server smtp host
SMTP メールサーバー名の設定	mail server smtp name
メール通知のトリガー設定	mail notify trigger
メール送信のテンプレート 設定モード	mail template
メール送信のサーバーIDの設定	send server
メール送信の送信元メールアドレスの設定	send from
メール送信の宛先メールアドレスの設定	send to
メール送信の件名の設定	send subject
メール送信待ち時間の設定	send notify wait-time
証明書送付時のメール設定	mail send certificate
証明書通知時のメール設定	mail send certificate-notify
証明書の有効期限切れ通知タイミングの設定	mail certificate expire-notify
メール送信情報の表示	show mail information

注意事項

SMTP認証に関する注意事項です。

- SMTP認証の方式は、LOGINにのみ対応しています。
- PLAINやCRAM-MD5などによる認証は行えません。

メール通知機能のコマンド未対応ファームに関する注意事項です。

- コマンド未対応ファームからコマンド対応ファームにレビジョンアップした場合、WebGUIで設定していたものはコマンド設定として引き継ぎます。
- コマンド未対応ファームに戻す場合、コマンド対応ファームで設定変更したものについては引き継ぐことができませんので、レビジョンダウン後に再設定が必要となります。
- 設定変更をしていないのであれば、そのまま設定を維持することができます。

LANマップの異常検知に関する注意事項です。

- 異常が解消されていない状態でその異常の通知を無効にしても、異常が解消されるまでの間は有効な通知として扱われます。
- 具体的には、通知が無効になったあとでも、異常が解消されたときにメールが送信されたり、別の異常が発生したときのメール本文と一緒に記載されます。

関連文書

- [L2MS制御](#)
- [端末監視](#)
- [スタック](#)

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。自身の機器の情報を一方的に通知し、隣接機器がこれを受信するだけの単純なプロトコルですが、LLDPに対応した機器は、隣接機器から受信した情報をMIBオブジェクトとして保持するため、ユーザーはSNMP経由でその情報にアクセスして、どのような機器がどのインターフェースに接続されているかを把握することができます。

また、PoE (Power Over Ethernet)に対応した機器間でのネゴシエーションにも利用します。

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/SFP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/SFP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で送信する自身の機器の情報、LLDPで収集した隣接機器の情報などをSNMP経由で参照する。

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。

本製品のLLDPでは、SNMPの以下のMIBをサポートします。詳細は **3.3 サポートMIB** を参照してください。

- LLDP-MIB
- LLDP-EXT-DOT3-MIB
- LLDP-V2-MIB
- LLDP-EXT-DOT3-V2-MIB
- LLDP-EXT-MED-MIB

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。

PoEのネゴシエーションでLLDPを利用する場合、必ずPoE受電機器を接続するポートで、LLDPの送受信が可能になるように設定が必要です。

送信情報の設定

自身の機器から送信するLLDPフレームは、以下のコマンドで設定します。また、以下のコマンドの設定に関係なく、かならず送信するTLV (必須TLV) も存在します。

- **tlv-select basic-mgmt** コマンド (基本管理TLV)
- **tlv-select ieee-8021-org-specific** コマンド (IEEE 802.1 TLV)
- **tlv-select ieee-8023-org-specific** コマンド (IEEE 802.3 TLV)
- **tlv-select med** コマンド (LLDP-MED TLV)

基本管理TLVで送信するシステムの名称と説明文は、 **lldp system-name** コマンド、 **lldp system-description** コマンドで設定します。

管理アドレスの種類は、 **set management-address-tlv** コマンドで設定します。

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。

- $TTL = (\text{set timer msg-tx-interval コマンドの設定値}) \times (\text{set msg-tx-hold コマンドの設定値}) + 1 \text{ (秒)}$

LLDP フレームの送信が有効なLAN/SFPポートに隣接機器が接続されたとき、高速送信期間の設定にしたがって、一定期間LLDPフレームを高速で送信します。

高速送信期間の送信間隔や送信個数は、 **set timer msg-fast-tx** コマンド、 **set tx-fast-init** コマンドで設定します。

LLDP フレームの送信が有効な状態から **set lldp** コマンドで無効な状態に設定したとき、本製品はシャットダウンフレームを送信して、隣接機器にLLDP フレームの送信停止を通知します。

その後、再度 LLDP フレームの送信を有効にしても、隣接機器に対するLLDP フレームの送信を一定期間停止します。

シャットダウンフレームを送信してから、次の送信を行うまでの停止期間は、 **set timer reinit-delay** コマンドで設定します。

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。

LLDPを利用したその他の機能

- AP連携
ヤマハスイッチとヤマハ無線AP間で独自の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。
AP連携機能は、**lldp auto-setting** コマンドで設定します。
詳細は [LLDP自動設定\(AP連携\)](#) を参照してください。
- Dante最適設定
自動的にデジタルオーディオネットワーク「Dante」に最適な設定をする機能です。
Dante最適設定機能は、**lldp auto-setting** コマンドで設定します。
詳細は [Dante最適設定機能](#) を参照してください。
- LLDP受信間隔監視
接続されている特定の端末の死活監視をする機能です。
詳細は [端末監視](#) を参照してください。
- ボイスVLAN
ボイスVLAN機能では、LLDP-MEDを利用して、IP電話の音声トラフィックの設定が可能です。
詳細は [VLAN](#) を参照してください。

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フレームの送信が有効な場合、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(portX.X)
Time To Live (TTL)	機器情報の保持時間(秒)	2 Byte	

基本管理TLV

LLDPフレームの送信が有効、かつ、**tlv-select basic-mgmt** コマンドが設定されている場合に送信するTLVです。
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を送信します。
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	0 ～ 255 Byte	
System Name	システム名称文字列 デフォルト: ホスト名	0 ～ 255 Byte	
System Description	システムの説明文字列 デフォルト: 機種名+ファームウェア リビジョン	0 ～ 255 Byte	
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	
	インタフェースサブタイプ	1 Byte	0x02 (ifIndex)
	インタフェース番号	4 Byte	ifIndex値

IEEE 802.1 TLV

LLDPフレームの送信が有効、かつ、**tlv-select ieee-8021-org-specific** コマンドが設定されている場合に送信するTLVです。

該当ポートのVLANやリンクアグリゲーションなどの情報を送信します。

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	1 Byte	
	アグリゲーション論理インターフェース のifIndex番号	4 Byte	
VLAN Name	ポートが所属するVLANの名称	0 ～ 32 Byte	

IEEE 802.3 TLV

LLDPフレームの送信が有効、かつ、**tlv-select ieee-8023-org-specific** コマンドが設定されている場合に送信するTLVです。

該当ポートのオートネゴシエーションサポート情報やPoEの情報などを送信します。

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	
	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	
Link Aggregation	アグリゲーション能力の有無と状態	1 Byte	
	アグリゲーション論理インターフェースのifIndex番号	4 Byte	
Maximum Frame Size	最大フレームサイズ	2 Byte	

LLDP-MED TLV

LLDPフレームの送信が有効、かつ、**tlv-select med** コマンドが設定されている場合に送信するTLVです。ネットワークポリシーや拡張したPoEの情報を送信します。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	0x000B (LLDP-MED Capabilities, Network Policy, Extended Power-via-MDI TLV)
	デバイスタイプ	1 Byte	0x04 (Network Connectivity)
Network Policy	アプリケーションタイプ	1 Byte	0x01 (Voice)
	Voice VLAN情報	3 Byte	

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	

Network Policy は Voice VLAN が設定されたポートからのみ送信されます。

サポートMIB

サポートしているMIBについては、以下のSNMP MIBリファレンスを参照願います。

- [SNMP MIBリファレンス](#)

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機能の有効化	lldp run
システムの説明文の設定	lldp system-description
システムの名称の設定	lldp system-name
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
基本管理TLVの設定	tlv-select basic-mgmt
IEEE-802.1 TLVの設定	tlv-select ieee-8021-org-specific
IEEE-802.3 TLVの設定	tlv-select ieee-8023-org-specific
LLDP-MED TLVの設定	tlv-select med
LLDP フレームの送信間隔の設定	set timer msg-tx-interval
LLDP 送信停止後に再度送信可能になるまでの送信停止期間の設定	set timer reinit-delay
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
高速送信期間の LLDP フレーム送信間隔の設定	set timer msg-fast-tx
高速送信期間の LLDP フレーム送信個数の設定	set tx-fast-init
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

操作項目	操作コマンド
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
LLDP によるDante最適設定機能、AP連携機能の設定	lldp auto-setting

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。

基本管理TLV、IEEE 802.1 TLV、IEEE 802.3 TLV、LLDP-MED TLVを送信します。

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。

送信するシステムの名称は、"SWITCH1"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)#lldp system-name SWITCH1 ①
Yamaha(config)#interface port1.1
Yamaha(config-if)#lldp-agent ②
Yamaha(lldp-agent)#tlv-select basic-mgmt ③
Yamaha(lldp-agent)#tlv-select ieee-8021-org-specific ④
Yamaha(lldp-agent)#tlv-select ieee-8023-org-specific ⑤
Yamaha(lldp-agent)#tlv-select med ⑥
Yamaha(lldp-agent)#set timer msg-tx-interval 60 ⑦
Yamaha(lldp-agent)#set msg-tx-hold 3 ⑧
Yamaha(lldp-agent)#set too-many-neighbors limit 10 ⑨
Yamaha(lldp-agent)#set lldp enable txrx ⑩
Yamaha(lldp-agent)#exit
Yamaha(config-if)#exit
Yamaha(config)#lldp run ⑪
Yamaha(config)#exit

```

- ① システムの名称の設定
- ② LLDPエージェントの作成、モード遷移
- ③ 基本管理TLVの設定
- ④ IEEE 802.1 TLVの設定
- ⑤ IEEE 802.3 TLVの設定
- ⑥ LLDP-MED TLVの設定
- ⑦ 送信間隔の設定
- ⑧ TTL算出の乗数の設定 : $TTL = 60 \times 3 + 1 = 181$ 秒
- ⑨ 最大接続台数の設定
- ⑩ LLDP送受信モードの設定
- ⑪ 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 : 30
Reinitialization delay    : 2
MED Enabled                : Y
Device Type                : NETWORK_CONNECTIVITY
LLDP Agent traffic statistics
  Total frames transmitted : 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              : SWX3100-10G
System Description       : SWX3100 Rev.4.01.02 (Mon Dec  4 12:33:18 2017)
Port Description         : port1.3
System Capabilities      : L2 Switching
Interface Numbering     : 2
Interface Number        : 5003
OID Number               :
Management MAC Address  : ac44.f230.0000
Mandatory TLVs
  CHASSIS ID TYPE
    IP ADDRESS           : 0.0.0.0
  PORT ID TYPE
    INTERFACE NAME       : port1.3
    TTL (Time To Live)  : 41
8021 ORIGIN SPECIFIC TLVs
  Port Vlan id           : 1
  PP Vlan id             : 0
  Remote VLANs Configured
    VLAN ID              : 1
    VLAN Name             : default
  Remote Protocols Advertised :
    Multiple Spanning Tree Protocol
  Remote VID Usage Digestt : 0
  Remote Management Vlan  : 0
  Link Aggregation Status :
  Link Aggregation Port ID :
8023 ORIGIN SPECIFIC TLVs
  AutoNego Support       : Supported Enabled
  AutoNego Capability    : 27649
  Operational MAU Type   : 30
  Power via MDI Capability (raw data)
    MDI power support    : 0x0
```

```

PSE power pair      : 0x0
Power class         : 0x0
Type/source/priority : 0x0
PD requested power value : 0x0
PSE allocated power value : 0x0
Link Aggregation Status :
Link Aggregation Port ID :
Max Frame Size      : 1522
LLDP-MED TLVs
MED Capabilities    :
  Capabilities
  Network Policy
MED Capabilities Dev Type : End Point Class-3
MED Application Type   : Reserved
MED Vlan id           : 0
MED Tag/Untag         : Untagged
MED L2 Priority        : 0
MED DSCP Val          : 0
MED Location Data Format : ECS ELIN
  Latitude Res        : 0
  Latitude            : 0
  Longitude Res       : 0
  Longitude           : 0
  AT                  : 0
  Altitude Res        : 0
  Altitude            : 0
  Datum               : 0
  LCI length          : 0
  What                : 0
  Country Code        : 0
  CA type             : 0
MED Inventory

```

① 接続機器の情報の表示

注意事項

特になし

関連文書

- [SNMP](#)
- [端末監視](#)
- [Dante最適設定](#)
- [PoE制御](#)
- [VLAN](#)
- [LLDP自動設定\(AP連携\)](#)

LLDP自動設定(AP連携)

機能概要

LLDP自動設定は、ヤマハスイッチとヤマハ無線AP間で独自の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自動設定により実現する機能は以下のとおりです。

- RADIUSサーバーの自動設定
 - ヤマハ無線APで動作中のRADIUSサーバー情報を自動的に本製品へ設定します。これにより、ヤマハ無線APをRADIUSサーバー、本製品をRADIUSクライアントとした認証機能を簡単に構築できます。
- ヤマハ無線APの死活監視
 - 本製品に接続されたヤマハ無線APを自動的にLLDPで死活監視します。
- ヤマハ無線AP停止前のログ保存
 - ヤマハスイッチからヤマハ無線APへPoE給電停止タイミングを事前に通知することで、ヤマハ無線APが給電停止する直前までのログを保存することができます。

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、以下を参照してください。

- [技術資料 LLDP自動設定の設定例](#)

用語の定義

LLDP

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

機能詳細

基本仕様

LLDP自動設定を有効にすると、ヤマハスイッチとヤマハ無線APは独自のLLDPフレームの送受信を行います。

LLDP自動設定は、**lldp auto-setting** コマンドで設定します。
本製品の初期設定では、LLDP自動設定は **有効** です。

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。

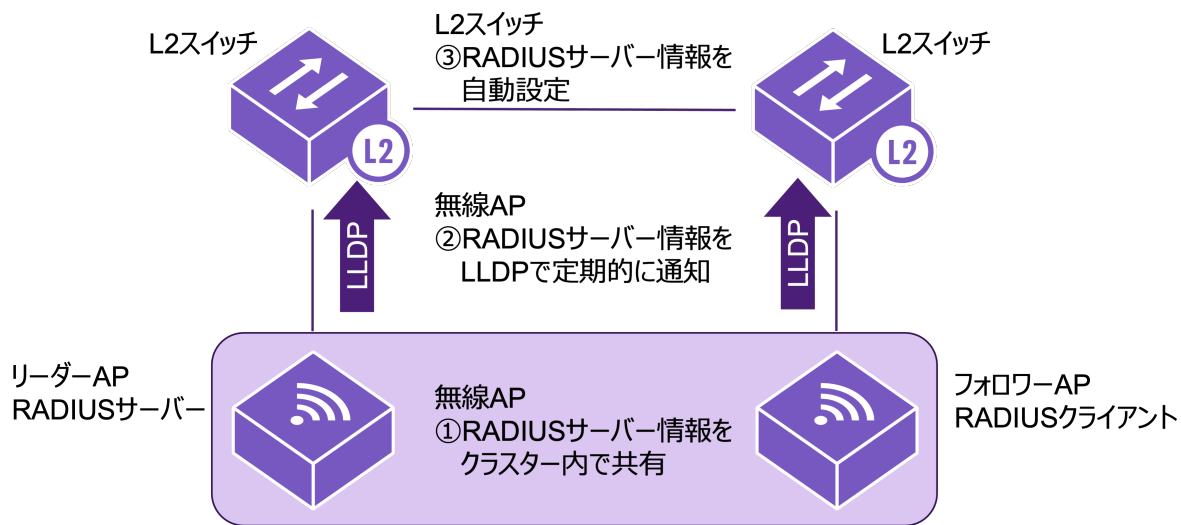
本製品の初期設定では、LLDPフレームの送受信は **有効** です。

RADIUSサーバーの自動設定

本機能では、ヤマハ無線AP(クラスター)で動作中のRADIUSサーバー情報を自動的に本製品へ設定します。これにより、ヤマハ無線APをRADIUSサーバー、本製品をRADIUSクライアントとした認証機能を簡単に構築できま

す。

本製品におけるポートごとの認証設定は環境にあわせてユーザーが手動で行う必要があります。設定の詳細は技術資料の [ポート認証機能](#) を参照してください。



ヤマハ無線APが送信するRADIUSサーバー情報

ヤマハ無線APがRADIUSサーバー情報を送信する条件は以下のとおりです。

- LLDPおよびLLDP自動設定が有効であること
- クラスタ機能有効であること
- クラスタのリーダーAPの場合、RADIUSサーバーとして動作していること
- クラスタのフォロワーAPの場合、リーダーAPのRADIUSサーバーに接続するRADIUSクライアントとして動作していること

ヤマハ無線APの設定については、ヤマハ無線APの [技術資料](#) を参照してください。

送信条件を満たす場合、ヤマハ無線APはLLDPの定期送信タイミングで以下のRADIUSサーバー情報を通知します。

- RADIUSサーバーのIPアドレス
- RADIUSサーバーの認証用UDPポート番号
- RADIUSサーバーとの通信時に使用する共有パスワード

RADIUSサーバーエントリー管理

本製品のLLDP自動設定が有効な状態でヤマハ無線APからRADIUSサーバー情報を受信すると、コマンドの末尾に **dynamic** オプションが付与された **radius-server host** コマンドを running-config に自動的に設定します。

以降の説明では、**dynamic** オプションが付与された **radius-server host** コマンドを「動的エントリー」、手動で設定した **radius-server host** コマンドを「静的エントリー」と呼びます。

dynamic オプションが付与された動的エントリーは、**write** コマンドを実行してもstartup-configに保存されません。

動的エントリーが自動設定された後に、**dynamic** オプションを手動で削除して静的エントリーとして設定することができます。

ただし、静的エントリーに手動で **dynamic** オプションを付与して動的エントリーに変更することはできません。

- ・ radius-server host コマンドの動的エントリー例

```
radius-server host 192.168.100.241 auth-port 1234 key EXAMPLE dynamic
```

LLDP自動設定で設定された動的エントリーには、「LLDP受信ポート番号」と「有効期間」の情報が付与されます。

同一のRADIUSサーバー情報を複数のポートから受信した場合、**最も小さいポート番号** で受信したRADIUSサーバー情報が保持されます。

有効期間には、受信したLLDPフレーム内に含まれる **TTL (Time to Live)** の値が設定されます。

ヤマハ無線APから送信されるLLDPフレームのデフォルトのTTLの値は **120** 秒です。

TTL秒以内に新たにRADIUSサーバー情報を受信すると有効期間が更新され、TTL秒以内に新たにRADIUSサーバー情報を受信できなかった場合は動的エントリーが削除されます。

なお、TTL=0のLLDPシャットダウンフレームを受信した場合、動的エントリーは即時削除されます。

show radius-server コマンドでRADIUSサーバー情報を確認することができ、自動設定されたRADIUSサーバーホストにはアスタリスク (*) が付与され、

LLDP受信ポート番号 (LLDP Received port) と有効期間 (Expires) の情報が表示されます。

- ・ show radius-server コマンドによる動的エントリー情報表示例

```
SWX#show radius-server
Server Host : 192.168.100.241*
LLDP Received port : port1.2
Expires : 00:00:33
Authentication Port : 1234
Secret Key : EXAMPLE
Timeout : 10 sec
Retransmit Count : 5
Deadtime : 0 min

* - Assigned by LLDP.
```

本製品では、動的エントリーと静的エントリーを合わせてRADIUSサーバー情報を最大 **8** 件まで設定することができます。

静的エントリーは動的エントリーよりも優先的に使用されます。

そのため、RADIUSサーバー情報が最大数まで設定されている場合であっても、既存エントリーの中に動的エントリーが存在する場合は静的エントリーを新規設定できます。

このとき、最も大きいLLDP受信ポート番号の動的エントリーが自動的に削除されます。

注意事項

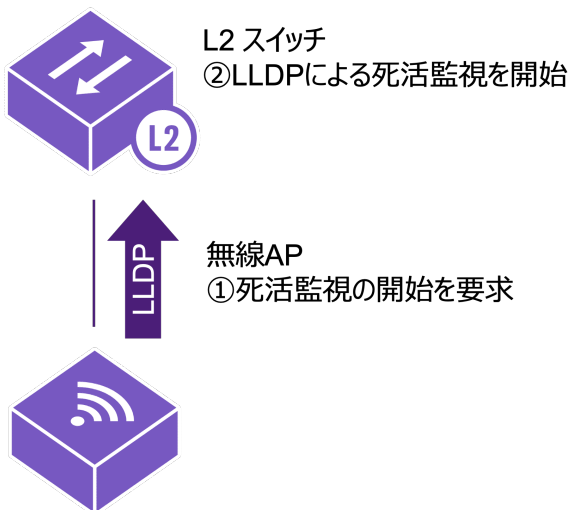
本機能を使用する場合、以下の点に注意してください。

- ・ ヤマハ無線APとの接続
 - RADIUSサーバー情報を自動設定するためには、LLDP自動設定に対応したヤマハ無線APが、本製品に直接接続されている必要があります。
 - ヤマハ無線APが直接接続されていないヤマハスイッチについては、手動でRADIUSサーバーの設定を行ってください。
- ・ スタック機能有効時のコマンド入力モード制限
 - スタック機能有効時にはグローバルコンフィグレーションモードへ遷移できるユーザーが制限されます。詳細は[スタック機能](#)を参照してください。

- ヤマハ無線APからLLDPを受信しRADIUSサーバーの設定を適用する際には内部的にグローバルコンフィグレーションモードへ遷移するため、コンソールによりグローバルコンフィグレーションモードもしくは個別コンフィグレーションモードに入っているユーザーは強制的に特権EXECモードへ遷移されます。
- RADIUSサーバーとの通信時に使用する共有パスワードの使用可能文字
 - 本製品では "?"、スペースを使用することができません。ヤマハ無線APの共有パスワード(RADIUSサーバー - クライアント - シークレット)設定でこれらの文字を使用しないでください。
- RADIUSサーバー全体の応答待ち時間の設定
 - RADIUSサーバーが複数設定されている場合、全てのRADIUSサーバーの合計待ち時間を設定する **auth timeout server-timeout** コマンドの設定値を、(**radius-server timeout** コマンドの設定値) × (**radius-server retransmit** コマンドの設定値 + 1) × (RADIUS サーバー数) 以上の値に設定してください。コマンドの詳細については、コマンドリファレンスを参照してください。

ヤマハ無線APの死活監視

本製品はヤマハ無線APから死活監視開始要求を受信すると、自動的にLLDPによる死活監視を開始します。



ヤマハ無線APが死活監視の開始要求を送信する条件は以下のとおりです。

- LLDPおよびLLDP自動設定が有効であること

本製品のLLDP自動設定が有効な状態で死活監視開始要求を受信すると、LLDP受信ポートに対してLLDP受信間隔監視設定を登録します。

設定が登録されたポートではLLDPによる死活監視を行い、一定時間LLDPを受信しなかった場合はPoE給電を一時的に(5秒間)OFF状態にして、ヤマハ無線APの復旧を試みます。

またSNMPトラップおよびL2MSトラップで通信断を検出したことを通知します。詳細については[端末監視](#)の技術資料を参照してください。

注意事項

本機能を使用する場合、以下の点に注意してください。

- ヤマハ無線APの接続ポートを変更するなどして元の接続ポートで死活監視が不要となった場合は、ヤマハ無線APの接続ポートを変更した後に不要となった設定を手動で削除してください。

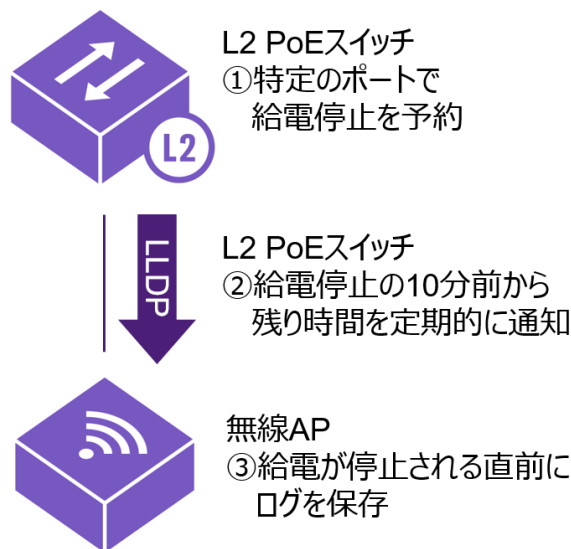
ヤマハ無線AP停止前のログ保存

本製品ではスケジュール機能を使用することで「特定の時間帯だけ無線APへのPoE給電を停止する」といった動作を実現できます。

このとき、無線APは突然給電を停止されることになり通常であれば未保存のログは消失してしまいますが、本製品ではPoE給電停止タイミングをLLDPで通知することでヤマハ無線APでのログの保存を可能とします。

給電停止タイミングの通知は、任意のLANポートで **power-inline disable delay** コマンドによりPoE給電停止の遅延時間(delayオプション)が指定されているときに行います。

Web GUIによるスケジュールテンプレート設定のかんたん入力機能で「ヤマハ無線 AP へ通知してから給電を停止する」にチェックを入れると、スケジュール実行から10分後に給電停止する設定 (**power-inline disable delay 600** コマンド) が登録されます。



給電停止遅延中のポートで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の送信間隔が30秒よりも大きな値に設定されていること
- LLDPおよびLLDP自動設定が有効であること

なお、給電が停止されるか、給電停止遅延が **power-inline enable** コマンドによりキャンセルされた場合、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.

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
LLDPフレームの送信間隔の設定	set timer msg-tx-interval
RADIUSサーバーホストの設定	radius-server host
RADIUSサーバー1台あたりの応答待ち時間の設定	radius-server timeout
RADIUSサーバーへの要求再送回数の設定	radius-server retransmit
RADIUSサーバー設定情報の表示	show radius-server
RADIUSサーバー全体の応答待ち時間の設定	auth timeout server-timeout
PoE給電機能の設定(インターフェース)	power-inline
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

機能ごとの注意事項を参照してください。

関連文書

- ・ [LLDP](#)
- ・ [RADIUS server](#)
- ・ [ポート認証機能](#)
- ・ [端末監視](#)
- ・ [PoE制御](#)

-
- [スケジュール機能](#)
 - [スタック機能](#)
 - [技術資料 LLDP自動設定の設定例](#)

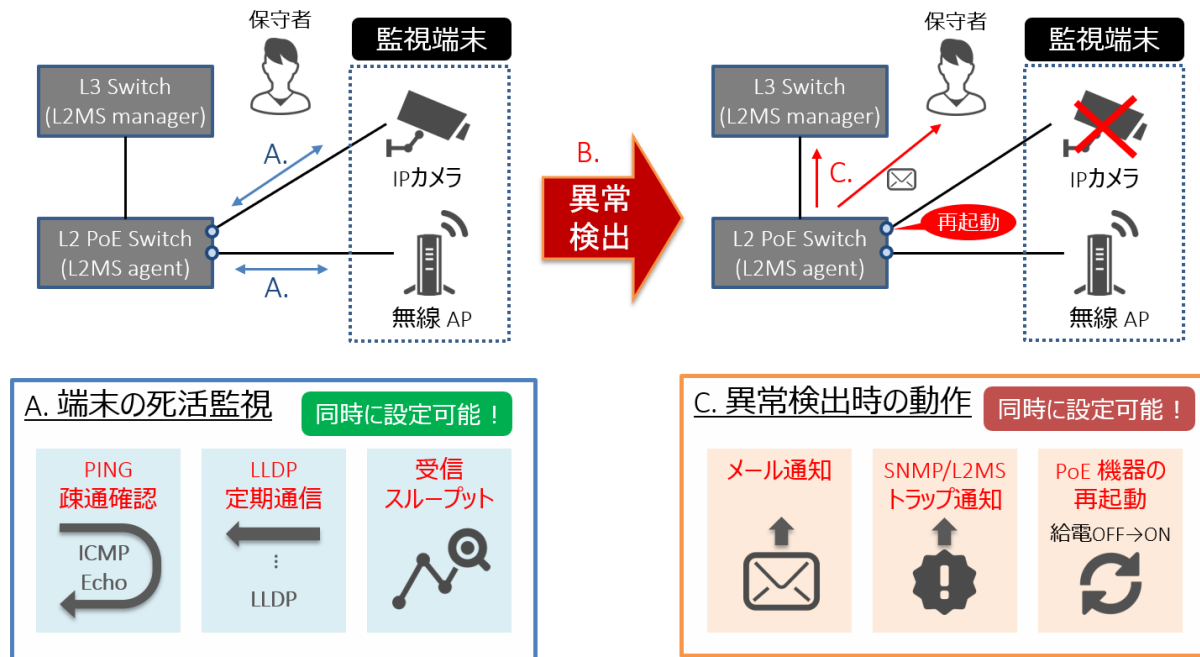
端末監視

機能概要

端末監視機能は、ネットワークスイッチに接続されている特定の端末の死活監視を行います。
端末監視機能の概要について、以下に示します。

- ・ 端末監視 機能概要

L2MSマネージャー:L3スイッチ, L2MSエージェント:インテリ L2 PoE スwitchの例



死活監視の方法としては、以下の **3種類** を提供します。

1. **Pingによる疎通監視**

IPアドレスを保持する端末に対して定期的に Ping (ICMP Echo request/reply) を実行し、応答が無くなった場合にダウンと判定します。

Ping 応答待ち時間・ダウン判定までの失敗回数は、ユーザーが設定することができます。

2. **フレーム受信量監視**

ポート単位で定期的にフレーム受信量を確認し、指定した流量を下回った場合にダウンと判断します。

監視開始閾値とダウン判定閾値はユーザーが設定することができます。

流量が監視開始閾値を上回った時点で監視が開始され、ダウン判定閾値を下回った時点でダウンとなります。

3. **LLDP受信間隔監視**

ポート単位で定期的に受信するLLDPを監視します。

LLDP パケットのデータ部必須項目であるTTLを利用し、TTL 間 LLDP の受信がなければダウンと判断します。

監視により、端末異常 (ダウン) を検出した場合、**自動で** 以下の処理を行います。

1. **ダッシュボード画面でのアラート表示**

ダッシュボードの警告画面に監視端末で異常が発生 (ダウン) したことを表示します。

2. **LAN マップ画面でのアラート表示**

。 端末監視を行っているスイッチが L2MS マネージャーの場合

LAN マップの通知および履歴情報として、監視端末で異常が発生 (ダウン) したことを表示しま

す。

- 端末監視を行っているスイッチが L2MS エージェントの場合
L2MS のトラップ機能を使用して、L2MS マネージャーに通知します。
通知を受信した L2MS マネージャーは、LAN マップ画面で監視端末で異常が発生 (ダウン) したことを表示します。

また、**ユーザーの選択**により、並行して以下の動作を実施可能とします。

1. **メールによる異常検出通知**
任意の宛先に監視端末で異常が発生したことを通知します。
2. **SNMP マネージャへの通知**
コマンドにより設定した SNMP マネージャへ Trap を送信します。
3. **PoE 給電の一時停止による端末再起動**
PoE 給電しているポートでダウンを検出した場合、PoE 給電を一時的に OFF 状態にして監視端末の復旧を試みます。

用語の定義

特になし

機能詳細

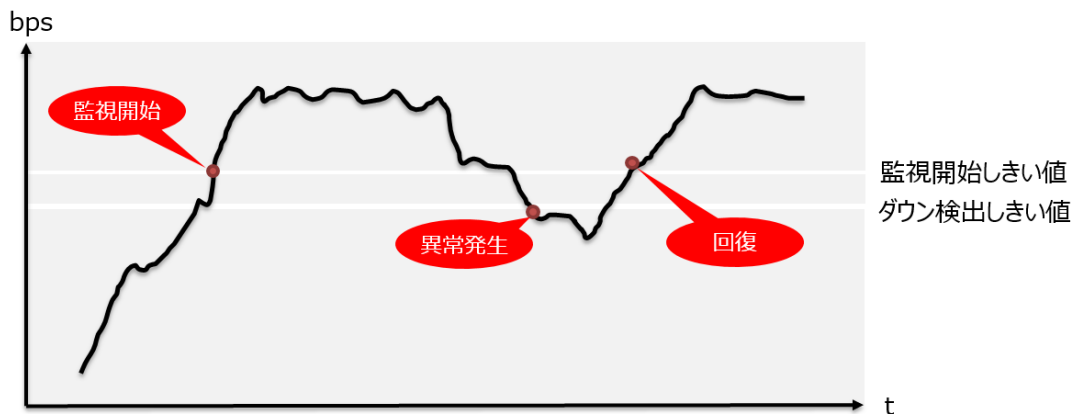
Ping (ICMP Echo request / reply) による監視

Ping による端末監視の仕様について、以下に示す。

1. ネットワークスイッチからの ICMP Echo request の送信周期は **5sec** 固定とします。
2. 送信する ICMP Echo request は、以下のフォーマットとします。
 - ICMP ヘッダの ID フィールドには、**監視端末ごとに割り振られるユニークなID**を設定します。
 - ICMP ヘッダのシーケンスフィールドには、0 からシーケンシャルにインクリメントした数値を設定します。
3. ICMP Echo reply の正常性は、以下で確認をします。
 - ICMP ヘッダの ID フィールドに request 送信時に設定した ID が設定されているか
 - ICMP ヘッダのシーケンスフィールドに request 送信時に設定したシーケンス番号が設定されているか
4. ICMP Echo reply の待ち時間は、**1 ～ 60sec** で変更可能で、デフォルト **2sec** とします。
5. 監視端末からの ICMP Echo reply を受信できずに異常と判断するまでの回数は、**1 ～ 100** で設定可能で、デフォルト **2回** とします。
6. Ping による監視は、**最大で64台まで** 可能とします。
7. メール通知や SNMP Trap の送信が有効になっている場合、以下の条件で送信します。
 - 端末のダウンを検出したとき (ダウン中も24時間毎に送信)
 - 端末のアップを検出したとき (監視開始時と復旧時)

フレーム受信量による監視

本装置におけるフレーム受信量の監視方法について、以下に示します。



1. 1sec 周期でポートの受信オクテット数を参照し、1秒間の受信オクテット数を計算します。
 - **全ポート観測対象** とします。
2. 1秒間の受信オクテット数とリンクスピードを使用して、**受信スループット (bps)** と **受信率 (%)** を計算します。
3. フレーム受信量による監視は、**ユーザが設定した監視開始しきい値 (bps)** を超えた時点で始まります。
4. 監視開始後、**ユーザが設定したダウン検出しきい値 (bps)** を下回った場合に異常が発生 (ダウンした) と判断します。
5. メール通知や SNMP Trap の送信が有効になっている場合、以下の条件で送信します。
 - 端末のダウンを検出したとき
 - 端末のアップを検出したとき (監視開始時と復旧時)

LLDP による監視

1. LLDP フレームのデータ部必須項目である TTL を利用し、TTL 時間の間、LLDP の受信がなければダウンと判定します。
2. LLDP フレームを初めて受信した時点で監視がスタートします。
3. 本監視は、ポート毎に設定することが可能です。
4. メール通知や SNMP Trap の送信が有効になっている場合、以下の条件で送信します。
 - 端末のダウンを検出したとき
 - 端末のアップを検出したとき (監視開始時と復旧時)
 - 端末が LLDP 機能を停止したとき

関連コマンド

本機能は、コマンドでの設定に対応していません。

Web GUI による設定

端末監視の設定は、Web GUI の **[詳細設定] - [端末監視]** から行うことができます。
各画面の設定方法については、Web GUI のヘルプより参照することができます。

端末監視 トップページ

端末監視のトップページを以下に示します。

2. フレーム受信量監視

■ 設定に必要な情報入力	
機器名	半角英数記号80文字以内
監視種別	☐ IPアドレスを指定 ☒ ポートを指定
ポート	選択
フレーム監視種別	☒ フレーム受信量監視 ☐ LLDP監視
監視開始帯域値	bps
ダウン検出帯域値	bps ※監視開始帯域値より小さい値
状態変化を検出した時の動作	☐ PoE給電一時停止による端末再起動（ダウン検出時のみ） 給電停止期間： 5 秒 (1 - 60) ☐ SNMP Trapの送信 ☐ メール通知
戻る 確認	

3. LLDP 受信間隔監視

■ 設定に必要な情報入力	
機器名	半角英数記号80文字以内
監視種別	☐ IPアドレスを指定 ☒ ポートを指定
ポート	選択
フレーム監視種別	☐ フレーム受信量監視 ☒ LLDP監視
状態変化を検出した時の動作	☐ PoE給電一時停止による端末再起動（ダウン検出時のみ） 給電停止期間： 5 秒 (1 - 60) ☐ SNMP Trapの送信 ☐ メール通知
戻る 確認	

- PoE 給電に対応したモデルのみ、PoE 給電制御による端末再起動 を指定することが可能です。
- フレーム受信量監視で、監視開始しきい値、ダウン検出しきい値を決める際は、トラフィック観測機能を活用ください。
- 異常時の処置として、メールを通知する場合には、別途 **メール通知設定** が必要です。
詳細は、[技術資料: \[保守・運用機能\] - \[メール通知\]](#)、[Web GUI ヘルプ: \[管理\] - \[メール通知\]](#)

を参照ください。

監視端末の状態確認

設定した監視端末の状態は、**ダッシュボードの端末監視ガジェット**にて確認することができます。

端末監視状態				SWX2310P-18G
Up 1 Down 1 Idle 1 All 3				
	監視対象	機器名	監視種別	状態
1	192.168.100.124	Note_PC_1	Ping	
2	port1.7	IP_Camera_1	フレーム	
3	port1.21	IP_Camera_2	LLDP	

- ・ 監視端末ごとに監視対象、機器名、監視種別、状態が表示されます。
- ・ 監視端末の状態としては、以下の3つを表示します。
 - **Idle** : 監視がまだ行われていない状態 :
 - **Up** : 監視端末が正しく動作している状態 :
 - **Down** : 監視端末が正しく動作していない状態 :
- ・ 状態欄にマウスカーソルを重ねると、監視端末の状態が表示されます。
- ・ ダッシュボード上部の **Idle**、**Up**、**Down** ボタンをクリックすると、各状態の監視端末のみが表示されます。(**All** ボタンはすべての状態)
- ・ 監視端末が1つも登録されていない時は「監視端末が登録されていません」と表示されます。

注意事項

特になし

関連文書

- ・ [パフォーマンスの観測](#)

パフォーマンスの観測

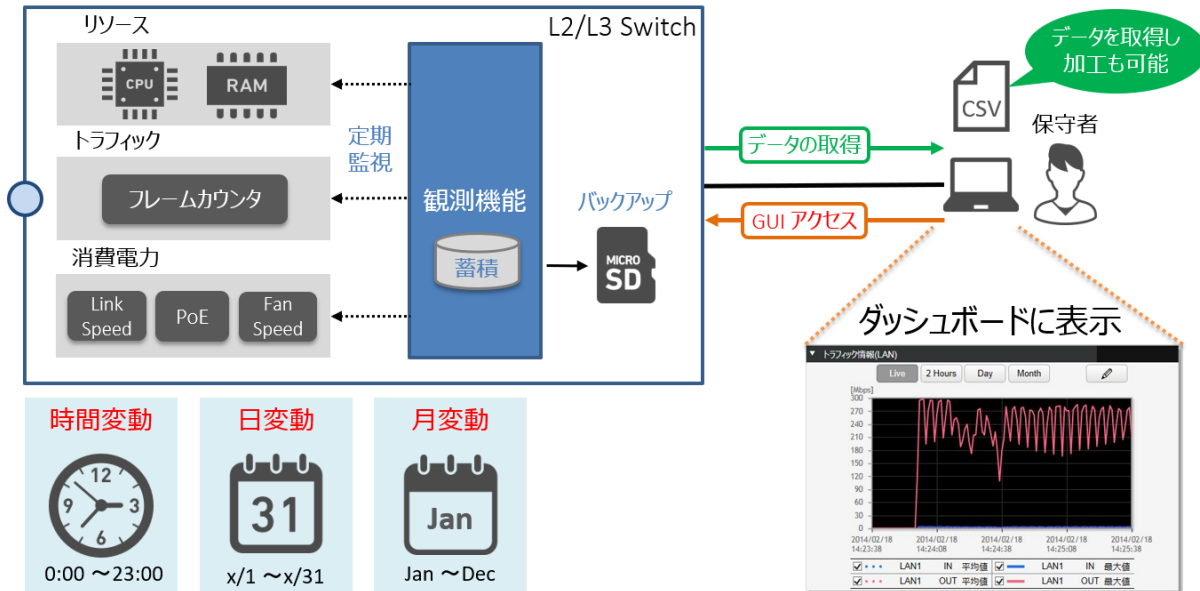
機能概要

本製品は、システムのパフォーマンスを定常的に観測する仕組みを提供します。

機能概要を以下に示します。

定常観測項目

リソース (CPU, Memory) 使用量
ポートのフレームカウンタをもとに帯域使用量などのトラフィック量
リンク速度、PoE給電量、FAN回転数から推測した消費電力量



本製品では、以下の3種類のデータを定常的に観測します。

1. リソースの使用量: CPU, メモリの使用量
2. トラフィック量 : 通信ポートの帯域使用量 (送受信)
3. 消費電力量 : リンク速度、PoE給電量、FAN回転数から推測した消費電力量

観測した結果をもとに、以下の変動データを 製品内部に 1年分蓄積します。

- ・ **時間変動** : 時刻ごと(e.g. 0:00, 1:00, …)の変化
- ・ **日変動** : 何月何日ごと(e.g. 1/1, 1/2, …)の変化
- ・ **曜日変動** : 曜日ごと(e.g. SUN, MON, …)の変化
- ・ **月変動** : 月ごと(e.g. Jan, Feb, …)の変化

蓄積したデータは、**SDカードにバックアップすることが可能です。**

保守者は 本製品に Web GUI アクセスすることで、ライブデータを含めた各変動データをダッシュボードに表示、また、蓄積した結果を PCに取得することも可能です。

取得したデータは **CSV フォーマット** であるため、PCの表計算ソフトで加工することも可能です。

保守者は、本機能を使うことで以下のように活用することができます。

- ・ 短期的な通信状況を把握する
- ・ 長期的なネットワーク設備の需要を予測する
- ・ 現状の消費電力量を把握することで、無駄な電力消費の発生に気づく

用語の定義

特になし

機能詳細

リソース・トラフィック使用量の観測

本装置は、起動直後から自動で **毎秒**、CPU・メモリ、ポート毎の送信・受信スループットを観測します。観測データは、**移動平均処理でノーマライズしたもの**を採用し、**1年分のデータをRAMに保存**します。

観測データのバックアップ

観測データのバックアップは、Web GUI でのみ設定することができます。

観測データのバックアップは、本装置に **SDカードが挿入されていることが前提** となっています。バックアップが有効に設定されていると、有効時点から毎時(e.g. 1:00, 2:00 …) 直近1時間の観測データをSDカードに保存します。

保存したデータは、本装置専用のバイナリデータとなっています。

SDカードの保存先、バックアップデータのファイル名について、以下に示します。

1. リソース情報

1. 時間変動データ

/[機種名]/data/resource/YYYYMM_smsys_res_monitor_hour.bin

2. 日変動データ (日毎のデータ)

/[機種名]/data/resource/YYYYMM_smsys_res_monitor_day.bin

3. 曜日変動データ

/[機種名]/data/resource/YYYYMM_smsys_res_monitor_week.bin

4. 月変動データ

/[機種名]/data/resource/YYYY_smsys_res_monitor_month.bin

2. トラフィック情報

1. 時間変動データ

/[機種名]/data/trf/YYYYMM_trf_bandwidth_hour.bin

2. 日変動データ

/[機種名]/data/trf/YYYYMM_trf_bandwidth_day.bin

3. 曜日変動データ

/[機種名]/data/trf/YYYYMM_trf_bandwidth_week.bin

4. 月変動データ

/[機種名]/data/trf/YYYY_trf_bandwidth_month.bin

3. 消費電力情報

1. 時間変動データ

/[機種名]/data/power/YYYYMM_smsys_pwr_monitor_hour.bin

2. 日変動データ

/[機種名]/data/power/YYYYMM_smsys_pwr_monitor_day.bin

3. 曜日変動データ

/[機種名]/data/power/YYYYMM_smsys_pwr_monitor_week.bin

4. 月変動データ

/[機種名]/data/power/YYYY_smsys_pwr_monitor_month.bin

- ・ **[機種名]** には以下が設定されます。
 - SWX2320-16MT の場合: **swx2320**
 - SWX2322P-16M の場合: **swx2322p**
 - SWX3220-16MT/16TMs の場合: **swx3220**
 - SWX3200-28GT/52GT の場合: **swx3200**
 - SWX3100-10G/18GT の場合: **swx3100**
 - SWX2310P-10G/18G/28GT の場合: **swx2310p**
 - SWX2310-10G/18GT/28GT/52GT の場合: **swx2310**
- ・ **YYYY: 西暦, MM: 月** が設定されます。
- ・ ヤマハ独自フォーマットであるため、参照することはできません。

観測データのエクスポートデータ

観測データのPCへのエクスポートは、Web GUI でのみ実行することができます。

エクスポートしたデータは、**複数の CSV ファイル が zip形式で圧縮されています。**
圧縮ファイルの構成について、以下に示します。

1. リソース観測データをエクスポートした場合

- zipファイル名: **YYYYMMDDhhmmss_resource_csv.zip**
- フォルダ構成

```
YYYYMMDDhhmmss_resource_csv
+- 20170922_resource_hour.csv ①
+-      :
+- 20170925_resource_hour.csv ②
+- 201709_resource_day.csv ③
```

① 2017/9/22のCPU・メモリ・時間変動データ

② 2017/9/25のCPU・メモリ・時間変動データ

③ 2017/9のCPU・メモリ・日変動データ

2. 送信トラフィック観測データをエクスポートした場合

- zipファイル名: **YYYYMMDDhhmmss_trf_tx_csv.zip**
- フォルダ構成

```
YYYYMMDDhhmmss_trf_tx_csv
+- 20170922_trf_tx_hour.csv ①
+-      :
+- 20170925_trf_tx_hour.csv ②
+- 201709_trf_tx_day.csv ③
```

① 2017/9/22の送信トラフィック・時間変動データ

② 2017/9/25の送信トラフィック・時間変動データ

③ 2017/9の送信トラフィック・日変動データ

3. 受信トラフィック観測データをエクスポートした場合

- ・ zipファイル名: **YYYYMMDDhmmss_trf_rx_csv.zip**
- ・ フォルダ構成

```
YYYYMMDDhmmss_trf_rx_csv
+- 20170922_trf_rx_hour.csv ①
+-      :
+- 20170925_trf_rx_hour.csv ②
+- 201709_trf_rx_day.csv ③
```

- ① 2017/9/22の受信トラフィック・時間変動データ
- ② 2017/9/25の受信トラフィック・時間変動データ
- ③ 2017/9の受信トラフィック・日変動データ

4. 消費電力観測データをエクスポートした場合

- ・ zipファイル名: **YYYYMMDDhmmss_pwr_csv.zip**
- ・ フォルダ構成

```
YYYYMMDDhmmss_pwr_csv
+- 20170922_pwr_hour.csv ①
+-      :
+- 20170925_pwr_hour.csv ②
+- 201709_pwr_day.csv ③
```

- ① 2017/9/22の消費電力・時間変動データ
- ② 2017/9/25の消費電力・時間変動データ
- ③ 2017/9の消費電力・日変動データ

- ・ **YYYYMMDDhmmss** には、エクスポートを実行した日時(ファイルを生成した日時)が設定される。

関連コマンド

本機能は、コマンドでの設定に対応していません。

Web GUI による設定

パフォーマンスの観測は、Web GUI の 以下のページより制御することができます。

- ・ リソース使用量の参照
 - **[ダッシュボード]** の **[リソース情報(グラフ)]** で参照できます。
- ・ トラフィック使用量の参照
 - **[ダッシュボード]** の **[トラフィック情報(グラフ)]** で参照できます。
- ・ 消費電力量の参照
 - **[ダッシュボード]** の **[消費電力情報(グラフ)]** で参照できます。
- ・ 観測データのバックアップ・クリア・エクスポート
 - **[管理]** 選択後、**[保守]** - **[統計情報の管理]** より設定できます。
(クリア・エクスポートは **[ダッシュボード]** の各ガジェットの **メニューボタン (***)** から行う

こともできます)

各画面の参照・設定方法については、Web GUI のヘルプより参照することができます。

リソース使用量の参照

リソース情報(グラフ)の画面を以下に示します。

- ・リソース情報(グラフ) **Live** 選択時の例



1. グラフの描画は、以下からボタンにて変更することができます。
 - 現在の状況: Live
現時点の各使用率を1秒おきに取得しグラフに表示します。
 - 時間変動 : Day
指定した日にちの各使用率を1時間単位でグラフに表示します。
日にちの指定は、ガジェット右上の日付指定ボックスより行って下さい。
 - 日変動 : Month
指定した月の各使用率を1日単位で表示します。
月の指定は、ガジェット右上の月指定ボックスより行って下さい。
 - 月変動 : Year
指定した年の各使用率を1ヶ月単位に表示します。
年の指定はガジェット右上のセレクトボックスで行って下さい。
 - 現在、曜日変動は参照することができません。
2. CPU、メモリ使用率は、使用率が **80%** を超えると、**ダッシュボード上に警告メッセージが表示されます。**
80%を超えた後、80%を下回ると、警告が自動的に解除されます。

トラフィック使用量の参照

トラフィック使用量(グラフ)の画面を以下に示します。

- ・トラフィック使用量(グラフ) **Day** 選択時・**受信トラフィック** の例



1. 各ポートのトラフィック使用量を **送信**、**受信** 別々に表示することができます。

2. グラフの描画は、以下からボタンにて変更することができます。

◦ 現在の状況: Live

現時点の各使用率を1秒おきに取得しグラフに表示します。

取得したデータは 直近 **2分** のデータを保持し、グラフに描画します。

◦ 時間変動 : Day

指定した日にちの各使用率を1時間単位でグラフに表示します。

日にちの指定は、ガジェット右上の日付指定ボックスより行って下さい。

◦ 日変動 : Month

指定した月の各使用率を1日単位で表示します。

月の指定は、ガジェット右上の月指定ボックスより行って下さい。

◦ 月変動 : Year

指定した年の各使用率を1ヶ月単位に表示します。

年の指定はガジェット右上のセレクトボックスで行って下さい。

◦ 現在、曜日変動は参照することができません。

3. 描画するインターフェースは、**メニューボタン** (***) で **[インターフェースの選択]** をクリック後、以下の画面で選択します。

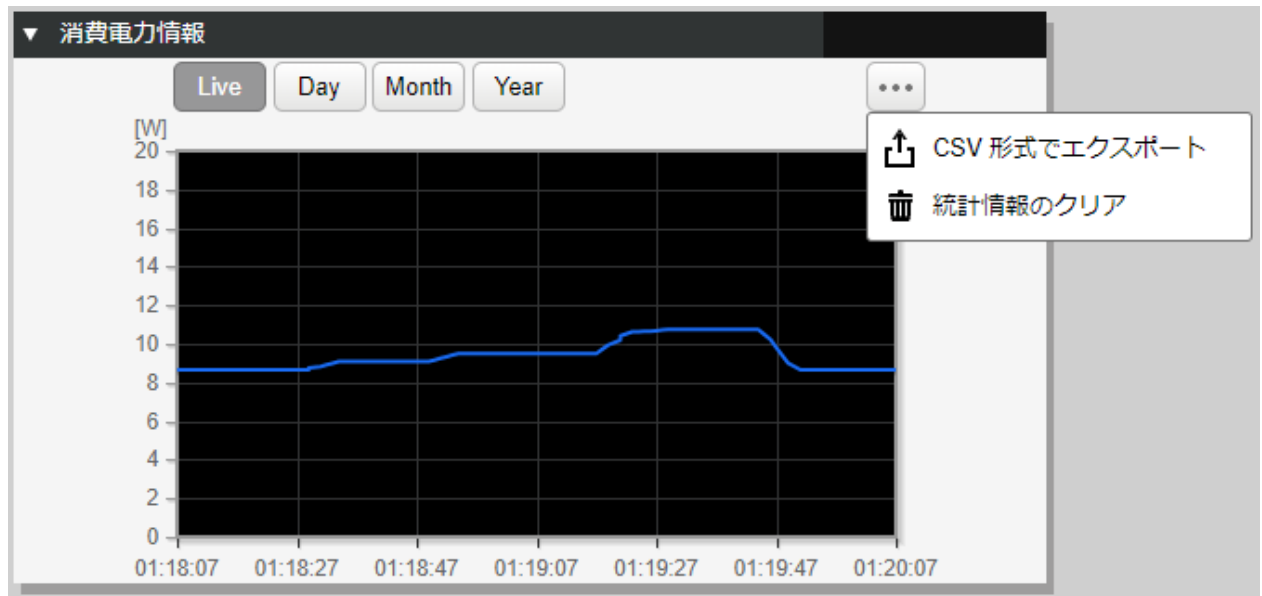
4. トラフィック使用率は、使用率が 60% を超えると、ダッシュボード上に警告メッセージが表示されま

す。
60%を超えた後、50%を下回ると、警告が自動的に解除されます。

消費電力量の参照

消費電力情報(グラフ)の画面を以下に示します。

- 消費電力情報(グラフ) **Live** 選択時の例



1. グラフの描画は、以下からボタンにて変更することができます。

- 現在の状況: Live
現時点の各消費電力量を1秒おきに取得しグラフに表示します。
- 時間変動 : Day
指定した日にちの各消費電力量を1時間単位でグラフに表示します。
日にちの指定は、ガジェット右上の日付指定ボックスより行って下さい。
- 日変動 : Month
指定した月の各消費電力量を1日単位で表示します。
月の指定は、ガジェット右上の月指定ボックスより行って下さい。
- 月変動 : Year
指定した年の各消費電力量を1ヶ月単位に表示します。
年の指定はガジェット右上のセレクトボックスで行って下さい。
- 現在、曜日変動は参照することができません。

2. 消費電力を抑えるためには、以下のような方法が推奨されます。

- 帯域使用量が少ないポートのリンク速度を落とす
- スケジュール実行機能を使って、深夜や休日に使用していないポートをシャットダウンしたり、PoE 給電を停止する

観測データのバックアップ・クリア・エクスポート

観測データのバックアップ・クリア・エクスポートは、**[管理] - [保守] - [統計情報の管理]** より行います。

(クリア・エクスポートは**[ダッシュボード]**の各ガジェットの**メニューボタン**(***) から行うこともできます)

統計情報の管理画面を以下に示します。

- 統計情報の管理画面 (トップページ)

The screenshot shows the management interface of a YAMAHA SWX2310P-10G switch. The top navigation bar includes the YAMAHA logo, model name, user information (admin), and a help icon. Below this is a secondary navigation bar with tabs for Dashboard, LAN Map, Detailed Settings, and Management. The left sidebar contains a tree view of configuration categories, with 'Statistics Information Management' highlighted under the 'Maintenance' section. The main content area is titled 'Statistics Information Management' and includes a brief description. It features three main sections: 'Backup Settings for Collected Data' (with a table of settings for Traffic, Resource, and Power consumption data), 'Clear Collected Data', and 'Export Collected Data'.

統計情報の管理

集計データに関する操作を行うことができます。

■ 集計データのバックアップ設定

設定項目	設定内容	
トラフィック情報	有効	設定
リソース情報	無効	
消費電力情報	無効	

■ 集計データのクリア

集計データをクリアする 進む

■ 集計データのエクスポート

集計データをエクスポートする 進む

観測データのバックアップ設定

観測データのバックアップ設定は、**[トップページ]** - **[集計データのバックアップ設定]** より行います。**[設定]** ボタン押下後に表示される画面を以下に示します。

- 観測データのバックアップ設定画面

■ 統計情報の管理

集計データのバックアップ設定

各項目を入力してください。入力が完了したら、「確認」ボタンを押してください。

■ 集計データのバックアップ設定

バックアップする集計データ

☒ トラフィック情報
☒ リソース情報
☐ 消費電力情報

戻る
確認

- バックアップを有効化する集計データのチェックボックスにチェックを入れ、**[確認]** ボタンを押下してください。
押下後、以下の画面が表示されます。

■ 統計情報の管理

入力内容の確認

入力内容をご確認の上、変更がなければ「設定の確定」ボタンを押してください。

⚠ SDカードが挿入されていない場合、バックアップデータは保存されません。

集計データのバックアップ設定

バックアップする集計データ トラフィック情報
リソース情報

戻る

設定の確定

- ・本設定をキャンセルする場合は、各画面の **[戻る]** ボタンを押下してください。

観測データのクリア

観測データのクリアは、**[トップページ]** - **[集計データのクリア]** より行います。

(**[ダッシュボード]** の各ガジェットの **メニューボタン** (***) から行うこともできます)
[進む] ボタン押下後に表示される画面を以下に示します。

- ・観測データのクリア画面

■ 統計情報の管理

集計データのクリア

各項目を入力してください。入力が完了したら、「確認」ボタンを押してください。

■ 集計データのクリア

クリアする集計データ トラフィック情報 ▼

戻る 確認

- ・クリアする集計データをセレクトボックスから選択し、**[確認]** ボタンを押下してください。
押下後、以下の画面が表示されます。

■ 統計情報の管理

入力内容の確認

内容をご確認の上、よろしければ「実行」ボタンを押してください。

集計データのクリア

クリアする集計データ トラフィック情報

戻る

実行

- ・本操作をキャンセルする場合は、各画面の **[戻る]** ボタンを押下してください。

観測データのエクスポート

観測データのエクスポートは、統計情報の管理の[トップページ] - [集計データのエクスポート] より行います。

([ダッシュボード] の各ガジェットの **メニューボタン** (***) から行うこともできます)
[進む] ボタン押下後に表示される画面を以下に示します。

- ・ 観測データのエクスポート画面

■ 統計情報の管理

集計データのエクスポート

各項目を入力してください。入力が完了したら、「実行」ボタンを押してください。

■ 集計データのエクスポート	
エクスポートする集計データ	トラフィック情報(送信) ▼
期間の指定	2018年1月 ▼
戻る 実行	

- ・ Web GUI アクセスしている PC にエクスポートする観測データをセレクトボックスから選択し、エクスポートする観測データの期間を選択します。
選択後、**[実行]** ボタンを押下すると、zip ファイルがダウンロードされます。
- ・ 本操作をキャンセルする場合は、**[戻る]** ボタンを押下してください。

注意事項

特になし

関連文書

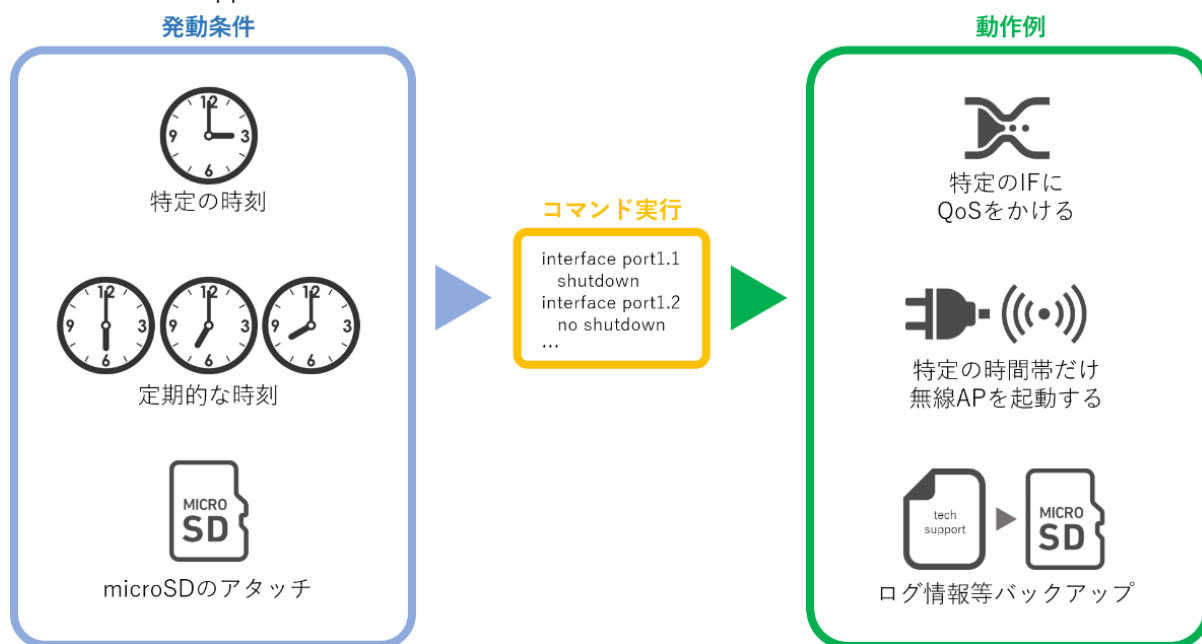
特になし

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。

- ・ 特定の時間帯だけ特定のVLANにQoSをかける
- ・ 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
- ・ 定期的にtech-supportをmicroSDメモリに保存する



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

イベントトリガー

任意のイベントが発生するという条件

アクション

トリガー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。

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

種別		指定方法	設定値の例
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) 省略可能	59

イベントトリガー

任意のイベントをイベントトリガーとして指定することができます。

イベントトリガーは **schedule** コマンドで設定します。

指定可能なイベントは以下となります。

種別	説明
startup	起動した時点で実行される
sd-attached	microSDカードがアタッチされた時点で実行される

アクション

時刻トリガーまたはイベント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、または **script** コマンドで設定します。

アクションには以下の2つがあります。

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。
指定スクリプトの実行	script コマンド	外部メモリ (microSD メモリ) 内の指定されたファイル /(機種名)/schedule/script.txt の中の文字列をファイルの先頭から100行目まで コマンドとして実行する。

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願います。

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

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 port1.1-2
Yamaha(config-schedule)# cli-command 3 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 port1.1-2
Yamaha(config-schedule)# cli-command 3 power-inline disable
Yamaha(config-schedule)# end
Yamaha#
```

microSD挿入時に内部情報を取得

microSDカードを挿したときに自動でtech-supportをmicroSDに保存する

```
Yamaha#
Yamaha# configure terminal
Yamaha(config)# schedule 1 event sd-attached 1
Yamaha(config)# schedule template 1
Yamaha(config-schedule)# cli-command 1 copy tech-support sd
Yamaha(config-schedule)# end
```

実行禁止コマンド

スケジュール機能では、以下のコマンドを実行することはできません。

- backup system
- baudrate select
- boot prioritize sd / no boot prioritize sd
- certificate user
- clock で始まるコマンド
- cold start
- copy radius-server local
- crypto pki generate ca / no crypto pki generate ca
- disable
- enable password
- exit
- firmware-update execute
- firmware-update sd execute
- logout
- ntpdate / no ntpdate で始まるコマンド
- password / no password
- password-encryption / no password-encryption
- ping /ping6
- quit
- reload
- remote-login
- restart
- restore system
- schedule / no schedule
- schedule template / no schedule template
- show で始まるコマンド
- ssh
- ssh-server host key generate
- stack / no stack で始まるコマンド
- startup-config select / no startup-config select
- telnet
- traceroute / traceroute6

SYSLOG

スケジュール機能では、以下のSYSLOGが出力されます。

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
	[SCHEDULE]:inf:ID:X script 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のスクリプトが実行された
Error	[SCHEDULE]:err:ID:X cmd[ID][COMMAND] is prohibited to execute	スケジュールテンプレートID:Xで禁止コマンドCOMMANDの実行が抑止された
	[SCHEDULE]:err:ID:X cmd[ID][COMMAND] is failed to execute	スケジュールテンプレートID:Xでコマンドフォーマットが不正だったり、不適切なパラメーターによってコマンド実行に失敗した
	[SCHEDULE]:err:ID:X microSD is not mounted	スケジュールテンプレートID:Xでスクリプトを実行しようとしたときにmicroSDが挿入されていなかった
	[SCHEDULE]:err:ID:X failed to get the schedule forlder path	スケジュールテンプレートID:Xでスクリプトを実行しようとしたときに、実行するスクリプトが存在するべきディレクトリが存在しなかった
	[SCHEDULE]:err:ID:X script is not found	スケジュールテンプレートID:Xでスクリプトを実行しようとしたときに、スクリプトファイルが存在しなかった
	[SCHEDULE]:err:ID:X failed to add action to queue	スケジュールテンプレートID:Xでアクションを実行しようとしたが、実行待ちアクションが多いためアクションを破棄した

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-comannd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。
- 1つのスケジュールテンプレートにcli-commandとscriptコマンドの両方が設定されている場合、scriptコマンドが実行され、cli-commandは実行されません。
- 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。
- スタックが構成された機器では以下の注意事項があります。
 - スタックのメンバースイッチでは、startup イベントトリガーは起動しません。
 - スタックのメンバースイッチでは、sd-attached イベントトリガーは起動しません。
- スタックが有効でスタンドアローン状態のとき、トリガーは起動しません。
- 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

- ・ なし

Dante最適設定機能

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、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	○	○	○

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	DSCP値による送信キューの最適化	qos dscp-queue 48 5	-	○	○
		qos dscp-queue 56 7	○	○	○
		qos dscp-queue [上記以外] 0	○	○	○
		no qos wrr-weight [0~7]	-	○	○
	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	-	○	○
	LLDPを有効	lldp run	-	-	○
VLANインターフェイス	シャットダウンを無効	no shutdown	-	-	○
	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	-	○	○

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	-	○	○
	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	-	○	○

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
LAN/SFPポート	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	○	○	○
	MRUを設定	mru 1522	-	○	○
	L2MSフィルターの設定	l2ms filter disable	-	-	○
	BPDUフィルターを設定	spanning-tree bpdu-filter disable	-	-	○
	LLDPエージェントの作成	lldp-agent	-	-	○
	LLDPの送受信を有効	set lldp enable txrx	-	○	○
	基本管理TLVの設定	tlv-select basic-mgmt	-	○	○

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。

ADECIAコンポーネントは、以下の内容が含まれるヤマハ独自のLLDPフレームを送信します。

- EEE (省電力機能)の無効化設定
- フロー制御の無効化設定
- Diffserv base QoSの設定
- IGMPスヌーピングの設定

本機能が有効、かつ、該当する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、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。スタック機能に対応した機種でスタック機能が有効な場合は利用できません。

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

Web GUIでのDante最適設定方法は、[ProAV設定機能](#)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
基本管理TLVの設定	tlv-select basic-mgmt
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
送信キューのスケジューリング設定	qos wrr-weight
QoSトラストモードの設定	qos trust
シャットダウン	shutdown
マルチキャストフレームの転送設定	l2-mcast flood
未知のマルチキャスト転送の設定	l2-unknown-mcast
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

操作項目	操作コマンド
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レポート転送機能を有効	ip igmp snooping report-forward
マルチキャストルーターポート転送抑制機能の設定	ip igmp snooping mrouter-port data-suppression
L2MSフィルタの設定	l2ms filter
BPDUフィルタの設定	spanning-tree bpdu-filter
EEE設定	eee
MRU設定	mru

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

- ・ 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。

-
- スタック機能に対応した機種でスタック機能が有効な場合は利用できません。
 - 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設定機能](#)
- [LLDP](#)
- [QoS](#)
- [フロー制御](#)
- [IGMP Snooping](#)
- [インターフェース基本機能](#)
- [スパニングツリー](#)
- [L2MS](#)
- [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、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
		no qos wrr-weight [0～7]
	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
	LLDPを有効	lldp run
	PTPを有効	ptp enable

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
	シャットダウン解除	no shutdown
	未知のマルチキャストをフラッディング	l2-unknown-mcast flood
	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
	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
	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

設定対象	機能	コマンド
LAN/SFPポート	フロー制御を無効	flowcontrol disable
	MRUを設定	mru 1522
	QoSトラストモードをDSCPに設定	qos trust dscp
	L2MSフィルタの設定	l2ms filter disable / enable (※1)
	BPDUフィルタを設定	spanning-tree bpdu-filter disable / enable (※2)
	EEEを無効	eee disable
	LLDPの送受信を有効	lldp-agent set lldp enable txrx tlv-select basic-mgmt
	PTPを有効	ptp enable

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。

- ・ **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、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。
- **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、不必要な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。
- ・ **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。
- ・ **BPDUフィルターの設定 (※2)**
 - 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 **BPDUフィルターを有効** にします。
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、BPDUフィルターを有効にすることでポートのブロックを防止します。
なお、二重化構成以外のネットワーク構成では、**BPDU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	I2-unknown-mcast forward link-local
	LLDPを有効	lldp run
	PTPを無効	ptp disable
VLANインターフェース	プロファイル種別の設定	proav profile-type ndi
	シャットダウン解除	no shutdown
	未知のマルチキャストをフラッディング	I2-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
	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

設定対象	機能	コマンド
LAN/SFPポート	フロー制御を有効	flowcontrol both
	MRUを設定	mru 1522
	L2MSフィルターを無効	l2ms filter disable
	EEEを無効	eee disable
	LLDPの送受信を有効	lldp-agent set lldp enable txrx tlv-select basic-mgmt
	PTPを有効	ptp disable

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場合は、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、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。
- **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、不必要な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。

- ・ **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。

- ・ **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。

プロファイル併用時

- ・ プロファイル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	
		no qos wrr-weight [0～7]	
	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	
	LLDPを有効	lldp run	
	PTPを有効	ptp enable	

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
	シャットダウン解除	no shutdown +	no shutdown
	未知のマルチキャストをフラディング	I2-unknown-mcast flood +	I2-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
	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
	PTPパケットの常時転送	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	

設定対象	機能	Danteプロファイル	NDIプロファイル
LAN/SFPポート	フロー制御の設定	flowcontrol disable	flowcontrol both
	MRUを設定	mru 1522 +	mru 1522
	QoSトラストモードの設定	qos trust dscp +	qos trust port-priority qos port-priority-queue 2
	L2MSフィルターの設定	l2ms filter disable +	l2ms filter disable
	EEEを無効	eee disable +	eee disable
	LLDPの送受信を有効	lldp-agent set lldp enable txrx tlv-select basic-mgmt +	lldp-agent set lldp enable txrx tlv-select basic-mgmt

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

- QoSを有効にするため、システム全体で **フロー制御を無効** 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

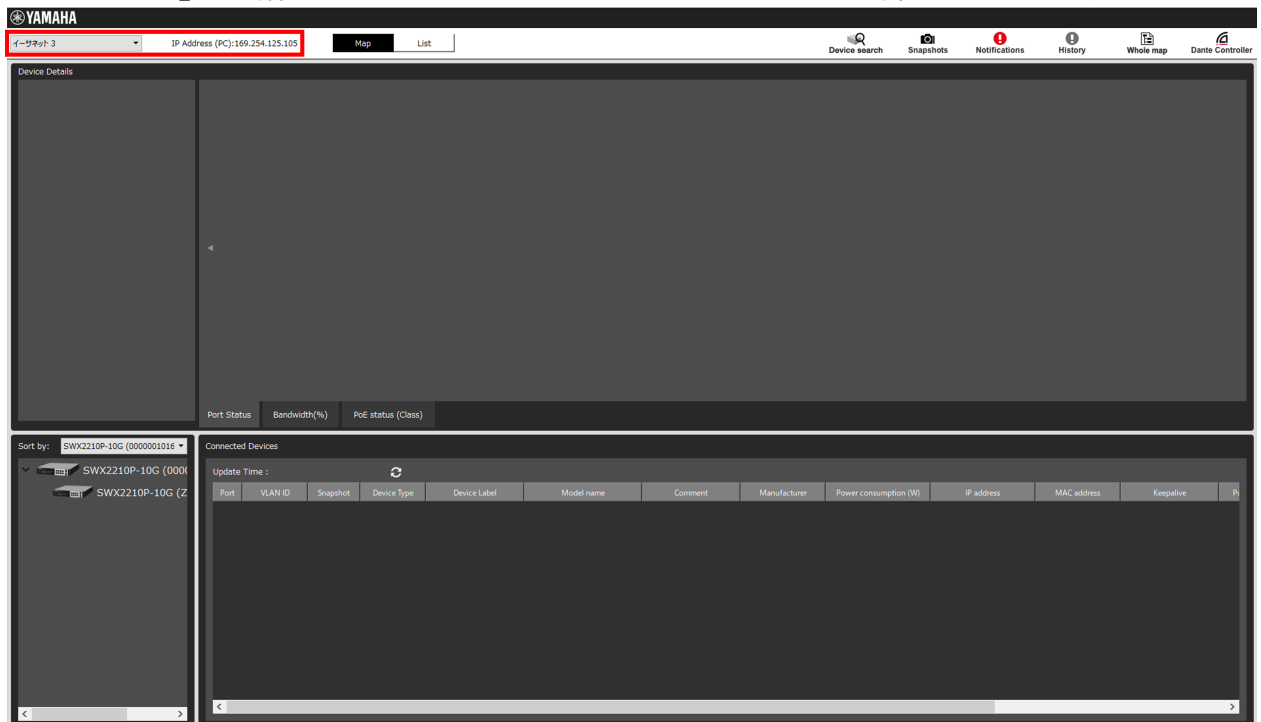
ヤマハネットワーク機器の統合管理ツール「Yamaha LAN Monitor」を活用することにより、かんたんにキッティング（初期設定）やトラブルシューティングを行うことができます。
Yamaha LAN Monitor は無料でダウンロードすることができます。Yamaha LAN Monitorのインストール方法や使い方の詳細はユーザーガイドを参照してください。

[キッティング] IPアドレスを意識せずに初期設定する

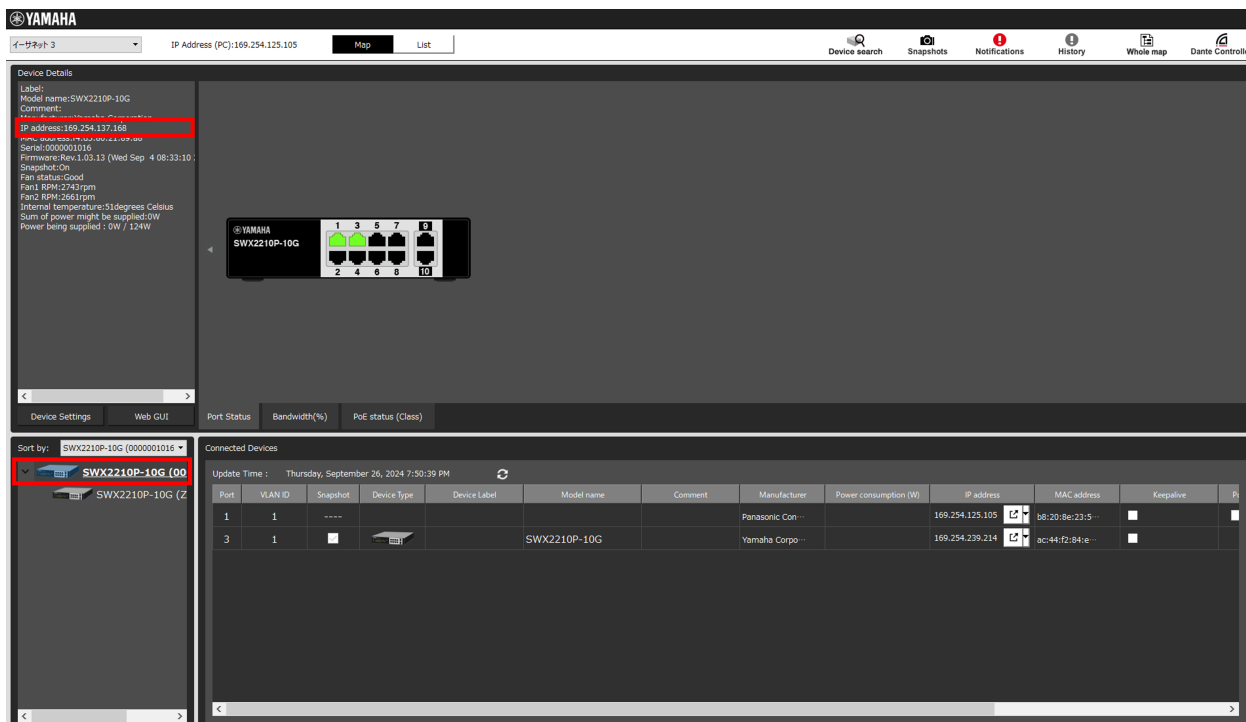
通常、ネットワークで2台以上のスイッチを使用する場合、IPアドレスの重複が発生しないように、スイッチごとに適切にIPアドレスを設定する必要があります。
しかし、外部ネットワークに接続する必要のないクローズドなAVoIPネットワークであれば、スイッチの **Auto IP機能** によって、自動的にリンクローカルアドレスを割り当てることができます。
工場出荷状態のヤマハスイッチとYamaha LAN Monitorを組み合わせることで、IPアドレスの設定を意識することなく、かんたんにProAVプロファイルを適用することができます。

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。

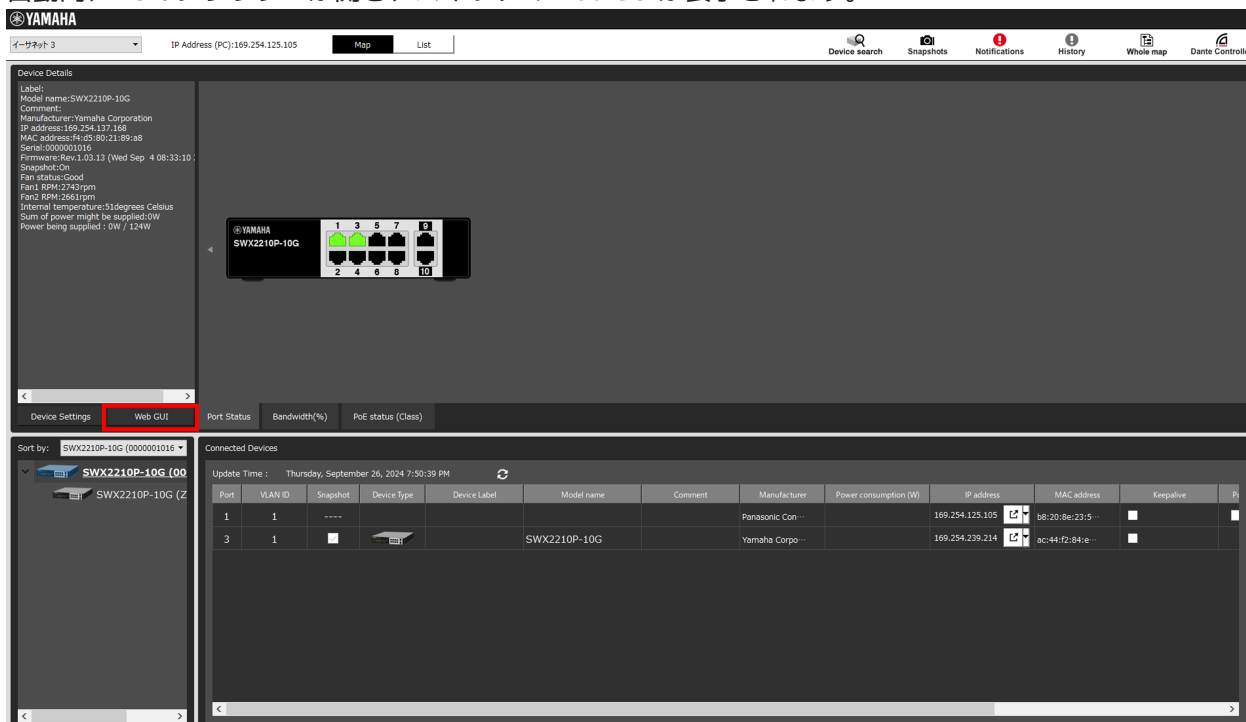


3. Yamaha LAN Monitor上のスイッチのアイコンをクリックすると、IPアドレスを確認することができます。ヤマハスイッチの初期IPアドレスは「192.168.100.240/24」ですが、**工場出荷状態(何も設定が変更されていない状態)でYamaha LAN Monitorの管理下に入ると、自動的にリンクローカルアドレスに切り替わります。**スイッチのIPアドレスが「169.254.」で始まっていれば、リンクローカルアドレスで動作しています。「192.168.100.240」のままになっている場合は、リンクローカルアドレスに切り替わるまでしばらく待って、表示を更新してください。**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。

SWX3220-16MT

SWX3220

ユーザー名を入力してください
Please enter your username.

パスワードを入力してください
Please enter your password.

Login

Yamaha Corporation

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。

SWX3220-16MT

? 🌐
Administrative User: admin Log out

Dashboard
LAN MAP
ProAV settings
Detailed settings
Management

CONSOLE
CONFIG
SYSLOG
TECHINFO

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

SWX3220-16MT

1	3	5	7	9	11	13	15
2	4	6	8	10	12	14	16

■ Unset

ProAV profile settings

Return to defaults

Select this option if only a Dante profile is used.

Select

Select this option if only a NDI profile is used.

Select

Select this option if only a SDVoE profile is used.

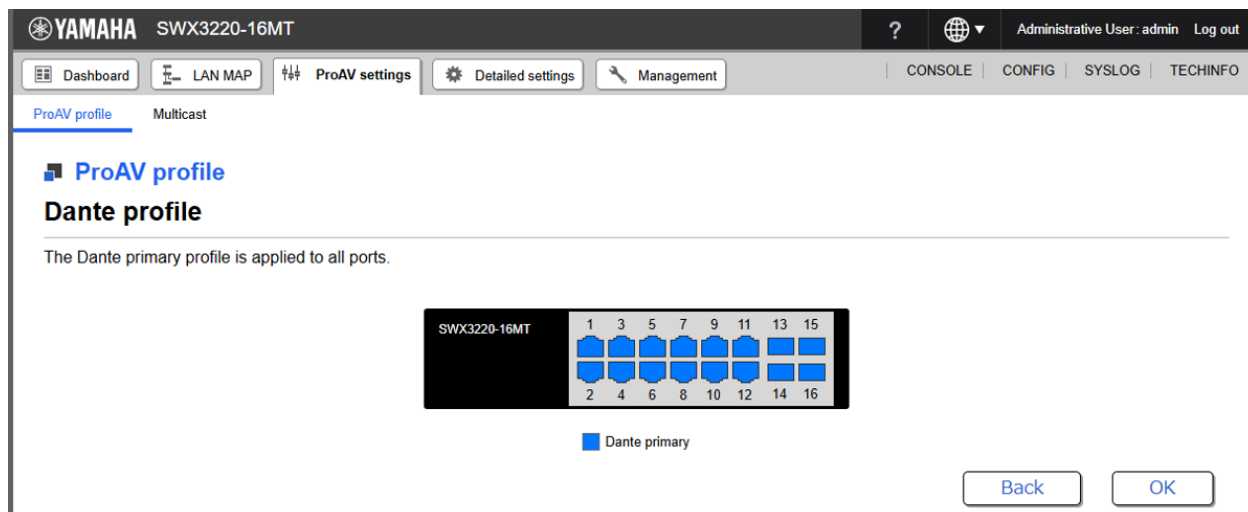
Select

CUSTOM

Select this option if multiple profiles are used.

Select

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。



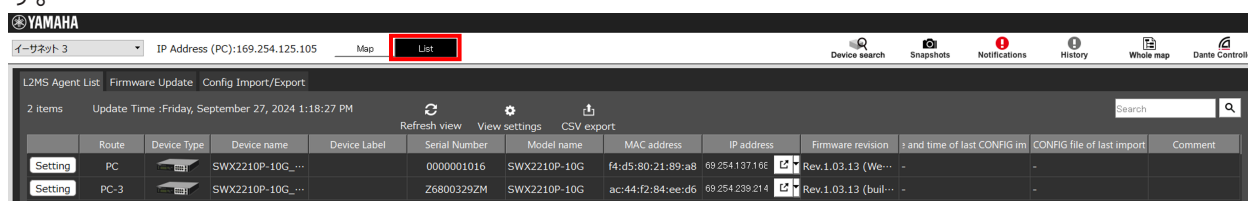
[キッティング] 複数のヤマハスイッチに同一設定を一括適用する

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。

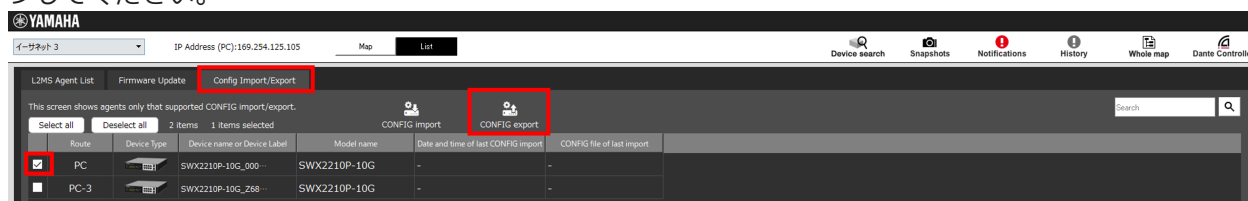
IPアドレスにリンクローカルアドレスを使用していて、すべてのスイッチに同一の設定を適用したい場合、効率的に複数台のスイッチを設定することができます。

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。

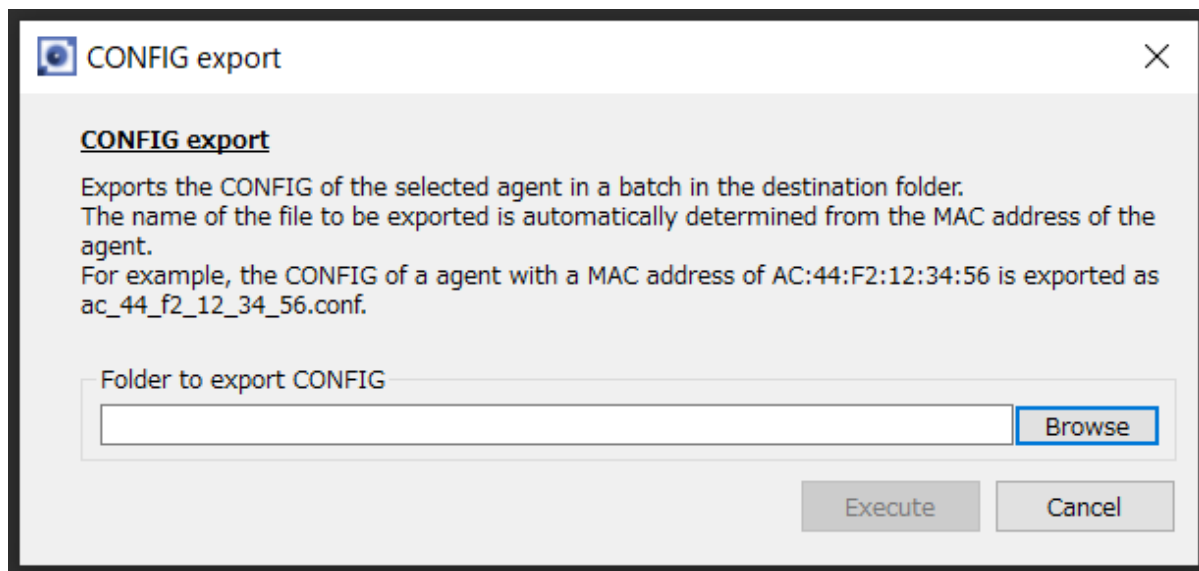
1. 4.1の手順に従って、1台のスイッチにProAVプロファイルを適用してください。
2. 画面上部の「List」タブをクリックしてください。検出しているヤマハスイッチの一覧が表示されます。



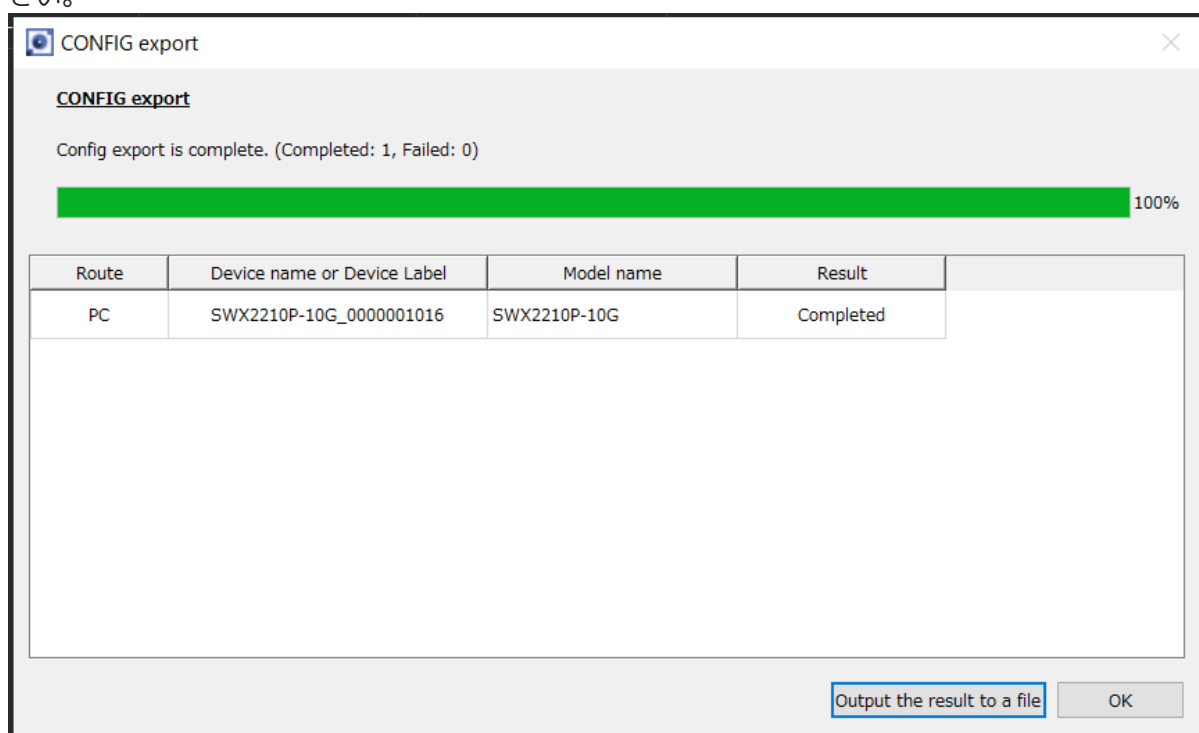
3. 画面上部の「Config Import/Export」タブをクリックしてください。さらに、既にProAVプロファイルを適用したスイッチをチェックし、「Config export」ボタンをクリックしてください。



4. 「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。

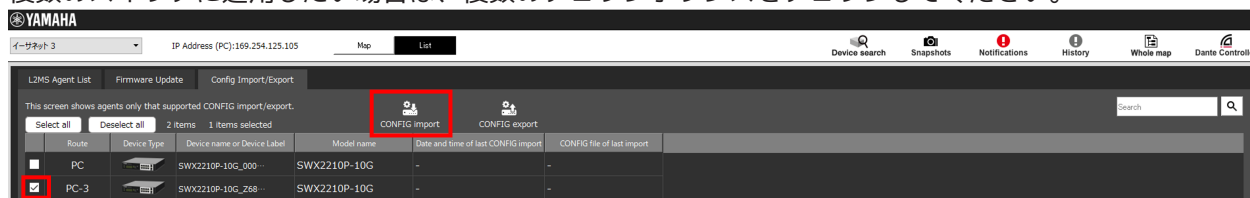


5. ダイアログにExportの進捗状況と結果が表示されるため、完了したら「OK」ボタンをクリックしてください。



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、Import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。

CONFIG import

Import CONFIG to the selected agents at once.
 * After the CONFIG import is complete, each agent will reboot.

Specify the CONFIG file to be import

☒ Specify the CONFIG file to be imported to each agent

Device name or Device Label	CONFIG file to be applied
SWX2210P-10G_Z6800329ZM	...fig_20240927132831/f4_d5_80_21_89_a8.conf Browse

☐ Send one CONFIG file to all specified agents Browse

☐ Search the specified directory and import the CONFIG corresponding to the MAC address of the agent Browse

Execute Cancel

8. ダイアログにImport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。

CONFIG import

Config import is complete. (Completed: 1, Failed: 0)

100%

Route	Device name or Device Label	Model name	Result
PC-3	SWX2210P-10G_Z6800329ZM	SWX2210P-10G	Completed

Output the result to a file OK

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。

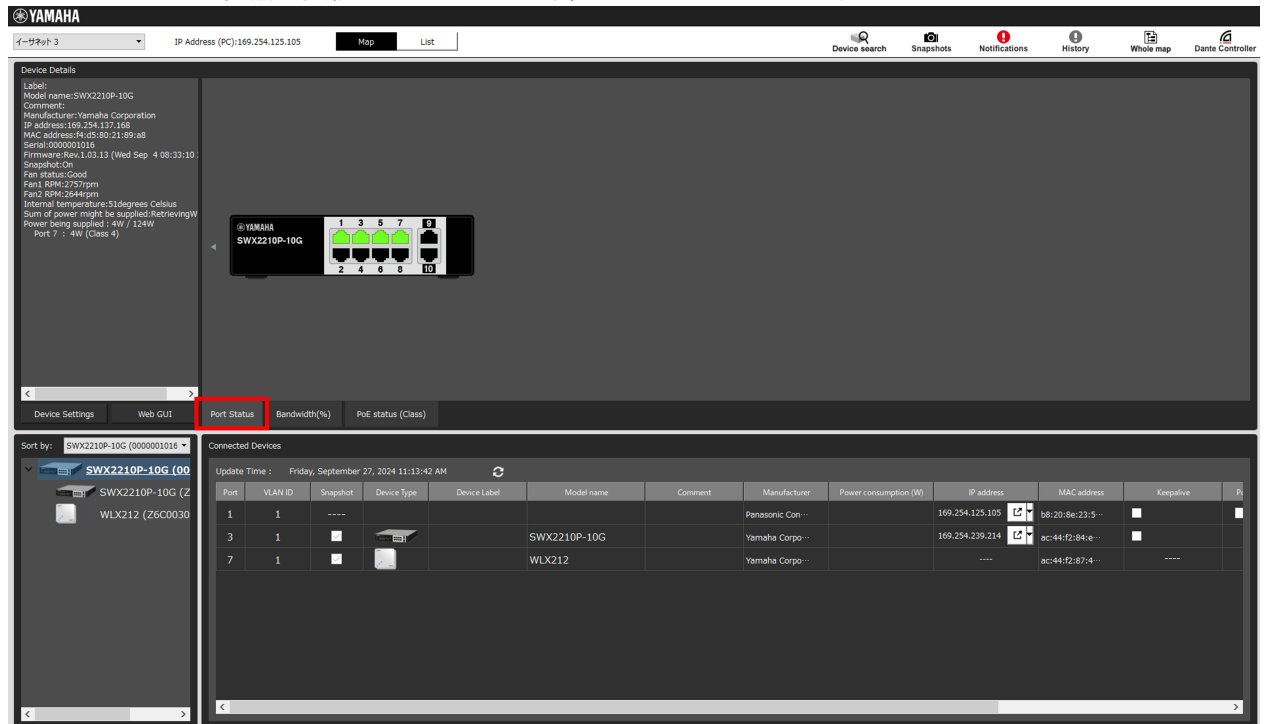
このように、Yamaha LAN Monitorは多台数環境のキッティングツールとして使用することができるため、是非ご活用ください。

[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

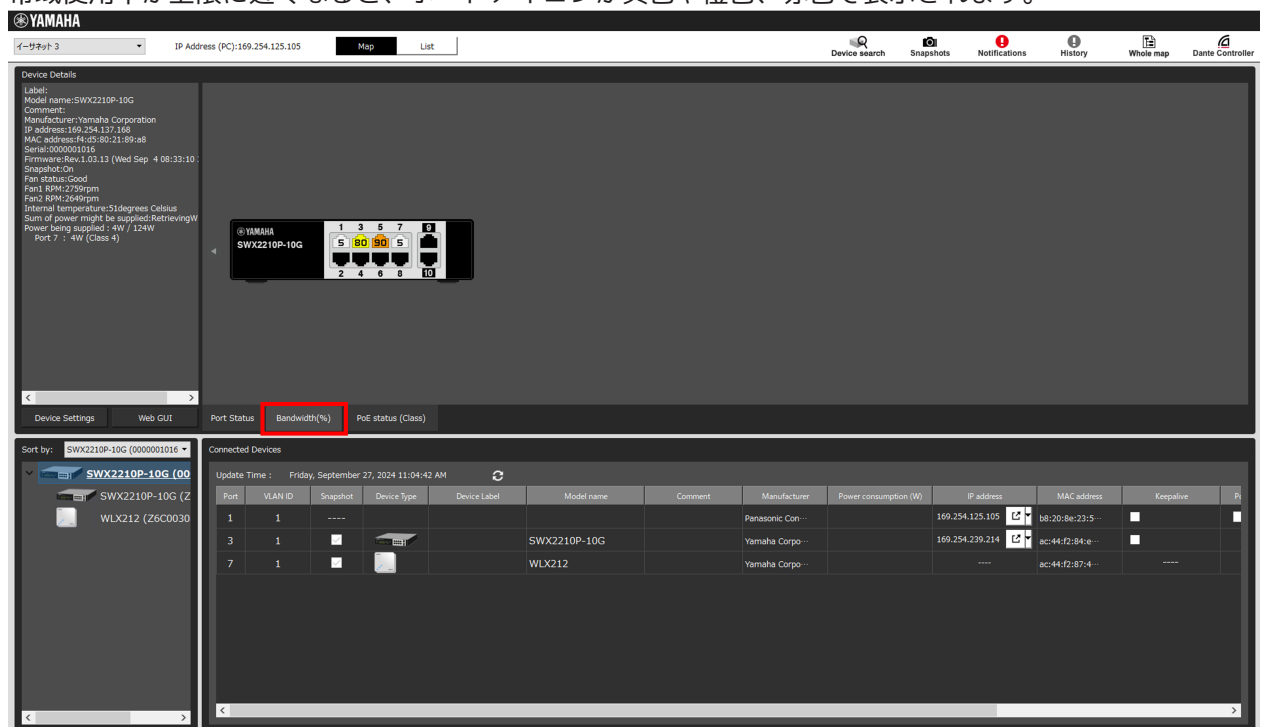
Yamaha LAN Monitorを使用することで、ネットワーク全体の接続構成を見える化することができ、さらにトラフィックの帯域使用状況や、PoE給電状況を確認することができます。

1. スwitch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

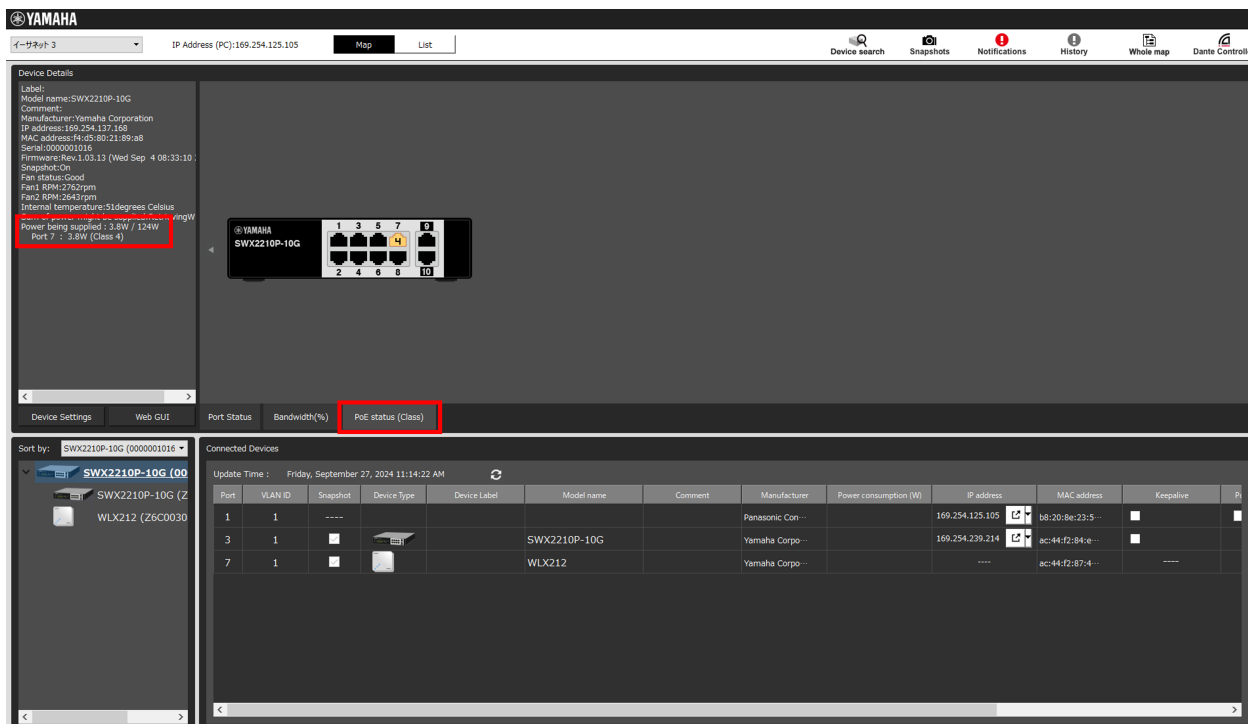
どのポートにどの機器が接続されているかを確認することができます。



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橙色、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。

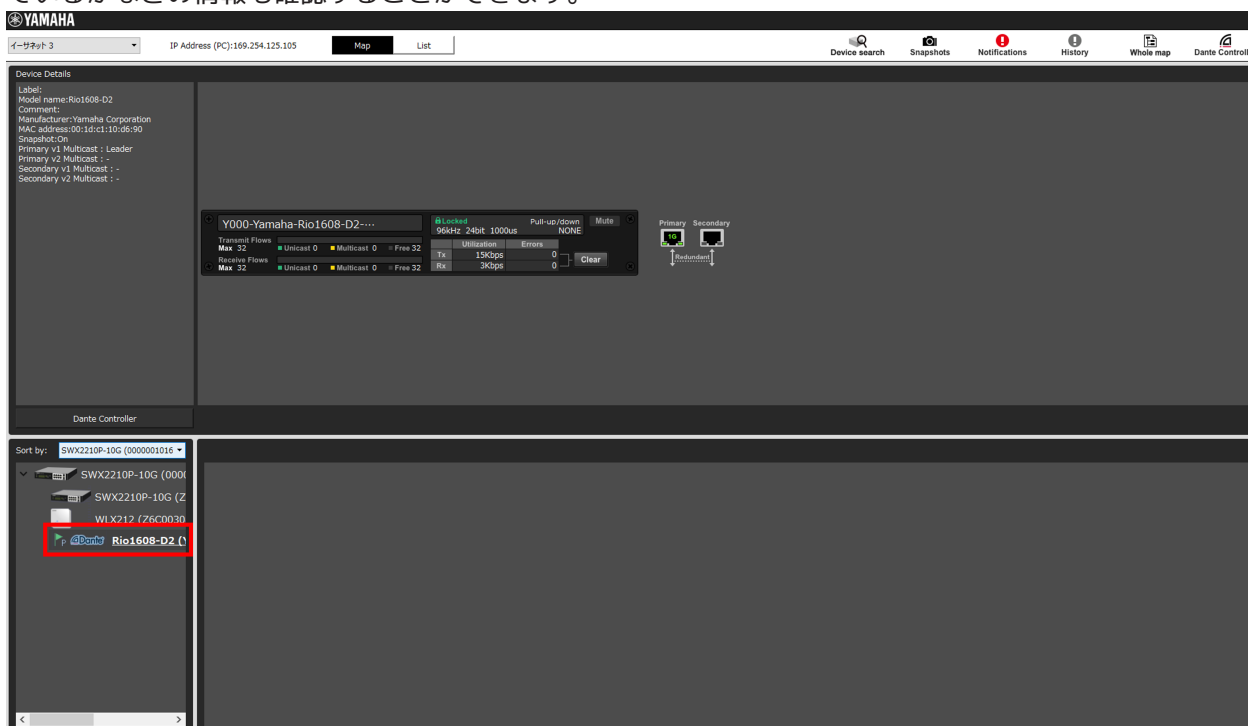


[トラブルシューティング] Dante機器の状態を確認する

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る場合はワンクリックでDante Controllerを開くことができます。

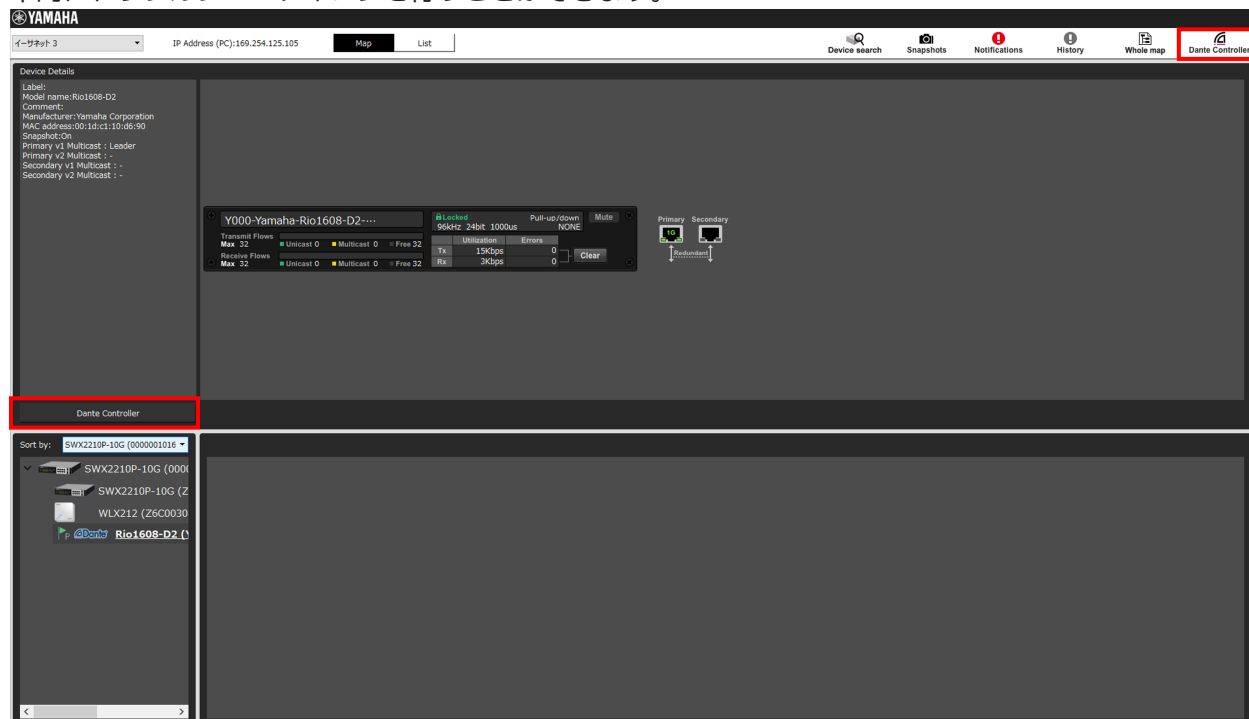
Dante機器を表示するには、Yamaha LAN Monitorのインストール時にDante Control and MonitoringとDante Discoveryをインストールしている必要があるため、ご注意ください。

1. 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이지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。



2. 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、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の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。
- ・ スタック機能に対応した機種でスタック機能が有効になっている場合、ProAV設定は使用できません。

関連文書

- ・ 特になし。

商標名称について

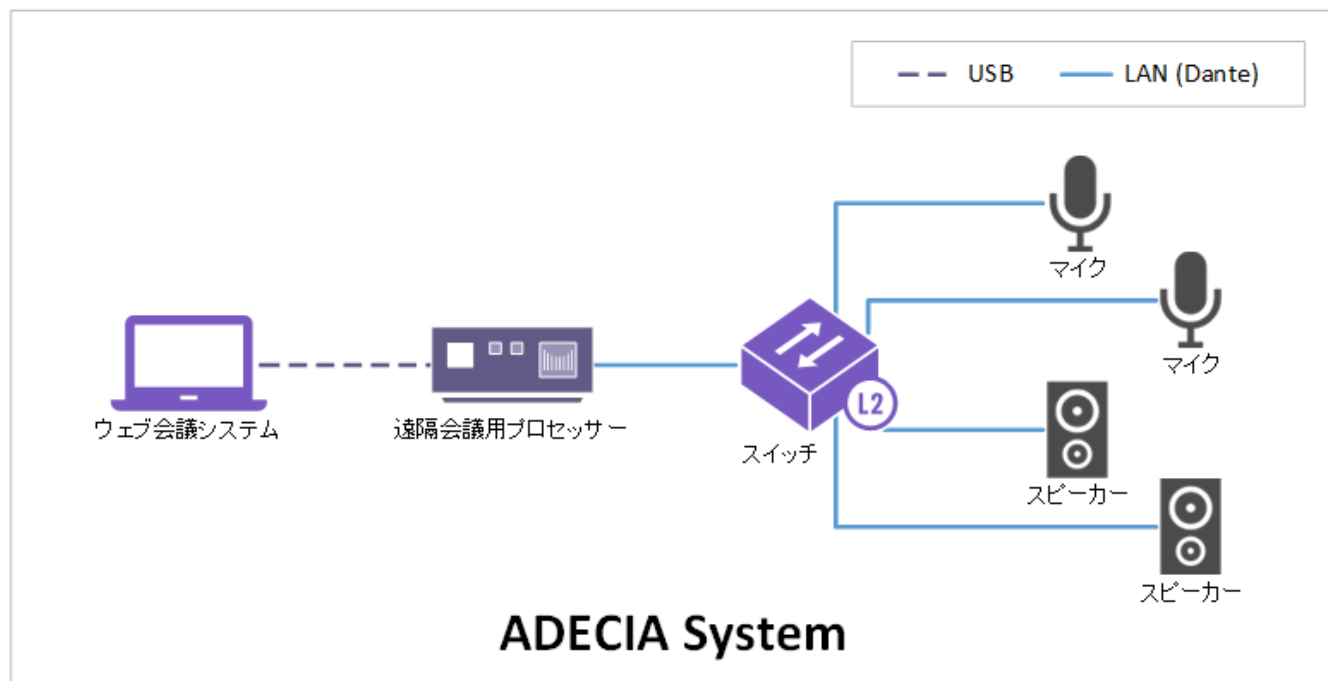
- ・ Dante™は、Audinate Pty Ltd. の登録商標です。
- ・ NDI®は Vizrt NDI AB の登録商標です。

ADECIAとのセキュリティ連携

機能概要

会議システムのIP化において、ネットワークの不正侵入を防御するセキュリティ機能は必須になってきています。

ヤマハの遠隔会議用ワンストップサウンドソリューション「ADECIA」では、IT業界で実績のある技術(デバイス認証)を活用することにより、セキュリティリスクに対して堅牢なシステムを実現します。



本製品はADECIAと連携することで、ITに不慣れなユーザーでも簡単にセキュリティ機能を利用可能としています。

具体的には、ADECIAコンポーネントである遠隔会議用プロセッサーのGUIから本製品のセキュリティ機能を有効化できます。(遠隔会議用プロセッサーの仕様に関しては [ADECIA製品情報](#) を参照してください。)

本製品のセキュリティ機能を有効化すると、認証登録されていないデバイスがネットワークにアクセスできなくなります。

本製品は次の3つの機能でセキュリティ連携を実現しています。

1. ADECIAコンポーネントの自動認識
遠隔会議用プロセッサーのGUIで制御対象スイッチの情報を自動的に表示します。
2. スイッチの遠隔制御
遠隔会議用プロセッサーからスイッチのデバイス認証を有効化します。
3. スイッチからの状態通知
スイッチが検知した不正アクセスを遠隔会議用プロセッサーへ通知します。

用語の定義

ADECIA

遠隔会議や授業を行う部屋・教室に最適なマイクロフォン・スピーカーを一式揃えた音響システム。
ADECIAを構成する機器(コンポーネント)は次の通りです。

- ・システム内のルーティング、音声プロセッシング、会議アプリケーションPCとの接続を担う遠隔会議用プロセッサー

- ・ 各コンポーネントを接続するネットワークスイッチ
- ・ Dante 対応マイクロフォン
- ・ Dante 対応スピーカー

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。

Yamaha Unified Network Operation Service (Y-UNOS)

ネットワークを介してデバイス同士を連携するサービス。

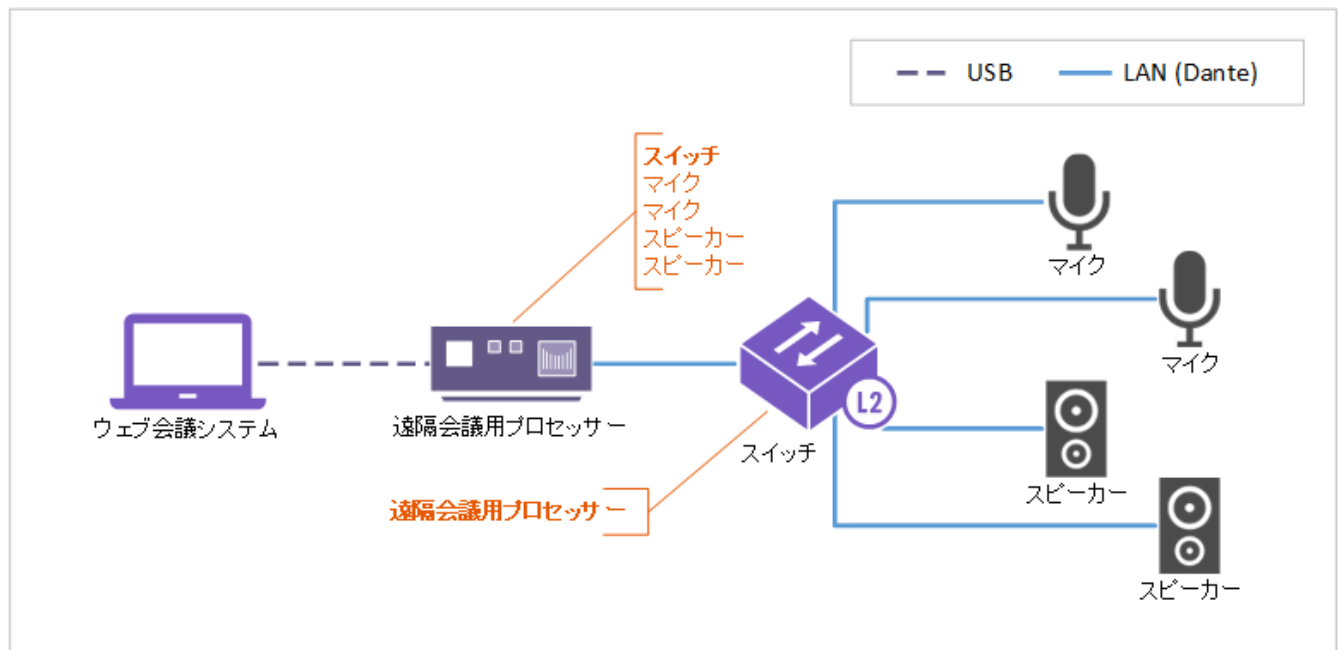
スイッチとADECIAのセキュリティ連携もY-UNOSに対応することで実現しています。ADECIAコンポーネントでは本製品と遠隔会議用プロセッサがY-UNOSに対応しています。

機能詳細

ADECIAコンポーネントの自動認識

本製品は同じネットワーク(保守VLAN)に存在するY-UNOS対応機器と相互に自動認識します。ADECIAとのセキュリティ連携では、この機能を以下に利用しています。

- ・ 遠隔会議用プロセッサのGUIでセキュリティを設定するスイッチの一覧を表示する
- ・ 遠隔会議用プロセッサのGUIでデバイス認証の対象とする機器(ネットワークへの接続を許可する機器)の一覧を表示する
- ・ スwitchが不正アクセスの通知先遠隔会議用プロセッサを決定する

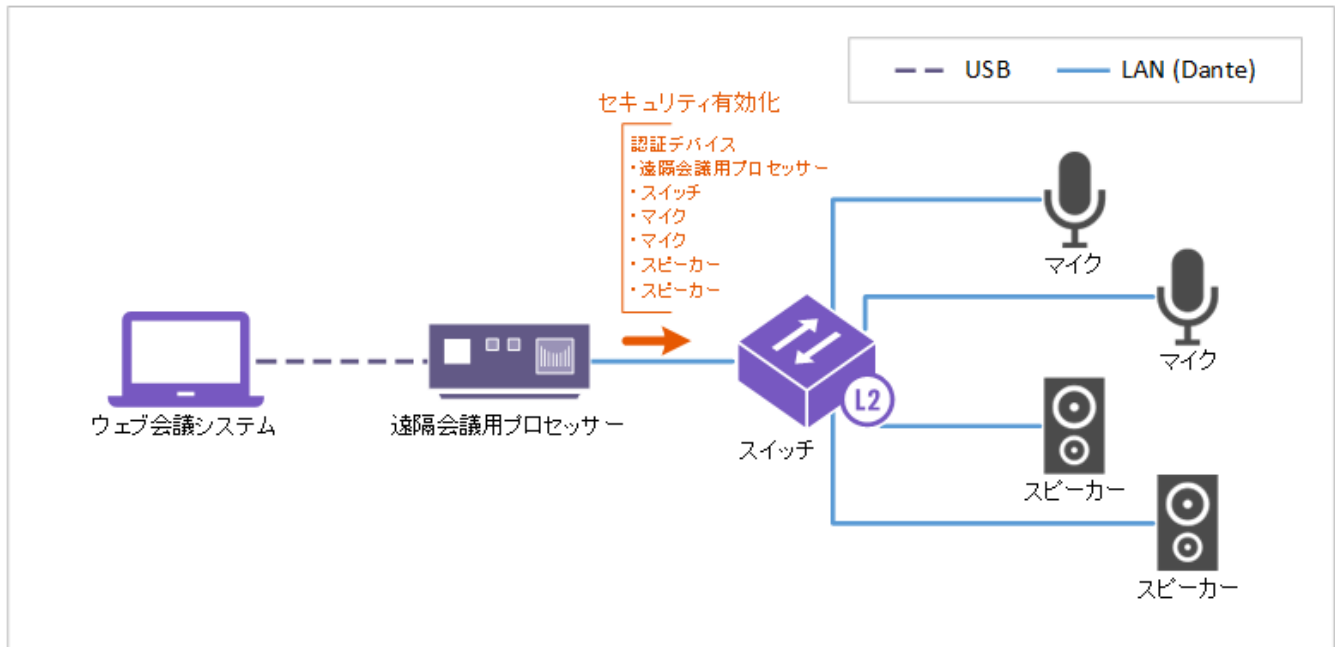


スイッチの遠隔制御

本製品はY-UNOSの機能により同じネットワーク(保守VLAN)に接続された他の機器から設定を適用できます。セキュリティ連携では、遠隔会議用プロセッサからの指示で以下の設定をスイッチに適用します。なお、これらはセキュリティ連携機能によって自動的に一括設定するためユーザーが各々の設定を意識する必要はありません。

- ・ ルート認証局の生成

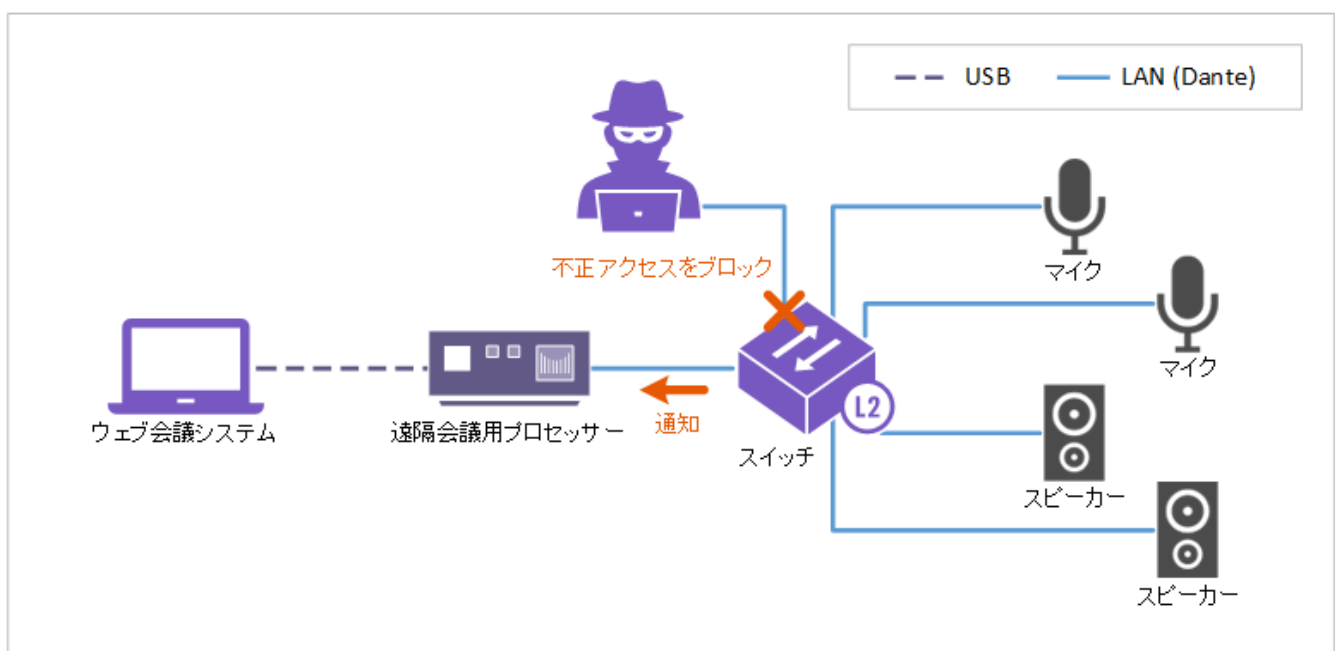
- ・ 認証ユーザー(デバイス)の設定
- ・ ローカルRADIUSサーバー機能の設定
- ・ ホストモードの設定(全インターフェース)
- ・ MAC認証機能の設定(全インターフェース)
- ・ RADIUSサーバーホストの設定
- ・ システム全体でのMAC認証機能の設定



スイッチからの状態通知

本製品はY-UNOSの機能により同じネットワーク(保守VLAN)に接続された他の機器へ自身の状態を通知できます。

セキュリティ連携では、本製品に不正アクセスがあった(未登録のデバイスが接続された)場合にすべての遠隔会議用プロセッサに対してその旨を通知します。



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
セキュリティ連携機能(Y-UNOS)の有効化/無効化	y-unos
Y-UNOS の状態表示	show y-unos

セキュリティ連携の初期設定

ADECIAとのセキュリティ連携を利用する際は、最新のファームウェアを使用しセキュリティ連携用の設定を適用してください。

ファームウェアアップデートと設定の適用方法についてはヤマハスイッチ製品技術情報サイトの [ADECIAとのセキュリティ連携](#) を参照してください。

注意事項

1. 本機能の利用を開始する際は、必ず [セキュリティ連携の初期設定](#) を実行してください。
2. 運用中は本製品のコマンドやGUIなどで設定を変更しないでください。
 - 設定が変更された場合、本機能が正しく動作しなくなる可能性があります。
3. セキュリティ連携の初期設定を実行後には必ずmicroSDカードを抜いてください。
 - microSDカードが挿されたままの場合、次回起動時にもファームウェアアップデートとコンフィグの適用が実行されます。
4. スタック機能が有効な場合、本機能は使用できません。
 - 本機能を利用する際はスタック機能を無効化してください。
 - なお、SDカードブート自動適用(ファームウェア、コンフィグ)機能もスタック機能が有効な場合には動作しませんのでご注意ください。

関連文書

- [外部メモリの利用](#)
- [ファームウェア更新](#)
- [スタック機能](#)
- [ヤマハスイッチ製品技術情報サイト ADECIAとのセキュリティ連携](#)
- [ヤマハスイッチ製品技術情報サイト ファームウェア情報](#)
- [ADECIA製品情報](#)

スタック機能

機能概要

スタックは、複数のスイッチを接続し、**仮想的な1台のスイッチとして動作させる機能**です。
スタックの特長について、以下に示します。

1. 利用効率の高い冗長性の実現

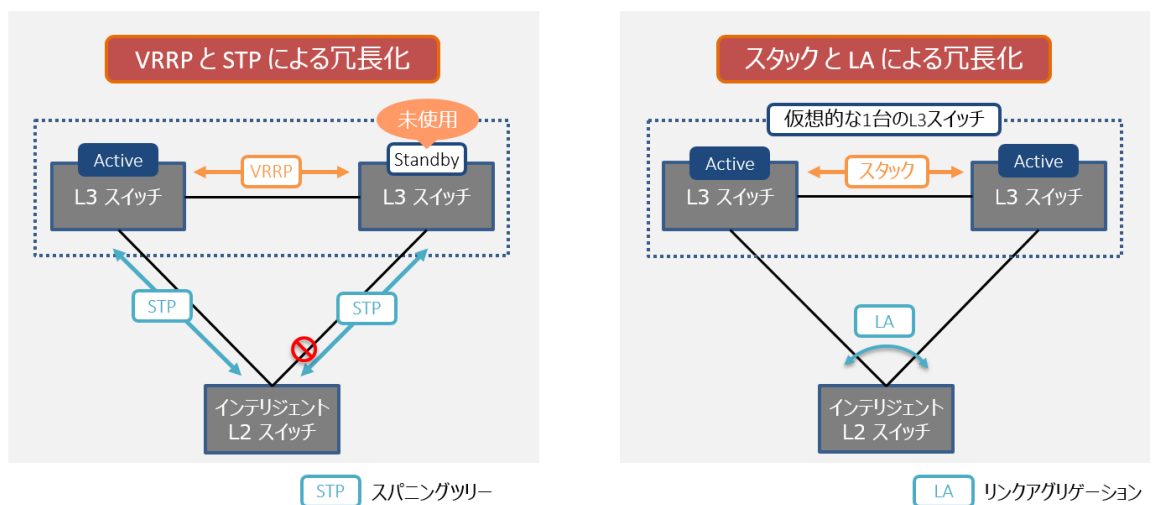
ネットワーク構成の単一障害点 (SPOF) を除去するための構成としては、**VRRP とSTP で構成する方法**と、**スタックとリンクアグリゲーションで構成する方法**があります。

スタックを利用することで、VRRPと違い、待機スイッチがないことから、冗長性を確保しながらスイッチの利用効率を高めることができます。

2. 容易なポート増設

スイッチを追加することで、利用できるポート数を容易に増やすことができます。

° スタックの概要



冗長性を確保しながら、スイッチの利用効率を高めることができます！
容易にポート増設を行うことができます！

スタック機能は、工場出荷時、**無効** に設定されています。

用語の定義

メンバースイッチ

スタックを構成するネットワークスイッチ。
各スイッチは、スタックIDにより識別されます。

スタックID

スタックを構成するメンバースイッチを識別するためのID。
スタックIDは、1からスタック構成可能な最大数 (現状は2) まで設定することができます。

メインスイッチ

メンバースイッチの中から選出され、他のメンバースイッチを管理するスイッチ。
初期設定では、スタックIDが1のスイッチがメインスイッチとして動作します。

仮想スイッチ

スタック機能により 複数のメンバースイッチで構成された論理的な1台のスイッチ。

スタックポート

スタックを構成するネットワークスイッチを接続するために使用するSFP+スロット。

スタックリンク

スタックを構成するメンバースイッチ間の接続のこと。

機能詳細

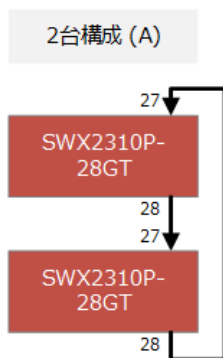
スタックの構成

モデル毎にスタック可能な構成について、以下に示します。

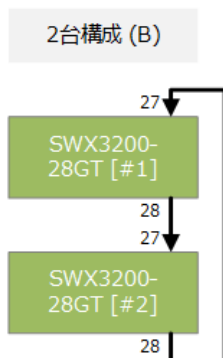
同一モデルの二台構成のみをサポート します。

なお、スタックは、障害時の影響を少なくすることを考慮し、**必ず、二つのスタックリンクで構成するようにしてください。**

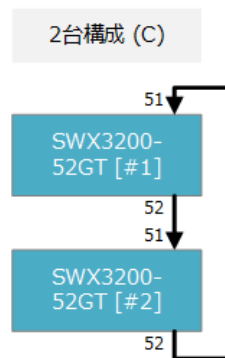
- ・ SWX2310P-28GT スタック構成



- ・ SWX3200-28GT スタック構成



- ・ SWX3200-52GT スタック構成



メンバースイッチ間の接続

スタック機能を有効にすると、メンバー間の接続用ポートとして、以下の SFP+スロット が スタックポート に切り替わります。

- SWX2310P-28GT : ポート27, 28
- SWX3200-28GT : ポート27, 28
- SWX3200-52GT : ポート51, 52

スタックポートは通常の通信ポートと異なり、メンバースイッチ間の通信にのみ利用されます。
メンバースイッチ間の接続は、ヤマハが提供する **ダイレクトアタッチケーブル(YDAC-10G-1M/3M)**、**SFP+モジュール(YSFP-10G-SR/LR)** でのみ可能です。

他社製品で接続した場合、スタックリンクは強制的にダウンします。

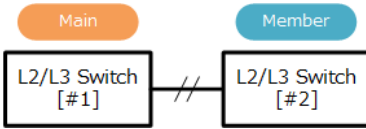
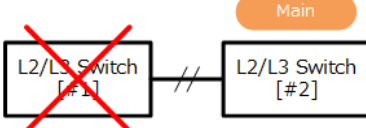
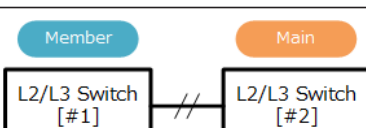
接続するスタックポートは、メンバースイッチの **若番 (Lower number) ポートと 老番 (Higher number) ポート** を接続します。

メインスイッチの選出とMACアドレスの付与

メインスイッチの選出とMACアドレスの付与ルールについて、以下に示します。
なお、スタック構成時に使用するMACアドレスは、通信への影響をなくするため、以下のルールで適用します。

1. 初期スタック構成時は、メインスイッチ (ID 1のスイッチ) のMAC アドレスを仮想スイッチのMACアドレスとして使用します。
2. スタック構成中にメインスイッチ以外のメンバースイッチが (何らかの異常で) 離脱した場合、仮想スイッチは、設定中のMACアドレスを継続して使用します。
3. スタック構成中にメインスイッチが (何らかの異常で) 離脱した場合、仮想スイッチは、設定中のMACアドレスを継続して使用します。
すなわち、スタック構成に組み込まれていないスイッチのMACアドレスを使用します。
4. 障害が発生したスイッチとは別のスイッチ (MAC アドレスが異なるスイッチ) をメンバースイッチとして組み込んだ場合も、仮想スイッチは、設定中のMACアドレスを継続して使用します。
現在の構成状況でスタック構成を組みなおしたい場合は、仮想スイッチを同時に再起動することで、再構築が行われます。
(ID 1 がメインスイッチとなり、仮想スイッチは、メインスイッチのMACアドレスを使用します)

- メインスイッチの選出とMACアドレスの付与

N o	スタック構成	メインスイッチの選択ルール
1	初期構成 	スタックID 1が設定されているスイッチがメインスイッチに選出されます。 このとき、仮想スイッチのMAC アドレスは、スタックID 1の MAC アドレスを使用します。
2	障害発生 	メインスイッチで異常が発生した場合、メンバースイッチの中で一番小さなスタックIDをもつスイッチがメインスイッチに選出されます。 このとき、仮想スイッチのMAC アドレスは、スタックID 1の MAC アドレスを維持します。
3	異常状態の回復 	障害発生スイッチを再度スタックに組み込んだ場合、現在選出中のメインスイッチがそのままメインスイッチとして機能します。 このとき、仮想スイッチのMAC アドレスは、異常発生した スタックID 1の MAC アドレスを維持します。

仮想スイッチに対する操作

スタック構成中の仮想スイッチに対する操作は、基本的にメインスイッチから制御します。
オペレーションに関する仕様について、以下に示します。

1. 仮想スイッチにログインすると、**必ず、メインスイッチにログインします。**
必要に応じて、他のメンバースイッチにログインしたい場合は、**remote-login** コマンドを使用してください。

- 。メインスイッチログイン時のプロンプト

```
Yamaha>
```

- 。メンバースイッチログイン時のプロンプト

```
Yamaha-2> ①
```

- ① ホスト名の後ろに スタックID が表示される

2. 仮想スイッチに対する設定 (running-config, startup-config) は、常にメンバースイッチ間で同期します。
設定完了後は、必ず、**write** コマンドで running-config を保存するようにしてください。
なお、**write** コマンドはメインスイッチ側からのみ実行可能です。
3. 仮想スイッチ運用時、L2/L3ネットワークスイッチとしての保存している情報 (e.g. FDB学習情報、ARP キャッシュなど)は、自動で同期されます。
ユーザが意識する必要はありません。
4. 仮想スイッチのログ参照は、ログイン後、**show logging** コマンドで行います。
本状態で参照しているログは、メインスイッチのログであるため、他のメンバースイッチのログを参照したい場合は、**remote-login** コマンドで該当スイッチにログインしてからログを参照してください。

スタック構成時のスイッチの状態

メンバースイッチは、スタック構成中の状態を以下で管理します。
本状態は、**show stack** コマンドで参照することができます。

1. **Setting**

- 1つ以上のスタックポートのリンクが上がり、メンバースイッチ間でスタックを行うために必要な設定を行っている状態。
具体的には、メンバースイッチ間で自動的に構成を把握しています。

2. **Active**

- メンバースイッチ間の構成の自動認識が終わり、各種設定の同期が行われ、複数のメンバースイッチで仮想化されている状態。
2台以上のスイッチで仮想化が行われています。

3. **Inactive**

- 障害が発生し、仮想化されたスイッチから離脱している状態。
スタックポートを含む全通信ポートは強制的にシャットダウン され、通信が確立できません。(閉塞状態)

4. **Standalone**

- スタック機能が有効だが、メンバースイッチとネゴシエーションが取れないために1台で運用している状態。
初期導入時など、一時的に対向スイッチが存在しない場合に、本状態に遷移します。
本状態では、設定しているスタックIDが有効である必要があるため、**設定されているIDで運用** されます。

5. **Standalone(separated)**

- 上記Standaloneと同様の状態。
ただし、一度スタックが構成されたことを記憶しており、再度構成される時のメインスイッチ選出情報を保持した状態。

6. **Disable**

- スタック機能が無効な状態。
本状態では、**強制的にスタックIDは1で運用** されます。(スタックIDが1以外に設定されていた場合も)

異常状態の検出と措置

スタック構成中のメンバースイッチは、異常を検出すると、ネットワークサービスに影響がないように仮想スイッチ内で自律的に解決しようとします。
本スイッチは、以下の異常状態を監視します。

・ **自ノードでの異常検出**

1. スタック構成条件に合っていない (スタックID異常、ファームバージョン異常)
2. スタックリンク異常 (ダウン検出)
3. FAN 停止
4. 温度センサ異常 (SWX2310P-28GTのみ)
5. 電圧値異常
6. 電流値異常

・ **接続ノードの異常検出**

1. ハートビートフレーム 受信タイムアウト

ハートビートは、メンバースイッチが正常に稼働しているかどうかを確認するための機能です。
ハートビートフレームが一定期間（現在は4秒）受信できなかった場合、メンバースイッチに異常が発生したと判断します。

以下に異常検出時の動作について、示します。

検出ノード	検出内容	検出後の動作	検出後の状態	備考
メインスイッチ	設定異常	スタックID、ファームバージョン異常	Inactive	
	スタックリンクダウン	二本のうち、片方がリンクダウン	Active	
		両リンクダウン	Standalone(separated)	ダブルメイン状態の可能性あり
	HW異常	FAN停止, 温度異常, 電圧/電流値異常	Inactive	
	ハートビートエラー	メンバースイッチからの通知が無くなった	Standalone(separated) or Active	残構成台数が1つの場合、Standalone(separated)
メインスイッチ以外のメンバースイッチ	設定異常	スタックID、ファームバージョン異常	Inactive	
	スタックリンクダウン	二本のうち、片方がリンクダウン	Active	
		両リンクダウン	Standalone(separated)	ダブルメイン状態の可能性あり
	HW異常	FAN停止, 温度異常, 電圧/電流値異常	Inactive	
	ハートビートエラー	メインスイッチからの通知が無くなった	Standalone(separated) or Active	残構成台数が1つの場合、Standalone(separated)

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願います。

操作項目	操作コマンド
スタック機能の設定	stack
スタックIDの変更	stack renumber
スタックポートで使うIPアドレスの範囲設定	stack subnet
スタック情報の表示	show stack

スタックの初期設定

スタック構成時の初期設定フローについて、以下に示します。

1. 必要機材の準備
2. メンバースイッチの設定
3. メンバースイッチの接続

必要機材の準備

スタックを構成するために必要な機材を準備します。

- ・ メンバースイッチ
スタック構成するメンバースイッチを準備します。
スタック可能な構成については、 **3.1 スタックの構成** を参照ください。
- ・ スタックポート接続ケーブル
メンバースイッチを接続するインターフェースを決定し、準備します。
ラック内でスタックを構成する場合は **ダイレクトアタッチケーブル** を、フロア間、建屋間などある程度の距離が必要となる場合には **SFP+モジュール** を利用します。
詳細は、 **3.2 メンバースイッチ間の接続** を参照ください。
- ・ 外部メモリ(SDカード)
スタック稼働中のコンフィグ、ログなどのバックアップデータを保存するために外部メモリの利用をお勧めします。
外部メモリを利用することで、障害発生時、コンフィグの復旧に役立てることができます。

メンバースイッチの設定

スタックを構成するメンバースイッチの設定を行います。
設定を開始する前に、以下について、検討します。

1. メンバースイッチに割り当てるスタックIDの決定
メンバースイッチに割り当てるスタックIDは、 **静的に決める** 必要があります。
初期設定時、 **スタックID: 1** が、**メインスイッチ**となります。
2. スタートアップコンフィグの保存先の決定
スタック構成時のスタートアップコンフィグの保存先を決定します。
保存先として フラッシュROM 内の 0~4 を選択し、説明文でスタック保存用とわかるようにします。

検討後、以下の手順で **メンバースイッチを個別に設定** します。

1. **メンバースイッチの起動**

メンバースイッチを個別で起動し、シリアルコンソールからアクセスします。

2. **ファームウェアバージョンの確認と更新**

show environment コマンドで現在のファームウェアバージョンを確認します。

```
Yamaha> show environment
SWX3200-52GT BootROM Ver.1.00
SWX3200-52GT Rev.4.00.05 (Fri Mar 9 09:34:05 2018) ①
main=SWX3200-52GT ver=00 serial=S000000000 MAC-Address=00a0.de00.0000
...
```

① ファームウェアバージョンの確認

最新の公開ファームウェアを **RTpro** にて確認します。

公開されている該当スイッチのファームウェアのバージョンが起動中のファームウェアより新しい場合は、更新を行います。

- ・メンバースイッチは、**既知の問題が改善された最新のファームウェアに更新** することをお勧めします。
- ・初期設定では、**SDカードを使用したファームウェア更新** が有効です。
SDカードを使用した更新方法については、**ファームウェア更新** を参照ください。

3. **スタートアップコンフィグの保存先の設定**

startup-config select コマンドで、スタック運用時に使用するコンフィグを選択します。

このとき、スタック運用時のコンフィグに使用することを **説明文** に設定することをお勧めします。

```
Yamaha> enable
Yamaha# startup-config description 2 Stack ①
Yamaha# startup-config select 2 ②
reboot system? (y/n): y ③
```

① startup-config #2 に "Stack" と説明文を設定

② startup-config #2を選択

③ 再起動する

4. **スタック ID の設定**

スイッチの状態を **show stack** で確認し、スタック機能が無効になっていることを確認します。

また、スタックIDを確認します。スタックID は初期値が **1** に設定されています。

```
Yamaha> enable
Yamaha#
Yamaha# show stack
Stack: Disable

Configured ID      : 1
Subnet on stack port : Auto-ip
Virtual MAC-Address : 00a0.de00.0000

ID  Model          Status   Role   Serial      MAC-Address
-----
```

```
Interface      Status
-----
```

```
Yamaha#
```

必要に応じて、スタックIDを **stack renumber** コマンドを使用して、変更します。

```
Yamaha(config)# stack 1 renumber 2 ①
```

```
Yamaha(config)# do show stack
```

```
Stack: Disable
```

```
Configured ID      : 2
```

```
Subnet on stack port : Auto-ip
```

```
Virtual MAC-Address : 00a0.de00.0000
```

```
ID  Model          Status      Role      Serial      MAC-Address
-----
```

```
Interface      Status
-----
```

```
Yamaha#
```

① スタックID を #1 から #2 に 変更する

5. スタック機能の有効化

stack enable コマンドを使用して、スタック機能を有効にします。

コマンド投入後、本装置のリブートをを行います。

リブート完了後、default-config が適用されます。

```
Yamaha(config)#stack enable ①
```

```
reset configuration and reboot system? (y/n): y ②
```

① スタック機能を有効化

② 再起動の実行

再起動後、スイッチの状態を **show stack** で確認し、スタック機能が有効になっていることを確認します。

また、スタートアップコンフィグの保存先も確認します。

```
Yamaha> enable
```

```
Yamaha#
```

```
Yamaha# show stack
```

```
Stack: Enable ①
```

```
Configured ID      : 1
```

```
Running ID         : 1
```

```
Status            : Standalone
```

```
Subnet on stack port : Auto-ip
```

```
Virtual MAC-Address : 00a0.de00.0000
```

ID	Model	Status	Role	Serial	MAC-Address
1	SWX3200-52GT	Standalone	Main	S000000000	00a0.de00.0000

... (1台で動作しているため、Standalone で Main となる)

Interface	Status
port1.51	down
port1.52	down

```
Yamaha>show environment
SWX3200-52GT BootROM Ver.1.00
SWX3200-52GT Rev.4.00.05 (Fri Mar 9 09:34:05 2018)
main=SWX3200-52GT ver=00 serial=S000000000 MAC-Address=00a0.de00.0000
CPU: 2%(5sec) 2%(1min) 1%(5min) Memory: 10% used
Fan status: Normal
Fan speed: FAN1=4000RPM FAN2=3870RPM
Startup firmware: exec0
Startup Configuration file: config2 ②
Serial Baudrate: 9600
Boot time: 2018/01/01 11:06:36 +09:00
Current time: 2018/01/02 16:12:23 +09:00
Elapsed time from boot: 1days 05:05:49
Temperature status: Normal
Temperature: 37 degree C
Voltage: 11.99V Current: 0.741A
```

- ① スタック機能が有効になっている
- ② 設定したスタートアップコンフィグになっていることを確認

メンバースイッチの接続

スタックを有効化したスイッチを、**ダイレクトアタッチケーブル** または、**SFP+モジュール** を使用して接続します。

接続方法は [メンバースイッチ間の接続](#) を参照ください。

なお、メンバースイッチの接続は、**電源を落とした状態**、**電源を入れた状態**、どちらで行っても問題ありません。

メンバースイッチの接続後、**show stack** コマンドでシステムの状態を確認してください。

```
Yamaha# show stack
Stack: Enable
```

```
Configured ID      : 1
Running ID         : 1
Status             : Active
Subnet on stack port : Auto-ip
Virtual MAC-Address : 00a0.de00.0000
```

ID	Model	Status	Role	Serial	MAC-Address
1	SWX3200-52GT	Active	Main	S000000000	00a0.de00.0000
... (スタックID 1 のスイッチが メインスイッチ)					
2	SWX3200-52GT	Active	Member	S000000000	00a0.de00.0000
... (スタックID 2 のスイッチが メンバースイッチ)					

Interface	Status
port1.51	up
port1.52	up
port2.51	up
port2.52	up

メンバースイッチの初期設定状態を **backup system** コマンドを使用してSDカードにバックアップします。SDカード内の以下のフォルダに以下のファームウェアファイルを保存しておくことで、バックアップ実行時に設定とファームウェアの両方をバックアップすることができます。

- ・ SWX2310P-28GT : [フォルダ]/swx2310p/firmware、[ファームウェアファイル]swx2310p.bin
- ・ SWX3200-28GT, SWX3200-52GT : [フォルダ]/swx3200/firmware、[ファームウェアファイル]swx3200.bin

```
Yamaha> enable
Yamaha# backup system ①
Succeeded to backup system files and firmware file.
Yamaha# remote-login 2 ②

Entering character mode
Escape character is '^]'.

SWX3200-52GT Rev.4.00.XX
Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.

Yamaha-2> enable
Yamaha-2# backup system ③
Succeeded to backup system files and firmware file.
```

- ① メインスイッチの全設定を SDカードへコピー
- ② メンバースイッチ (スタックID: 2) にリモートログイン
- ③ メンバースイッチ (スタックID: 2) の全設定を SDカードへコピー

スタックの初期設定は、以上で終了となります。

利用ネットワークに仮想スイッチを組み込み、運用に必要な設定を行います。

運用に必要な設定を完了した後は、初期設定後と同じく、異常時に備え、バックアップを行うようにしてください。

メンバースイッチの交換

2台の SWX3200-52GT を使用した構成で、メンバースイッチに異常が発生した場合の交換手順を紹介します。

SDカードを使用する場合と使用しない場合のそれぞれについて、以下に示します。

SDカードを使用した交換手順

SDカードを使ったバックアップ/リストアによってメンバースイッチの交換を行います。

- ・ 交換手順
 1. 通常運用時

メンバースイッチへの設定完了後、障害発生を考慮して、SDカードへシステム情報をバックアップします。

システム情報のバックアップは **backup system** コマンドを実行して行います。

バックアップ実行前に、SDカード内の /swx3200/firmware フォルダに swx3200.bin(ファームウェアファイル) を保存しておきファームウェアのバックアップも行います。

2. 障害発生

スタックID: 2 のメンバースイッチで異常が発生したと仮定します。

3. 障害復旧

交換するメンバースイッチを用意し、障害が発生したスイッチのバックアップを保存したSDカードを接続します。

restore system コマンドを実行することでファームウェアとシステム情報を適用します。

適用後、**電源をOFFにして、動作中のメインスイッチと接続し、電源をONにする** ことで、スタック構成を復旧します。

SDカードを使用しない交換手順

SDカードを使わずにメンバースイッチの交換を行います。

1. 運用開始時

メンバースイッチの設置完了後、メンバースイッチに書き込まれているファームウェアと同じリビジョンのファームウェアをPCなどに保管します。

各メンバースイッチのシリアル番号、使用中のコンフィグID、スタックIDを記録します。

```
Yamaha> show environment
SWX3200-52GT BootROM Ver.1.00
SWX3200 Rev.4.00.05 (Fri Mar 9 09:34:05 2018)
main=SWX3200-52GT ver=00 serial=S000000000 MAC-Address=00a0.de00.0000 ①
CPU: 2%(5sec) 2%(1min) 1%(5min) Memory: 10% used
Fan status: Normal
Fan speed: FAN1=4000RPM FAN2=3870RPM FAN3=3870RPM FAN4=4000RPM
Startup firmware: exec0
Startup Configuration file: config1 ②
Serial Baudrate: 9600
Boot time: 2018/01/01 11:06:36 +09:00
Current time: 2018/01/02 16:12:23 +09:00
Elapsed time from boot: 1days 05:05:49
Temperature status: Normal
Temperature: 37 degree C
Voltage: 11.99V Current: 0.741A
Yamaha>
Yamaha> show stack
Stack: Enable
```

```
Configured ID      : 1 ③
Running ID         : 1
Status             : Active
Subnet on stack port : Auto-ip
Virtual MAC-Address : 00a0.de00.0000
```

ID	Model	Status	Role	Serial	MAC-Address
1	SWX3200-52GT	Active	Main	S000000000	00a0.de00.0000
2	SWX3200-52GT	Active	Member	S000000000	00a0.de00.0000

Interface	Status
port1.51	up
port1.52	up
port2.51	up
port2.52	up

① シリアル番号

② コンフィグID

③ スタックID

2. 障害発生

スタックID: 2 のメンバースイッチで異常が発生したと仮定します。

3. 障害復旧

交換するメンバースイッチを用意し、保管しておいたファームウェアを書き込みます。

メンバースイッチを起動させて、起動時に使用するコンフィグIDを変更します。

※運用開始時に使用していたコンフィグIDが 0 だった場合、コンフィグIDを変更する必要はありません。

```
Yamaha> enable
Yamaha# startup-config select 1
reboot system? (y/n): y
```

再起動後、スタック機能を有効にします。

設定するスタックIDは、運用開始時に記録したメンバースイッチのシリアル番号とスタックIDを参考にしてください。

```
Yamaha> enable
Yamaha# configure terminal
Yamaha(config)# stack 1 renumber 2 ①
Yamaha(config)# stack enable ②
reset configuration and reboot system? (y/n): y
```

① スタックID 2 を設定する

② スタック機能を有効にする

スタック機能を有効にした後、電源をOFFにして、動作中のメインスイッチと接続し、電源をONにすることで、スタック構成を復旧します。

ファームウェア更新

スタック構成時のファームウェア更新方法として、以下の二つの方法を提供します。

1. 構成中のメンバースイッチを同時に更新する方法 (パラレル更新)

2. ネットワークサービスの停止なしに更新する方法 (シーケンシャル更新)

パラレル更新は、サービス停止が発生してもよい時間を確保できる場合には、有効な方法です。

しかし、スタック構成中は、サービス停止を伴わないシーケンシャル更新をお勧めします。

なお、スタック構成中のファームウェア更新は、以下のみに対応します。

- ・ tftp クライアント、Web GUI を使用した更新ファームウェア送付による更新
- ・ SDカードを使用した更新

SDカードを挿入したままファームウェアの更新を行うと、再起動時にSDカードブートが行われる可能性があります。

boot prioritize sd コマンドでSDカードブートを無効化することができます。

```
Yamaha> enable
Yamaha# boot prioritize sd disable ①
reboot system? (y/n): y
```

① SDカードブートを無効にする

詳細は、[ファームウェア更新](#) を参照ください。

ファームウェアの平行更新

ファームウェアの平行更新は、スタック構成中のメンバースイッチのファームウェアを同時に更新します。

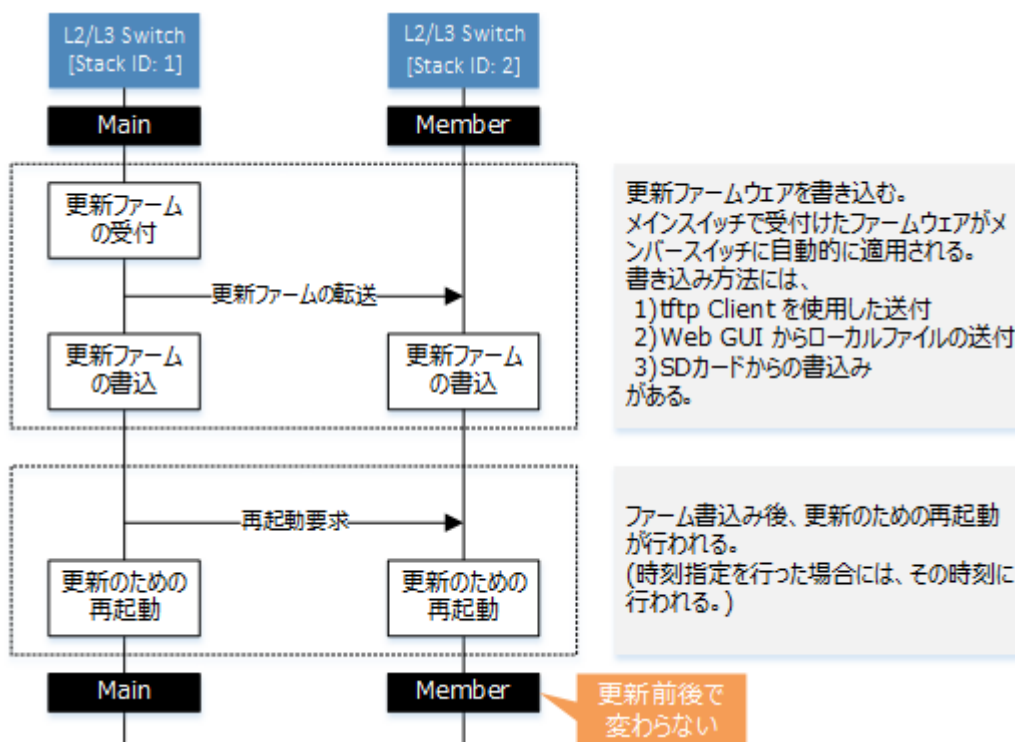
仮想スイッチ全体で更新のための再起動が発生するため、サービス停止が伴います。

平行更新を行う場合には、以下の点に注意をしてください。

- ・ ファームウェア更新方法の設定が **normal** になっていること (**firmware-update reload-method** コマンド)
- ・ ファームウェア更新適用時刻の設定が **設定した時刻** になっていること (**firmware-update reload-time** コマンド)

平行更新の概要について、以下に示します。

- ・ 平行更新処理フロー



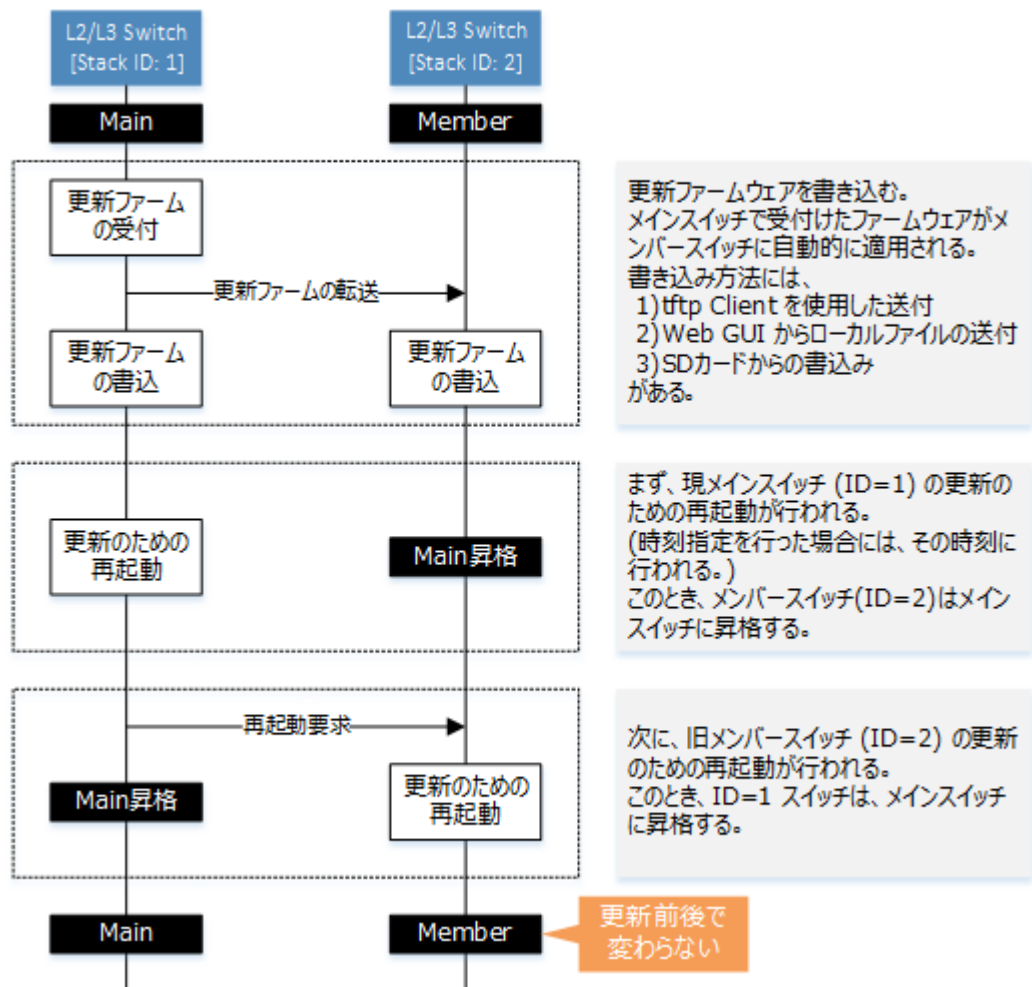
ファームウェアのシーケンシャル更新

ファームウェアのシリアル更新は、スタック構成中のメンバースイッチのファームウェアを順次更新します。仮想スイッチ全体で更新のための再起動が発生しないため、サービス停止を伴いません。（※[注意事項 6](#)参照）シーケンシャル更新を行う場合には、以下の点に注意してください。

- ・ファームウェア更新方法の設定が **sequential** になっていること (**firmware-update reload-method** コマンド)
- ・ファームウェア更新適用時刻の設定が **設定した時刻** になっていること (**firmware-update reload-time** コマンド)

シーケンシャル更新の概要について、以下に示します。

- ・シーケンシャル更新処理フロー



注意事項

1. スタック機能を有効にすると、以下の機能を使用することができません。
 - RMON
 - IPv6
 - VRRP
 - MLDスヌーピング
2. スタック機能有効時、機能としては利用できますが、一部制限が発生します。
 - ミラーリング機能

- メンバスイッチ間のミラーリングはできません。
 - フロー制御
 - Pauseフレームを送信することができません。
 - バックプレッシャー機能
 - スタックポートを経由する通信の場合、ジャム信号を送信しません。
 - ポートLED
 - SWX2310P-28GT のみ、Link/ActモードでLEDは点滅しません。
 - SFP 受光レベル監視
 - スタックポートの受光レベル監視は行いません。
 - リンクアグリゲーション
 - 最大論理インターフェース数が1つ減ります。
 - MODE ボタン
 - SWX2310P-28GT でスタックを構成した場合、MODE ボタンによる制御は **無効** です。SWX3200-28GT/52GT と同じく、ループ発生時 **STATUSモードに自動遷移します**。
 - コマンドライン入力
 - グローバルコンフィグレーションモードへ遷移できるユーザーが制限されます。コンソール側がグローバルコンフィグレーションモード時、telnet側でグローバルコンフィグレーションモードに遷移した場合は、コンソール側が自動的に特権EXECモードに遷移します。コンソール、telnet、ssh、リモートログイン、GUI設定が排他制御されます。
 - メインスイッチと他のメンバースイッチのコンソールから同時にログインすることはできません。
 - DHCPクライアント
 - スタック機能が有効かつスタックポートでAuto IP機能を使用している場合はDHCPクライアントは使用できません。
 - startup-config select コマンド
 - スタックを構成している状態で **startup-config select** コマンドを使用しないでください。正しく構成できなくなる可能性があります。startup-config select コマンドを使用しコンフィグを切り替えたい場合は、ダイレクトアタッチケーブルを抜去しスタック構成を解除してから実行してください。
3. スタック機能有効時、コマンドやGUIで各機能の設定をする際は、必ずスタック構成を組んでいる状態で行ってください。
スタックが正しく構成できていない状態で行った場合は、設定が正しく反映されない場合があります。
write コマンドと **copy running-config startup-config** コマンドは、メインスイッチ側(Active状態)のみ実行できます。
メンバースイッチ側、および、スタックが正しく構成できていない状態では実行できません。
4. スタック機能有効時、スタックの制御パケットが送信キュー#7, #6を使用しているため、その他のパケットを送信キュー#7, #6に割り当てないようにしてください。
Qos有効時、CoS-送信キューID変換テーブルの初期設定では送信キュー#7, #6に割り当てがあるため、割り当てを変更してください。
5. スタック機能有効時、スイッチ本体から送信されるフレームの送信キュー指定の初期設定が送信キュー#6になります。
スイッチ本体から送信されるフレームの送信キュー指定の設定を初期設定から変更しないでください。

-
6. スタック構成時にメインスイッチと他のメンバースイッチで設定(startup-config)に差異がある場合、メンバースイッチの設定を更新し再起動します。
 7. スタック構成時にメインスイッチと他のメンバースイッチでスタックポートのIPアドレス範囲設定に差異がある場合、スタック間の通信が正常に行えません。

関連文書

- ・ [ファームウェア更新](#)

初期設定一覧

SWX2310Pシリーズの初期設定について、以下に示します。

- ・ システム全体の初期設定

カテゴリ	設定項目	設定値
コンソール	コンソールタイムアウト	600 sec
	VTY数	8
	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	1時間に1回
SNMP	動作	無効
RMON	動作	有効
sFlow	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	firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swx2310p.bin
	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
スタック	動作	無効
	スタックID	1
	スタックポートで使うIPアドレス範囲	Auto IP

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
	TELNETサーバーアクセス	VLAN #1 のみ許可
	SSHサーバー状態	起動しない
	TFTPサーバー状態	起動しない
	HTTPサーバー状態	起動する
	HTTPサーバーアクセス	VLAN #1 のみ許可
	セキュアHTTPサーバー状態	起動しない
保守VLAN	VLANインターフェース	VLAN #1
インターフェース制御	リンクアグリゲーション	なし
	ポート認証	無効
	ポートセキュリティ	無効
	PoE給電	有効
Layer2機能	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
	スパニングツリー	有効
	独自ループ検出	無効
	マルチプルVLAN	なし
Layer3機能	スタティックルーティング	なし
	VLAN間でのルーティング	無効
	ポリシーベースルーティング	-
	OSPF	-
	RIP	-
	VRRP	-
IPマルチキャスト	IGMP snooping	無効
	MLD snooping	無効
	IGMP	-
	PIM	-
DNSクライアント	動作	有効

カテゴリ	設定項目	設定値
トラフィック制御	QoS	無効
	QoS(DSCP-送信キューID変換テーブル)	なし
	フロー制御 (IEEE 802.3x)	無効
	ACL	なし
AP層機能	DHCPサーバー	-
	DHCPv6サーバー	-
	DHCPリレー	-
	DNSリレー	-
	RADIUSサーバー	無効
WebGUI	言語設定	日本語

・ LAN/SFPポート単位の初期設定

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
	MRU	1,522 Byte
	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
L2スイッチング	スパニングツリー	有効
	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	送信および受信
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

カテゴリ	設定項目	設定値
Layer3機能	IPv4アドレス	192.168.100.240/24
IPマルチキャスト	マルチキャストフレームの転送	239.192.128.250 (Y-UNOS用)
	IGMP Snooping	動作
		無効
		Querier
		無効
		Fast-Leave
		無効
		Check TTL
		有効
		Check RA
		無効
		Check ToS
		無効
		Report-Suppression
		有効
		Report-Foward
		無効
		Mrouter-Port Data-Suppression
		無効
	MLD Snooping	動作
		無効
		Querier
		無効
		Fast-Leave
		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

コンボポート

LANポート、SFPポートの2種類を選択できるポートです。

LANポートとSFPポートは同時に使用できません。両方のポートが接続された場合、SFPポートが優先して使用されます。

LANポートのみに有効な設定がある場合、SFPポートには適用されません。

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。 固定のLANポートと取り外し可能なSFP/SFP+ポートの3種類があります。 本インターフェースは、 port に続けて"スタックID" + "." + "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: port1.1
コンボポート		
SFP+ポート		
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、 vlan に続けて "VLAN ID" で表現します。 VLAN1の指定: vlan1
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/SFP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、 sa または po に続けて "論理リンクID" で表現します。 論理リンクID #1のLACP論理インターフェースの指定: po1
LACP論理インターフェース	po	

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。

- ・ 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	descripti on	インターフェースに対して説明文を設定します。
有効化 / 無効化	shutdow n	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	speed- duplex	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。) ・オートネゴシエーション ・10Gbps / 全二重 ・1Gbps / 全二重 ・100Mbps / 全二重 ・100Mbps / 半二重 ・10Mbps / 全二重 ・10Mbps / 半二重
MRU	mru	インターフェースで受信可能な最大フレームサイズを 64～10,240 Byte の範囲で設定します。
クロス/ストレート自動判別 (Auto MDI/MDI-X機能)	mdix	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	eee	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。

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	MR U	クロス/ストレート 自動判別	EEE
LANポート	○	○	○(*1)	○	○	○
コンボポート	○	○	○(*2)	○	○(*3)	○ (*3)
SFP+ポート	○	○	○(*4)	○	×	×
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	○	○	×	×	×	×
LACP論理インターフェース	○	○	×	×	×	×

- 1 : LANポートに対する通信速度/通信モードの設定は、*10Gbps / 全二重 を選択できません。
- 2 : コンボポートに対する通信速度/通信モードの設定は、*オートネゴシエーション か 1Gbps / 全二重 のいずれかになります。
- 3 : コンボポートに対する設定は、LANポート側にのみ適用されます。
- *4 : SFP+ポートに対する通信速度/通信モードの設定は、*オートネゴシエーション か 10Gbps / 全二重 のいずれかになります。
- 10Gbps / 全二重 を設定しSFPモジュールを接続した場合には 1Gbps / 全二重 として動作します。

LAN/SFPポートの初期状態

本製品のLAN/SFP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/SFP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/SFPポートが所属するデフォルトVLAN(VLAN #1)に対して、以下の機能が有効になっています。
 - MSTP : Multiple Spanning Tree Protocol
 - IGMP Snooping
 - IPv4アドレス (192.168.100.240/24)
 - Telnetクライアントからのアクセス
 - Webクライアントからのアクセス

ポートミラーリング

本製品は、任意のLAN/SFP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、スニファースポーツは1つまで設定が可能です。

また、監視ポートに対しては、監視方向（送受信・送信のみ・受信のみ）を選択することが可能です。

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、ポートミラーリング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/SFP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
Octets	受信オクテット数	18,446,744,073,709,551,615
Packets (*1)	受信パケット数	34,359,738,360
Broadcast packets (*2)	ブロードキャストパケット受信数	4,294,967,295

表示項目	説 明	最大値
Multicast packets (*2)	マルチキャストパケット受信数	4,294,967,295
Unicast packets (*2)	ユニキャストパケット受信数	4,294,967,295
Undersize packets (*2)	アンダーサイズパケット受信数 (64オクテット未満のパケット)	4,294,967,295
Oversize packets (*2)	オーバーサイズパケット受信数 (1,523オクテット以上のパケット (*3))	4,294,967,295
Fragments (*2)	フラグメントパケット受信数 (64オクテット未満でCRCが異常であるパケット)	4,294,967,295
Jabbers (*2)	ジャバーパケット受信数 (1,523オクテット以上でCRCが異常であるパケット (*3))	4,294,967,295
FCS errors (*2)	FCSエラーパケット受信数	4,294,967,295
RX errors	受信エラー数	4,294,967,295
Drop packets (*4)	受信バッファ溢れしたパケット数	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) : LAN/SFPポートに設定した *MRU に依存し、変動します。

(*4) : テールドロップが無効な場合のみ表示されます。

・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
Octets	送信オクテット数	18,446,744,073,709,551,615
Packets (*1)	送信パケット数	12,884,901,885
Broadcast packets (*2)	ブロードキャストパケット送信数	4,294,967,295
Multicast packets (*2)	マルチキャストパケット送信数	4,294,967,295
Unicast packets (*2)	ユニキャストパケット受信数	4,294,967,295
TX errors	送信エラー数	4,294,967,295
Collisions	コリジョン発生回数	4,294,967,295
Drop Packets(*3)	テールドロップした送信パケット数	536,870,911

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

(*3) : テールドロップが有効な場合のみ表示されます。

・送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
64 octet packets	64オクテット長のパケット送受信数	4,294,967,295

表示項目	説 明	最大値
65 ～ 127 octet packets	65～127オクテット長のパケット送受信数	4,294,967,295
128 ～ 255 octet packets	128～255オクテット長のパケット送受信数	4,294,967,295
256 ～ 511 octet packets	256～511オクテット長のパケット送受信数	4,294,967,295
512 ～ 1,023 octet packets	512～1,023オクテット長のパケット送受信数	4,294,967,295
1,024 ～ MAX octet packets	1,024～最大オクテット長 (*1) のパケット送受信数	4,294,967,295

(*1) : LAN/SFPポートに設定した **MRU** に依存し、変動します。

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

また、LAN/SFPポートの状態を表示する **show interface** コマンドを実行すると、送受信フレーム数の情報が表示されますが、

本情報は、フレームカウンタの情報をもとに表示しています。

以下に、 **show interface** コマンドで表示する送受信フレーム数とフレームカウンタの対応について示します。

- **show interface** コマンドで表示する送受信フレーム数とフレームカウンタの対応

表示項目		参照するフレームカウンタ情報
input	packets	受信フレームカウンタ の Packets
	bytes	受信フレームカウンタ の Octets
	multicast packets	受信フレームカウンタ の Multicast packets
	drop packets(*1)	受信フレームカウンタ の Drop packets
output	packets	送信フレームカウンタ の Packets
	bytes	送信フレームカウンタ の Octets
	multicast packets	送信フレームカウンタ の Multicast packets
	broadcast packets	送信フレームカウンタ の Broadcast packets
	drop packets(*1)	送信フレームカウンタ の Drop packets

(*1) : テールドロップが有効な場合に送信の情報、無効な場合には受信の情報のみ表示されます。

SFPモジュールの受光レベル監視

本製品は、SFP/SFP+ポートに接続されたSFP/SFP+モジュールの受光レベル監視機能を提供します。SFP/SFP+モジュールの受光レベル異常が発生した場合、本製品のポートランプ表示を専用の状態に変更し、SYSLOGメッセージを出力します。

受光レベル異常状態はMODEスイッチの3秒間長押しにより、強制的に解消することができます。

受光レベルが正常範囲に戻った場合、本製品のポートランプ表示を復旧し、SYSLOGメッセージを出力します。

該当ポートがリンクダウンした場合や受光レベル異常状態が強制的に解消された場合にはSYSLOGメッセージを出力しません。

SFP/SFP+モジュールの受光レベル監視設定は、 **sfp-monitor** コマンドで行うことができます。

初期設定では、SFPモジュールの受光レベル監視の設定は有効となっています。

送信キューの使用率監視

送信キューの使用率が高く(60%以上、100%以上)なった場合、SYSLOGメッセージを出力します。
送信キューの使用率が正常範囲(50%以下)に戻った場合も、SYSLOGメッセージを出力します。
送信キューの使用率監視設定は、**tx-queue-monitor** コマンドで行うことができます(システム全体・LAN/SFPポート単位)。
初期設定では、送信キューの使用率監視の設定は全て有効となっています。

ifIndexの割り当て

ifIndexはインターフェイスに紐づく識別番号です。SNMPやDHCPなどで使用されます。
以下の表に従って割り当てられます。

ifIndexの範囲	インターフェイスの割り当て	付与ルール	例
301 - 4394	VLANインターフェイス	ifIndex = 300 + VLAN ID	301: vlan1 4394: vlan4094
4501 - 4596	スタティック論理インターフェイス	ifIndex = 4500 + スタティック論理インターフェイス番号	4501: sa1 4596: sa96
4601 - 4727	LACP論理インターフェイス	ifIndex = 4600 + LACP論理インターフェイス番号	4601: po1 4727: po127
5001 - 6050	LAN/SFPポート	ifIndex = 4000 + 1000 × スタックID + ポート番号	5001: port1.1 6001: port2.1 6050: port2.50

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。

- ・ インターフェイス基本機能 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
MRU設定	mru
クロス/ストレート自動判別設定	mdix auto
EEE設定	eee
EEE対応可否を表示する	show eee capabilities
EEEステータス情報を表示する	show eee status

操作項目	操作コマンド
ポートミラーリングの設定	mirror
ポートミラーリングの状態表示	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
SFP/SFP+の状態表示	show ddm status
SFPモジュールの受光レベル監視の設定	sfp-monitor rx-power
送信キューの使用率監視の設定(システム)	tx-queue-monitor usage-rate
送信キューの使用率監視の設定(LAN/SFPポート)	tx-queue-monitor usage-rate
送信キューの使用率監視の設定表示	show tx-queue-monitor
インターフェースのリセット	interface reset

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 rtx1200-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
```

ポートミラーリング設定

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。

- ・ スニファースポート: LANポート#1 (port1.1)
- ・ 監視ポート: LANポート#4 (port1.4)、LANポート#5 (port1.5)
 1. スニファースポートであるLANポート#1 (port1.1) に対して、監視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. ポートミラーリング設定を確認します。

```
Yamaha#show mirror
Sniffer Port    Monitored Port  Direction
=====
port1.1        port1.4         both
port1.1        port1.5         transmit
```

LAN/SFP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
  Description: Connected to router
  ifIndex 5001, MRU 1522
  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      : 0
           bytes        : 0
           multicast packets: 0
    output packets      : 0
           bytes        : 0
           multicast packets: 0
           broadcast packets: 0
```

drop packets : 0

注意事項

特になし

関連文書

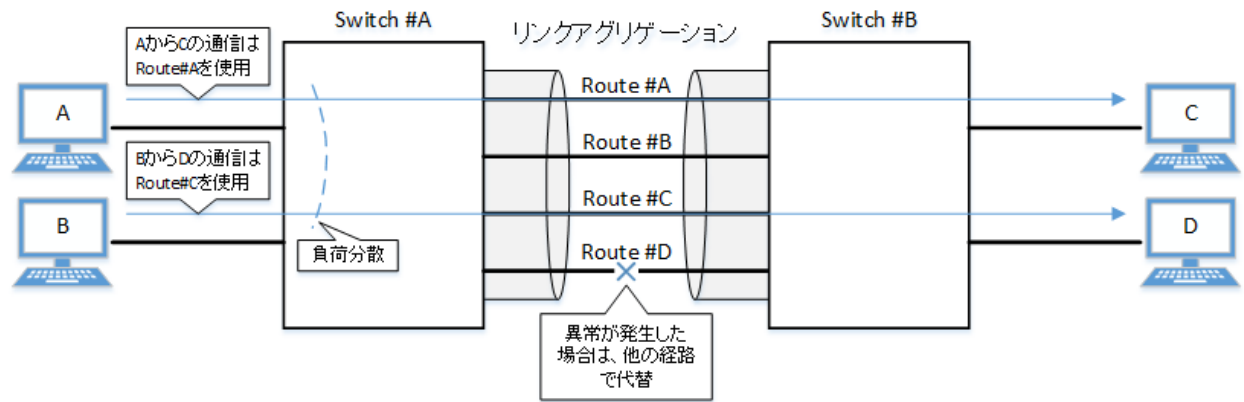
特になし

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/SFP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/SFP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



本スイッチ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/SFPポートを手動で設定するリンクアグリゲーション。LAN/SFP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。
LACPリンクアグリゲーション	LAN/SFPポートを束ねるのに LACP を利用するリンクアグリゲーション。接続機器間でLACPによるネゴシエーションが成功すると、論理インターフェースとして動き始めます。

用語の定義

LACP

Link Aggregation Control Protocol の略。IEEE802.1AX-2008 で標準化されている技術。
EtherChannel とも言われることがある。

・ [IEEE802.1AX-2008 Link Aggregation Task Force](#)

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/SFP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。

スタティック/LACP リンクアグリゲーション 共通仕様

本スイッチのスタティック/LACP リンクアグリゲーションの共通仕様について、以下に示します。

1. 本スイッチのリンクアグリゲーションは、スタティック/LACPの両方を合わせて、**127インターフェース** 定義することができます (ただし、スタック時には126インターフェースとなります)。
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/SFPポート** を所属させることができます。
2. 収容するLAN/SFP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
 - QoSのトラストモード (ポート優先度、デフォルトCos設定含む)
 - ループ検出 (ループ検出の有効/無効、ポートブロッキングの有効/無効)
3. LAN/SFPポートを論理インターフェースに所属させると、以下の処理を行います。
 - リンクアップしているLAN/SFPポートは、**リンクダウン** します。
安全に論理インターフェースをシステムに組み込むため、論理インターフェースの初期値は **シャットダウン** 状態となっています。
 - MSTP設定は破棄されデフォルト設定に戻ります。
LAN/SFPポートを論理リンクから脱退させた場合も、該当ポートのMSTP設定はデフォルト設定に戻ります。
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)
5. 動作中の論理インターフェースに対して、新たにLAN/SFPポートを所属させることはできません。
LAN/SFPポートを所属させる場合は、必ず論理インターフェースを **シャットダウン** してから行うようにしてください。
6. 動作中の論理インターフェースから、所属しているLAN/SFPポートを脱退させることはできません。
所属しているLAN/SFPポートを脱退させる場合も、必ず論理インターフェースを **シャットダウン** してから行うようにしてください。
論理インターフェースから脱退させたLAN/SFPポートは、**シャットダウン** 状態となります。必要に応じて、**有効化(no shutdown)** してください。
7. 論理インターフェースには**ロードバランス**の設定ができます。そのためのルールを以下の中から設定できます。
論理インターフェースを定義した際の初期値は、**宛先/送信元MACアドレス** となっています。
 - 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

スタティック リンクアグリゲーション

スタティック リンクアグリゲーションの動作仕様について、以下に示します。

1. スタティック論理インターフェースのインターフェース番号は、**1 ～ 96** の範囲で付与することができます。
2. LAN/SFPポートをスタティック論理リンク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/SFP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/SFP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。
3. 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。

LACP リンクアグリゲーション

LACP リンクアグリゲーションの動作仕様について、以下に示します。

スタティックリンクアグリゲーションとの共通仕様については、**3.1 スタティック/LACPリンクアグリゲーション 共通仕様** を参照願います。

1. LACP論理インターフェースのインターフェース番号は、**1 ～ 127** の範囲で付与することができます。
2. LAN/SFPポートをLACP論理リンクインターフェースに所属させるには、**channel-group** コマンドで行います。
 - LAN/SFPを所属させる際、以下の **動作モード** を指定します。(アクティブモードの指定を推奨します)
 - **アクティブモード**
LACPフレームを自発的に送信し、対向機器のポートとネゴシエーションを開始します。
 - **パッシブモード**
LACPフレームを自発的に送信しないで、対向機器からのフレームを受信した場合に送信します。
 - LACP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/SFP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。
 - LACP論理インターフェースからLAN/SFP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。
3. LACP論理インターフェースの動作に影響を与えるパラメータについて、以下に示します。
 - **LACP タイムアウト**
LACP タイムアウトは、対向機器からのLACP フレームを受信できなかった場合にダウンしたと判断するための時間です。
lacp timeout コマンドで、**Long (90秒)** または **Short (3秒)** のどちらかを指定します。
LACP タイムアウト値は、LACP フレームに格納されて対向機器に送信されます。
フレームを受信した対向機器は、格納されたLACPタイムアウトの **1/3の間隔** でLACPフレームを送信するようになります。
なお、論理インターフェース生成時の初期値は、**Long (90秒)** となります。
 - **LACP システム優先度**
LACP システム優先度は、対向機器との間で **論理インターフェースの制御をどちらの機器で行うのか** を決める際に使用します。対向機器との間で **LACP システム優先度** と **MACアドレス** (この組み合わせを **システムID** と呼びます) を交換し、LACP システム優先度の高い機器が制御権を持ちます。LACP システム優先度が同じ場合はMACアドレスの小さい機器が制御権を持ちます。

制御権を持つ機器は、論理インターフェースに所属するどのLAN/SFPポートを有効(Active)にするのかを決定します。

LACP システム優先度は、**lacp system-priority** コマンドで **1 ~ 65,535** の範囲で指定することができ、小さいほど優先度が高くなります。なお、論理インターフェース生成時の初期値は **32,768 (0x8000)** が設定されます。

◦ **LACP ポート優先度**

LACP ポート優先度は、**論理インターフェースに所属する LAN/SFPポート のアクティブ/スタンバイの制御** に使用します。論理インターフェースに所属するLAN/SFPポートが最大数 (8ポート) より多い場合に **LACP ポート優先度** に基づいてポートの状態を制御します。

LACP ポート優先度 が同じ場合は **ポート番号** の小さいポートを優先します。なお、スタック構成時には **スタックID** の小さいスイッチのポートをポート番号に関係なく優先します。例えば、port2.1 よりも port1.10 を優先します。

LACP ポート優先度は、**lacp port-priority** コマンドで、**1~65535** の範囲で指定することができます。値が小さいほど優先度が高くなります。なお、LACP ポート優先度の初期値は **32,768 (0x8000)** が設定されます。

4. 通信モードが半二重のLAN/SFPポートはLACPリンクアグリゲーションに対応していません。

- LACP論理インターフェースに所属している半二重のLAN/SFPポートをアクティブにすることはありません。

5. 通信速度の異なるLAN/SFPポートが同一論理インターフェースに所属している場合の動作について、以下に示します。

通信速度を混在してリンクアグリゲーションを構成したい場合は、異速度リンクアグリゲーションを有効にしてください。

- 異速度リンクアグリゲーションが有効(**lacp multi-speed enable**)の場合の動作

- 最大数 (8ポート) までのすべての所属ポートを通信速度に関わらずアクティブにします。
- ロードバランスはすべての所属ポートを同等に扱います。
 - 低速な所属ポートでは通信がオーバーフローする可能性が高くなります。
 - 所属しているLAN/SFPポートが最大数 (8ポート) より多い場合、より高速な所属ポートに高いポート優先度を設定してください。
- 対向機器が異なる通信速度を受け入れない場合、自機器と対向機器とで所属ポートの一覧を相互に交換し、双方が使用可能な所属ポートをアクティブとします。そのため異なる通信速度を受け入れない機器側の条件に制限されます。

- 異速度リンクアグリゲーションが無効(**lacp multi-speed disable**)の場合の動作

- 所属ポート内で最初にリンクアップしたポートと同じ通信速度のポートのみをアクティブにします。
 - 通信速度が異なる他のポートはスタンバイのままとします。
 - オートネゴシエーションに設定されている場合、所属ポート内で最初にネゴシエーションした結果と同じ通信速度のポートのみをアクティブにします。
- 最初にリンクアップしたポート群が全てリンクダウンしたとき、LACP論理インターフェースもリンクダウンします。

6. LACP論理インターフェースの状態は、**show etherchannel** コマンドで確認できます。

- 所属ポートのアクティブ状態は、**show etherchannel status detail** コマンドで確認できます。

7. スタック構成時においてもLACPリンクアグリゲーションを使用できます。ただし、以下の制限があります。

- 定義可能な論理インターフェース数が、スタティック/LACP の両方をあわせて **126** になります。

関連コマンド

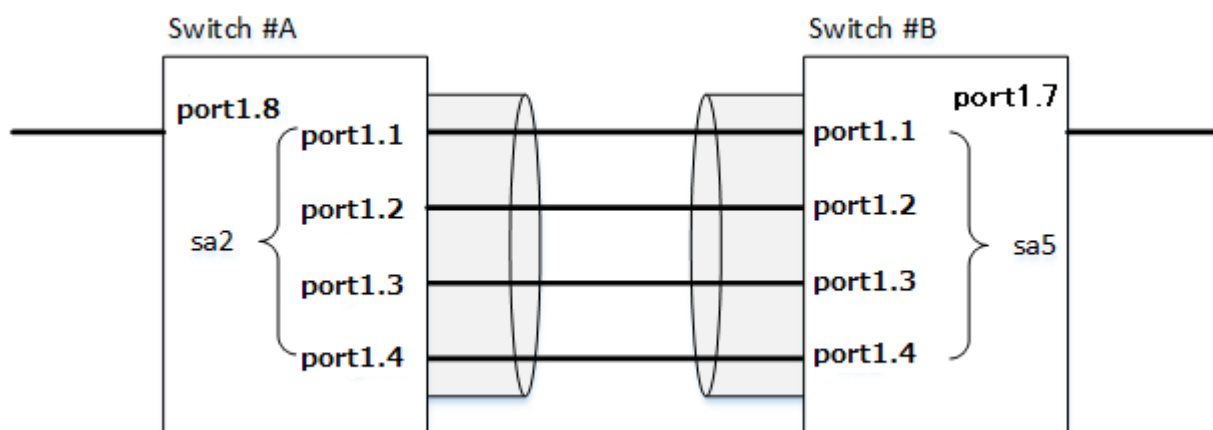
関連コマンドについて、以下に示します。
コマンドの詳細は、コマンドリファレンスを参照願います。

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
LACP論理インターフェースの設定	channel-group
LACP システム優先度の設定	lacp system-priority
LACP システム優先度の表示	show lacp sys-id
LACP 異速度リンクアグリゲーションの設定	lacp multi-speed
LACP タイムアウトの設定	lacp timeout
LACP パケットカウンタのクリア	clear lacp
LACP パケットカウンタの表示	show lacp counters
LACP論理インターフェースの状態表示	show etherchannel
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

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。
 1. [スイッチA] VLAN #1000 を定義し、LANポート(#1, #2, #3, #4, #8)を所属させます。
あわせて、LANポート(#1, #2, #3, #4)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 port1.8 ②
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#interface port1.1 ④
Yamaha(config-if)#switchport access vlan 1000 ⑤
Yamaha(config-if)#static-channel-group 2 ⑥
Yamaha(config-if)#interface port1.2
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
Yamaha(config-if)#interface port1.3
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 2
Yamaha(config-if)#interface port1.4
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 #8 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 #1 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:
  port1.1
  port1.2
  port1.3
  port1.4

```

3. [スイッチB] VLAN #1000 を定義し、LANポート(#1, #2, #3, #4, #7)を所属させます。
あわせて、LANポート(#1, #2, #3, #4)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 port1.1
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.2
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5
Yamaha(config-if)#interface port1.3
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)#static-channel-group 5

```



```
Yamaha(config-if)#interface port1.4
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:
  port1.1
  port1.2
  port1.3
  port1.4
```

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 ①
  Hardware is AGGREGATE
  ifIndex 4502, MRU 1522
  Vlan info :
    Switchport mode      : access
    Ingress filter       : enable
    Acceptable frame types : all
    Default Vlan         : 1000
    Configured Vlans      : 1000
  Interface counter:
    input  packets      : 1020
           bytes        : 102432
           multicast packets: 1020
    output packets      : 15
           bytes        : 1845
           multicast packets: 15
```



```
broadcast packets: 0
```

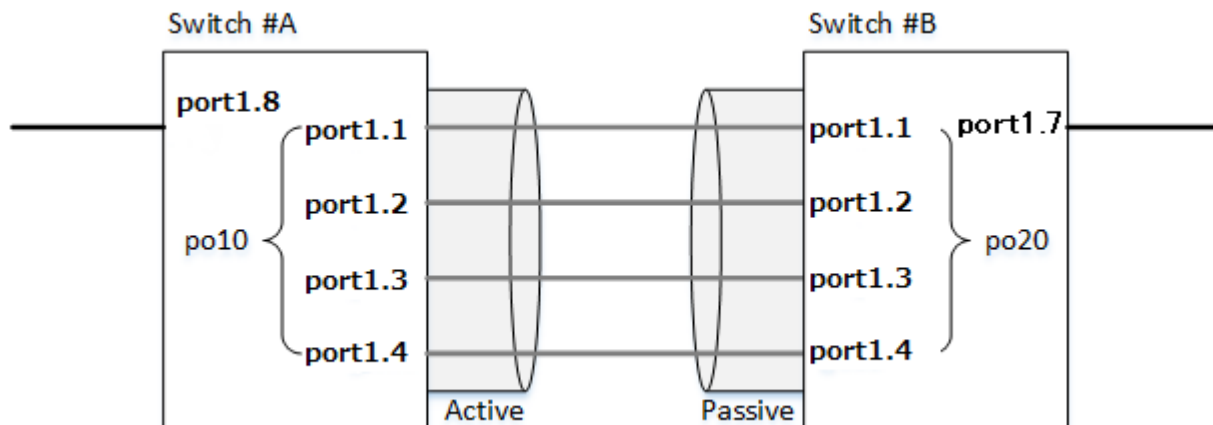
① 有効化されていること

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
  ifIndex 4505, MRU 1522
  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
           multicast packets: 24
    output packets      : 2109
           bytes        : 211698
           multicast packets: 2109
           broadcast packets: 0
```

LACP 論理インターフェースの設定

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には **LACP** を使用します。
論理インターフェース番号は、スイッチA: #10、スイッチB: #20 とします。
スイッチAの論理インターフェースを **アクティブ状態** に、スイッチBの論理インターフェースを **パッシブ状態** にします。
 - ・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。
 - ・**ロードバランス**は、宛先/送信元IPアドレスを設定します。
1. [スイッチA] VLAN #1000 を定義し、LANポート(#1, #2, #3, #4, #8)を所属させます。
あわせて、LANポート(#1, #2, #3, #4)を **アクティブ状態** で **論理インターフェース #10** に所属

させます。

この時点で論理インターフェースは、**シャットダウン** 状態となっています。

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.8
Yamaha(config-if)#switchport access vlan 1000 ②
Yamaha(config-if)#interface port1.1
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#channel-group 10 mode active ④
Yamaha(config-if)#interface port1.2
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 10 mode active
Yamaha(config-if)#interface port1.3
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 10 mode active
Yamaha(config-if)#interface port1.4
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 10 mode active
```

① VLAN #1000 の定義

② アクセスポートに設定し、VLAN #1000 に所属させる

③ アクセスポートに設定し、VLAN #1000 に所属させる

④ 論理インターフェース #10 に アクティブ状態 で所属させる

2. [スイッチA] 論理インターフェース #10 の設定状態を確認します。

```
Yamaha#show etherchannel
% LACP Aggregator: po10
% Member:
  port1.1
  port1.2
  port1.3
  port1.4
Yamaha#show lacp sys-id ①
% System 8000,00-a0-de-ae-b9-1f
Yamaha#show interface po10
Interface po10
  Link is DOWN ②
  Hardware is AGGREGATE
  ifIndex 4610, MRU 1522
  Vlan info :
    Switchport mode      : access
    Ingress filter       : enable
    Acceptable frame types : all
    Default Vlan         : 1000
    Configured Vlans     : 1000
  Interface counter:
    input  packets      : 0
           bytes        : 0
           multicast packets: 0
    output packets      : 0
```

```
bytes          : 0
multicast packets: 0
broadcast packets: 0
```

① LACP システムID の確認: デフォルト値の設定(0x8000)になっている

② リンクダウン状態になっている

3. [スイッチB] VLAN #1000 を定義し、LANポート(#1, #2, #3, #4, #7)を所属させます。
あわせて、LANポート(#1, #2, #3, #4)を **パッシブ状態** で **論理インターフェース #20** に所属させます。
この時点で論理インターフェースは、**シャットダウン** 状態となっています。

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 1000 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface port1.7
Yamaha(config-if)#switchport access vlan 1000 ②
Yamaha(config-if)#interface port1.1
Yamaha(config-if)#switchport access vlan 1000 ③
Yamaha(config-if)#channel-group 20 mode passive ④
Yamaha(config-if)#interface port1.2
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 20 mode passive
Yamaha(config-if)#interface port1.3
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 20 mode passive
Yamaha(config-if)#interface port1.4
Yamaha(config-if)#switchport access vlan 1000
Yamaha(config-if)# channel-group 20 mode passive
```

① VLAN #1000 の定義

② アクセスポートに設定し、VLAN #1000 に所属させる

③ アクセスポートに設定し、VLAN #1000 に所属させる

④ 論理インターフェース #20 に パッシブ状態 で所属させる

4. [スイッチB] 論理インターフェース #20 の設定状態を確認します。

```
Yamaha#show etherchannel
% LACP Aggregator: po20
% Member:
  port1.1
  port1.2
  port1.3
  port1.4
Yamaha#show lacp sys-id ①
% System 8000,00-a0-de-ae-b8-7e
Yamaha#show interface po20
Interface po20
  Link is DOWN ②
  Hardware is AGGREGATE
  ifIndex 4620, MRU 1522
  Vlan info :
```

```

Switchport mode      : access
Ingress filter       : enable
Acceptable frame types : all
Default Vlan         : 1000
Configured Vlans      : 1000
Interface counter:
  input  packets      : 0
         bytes        : 0
         multicast packets: 0
  output packets      : 0
         bytes        : 0
         multicast packets: 0
         broadcast packets: 0

```

① LACP システムID の確認: デフォルト値の設定(0x8000)になっている

② リンクダウン状態

5. [スイッチA] のロードバランスを宛先/送信元IPアドレスに設定し、有効化します。

```

Yamaha(config)#port-channel load-balance src-dst-ip ①
Yamaha(config)#interface po10 ②
Yamaha(config-if)#no shutdown ③

```

① ロードバランスを設定

② 論理インターフェース #10 の設定

③ 論理インターフェースの有効化

6. [スイッチB] のロードバランスを宛先/送信元IPアドレスに設定し、有効化します。

```

Yamaha(config)#port-channel load-balance src-dst-ip ①
Yamaha(config)#interface po20 ②
Yamaha(config-if)#no shutdown ③

```

① ロードバランスを設定

② 論理インターフェース #20 の設定

③ 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。

リンクアップし、フレームの送受信が開始されていることを確認します。

```

Yamaha#show interface po10
Interface po10
  Link is UP
  Hardware is AGGREGATE
  ifIndex 4610, MRU 1522
  Vlan info :
    Switchport mode      : access
    Ingress filter       : enable
    Acceptable frame types : all
    Default Vlan         : 1000
    Configured Vlans      : 1000

```

```

Interface counter:
  input  packets      : 560
         bytes        : 58239
         multicast packets: 560
  output packets      : 98
         bytes        : 12474
         multicast packets: 98
         broadcast packets: 0

Yamaha#
Yamaha#show lacp-counter
% Traffic statistics
Port      LACPDUs      Marker      Pckt err
          Sent   Recv   Sent   Recv   Sent   Recv
% Aggregator po10 , ID 4610
port1.1    50     47     0      0      0      0
port1.2    49     46     0      0      0      0
port1.3    49     46     0      0      0      0
port1.4    49     46     0      0      0      0

```

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。
 リンクアップし、フレームの送受信が開始されていることを確認します。

```

Yamaha#show interface po20
Interface po20
  Link is UP
  Hardware is AGGREGATE
  ifIndex 4620, MRU 1522
  Vlan info :
    Switchport mode      : access
    Ingress filter       : enable
    Acceptable frame types : all
    Default Vlan         : 1000
    Configured Vlans      : 1000
  Interface counter:
    input  packets      : 78
           bytes        : 9914
           multicast packets: 78
    output packets      : 438
           bytes        : 45604
           multicast packets: 438
           broadcast packets: 0

Yamaha#
Yamaha#show lacp-counter
% Traffic statistics
Port      LACPDUs      Marker      Pckt err
          Sent   Recv   Sent   Recv   Sent   Recv
% Aggregator po20 , ID 4620
port1.1    55     57     0      0      0      0
port1.2    54     56     0      0      0      0
port1.3    54     56     0      0      0      0
port1.4    54     56     0      0      0      0

```

注意事項

- ・ プライベートVLANに属しているホストポートは、リンクアグリゲーション論理インターフェースとして束ねることができません。
- ・ LAN/SFPポートの受信フレームに対するアクセスリスト設定がある場合、リンクアグリゲーション論理インターフェースとして束ねることができません。

関連文書

- ・ [LAN/SFPポート制御：インターフェース基本設定](#)

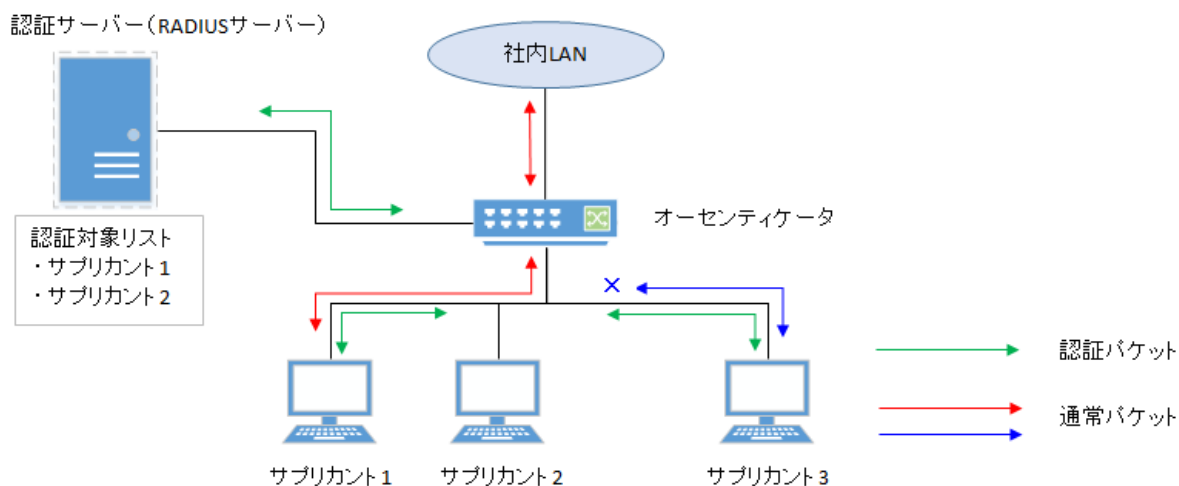
ポート認証機能

機能概要

ポート認証機能は機器またはユーザーを認証する機能です。

LAN/SFPポートに接続された機器を認証し、認証に成功した機器のみLANへのアクセスを許可することができます。

また、未認証の機器や認証に失敗した機器は、LANへのアクセスを拒否したり、特定のVLANへのアクセスのみ許可することができます。



用語の定義

IEEE 802.1X

LAN接続時に使用する認証規格。

オーセンティケータ

LAN/SFPポートに接続されたサブリカントを認証する機器またはソフトウェア。

サブリカントと認証サーバーの間を中継し、認証の成否によりLANへのアクセスを制御します。

サブリカント

オーセンティケータに接続して認証を受ける機器またはソフトウェア。

認証サーバー

オーセンティケータを介して、接続されたサブリカントを認証する機器またはソフトウェア。

ユーザー名、パスワード、MACアドレス、所属VLAN等の認証情報を管理します。

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で規定されます。

EAP over LAN (EAPOL)

EAPパケットをサブリカントとオーセンティケータ間で伝送するためのプロトコル。

EAP over Radius

EAPパケットをオーセンティケーターと認証サーバー(RADIUSサーバー)間で伝送するためのプロトコル。

EAP-MD5 (Message digest algorithm 5)

ユーザー名とパスワードによるクライアント認証。
MD5ハッシュ値を使用して認証します。

EAP-TLS (Transport Layer Security)

サーバーとクライアントの電子証明書による相互認証。
トランスポート層を暗号化して電子証明書を交換して認証します。
RFC2716、RFC5216で規定されます。

EAP-TTLS (Tunneled TLS)

EAP-TLSの拡張版。
サーバーの電子証明書を用いてTLS通信路を構築し、その暗号化された通信路内でパスワードによりクライアントを認証します。
RFC5281で規定されます。

EAP-PEAP (Protected EAP)

動作原理はEAP-TTLSと同等(暗号トンネル内のプロトコルの違いのみ)。
サーバーの電子証明書を用いてTLS通信路を構築し、その暗号化された通信路内でパスワードによりクライアントを認証します。

機能詳細

ポート認証機能の動作仕様について以下に示します。
本製品は、ポート認証機能としてIEEE 802.1X認証方式、MAC認証方式、およびWeb認証方式をサポートします。
各認証方式には、以下の表に示す特徴があります。

	MAC認証	IEEE 802.1X認証	Web認証
認証要素	MACアドレス	ユーザー名とパスワード (EAP-MD5,EAP-TTLS,EAP-PEAP)	ユーザー名とパスワード
認証対象(サブリカント)	機器	機器またはユーザー	機器またはユーザー
サブリカントに必要な機能	なし	IEEE 802.1X認証機能	Web ブラウザ
認証時の操作	なし	ユーザー名とパスワード入力 (EAP-MD5,EAP-TTLS,EAP-PEAP)	ユーザー名とパスワード入力

本製品は、認証サーバーとしてRADIUSサーバーを想定します。

また、本製品のポート認証機能には以下の制限がありますので、ご注意ください。

- ・ 認証可能なサブリカント数は、シングルホストモード/マルチホストモードは各ポートで1つ、マルチサブリカントモードはシステム全体で **512** までとなります。
- ・ プライベートVLANポート上で使用することはできません。

- ・ボイスVLANポート上で使用することはできません。
- ・ポート認証機能が有効な場合、認証結果に応じてスパンニングツリーのトポロジチェンジが発生します。
これを回避したい場合、サブリカントを接続する認証ポートでspanning-tree edgeportを設定してください。
- ・Web認証はマルチサブリカントモードでのみ利用できます。
- ・Web認証はゲストVLANと併用できません。
- ・スタック機能を利用しているとき、Web認証画面カスタマイズ用ファイルは、メインスイッチに保存されているファイルが参照されます。
- ・スタック機能を利用しているとき、メンバースイッチが追加されると、論理インターフェースに接続されていたサブリカントの認証情報はクリアされます。
- ・スタック機能を利用しているとき、メインスイッチからメンバースイッチに降格する場合、接続されていたサブリカントの認証情報はクリアされます。
- ・トランクポートは、マルチサブリカントモードのみ利用できます。
- ・トランクポートは、ダイナミックVLAN、および、ゲストVLANを使用できません。
- ・トランクポートでL2MS機能を併用する場合は、ネイティブVLANをありに設定する必要があります。
- ・ダイナミックVLANによって以下のサブリカントのVLANを変更した場合、認証機能が正しく動作しないことがあります。
 - DHCPサーバー
 - L2MS対応機器

IEEE 802.1X認証

IEEE 802.1X認証では、EAPを使用して機器またはユーザー単位で認証を行います。
認証を受けるサブリカントは、IEEE 802.1X認証に対応している必要があります。

本製品は、サブリカントとはEAP over LAN、RADIUSサーバーとはEAP over RADIUSを使用して通信を行うオーセンティケータとして動作します。

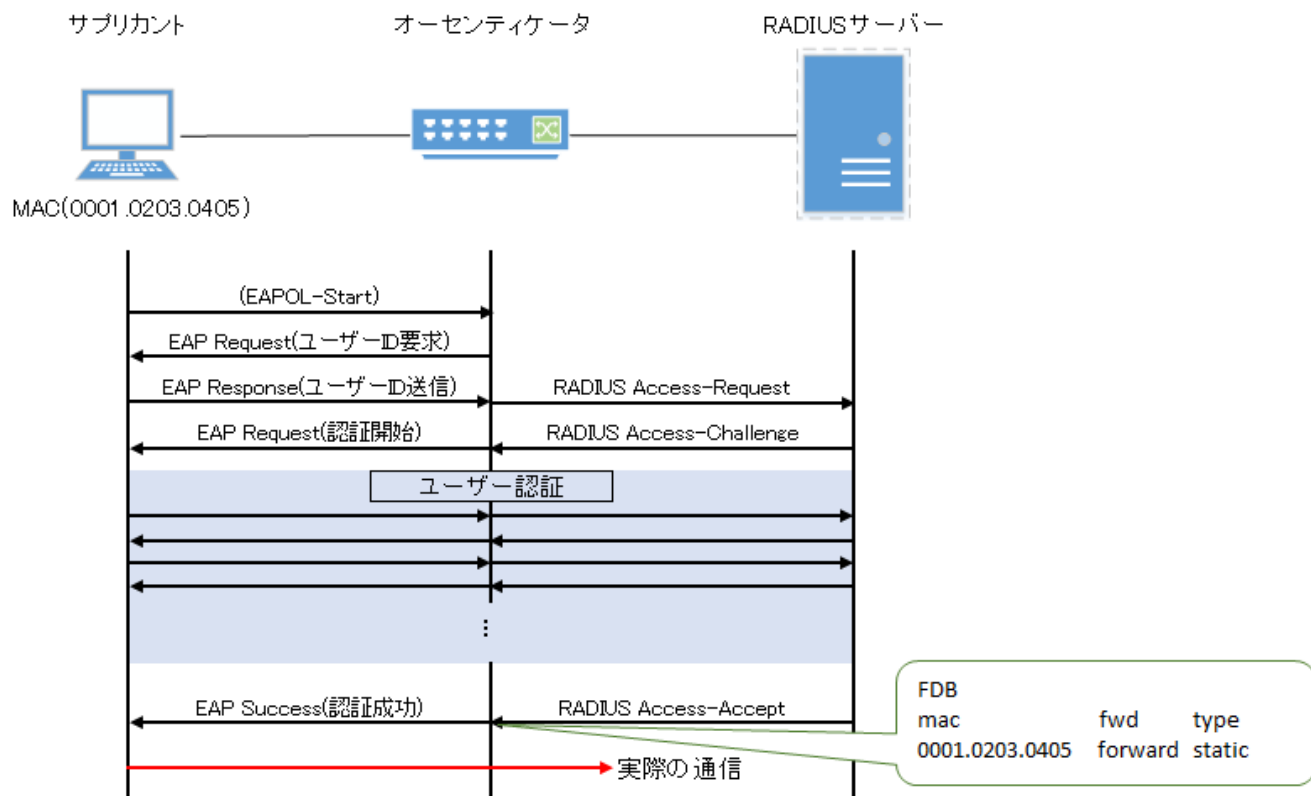
認証処理自体はサブリカントとRADIUSサーバー間で直接行われます。

本製品は、認証方式として、EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAPに対応します。
各認証方式の特徴を以下の表に示します。

	クライアント認証方法	サーバー認証方法	導入しやすさ	安全度
EAP-MD5	ユーザー名、パスワード入力	認証しない	簡単	低
EAP-TLS	クライアント証明書	サーバー証明書	複雑	高
EAP-TTLS	ユーザー名、パスワード入力	サーバー証明書	中	中
EAP-PEAP	ユーザー名、パスワード入力	サーバー証明書	中	中

使用する認証方式にあわせて、サブリカント、RADIUSサーバーの設定をしてください。

IEEE 802.1X認証の基本的な手順は以下の図のようになります。



サブリカントがLANへ接続され、サブリカントが通信開始メッセージ(EAPOL-Start)を送信することで認証を開始されます。

認証に成功すると、サブリカントに認証成功(Success)を通知し、サブリカントのMACアドレスをFDBに登録することで、サブリカントのネットワークアクセスを許可します。

認証に失敗すると、サブリカントに認証失敗(Failure)を通知され、サブリカントのネットワークアクセスを拒否します。

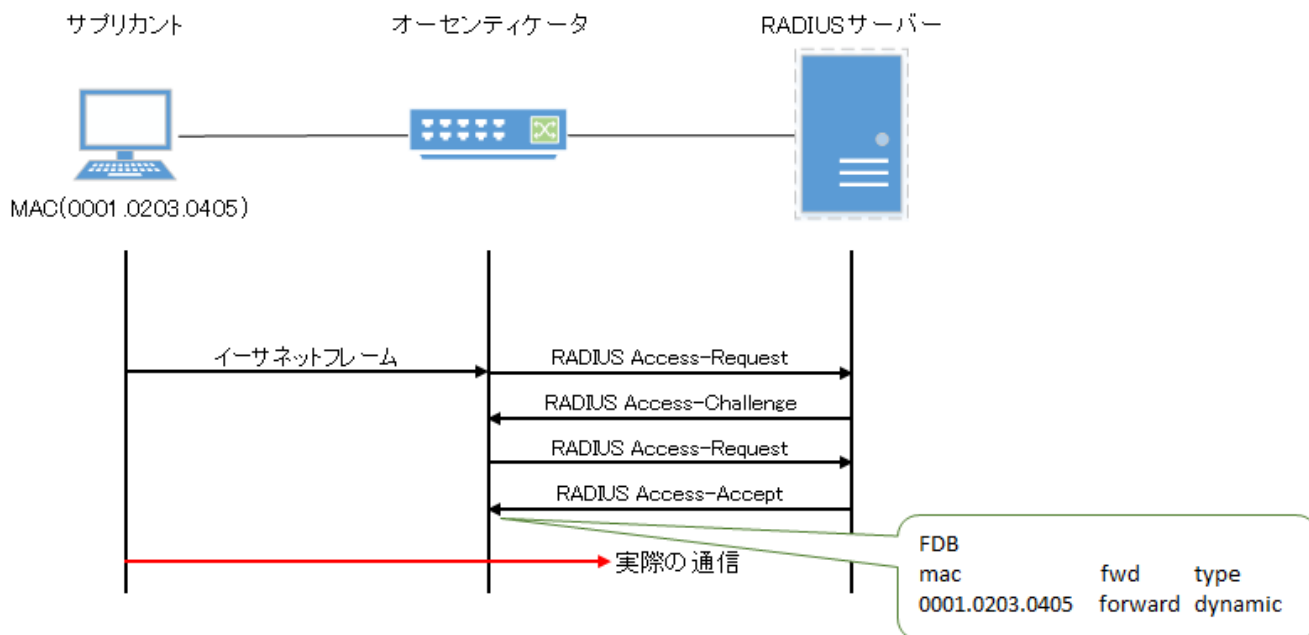
(未認証の状態でもゲストVLANが設定されている場合、特定のVLANへのアクセスを許可することも可能です。)

MAC認証

MAC認証では、機器のMACアドレスを使用して機器単位で認証を行います。

認証を受けるサブリカントに特別な機能が不要なため、IEEE 802.1X認証に対応していない機器でも認証可能です。

MAC認証の基本的な手順は以下の図のようになります。



本製品は、サブリカントから任意のイーサネットフレームを受信すると、サブリカントのMACアドレスをユーザー名およびパスワードとしてRADIUSサーバーに問い合わせます。
本製品とRADIUSサーバー間の認証方式は、EAP-MD5を使用します。

認証に成功すると、FDBにサブリカントのMACアドレスを登録して、サブリカントのネットワークアクセスを許可します。

なお、MAC認証のスタティック登録の設定(**auth-mac static** コマンド)により、スタティックエントリーとして登録することができます。

認証に失敗すると、サブリカントのネットワークアクセスを拒否します。

(未認証の状態でもゲストVLANが設定されている場合、特定のVLANへのアクセスを許可することも可能です。)

RADIUSサーバーには、ユーザー名とパスワードとして、以下のいずれかの形式で、サブリカントのMACアドレスを登録しておく必要があります。

- XX-XX-XX-XX-XX-XX (ハイフン区切り)
- XX:XX:XX:XX:XX:XX (コロン区切り)
- XXXXXXXXXXXX (区切りなし)

本製品では、**auth-mac auth-user** コマンドで、RADIUSサーバーに問い合わせるMACアドレスの形式を変更できます。

RADIUSサーバーに登録されているMACアドレスの形式にしたがってコマンドを適切に設定してください。

Web認証

Web認証は、サブリカントのWebブラウザからユーザー名とパスワードを入力することでユーザーを認証する機能です。

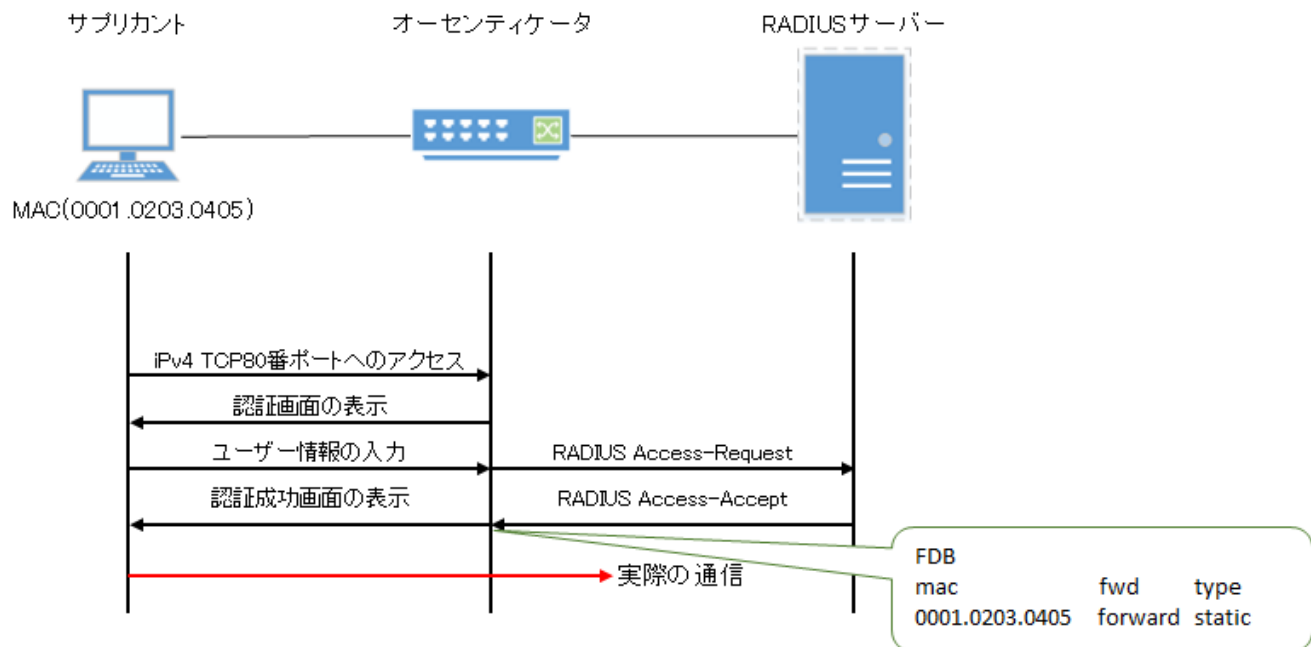
Webブラウザとスイッチ間の通信方式はHTTPに対応しています。

Web認証ではHTTPでの通信を使って認証を行う関係上、認証前であっても本製品とサブリカント間でIP通信ができる必要があります。

DHCPサーバーからIPアドレスをサブリカントに割り当てるか、サブリカント側で静的にIPアドレスを指定してください。

Web認証はマルチサブリカントモードでのみ動作します。
また、ゲストVLANとの併用はできません。

Web認証の基本的な手順は以下の図のようになります。



本製品は、サブリカントのWebブラウザで入力されたユーザー名およびパスワードをRADIUSサーバーに問い合わせます。

本製品とRADIUSサーバー間の認証方式は、EAP-MD5を使用します。

認証に成功すると、FDBにサブリカントのMACアドレスを登録して、サブリカントのネットワークアクセスを許可します。

認証に失敗すると、サブリカントのネットワークアクセスを拒否します。

サブリカント側の操作

サブリカントのWebブラウザからIPv4 TCP80番ポート宛のアクセスが行われたとき、以下のような認証画面を表示します。

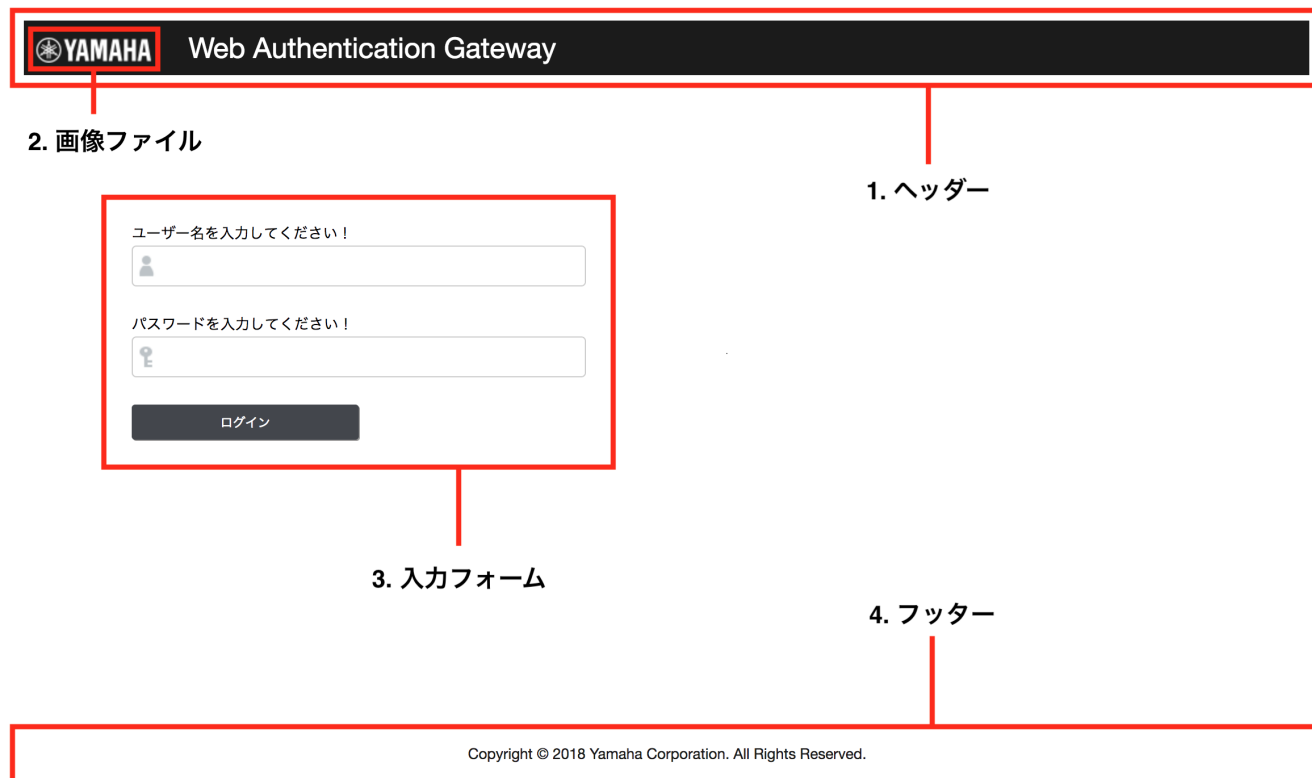
+
image::web-auth-default.png[image,width=700, role=th]

認証を受けるにはユーザー名とパスワードを入力して「ログイン」ボタンをクリックしてください。

FDBにサブリカントのMACアドレスを登録して、サブリカントのネットワークアクセスを許可します。
また認証に連続して3回失敗すると一時的に認証が制限されます。

認証画面のカスタマイズ

Web認証画面の表示内容は編集したHTMLファイル、CSSファイル、および画像ファイルを本製品にコピーすることで下記部分をカスタマイズすることができます。
HTML/CSSの書き方や書式、編集後の問題に関してはサポート対象外です。



1. ヘッダー
ヘッダー部分は、header.htmlとstyle.cssによって構成されます。これらのファイルを編集して本製品にコピーすることでカスタマイズが可能です。
2. 画像ファイル
用意した画像ファイルを本製品にコピーすることで画像ファイルの変更が可能です。
3. 入力フォーム
入力フォームの見た目はstyle.cssによって決定されます。文字列などの変更はできませんが、style.cssを編集して本製品にコピーすることで入力フォームのデザインを変更できます。
4. フッター
フッター部分は、footer.htmlとstyle.cssによって構成されます。これらのファイルを編集して本製品にコピーすることでカスタマイズが可能です。

以下ではWeb認証画面の変更方法について説明します。

認証画面カスタマイズ用ファイルの準備

Web認証画面のカスタマイズに使うファイルは以下のとおりです。

- header.html
- footer.html
- logo.png
- style.css

header.html、footer.html、およびstyle.cssはWebブラウザーを使ってスイッチから入手できます。

たとえば、スイッチのIPアドレスが192.168.100.240だった場合、Web認証が有効なポートに接続されたPCから以下のURLでファイルにアクセスできるので、ブラウザの「名前を付けて保存」などを使ってPCに保存してください。

- <http://192.168.100.240/web-auth/header.html>
- <http://192.168.100.240/web-auth/footer.html>
- <http://192.168.100.240/web-auth/style.css>

保存の際には拡張子を「.html」または「.css」にし、文字エンコーディングを「UTF-8」に設定して保存してください。

画像ファイルlogo.pngについては、PC上に任意の画像ファイルを用意してlogo.pngというファイル名で保存してください。

ファイルサイズの上限は1MBです。

認証画面カスタマイズ用ファイルの編集

PC上で前述のHTMLファイルとCSSファイルを適宜編集します。

各ファイルはHTML、CSSの仕様にしたがって自由に記述できますが、下記の点にはご注意ください。

- header.html、footer.htmlから参照できる画像ファイルはlogo.pngだけです。
- HTML/CSSファイルの拡張子は必ず「.html」および「.css」にし、文字エンコーディングはUTF-8に統一してください。

認証画面カスタマイズ用ファイルの設置

各ファイルの準備ができれば、SDカード内の /機種名/startup-config/web-auth/ に各ファイルを設置してください。

ファイル設置後は **copy auth-web custom-file** コマンド、または **copy startup-config** コマンドでスイッチに認証画面カスタマイズ用のファイルをコピーしてください。

起動中のCONFIGが保存されているフォルダの配下に下記のファイルが存在する場合、これらを使ってWeb認証画面が生成されます。

起動中のCONFIG番号は **show environment** コマンドで確認することができます。

また、SDカード内のCONFIGを使って起動している場合でも、SDカード内の /機種名/startup-config/web-auth/ に各ファイルを設置することでWeb認証画面のカスタマイズが可能です。

- header.html
認証画面から参照されるヘッダー部分として使用されます。このファイルが存在しない場合、オリジナルのheader.htmlが使用されます。
- footer.html
認証画面から参照されるフッター部分として使用されます。このファイルが存在しない場合、オリジナルのfooter.htmlが使用されます。
- logo.png
認証画面左上のロゴマーク部分に使用されます。このファイルが存在しない場合、オリジナルのヤマハロゴが表示されます。
- style.css
認証画面から参照される「style.css」として使用されます。このファイルが存在しない場合、オリジナルのstyle.cssが使用されます。

編集済みファイルの配置が完了したら、ブラウザからWeb認証画面にアクセスして表示を確認してください。

さらに変更が必要なときは、PC上のファイルを編集しなおして、再転送してください。

カスタマイズのとりやめ

認証画面のカスタマイズをやめたい場合は、起動中のCONFIGが保存されているフォルダからカスタマイズ用のファイルを削除してください。オリジナルの認証画面に戻ります。

ファイルの削除は **erase auth-web custom-file** コマンド、または **erase startup-config** コマンドで行うことができます。

ただし、**erase startup-config** コマンドではconfig.txt等も削除されるため、コマンド実施前にconfig.txt等をSDカード等にコピーしてバックアップをとるようにしてください。

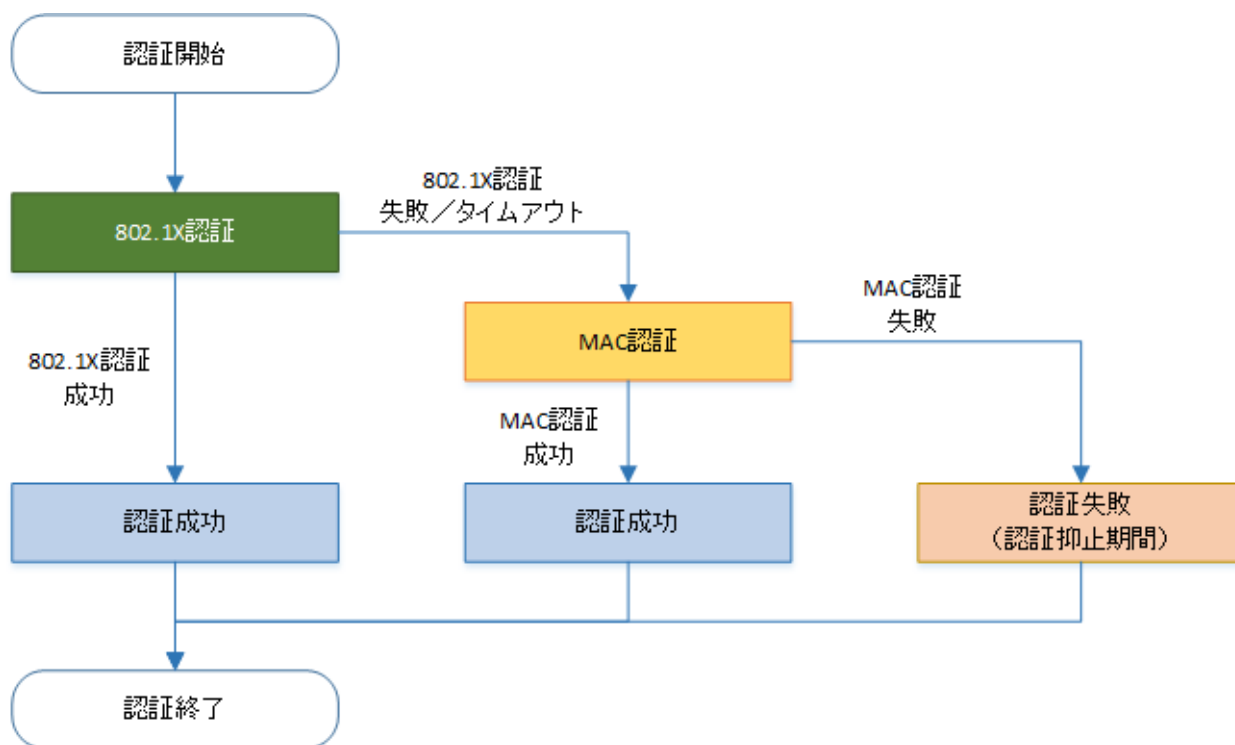
認証機能の併用

本製品では、同一ポート上でIEEE 802.1X認証、MAC認証、Web認証をそれぞれ併用することができます。併用時の認証は、認証順序の設定(auth orderコマンド)にしたがって順番に行われ、デフォルト設定の場合はIEEE 802.1X認証が優先されます。

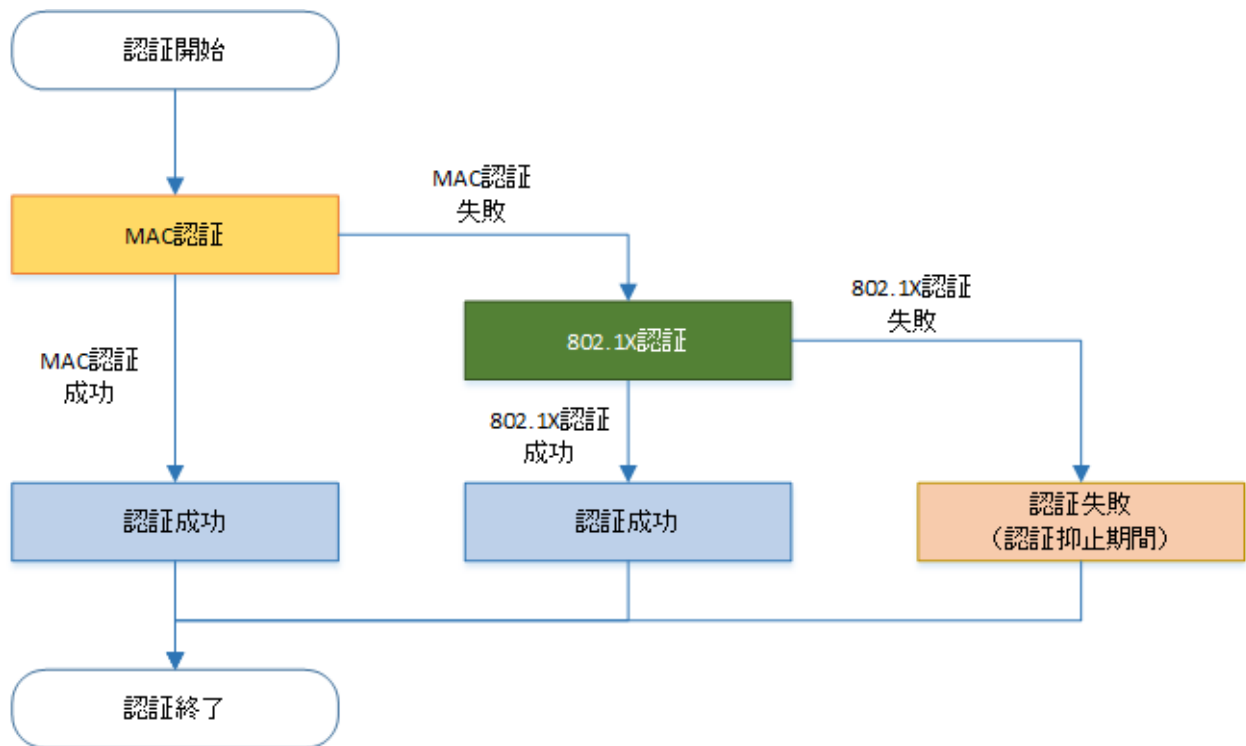
Web認証においては、Web認証画面でID/Passwordを入力したときに認証方式をWeb認証へ移行し認証を行います。

複数の認証方式が併用されている場合の基本動作は以下のようになります。

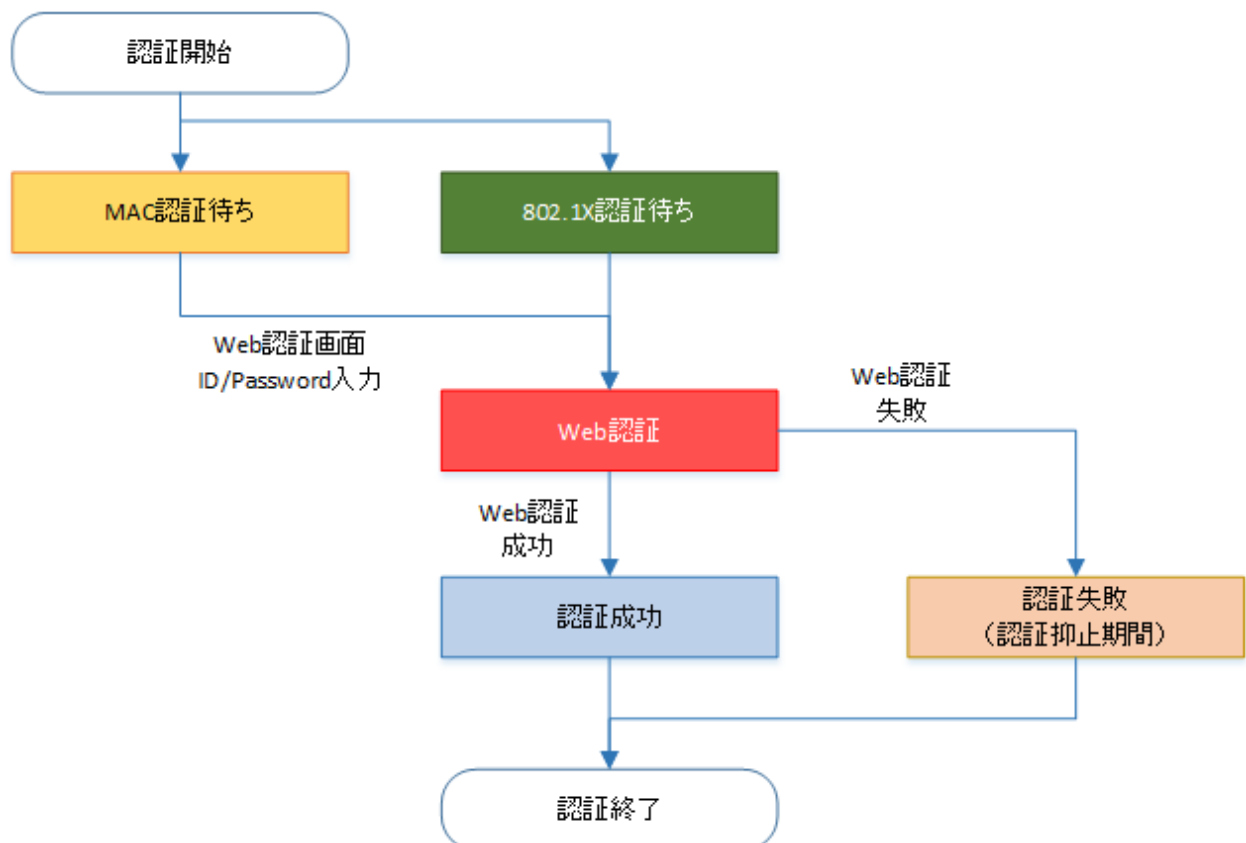
- IEEE 802.1X認証とMAC認証を併用し、IEEE 802.1X認証が優先の場合



- IEEE 802.1X認証とMAC認証を併用し、MAC認証が優先の場合



- Web認証とIEEE 802.1X認証／MAC認証を併用している場合



note

- いずれか一つの方式で認証に成功すれば、認証成功となります。
- 再認証の設定が有効な場合は、認証に成功した方式で再認証を行います。
- 認証方式を併用している場合、未認証ポートでの転送制御の設定は受信破棄になります。
- IEEE 802.1X認証とMAC認証を併用している場合、未認証のサブリカントからEAPOL startを受信する

ことでMAC認証動作中であってもIEEE 802.1X認証へ移行します。

- IEEE 802.1X認証とMAC認証を併用している場合、最初の認証方式に失敗しても認証抑止期間に入らず次の認証方式に移行します。
- IEEE 802.1X認証とMAC認証を併用している場合は、サブリカントから任意のイーサネットフレームを受信すると、本製品からEAPのRequestが送信されます。
- Web認証を併用している場合、未認証サブリカントはstatic/discardでFDBに登録されます。

ホストモード

本製品では、ポート認証機能において、ホストモードを選択できます。

ホストモードとは、認証ポートで対象サブリカントの通信をどのように許可するかを示すものです。

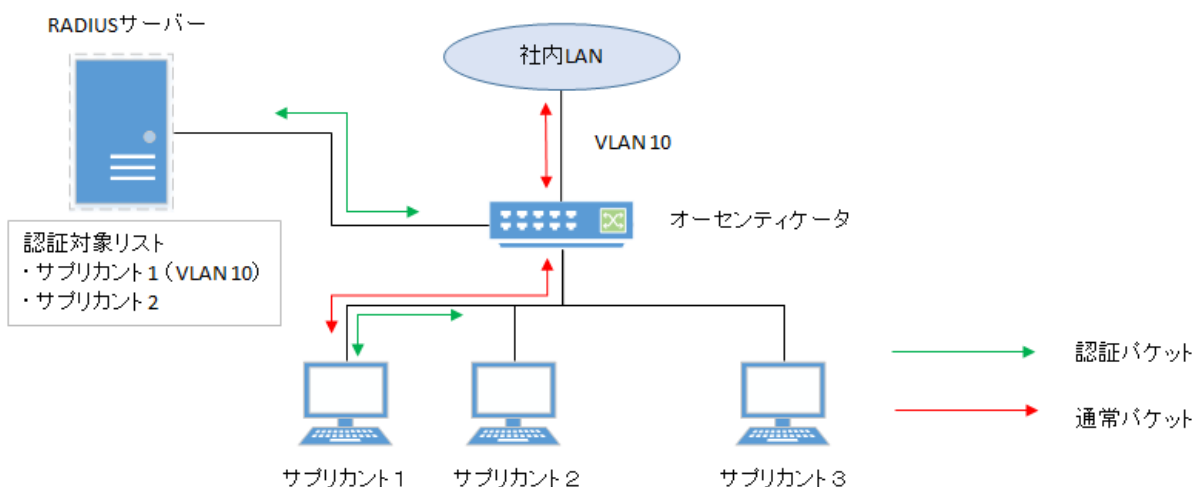
本製品では、ホストモードとして以下を選択できます。

- シングルホストモード
1つのLAN/SFPポートにつき、1サブリカントのみ通信を許可するモード。
最初に認証成功したサブリカントのみ、通信を許可します。
- マルチホストモード
1つのLAN/SFPポートにつき、複数のサブリカントの通信を許可するモード。
あるサブリカントが認証に成功して通信が許可されると、同じLAN/SFPポートに接続している他のサブリカントも同様に、認証に成功したサブリカントと同じVLAN上で通信を許可します。
- マルチサブリカントモード
1つのLAN/SFPポートにつき、複数のサブリカントの通信を許可するモード。
各サブリカントをMACアドレスで識別し、サブリカント単位で通信を許可します。
ダイナミックVLAN機能を使用することで、サブリカント単位でVLANを指定することができます。

ダイナミックVLAN

本製品のIEEE 802.1X認証、MAC認証、および、Web認証で、ダイナミックVLANに対応します。

ダイナミックVLANとは、RADIUSサーバーから通知された認証情報のVLAN属性値に基づいて、認証ポートの所属VLANを変更する機能です。



上の図のように、ポートの所属VLANが1、認証情報で通知されたVLAN属性値が10の場合、認証成功後、認証ポートの所属VLANは10として、VLAN 10上で通信を許可します。

RADIUSサーバーに対して、サーバーからの認証情報に以下の属性値が含まれるように設定してください。

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = IEEE-802 (6)
- Tunnel-Private-Group-ID = VLAN ID

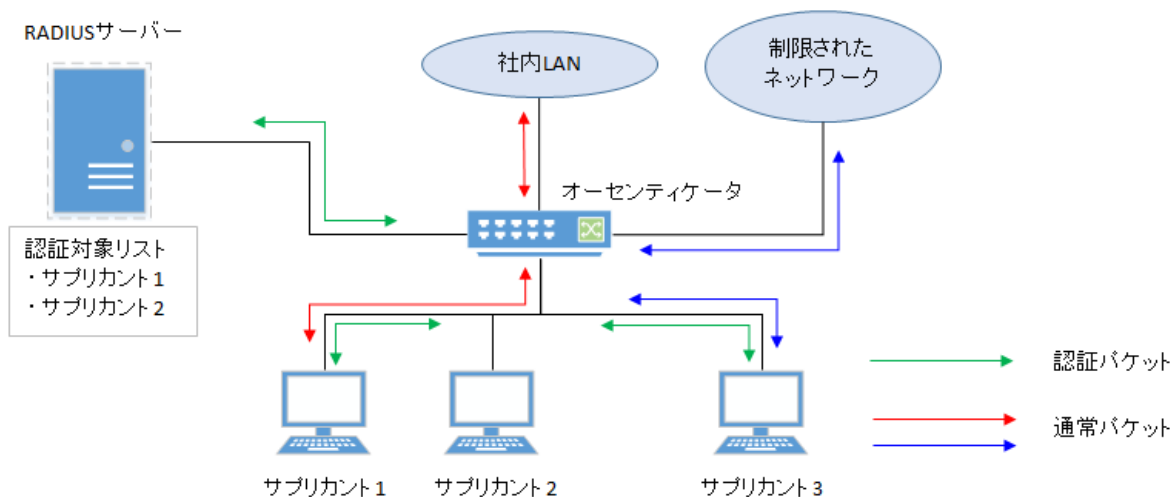
ダイナミックVLANを利用する場合、各ホストモードで以下の動作となります。

- シングルホストモード
認証に成功したサブスクリプターのVLAN属性値に基づいて認証ポートの所属VLANを変更します。
- マルチホストモード
認証に成功したサブスクリプターのVLAN属性値に基づいて認証ポートの所属VLANを変更します。
同じポートに接続されたその他のサブスクリプターも同じVLAN上で通信を許可します。
- マルチサブスクリプターモード
認証に成功したサブスクリプターのVLAN属性値に基づいて認証ポートの所属VLANを変更します。
サブスクリプター単位でVLANを指定することができます。

未認証・認証失敗ポートのVLAN

本製品のIEEE 802.1X認証とMAC認証では、ゲストVLAN設定をすることにより、未認証のポートや認証に失敗したポートを特定のVLANに割り当てることができます。

マルチサブスクリプターモードの場合は、サブスクリプター単位で指定することができます。



上の図のように、認証に成功していないサブスクリプターにも制限されたネットワークで一部の機能を提供したい場合に有効です。

EAPパススルー機能

EAPパススルーの有効/無効を切り替え、EAPOLフレームの転送可否を設定することができます。

802.1X認証機能が有効なインターフェースについては認証機能を優先し、EAPパススルーの設定は適用されません。

RADIUSサーバーに通知する属性値

RADIUSサーバーに、NAS-Identifier属性値を通知することができます。

auth radius attribute nas-identifier コマンドで設定した文字列を、NAS-Identifier属性値としてRADIUSサーバーへ通知します。

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願います。

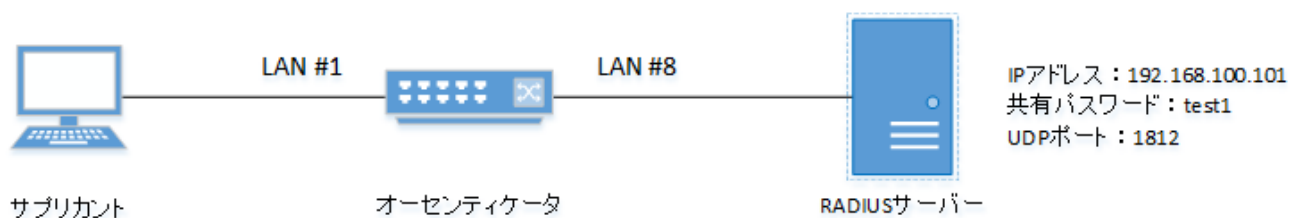
操作項目	操作コマンド
システム全体でのIEEE 802.1X認証機能の設定	aaa authentication dot1x
システム全体でのMAC認証機能の設定	aaa authentication auth-mac
システム全体でのWeb認証機能の設定	aaa authentication auth-web
IEEE 802.1X認証機能の動作モード設定	dot1x port-control
IEEE 802.1X認証の未認証ポートでの転送制御の設定	dot1x control-direction
EAPOLパケットの再送回数の設定	dot1x max-auth-req
MAC認証機能の設定	auth-mac enable
MAC認証時のMACアドレス形式の設定	auth-mac auth-user
MAC認証のスタティック登録の設定	auth-mac static
Web認証機能の設定	auth-web enable
Web認証成功後のリダイレクト先URLの設定	auth-web redirect-url
Web認証画面カスタマイズ用ファイルのコピー	copy auth-web custom-file
Web認証画面カスタマイズ用ファイルの削除	erase auth-web custom-file
ホストモードの設定	auth host-mode
認証順序の設定	auth order
再認証の設定	auth reauthentication
ダイナミックVLANの設定	auth dynamic-vlan-creation
ゲストVLANの設定	auth guest-vlan
認証失敗後の抑止期間の設定	auth timeout quiet-period
再認証間隔の設定	auth timeout reauth-period
RADIUSサーバー全体の応答待ち時間の設定	auth timeout server-timeout
サブリカント応答待ち時間の設定	auth timeout supp-timeout
RADIUSサーバーホストの設定	radius-server host
RADIUSサーバー1台あたりの応答待ち時間の設定	radius-server timeout
RADIUSサーバーへの要求再送回数の設定	radius-server retransmit
RADIUSサーバー共有パスワードの設定	radius-server key
RADIUSサーバー使用抑制時間の設定	radius-server deadtime
RADIUSサーバーに通知するNAS-Identifier属性の設定	auth radius attribute nas-identifier
ポート認証情報の表示	show auth status

操作項目	操作コマンド
RADIUSサーバー設定情報の表示	show radius-server
サブリカント情報の表示	show auth supplicant
統計情報の表示	show auth statistics
統計情報のクリア	clear auth statistics
認証状態のクリア	clear auth state
認証状態をクリアする時刻の設定(システム)	auth clear-state time
認証状態をクリアする時刻の設定(インターフェース)	auth clear-state time
EAPパススルーの設定	pass-through eap

コマンド実行例

IEEE 802.1X認証の設定

IEEE 802.1X認証を使用できるように設定します。



- ・ LANポート #1 は、サブリカントを接続する認証ポートとします。
- ・ ホストモード は **マルチサブリカントモード** とします。
- ・ ゲストVLAN をVLAN #10 とします。
- ・ 接続するRADIUSサーバーのIPアドレスは 192.168.100.101 とします。

■設定手順

1. ゲストVLAN用にVLAN #10 を定義します。

```
Yamaha(config)#vlan database
Yamaha(config-vlan)#vlan 10 ①
Yamaha(config-vlan)#exit
```

① VLAN #10の定義

2. システム全体で、IEEE 802.1X認証機能を有効にします。

```
Yamaha(config)#aaa authentication dot1x
```

3. LANポート #1 で、IEEE 802.1X認証の設定を行います。

```
Yamaha(config)#interface port1.1
```

```
Yamaha(config-if)#dot1x port-control auto ①
Yamaha(config-if)#auth host-mode multi-supPLICant ②
Yamaha(config-if)#auth guest-vlan 10 ③
Yamaha(config-if)#exit
```

- ① IEEE 802.1X認証の動作モードをautoにする
- ② ホストモードをマルチサブリカントモードにする
- ③ ゲストVLANをVLAN #10にする

4. RADIUSサーバーの設定を行います。

```
Yamaha(config)#radius-server host 192.168.100.101 key test1 ①
```

- ① ホストを192.168.100.101、共有パスワードを"test1"にする

5. RADIUSサーバー設定情報を確認します。

```
Yamaha#show radius-server
Server Host : 192.168.100.101
Authentication Port : 1812
Secret Key       : test1
Timeout          : 5 sec
Retransmit Count : 3
Deadtime         : 0 min
```

6. ポート認証情報を確認します。

```
Yamaha#show auth status
[System information]
802.1X Port-Based Authentication : Enabled
MAC-Based Authentication         : Disabled
WEB-Based Authentication         : Disabled

Clear-state time : Not configured

Redirect URL :
Not configured

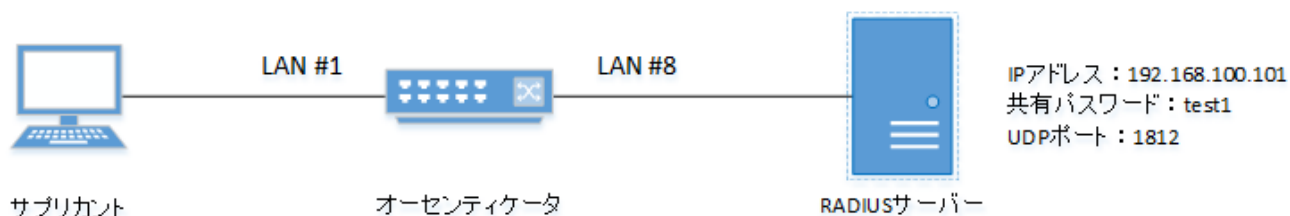
RADIUS server address :
192.168.100.101 (port:1812)

[Interface information]
Interface port1.1 (up)
802.1X Authentication : Force Authorized (configured:auto)
MAC Authentication    : Disabled (configured:disable)
WEB Authentication    : Enabled (configured:disable)
Host mode             : Multi-supPLICant
Dynamic VLAN creation : Disabled
Guest VLAN            : Enabled (VLAN ID:10)
Reauthentication      : Disabled
Reauthentication period : 3600 sec
MAX request           : 2 times
```

```
Supplicant timeout      : 30 sec
Server timeout          : 30 sec
Quiet period            : 60 sec
Controlled directions   : In (configured:both)
Protocol version        : 2
Clear-state time        : Not configured
```

MAC認証の設定

MAC認証を使用できるように設定します。



- ・ LANポート #1 は、サブリカントを接続する認証ポートとします。
- ・ ホストモード は **マルチサブリカントモード** とします。
- ・ 接続するRADIUSサーバーのIPアドレスは 192.168.100.101 とします。

■設定手順

1. システム全体で、MAC認証機能を有効にします。

```
Yamaha(config)#aaa authentication auth-mac
```

2. LANポート #1 で、MAC認証の設定を行います。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#auth-mac enable ①
Yamaha(config-if)#auth host-mode multi-supplicant ②
Yamaha(config-if)#exit
```

- ① MAC認証を有効にする
- ② ホストモードをマルチサブリカントモードにする

3. RADIUSサーバーの設定を行います。

```
Yamaha(config)#radius-server host 192.168.100.101 key test1 ①
```

- ① ホストを192.168.100.101、共有パスワードを"test1"にする

4. RADIUSサーバー設定情報を確認します。

```
Yamaha#show radius-server
Server Host : 192.168.100.101
Authentication Port : 1812
Secret Key      : test1
```

```
Timeout          : 5 sec
Retransmit Count  : 3
Deadtime         : 0 min
```

5. ポート認証情報を確認します。

```
Yamaha#show auth status
[System information]
  802.1X Port-Based Authentication : Disabled
  MAC-Based Authentication         : Enabled
  WEB-Based Authentication         : Disabled

Clear-state time : Not configured

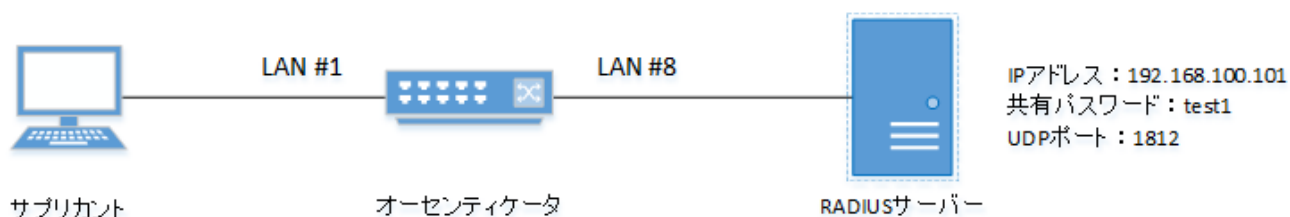
Redirect URL :
  Not configured

RADIUS server address :
  192.168.100.101 (port:1812)

[Interface information]
Interface port1.1 (up)
  802.1X Authentication : Force Authorized (configured:-)
  MAC Authentication    : Enabled (configured:enable)
  WEB Authentication    : Disabled (configured:disable)
  Host mode             : Multi-supPLICant
  Dynamic VLAN creation : Disabled
  Guest VLAN            : Disabled
  Reauthentication      : Disabled
  Reauthentication period : 3600 sec
  MAX request           : 2 times
  SupPLICant timeout    : 30 sec
  Server timeout        : 30 sec
  Quiet period          : 60 sec
  Controlled directions : In (configured:both)
  Protocol version      : 2
  Clear-state time      : Not configured
  Authentication status  : Unauthorized
```

Web認証の設定

Web認証を使用できるように設定します。



- ・ LANポート #1 は、サブリカントを接続する認証ポートとします。
- ・ サブリカントのIPアドレスは 192.168.100.10 が設定されているものとします。

- ・ 接続するRADIUSサーバーのIPアドレスは 192.168.100.101 とします。

■ 設定手順

1. IP通信を行うためオーセンティケータにIPアドレスを設定します。

```
Yamaha(config)#interface valn1
Yamaha(config-if)#ip address 192.168.100.240/24
Yamaha(config-if)#exit
```

2. システム全体でWeb認証機能を有効にします。

```
Yamaha(config)#aaa authentication auth-web
```

3. LANポート #1 で、Web認証の設定を行います。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#auth host-mode multi-supPLICant ①
Yamaha(config-if)#auth-web enable ②
Yamaha(config-if)#exit
```

① ホストモードをマルチサブリカントモードにする

② Web認証を有効にする

4. RADIUSサーバーの設定を行います。

```
Yamaha(config)#radius-server host 192.168.100.101 key test1 ①
```

① ホストを192.168.100.101、共有パスワードを"test1"にする

5. RADIUSサーバー設定情報を確認します。

```
Yamaha#show radius-server
Server Host : 192.168.100.101
Authentication Port : 1812
Secret Key       : test1
Timeout         : 5 sec
Retransmit Count : 3
Deadtime        : 0 min
```

6. ポート認証情報を確認します。

```
Yamaha#show auth status
[System information]
802.1X Port-Based Authentication : Disabled
MAC-Based Authentication         : Disabled
WEB-Based Authentication         : Enabled

Clear-state time : Not configured
```



```
Redirect URL :  
  Not configured  
  
RADIUS server address :  
  192.168.100.101 (port:1812)
```

[Interface information]

```
Interface port1.1 (up)  
  802.1X Authentication : Force Authorized (configured:-)  
  MAC Authentication    : Disabled (configured:disable)  
  WEB Authentication    : Enabled (configured:enable)  
  Host mode             : Multi-supPLICant  
  Dynamic VLAN creation : Disabled  
  Guest VLAN            : Disabled  
  Reauthentication      : Disabled  
  Reauthentication period : 3600 sec  
  MAX request           : 2 times  
  SupPLICant timeout    : 30 sec  
  Server timeout        : 30 sec  
  Quiet period          : 60 sec  
  Controlled directions : In (configured:both)  
  Protocol version      : 2  
  Clear-state time      : Not configured
```

注意事項

マルチサブリカントモードでダイナミックVLANを使用する場合、内部リソースを消費します。
このリソースは、ACL機能やQoS機能でも使用しており、設定によっては不足する場合があります。
リソースが不足している場合は、認証自体に成功しても通信可能にならないため注意が必要です。

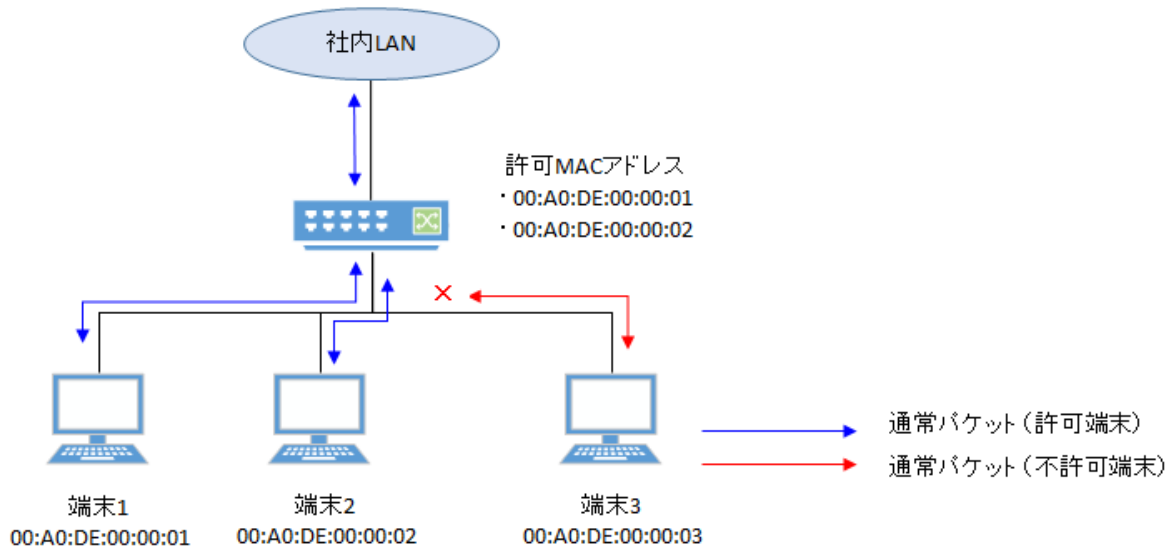
関連文書

- [内蔵RADIUSサーバー](#)
- [WLX402内蔵Radiusサーバー活用例](#)

ポートセキュリティ機能

機能概要

ポートセキュリティ機能は、許可された端末のみ通信できるように制限をかけ、不正な端末からのアクセスを防止する機能です。



用語の定義

特になし

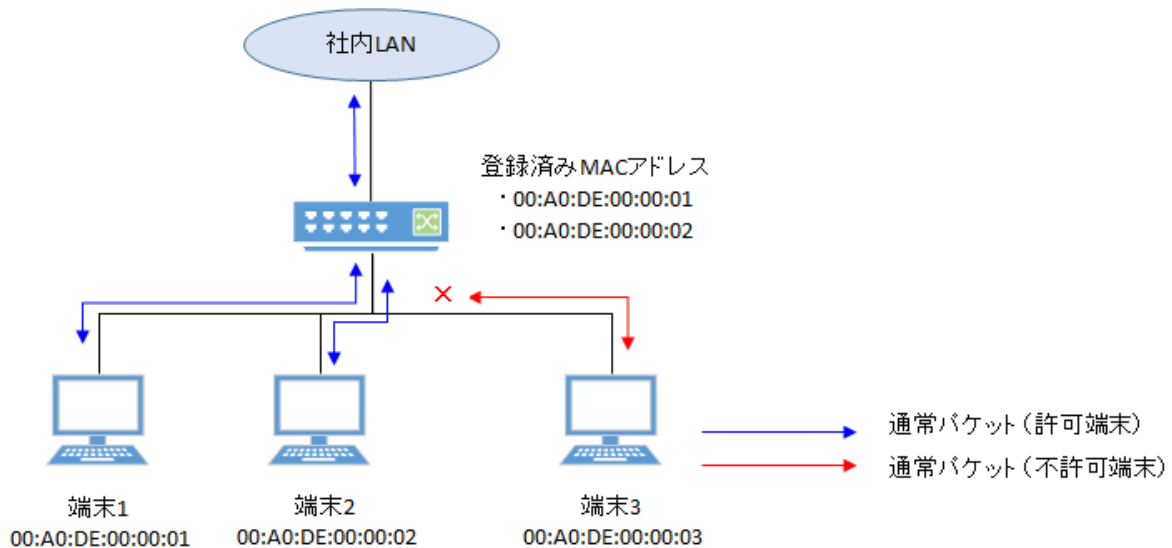
機能詳細

ポートセキュリティ機能を有効にしたポートに対し、通信を許可したい端末のMACアドレスをあらかじめ登録しておくことで、許可された端末のみの通信ができるようになります。逆に、登録していない端末(不正な端末)からアクセスがあった場合、不正アクセスと見なしパケットを破棄させます。設定によっては該当ポートをダウンすることも可能です。

なお、ポートセキュリティ機能はポート認証機能との併用はできません。

アクセスする端末を制限

ポートセキュリティ機能を有効にし、通信を許可する端末のMACアドレスを **port-security mac-address** コマンドを使用して登録するだけで、アクセス端末を制限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願います。

操作項目	操作コマンド
ポートセキュリティ機能の設定	port-security enable
許可MACアドレスの登録	port-security mac-address
セキュリティ違反時の動作の設定	port-security violation
ポートセキュリティ情報の表示	show port-security status

コマンド実行例

アクセスする端末を制限

許可された端末のみ通信ができるように、MACアドレスを手動で設定します。

1. LANポート #1 で、ポートセキュリティを有効にします。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#port-security enable
```

2. 許可したいMACアドレスを登録します。

```
Yamaha(config)#port-security mac-address 00A0.DE00.0001 forward port1.1 vlan 1
Yamaha(config)#port-security mac-address 00A0.DE00.0002 forward port1.1 vlan 1
```

3. ポートセキュリティ情報を確認します。

```
Yamaha#show port-security status
```

Port	Security	Action	Status	Last violation
port1.1	Enabled	Discard	Normal	00A0.DE00.0003
port1.2	Disabled	Discard	Normal	
port1.3	Disabled	Discard	Normal	
port1.4	Disabled	Discard	Normal	
port1.5	Disabled	Discard	Normal	
port1.6	Disabled	Discard	Normal	
port1.7	Disabled	Discard	Normal	
port1.8	Disabled	Discard	Normal	
port1.9	Disabled	Discard	Normal	
port1.10	Disabled	Discard	Normal	

注意事項

- 不正アクセス検知によりシャットダウンしたポートを復旧させたい場合は、**no shutdown** コマンドを用いてください。
show port-security status コマンドのステータスは、ポートがリンクアップするまでNormal状態に戻りません(Shutdown状態のまま)。
- port-security mac-address** コマンドで誤ったポートを指定した場合、通信および違反フレーム検知が正しく行われません。

関連文書

特になし

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。

- SWX2310P-10G : ポート 1-8
- SWX2310P-18G : ポート 1-16
- SWX2310P-28GT: ポート 1-24

本製品では、ポートごとに給電機能の有効/無効を設定可能です。

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。

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。

本製品では、ポートがシャットダウンされたときも PD への給電を継続します。

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、および同時に給電可能なポートの最大数の目安 (各 PD が上限まで電力を消費している場合の同時接続可能数) 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)		
			SWX2310P-10G(124W)	SWX2310P-18G(247W)	SWX2310P-28GT(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 (*)

- ・ (*): 受電機器の実際の使用電力によって、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供給可能電力上限に対して設定するマージンのことです。供給可能電力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。例えば、SWX2310P-10MT (供給可能電力上限 124W) でガードバンドが 10W に設定されている場合、全ポートの総供給電力が 114W 以上 (供給可能電力が 10W 以下) のときには新たに接続された PD に給電しません。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、工場出荷状態では **7W** となっています。

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、工場出荷状態では全ポート low の設定となっています。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。

PoE給電動作

本製品は使用電力によって以下の処理を行います。

- ・ ポート全体の総供給電力が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、総供給電力がPoE供給可能電力上限内に収まるようにします。
このとき、MODE LED の状態を STATUS モードに自動遷移し、電力供給を停止したポートのSPEED LEDが橙点滅します。
また、SYSLOGに "portX.X over system power limit" を出力します。
- ・ 供給可能電力がガードバンド以下の場合
既に給電中のPDへの給電は継続しますが、新たに接続されたPDには給電優先度に関わらず給電しません。
このとき、MODE LED の状態を STATUS モードに自動遷移し、電力供給が行われなかったポートのSPEED LEDを橙点灯します。
また、SYSLOGに、"portX.X restricted by guard band" を出力します。
- ・ 特定のPoEポートの供給電力がポート単位の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、MODE LED の状態を STATUS モードに自動遷移し、電力供給を停止したポートのSPEED LEDを橙点灯します。
また、SYSLOGに、"portX.X over load" を出力します。
- ・ 供給電力が上記以外 (正常範囲内) の場合
PDへの給電を継続します。
このとき、上記要因で MODE LED の状態が STATUS モードに遷移していた場合、MODE LEDは自動遷移前のMODEに戻します。

また、PoEポートの状態あるいは供給可能電力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。

MODE LED の状態が PoE モードの場合、給電を開始したポートのLINK 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。
MODE LED の状態が PoE モードの場合、給電を停止したポートのLINK LEDを消灯します。
- 供給可能電力がガードバンド以下になった場合
SYSLOGに、"Supplying power reached to guard band threshold" を出力します。
- 供給可能電力がガードバンド以下の状態から回復した場合
SYSLOGに、"Supplying power fell below guard band threshold" 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受信フレームの設定値に従い変更します。

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と変更する動作の対応は以下のとおりです。

Power via MDI TLV (IEEE802.3)	変更する動作
Power priority	給電優先度
PD requested power value	ポート単位の供給可能電力上限

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
システム全体でのPoE給電機能の設定	power-inline
インターフェース単位でのPoE給電機能の設定	power-inline
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 ※工場集荷状態の場合不要
- 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(critical)に設定
- ④ インターフェースのPoE給電機能を有効化 ※工場集荷状態の場合不要

注意事項

特になし

関連文書

- [LED制御](#)
- [LLDP](#)
- [SYSLOG](#)

Layer 2機能

フォワーディングデータベース(FDB)

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、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。
自動学習／手動登録合わせて 最大 16,384個のアドレスを登録できます。

管理要素	説明	
MACアドレス	デバイスのMACアドレスで、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/SFPポート、スタティック/LACP論理インターフェースが該当します。	
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。	
エントリー登録種別	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
	multicast	IGMP/MLD Snoopingで学習したエントリー

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。

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。

また、VLANインターフェースを作成することで、内部的にFDBエントリを1つ消費します。

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。

また、マルチキャストのMACアドレス場合を複数設定した場合、この場合は全体で1個とみなします。

VLAN	port	mac	fwd	type	timeout
1	port1.1	0100.0000.1000	forward	static	0
1	port1.2	0100.0000.1000	forward	static	0
1	port1.3	0100.0000.1000	forward	static	0
1	port1.4	0100.0000.1000	forward	static	0
1	port1.5	0100.0000.1000	forward	static	0
1	port1.6	0100.0000.1000	forward	static	0

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/SFPポート (port)
- ・スタティック/LACP論理インターフェース (sa,po)

アクション

キーレコードと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は、discardが設定できません。)

登録種別

- ・ dynamic … 自動的に登録、削除が行われます。config設定ファイルには、登録結果は残りません。
- ・ static … 手動で登録、削除するため、config設定ファイルに残ります。
- ・ multicast … IGMP/MLD Snooping機能によって、自動的に登録、削除が行われます。config設定ファイルには、登録結果は残りません。

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、エージングタイマーによりFDBエントリーから自動的に削除されます。

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効です。
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設定は、 **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. エージングタイマーによりエントリーから削除される実際の時間は、タイマー設定値x2秒以内となります。
5. 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。
6. 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。

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. 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。
3. 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。
4. 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/SFPポート、またはスタティック/LACP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。
5. 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MACアドレスは登録できません。
 - 0000.0000.0000
 - 0100.5e00.0000～0100.5eff.ffff
 - 0180.c200.0000～0180.c200.000f
 - 0180.c200.0020～0180.c200.002f
 - 3333.0000.0000～3333.ffff.ffff
 - ffff.ffff.ffff

関連コマンド

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.cbc2.218d  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 400秒 に変更する。

```
Yamaha(config)#mac-address-table ageing-time 400
```

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/SFP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

I2-unknown-mcast コマンドで未知のマルチキャストフレームを破棄(discard)するよう設定している場合、**mac-address-table static** コマンドで静的にマルチキャストMACアドレスを転送(forward)するように登録していても効果はありません。

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/SFP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/SFPポートで複数の異なるVLANを通信させることができます。
プライベートVLAN	同一VLAN内で通信可能なグループを分割できます。以下の3種類のVLANで構成します。 ・プライマリーVLAN ・アイソレートVLAN ・コミュニティVLAN
マルチプルVLAN	LAN/SFPポートを複数の通信可能なグループに分割できます。 マルチプルVLANについては こちら を参照してください。
ボイスVLAN	アクセスポート上で音声とデータをわけて扱えるようにすることができます。

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

1. 本製品のLAN/SFP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/SFP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/SFP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. アクセスポートに対して、ボイスVLANを指定することでタグ付きの音声フレームを通信することができます。
 8. LAN/SFPポートの所属VLANの確認は、**show vlan** コマンドで行います。

VLANに対するアクセス制御

本製品は、VLANに対するアクセス制御機能として、VLANアクセスマップ機能を提供します。
VLANアクセスマップは、VLAN IDに対するフィルタ条件として、標準/拡張IPアクセス制御リスト、MACアクセス制御リストを関連付けることができます。
VLANアクセスマップの操作は、以下のコマンドで行います。

- VLANアクセスマップの作成 : **vlan access-map** コマンド
- VLANアクセスマップの条件設定 : **match access-list** コマンド
- VLANアクセスマップの割り当て : **vlan filter** コマンド

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/SFP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/SFP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/SFP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)

プライベートVLAN

本製品は、同一サブネット内でさらに通信可能なグループを分割する プライベートVLAN を構成できます。動作仕様について、以下に示します。

1. プライベートVLANは、以下に示す3種類のVLANで構成します。
 - プライマリーVLAN
セカンダリーVLANの親となるVLANです。
1つのプライベートVLANに 1つだけ 設定することができます。
 - アイソレートVLAN
セカンダリーVLANの一つで、プライマリーVLANだけにトラフィックを流します。
1つのプライベートVLANに 1つだけ 設定することができます。
 - コミュニティVLAN
セカンダリーVLANの一つで、同じコミュニティVLANとプライマリーVLANにトラフィックを流します。
1つのプライベートVLANに 複数 設定することができます。
2. プライマリーVLANは、複数のプロミスカスポートを収容することができます。
プロミスカスポートとして使用できるポートは、 アクセスポート、 トランクポート、 スタティック/LACP論理インターフェース です。
3. セカンダリーVLAN (アイソレートVLAN、コミュニティVLAN) のホストポートとして使用できるポートは、 アクセスポート のみとなります。
4. セカンダリーVLAN (アイソレートVLAN、コミュニティVLAN) は、 1つのプライマリーVLAN と関連付けすることができます。
関連付けには、 **switchport private-vlan mapping** コマンドを使用します。
 - アイソレートVLANは、プライベートVLANに収容されている複数のプロミスカスポートと関連付けることができます。

- 。コミュニティVLANは、プライベートVLANに收容されている複数のプロミスカポートと関連付けることができます。

ボイスVLAN

ボイスVLANとは、IP電話の音声トラフィックとPCのデータトラフィックが混在しても音声に悪影響がでないようにするための機能です。



IP電話には、スイッチに接続するポートとPCを接続するためのポートの2ポートを持つものがあります。スイッチとIP電話、IP電話とPCを接続することで、スイッチの1ポートでIP電話の音声トラフィックとPCのデータトラフィックを扱うことが可能になります。このような構成でボイスVLAN機能を使用することにより、IP電話のノイズなどが発生しにくいように音声データとPCデータをわけたり、音声データを優先して扱うようになります。

ボイスVLANの設定は **switchport voice vlan** コマンドで行います。以下のいずれかを音声トラフィックとして扱うように設定します。

- ・ 802.1pタグつきフレーム
- ・ プライオリティタグフレーム(VLAN IDは0でCoS値だけを指定した802.1pタグ)
- ・ タグなしフレーム

タグ付きフレームを音声トラフィックとして扱う場合、タグ無しフレームはデータトラフィックとして扱われます。

本製品はLLDPを利用することで、接続されたIP電話に対して設定を自動で反映させることができます。自動設定するための条件は以下のとおりです。

- ・ ボイスVLANを有効にしているポートで、LLDP-MED TLV の送信を有効に設定している。
- ・ 接続するIP電話が LLDP-MED での設定に対応している。

上記条件を満たしている場合、該当ポートにIP電話が接続されると、LLDP-MED の Network Policy TLV によりボイスVLAN情報(タグあり/なし、VLAN ID、使用すべきCoS値、DSCP値)を通知します。IP電話は、本製品から通知された情報にしたがって音声データを送信ようになります。

IP電話に設定するCoS値は **switchport voice cos** コマンドで、DSCP値は **switchport voice dscp** コマンドで設定します。

また、音声トラフィックを優先的に処理するためには、IP電話の設定にあわせてQoSの設定(QoSの有効化、トラストモードの設定)が必要です。

ボイスVLAN の制限事項は以下のとおりです。

- ・ アクセスポートに設定されている物理インターフェースでのみ利用可能です。リンクアグリゲーション論理インターフェース、VLAN論理インターフェースでは利用できません。
- ・ ボイスVLAN機能とポート認証機能の併用はできません。

関連コマンド

関連コマンド一覧

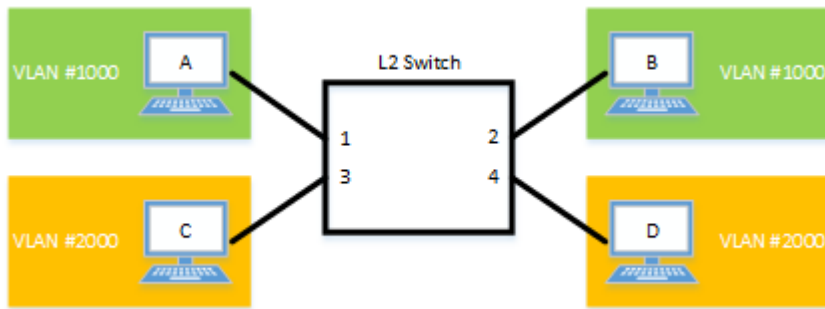
- ・ 関連コマンドについて、以下に示します。

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
プライベートVLANの定義	private-vlan
プライベートVLANのセカンダリーVLANの設定	private-vlan association
VLANアクセスマップの作成	vlan access-map
VLANアクセスマップへの条件設定	match
VLANアクセスマップのVLANへの割り当て	vlan filter
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
プライベートVLAN用ポート(プロミスカスポート, ホストポート)の設定	switchport mode private-vlan
プライベートVLAN用ポート・ホストポートのVLAN設定	switchport private-vlan host-association
プライベートVLAN用ポート・プロミスカスポートのVLAN設定	switchport private-vlan mapping
ボイスVLANの設定	switchport voice vlan
ボイスVLANのCoS値の設定	switchport voice cos
ボイスVLANのDSCP値の設定	switchport voice dscp
VLAN情報の表示	show vlan
プライベートVLAN情報の表示	show vlan private-vlan
VLANアクセスマップの表示	show vlan access-map
VLANアクセスマップフィルタの表示	show vlan filter

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 port1.1-2 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 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 port1.3-4  
Yamaha(config-if)# switchport mode access  
Yamaha(config-if)# switchport access vlan 2000  
Yamaha(config-if)# exit
```

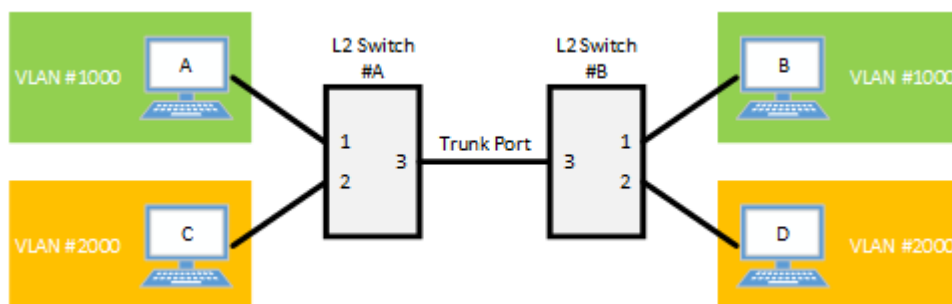
4. VLANの設定を確認します。

```
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)
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)
1000	VLAN1000	ACTIVE	port1.1(u) port1.3(t)
2000	VLAN2000	ACTIVE	port1.2(u) port1.3(t)

プライベートVLAN の設定

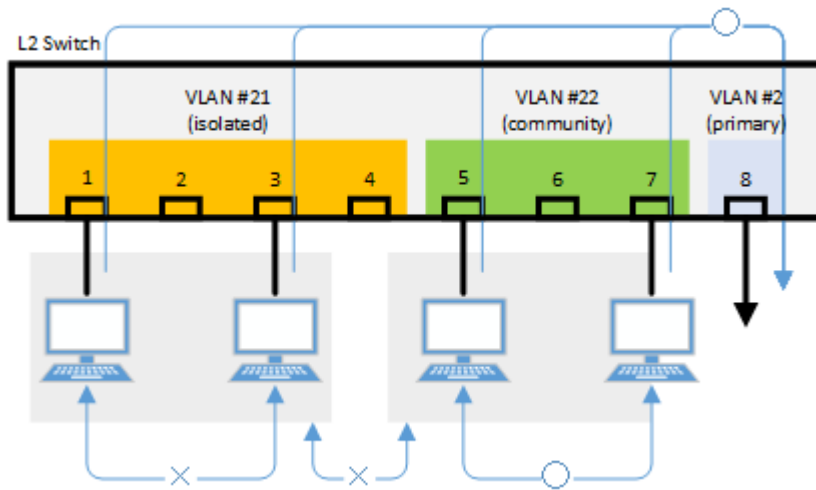
本製品にプライベートVLANを設定し、以下を実現します。

ポート1～7に接続したホストは、ポート8に接続した回線を介してインターネットなどの外部回線に接続します

ポート1～4に接続したホスト間の通信は遮断します (アイソレートVLAN : VLAN #21)

ポート5～7に接続したホスト間の通信は許可します (コミュニティVLAN : VLAN #22)

ポート1～4に接続したホストとポート5～7に接続したホスト間の通信は遮断します



1. プライベートVLANで使用するVLAN IDを定義します。

```
Yamaha(config)# vlan database ①
Yamaha(config-vlan)# vlan 2 ②
Yamaha(config-vlan)# vlan 21
Yamaha(config-vlan)# vlan 22
Yamaha(config-vlan)# private-vlan 2 primary ③
Yamaha(config-vlan)# private-vlan 21 isolated ④
Yamaha(config-vlan)# private-vlan 22 community ⑤
Yamaha(config-vlan)# private-vlan 2 association add 21 ⑥
Yamaha(config-vlan)# private-vlan 2 association add 22
Yamaha(config-vlan)# exit
```

- ① vlanモードに移行
- ② VLANの作成
- ③ Primary VLANの設定
- ④ Isolated VLANの設定
- ⑤ Community VLANの設定
- ⑥ Primary VLANとの関連付け

2. LANポート1～4にアイソレートVLAN(VLAN #21)を設定します。

```
Yamaha(config)#interface port1.1-4 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 21 ③
Yamaha(config-if)#switchport mode private-vlan host ④
Yamaha(config-if)#switchport private-vlan host-association 2 add 21
Yamaha(config-if)#exit
```

- ① interface modeに移行
- ② アクセスポートに設定
- ③ VLAN #21に所属
- ④ プライベートVLANのホストポートに設定

3. LANポート5～7にコミュニティVLAN(VLAN #22)を設定します。

```

Yamaha(config)#interface port1.5-7 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 22 ③
Yamaha(config-if)#switchport mode private-vlan host ④
Yamaha(config-if)#switchport private-vlan host-association 2 add 22
Yamaha(config-if)#exit

```

- ① interfaceモードに移行
- ② アクセスポートに設定
- ③ VLAN #22に所属
- ④ プライベートVLANのホストポートに設定

4. LANポート8にプライマリVLAN(VLAN #2)を設定します。(プロミスカスポート)

```

Yamaha(config)#interface port1.8 ①
Yamaha(config-if)#switchport mode access ②
Yamaha(config-if)#switchport access vlan 2 ③
Yamaha(config-if)#switchport mode private-vlan promiscuous ④
Yamaha(config-if)#switchport private-vlan mapping 2 add 21
Yamaha(config-if)#switchport private-vlan mapping 2 add 22
Yamaha(config-if)#exit

```

- ① interfaceモードに移行
- ② アクセスポートに設定
- ③ VLAN #2に所属
- ④ プライベートVLANのプロミスカスポートに設定

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	
2	VLAN0002	ACTIVE	port1.8(u)
21	VLAN0021	ACTIVE	port1.1(u) port1.2(u) port1.3(u) port1.4(u)
22	VLAN0022	ACTIVE	port1.5(u) port1.6(u) port1.7(u)

```

Yamaha#show vlan private-vlan

```

PRIMARY	SECONDARY	TYPE	INTERFACES
2	21	isolated	port1.1 port1.2 port1.3 port1.4
2	22	community	port1.5 port1.6 port1.7

ボイスVLAN の設定

本製品にボイスVLANを設定し、以下を実現します。

ポート1にIP電話を接続します。IP電話のもう一つのLANポートにPCを接続します。
LLDP-MED を利用して、本製品からIP電話に以下の設定をします。

- ・ IP電話の音声トラフィックとして、VLAN #2 の 802.1qタグつきフレームを送受信する。
- ・ PCのデータ通信はタグなしフレームを送受信する。
- ・ 音声トラフィック送信時のCoS値は 6 を使用する。

1. ボイスVLANで使用するVLAN IDを定義します。

```
Yamaha(config)# vlan database ①  
Yamaha(config-vlan)# vlan 2 ②  
Yamaha(config-vlan)# exit
```

① vlanモードに移行

② VLANの作成

2. LANポート #1にボイスVLANを設定します。

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

① interface modeに移行

② アクセスポートに設定

③ 音声トラフィックをVLAN #2のタグ付きフレームに設定

④ 音声トラフィックのCoS値を6に設定

3. LANポート #1にQoSを設定します。

```
Yamaha(config)#qos enable ①  
Yamaha(config)#interface port1.1 ②  
Yamaha(config-if)#qos trust cos ③  
Yamaha(config-if)#exit
```

① QoSの有効化

② interfaceモードに移行

③ トラストモードをCoSに設定

4. LANポート #1にLLDP-MEDの送受信を設定します。

```
Yamaha(config)#interface port1.1 ①  
Yamaha(config-if)#lldp-agent ②  
Yamaha(lldp-agent)#tlv-select med ③
```



```
Yamaha(lldp-agent)#set lldp enable txrx ④  
Yamaha(lldp-agent)#exit  
Yamaha(config-if)#exit  
Yamaha(config)#lldp run ⑤  
Yamaha(config)#exit
```

- ① interfaceモードに移行
- ② LLDPエージェントの作成、モード遷移
- ③ LLDP-MED TLVの設定
- ④ LLDP送受信モードの設定
- ⑤ LLDP機能の有効化

注意事項

プライベートVLANに属しているポートは、ホストポートに限り、リンクアグリゲーション論理インターフェースとして束ねることができません。

関連文書

- ・ [マルチプルVLAN](#)

マルチプルVLAN

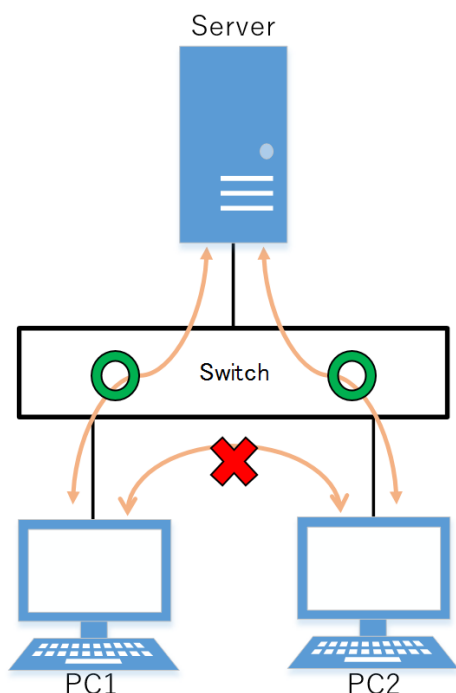
機能概要

マルチプルVLANでは、ポートをマルチプルVLANグループに所属させることで、同じマルチプルVLANグループに属さないポートとの通信を遮断できます。

また、ひとつのポートを複数のマルチプルVLANグループに参加させることもできます。

この機能を使うことで、以下使用例のように端末間の通信のみを遮断したい、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

動作仕様

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/SFPポート、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にもマルチプルVLANグループ設定が適用されます。

以下の機能との併用が可能です。これらの機能はマルチプルVLANグループ設定にしたがって通信可否が制御されます。

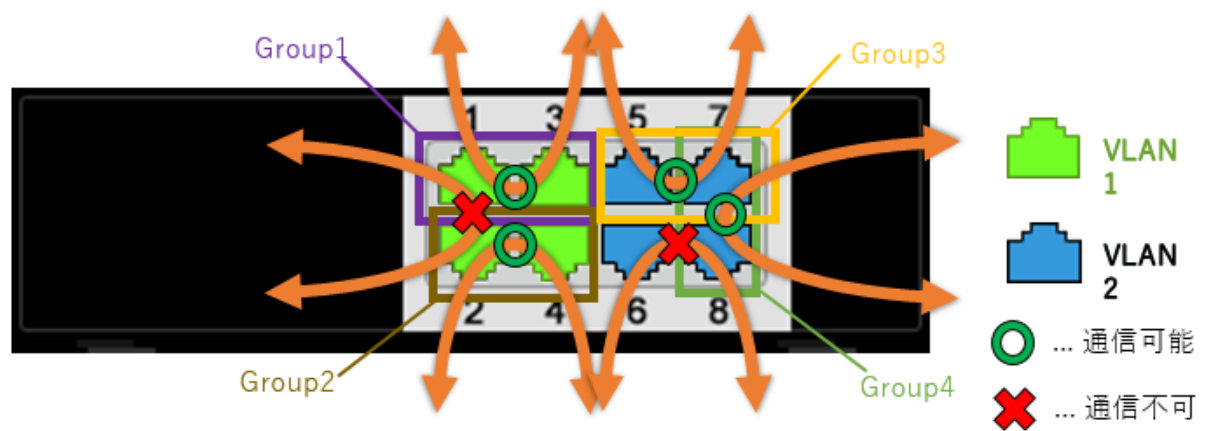
- ・ ポートベースVLAN/タグVLAN/ボイスVLAN
- ・ ポート認証

マルチプルVLANグループは最大 **256** グループです。

マルチプルVLANグループの各インターフェースへの設定状態は、 **show vlan multiple-vlan group** コマンドで確認できます。

マルチプルVLANグループ間の通信例

- マルチプルVLANグループの通信例



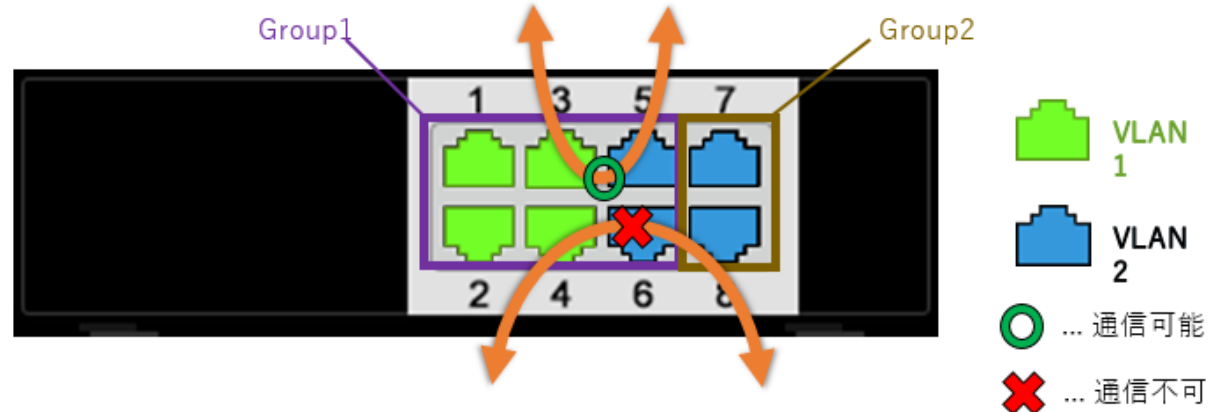
上図のようなマルチプルVLANグループ設定(Group #1 ~ #4) の場合、特定ポートA/B間の通信可否とその理由は以下の表のようになります。

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

また、マルチプルVLANグループに所属しないポート同士の通信は、同一VLAN内であれば通信可能です。

VLAN間ルーティング可能な場合の通信例

- VLAN間ルーティング通信例



L3スイッチではVLAN間ルーティングが可能です。VLAN間ルーティングにおいても、ハードウェアでルーティ

ング処理されるパケットについてはマルチプルVLANグループによる通信の制御が可能です。
上図のようなマルチプルVLANグループ設定(Group #1 ~ #2) 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
port1.3 (Group 1)	port1.5 (Group 1)	可	マルチプルVLANグループ #1 に所属
port1.4 (Group 1)	port1.8 (Group 2)	不可	マルチプルVLANグループが違うため

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。

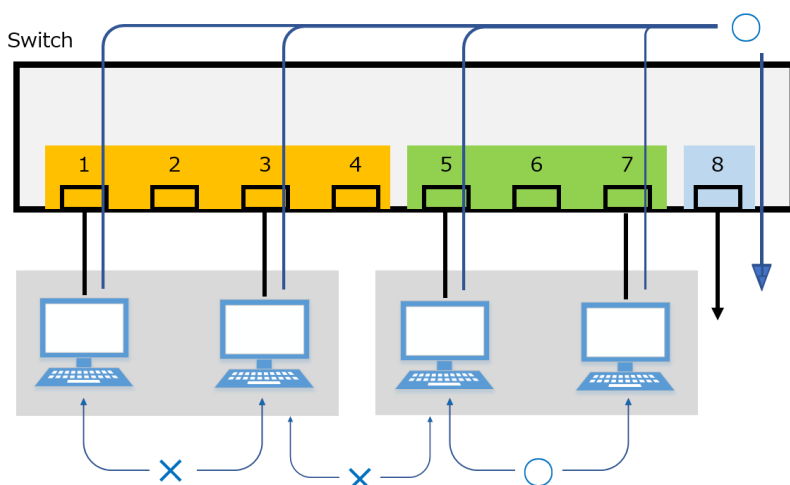
操作項目	操作コマンド
マルチプルVLANグループの設定	switchport multiple-vlan group
マルチプルVLANグループの名前の設定	multiple-vlan group name
マルチプルVLAN設定時のYMPIフレーム透過機能の設定	multiple-vlan transfer ympi
マルチプルVLANの表示	show vlan multiple-vlan

コマンド実行例

マルチプルVLANの設定例1

本製品にマルチプルVLANを設定し、以下を実現します。

ポート1～7に接続したホストは、ポート8に接続した回線を介してインターネットなどの外部回線に接続します
ポート1～4に接続したホスト間の通信は遮断します
ポート5～7に接続したホスト間の通信は許可します
ポート1～4に接続したホストとポート5～7に接続したホスト間の通信は遮断します



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 に所属

- ・ port1.2 : マルチプルVLANグループ #2 に所属
- ・ port1.3 : マルチプルVLANグループ #3 に所属
- ・ port1.4 : マルチプルVLANグループ #4 に所属
- ・ port1.5 : マルチプルVLANグループ #5 に所属
- ・ port1.6 : マルチプルVLANグループ #5 に所属
- ・ port1.7 : マルチプルVLANグループ #5 に所属
- ・ port1.8 : マルチプルVLANグループ #1 , #2 , #3 , #4 , #5 に所属

1. マルチプルVLANグループ #1 の名前を "Network1" に設定します。

```
Yamaha(config)# multiple-vlan group 1 name Network1 ①
```

- ① マルチプルVLANグループ #1 の名前の設定

2. マルチプルVLANグループ #5 の名前を "Network5" に設定します。

```
Yamaha(config)# multiple-vlan group 5 name Network5 ①
```

- ① マルチプルVLANグループ #5 の名前の設定

3. port1.1～port1.4をそれぞれマルチプルVLANグループ #1 ～ #4 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)# exit  
Yamaha(config)# interface port1.2 ③  
Yamaha(config-if)# switchport multiple-vlan group 2 ④  
Yamaha(config-if)# exit  
Yamaha(config)# interface port1.3 ⑤  
Yamaha(config-if)# switchport multiple-vlan group 3 ⑥  
Yamaha(config-if)# exit  
Yamaha(config)# interface port1.4 ⑦  
Yamaha(config-if)# switchport multiple-vlan group 4 ⑧  
Yamaha(config-if)# exit
```

- ① インターフェースモードに移行
- ② マルチプルVLANグループの設定
- ③ インターフェースモードに移行
- ④ マルチプルVLANグループの設定
- ⑤ インターフェースモードに移行
- ⑥ マルチプルVLANグループの設定
- ⑦ インターフェースモードに移行
- ⑧ マルチプルVLANグループの設定

4. port1.5～port1.7をマルチプルVLANグループ #5 に所属させます。

```
Yamaha(config)# interface port1.5-7 ①
```

```
Yamaha(config-if)# switchport multiple-vlan group 5 ②
Yamaha(config-if)# exit
```

- ① インターフェースモードに移行
- ② マルチプルVLANグループの指定

5. port1.8をマルチプルVLANグループ #1, #2, #3, #4, #5 に所属させます。

```
Yamaha(config)# interface port1.8 ①
Yamaha(config-if)# switchport multiple-vlan group 1-5 ②
Yamaha(config-if)# exit
```

- ① インターフェースモードに移行
- ② マルチプルVLANグループの指定

6. マルチプルVLANグループの設定を確認します。

```
Yamaha>show vlan multiple-vlan
GROUP ID  Name                               Member ports
=====  =====
1         Network1                          port1.1 port1.8
2         GROUP0002                        port1.2 port1.8
3         GROUP0003                        port1.3 port1.8
4         GROUP0004                        port1.4 port1.8
5         Network5                        port1.5 port1.6
                                         port1.7 port1.8
```

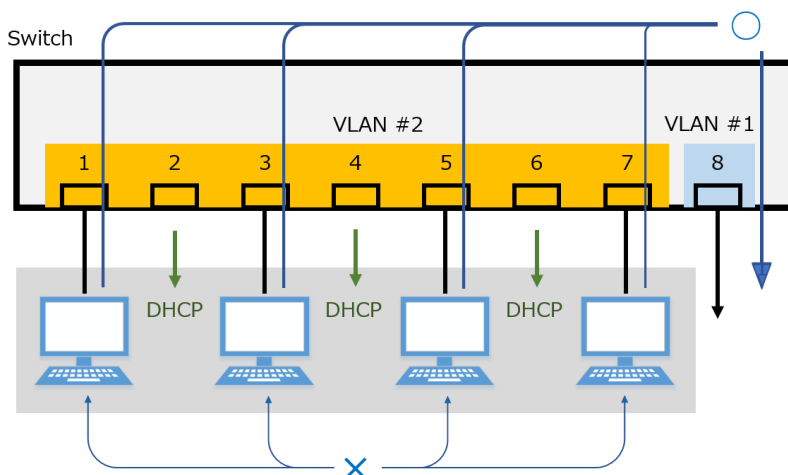
マルチプルVLANの設定例2

本製品にマルチプルVLANを設定し、以下を実現します。

ポート1～7に接続したホストは、ポート8に接続した回線を介してインターネットなどの外部回線に接続します
ポート1～7に接続したホストはVLAN #2 に所属させ、DHCPサーバー機能をつかってIPアドレスを割り当てま
す

VLAN #2 のIPアドレスは「192.168.110.240/24」とし、配布するアドレスの範囲は「192.168.110.2-
192.168.110.191/24」とします

ポート1～7に接続したホスト間の通信は遮断します



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 に所属
- port1.2 : マルチプルVLANグループ #2 に所属
- port1.3 : マルチプルVLANグループ #3 に所属
- port1.4 : マルチプルVLANグループ #4 に所属
- port1.5 : マルチプルVLANグループ #5 に所属
- port1.6 : マルチプルVLANグループ #6 に所属
- port1.7 : マルチプルVLANグループ #7 に所属
- port1.8 : マルチプルVLANグループ #1 , #2 , #3 , #4 , #5 , #6 , #7 に所属
- port1.1～port1.7までをVLAN #2 に割り当てます。

```
Yamaha(config)# interface port1.1-7
Yamaha(config-if)# switchport access vlan 2
Yamaha(config-if)#
```

```
Yamaha(config)# interface vlan2
Yamaha(config-if)# ip address 192.168.110.240/24
```

- DHCPプール「pool_vlan2」を作成します。

```
Yamaha(config)# dhcp pool pool_vlan2
Yamaha(config-dhcp)①
```

① DHCPモードへ移行

- VLAN #2 のネットワーク部「192.168.110.0/24」をDHCPプールに設定します。

```
Yamaha(config-dhcp)# network 192.168.110.0/24
```

- 配布するアドレスの範囲「192.168.110.2-192.168.110.191」をDHCPプールに設定します。

```
Yamaha(config-dhcp)# range 192.168.110.2 192.168.110.191
```

- DHCPのオプションで通知するデフォルトゲートウェイと、DNSサーバーをDHCPプールに設定します。

```
Yamaha(config-dhcp)# default-router 192.168.110.240 ①
Yamaha(config-dhcp)# dns-server 192.168.110.1 ②
Yamaha(config-dhcp)# exit ③
```

① デフォルトゲートウェイのアドレスは、192.168.110.240(自分自身)

② DNSサーバーのアドレスは、192.168.110.1

③ DHCPモード終了

- vlan2にて、DHCPサーバー機能を動作させます。

```
Yamaha(config)# interface vlan2 ①  
Yamaha(config-if)# dhcp-server enable ②  
Yamaha(config-if)# exit ③
```

- ① インターフェースモードに移行
- ② インターフェースのDHCPサーバー機能有効
- ③ インターフェースモード終了

- システム全体のDHCPサーバー機能を動作させます。

```
Yamaha(config)# dhcp-server enable ①
```

- ① システム全体のDHCPサーバー機能有効

- port1.1～port1.7をそれぞれマルチプルVLANグループ #1 ～ #7 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)# exit  
Yamaha(config)# interface port1.2 ③  
Yamaha(config-if)# switchport multiple-vlan group 2 ④  
Yamaha(config-if)# exit  
Yamaha(config)# interface port1.3 ⑤  
Yamaha(config-if)# switchport multiple-vlan group 3 ⑥  
Yamaha(config-if)# exit  
Yamaha(config)# interface port1.4 ⑦  
Yamaha(config-if)# switchport multiple-vlan group 4 ⑧  
Yamaha(config-if)# exit  
Yamaha(config)# interface port1.5 ... (インターフェースモードに移行)Yamaha(config-if)#  
switchport multiple-vlan group 5 ... (マルチプルVLANグループの設定)Yamaha(config-if)#  
exitYamaha(config)# interface port1.6 ... (インターフェースモードに移行)Yamaha(config-if)#  
switchport multiple-vlan group 6 ... (マルチプルVLANグループの設定)Yamaha(config-if)#  
exitYamaha(config)# interface port1.7 ... (インターフェースモードに移行)Yamaha(config-if)#  
switchport multiple-vlan group 7 ... (マルチプルVLANグループの設定)Yamaha(config-if)# exit
```

- ① インターフェースモードに移行
- ② マルチプルVLANグループの設定
- ③ インターフェースモードに移行
- ④ マルチプルVLANグループの設定
- ⑤ インターフェースモードに移行
- ⑥ マルチプルVLANグループの設定
- ⑦ インターフェースモードに移行
- ⑧ マルチプルVLANグループの設定

- port1.8をマルチプルVLANグループ #1 ～ #7 に所属させます。


```
Yamaha(config)# interface port1.8 ①
Yamaha(config-if)# switchport multiple-vlan group 1-7 ②
Yamaha(config-if)# exit
```

① インターフェースモードに移行

② マルチプルVLANグループの指定

- ・ マルチプルVLANグループの設定を確認します。

```
Yamaha>show vlan multiple-vlan
GROUP ID  Name                               Member ports
=====  =====
1          GROUP0001                          port1.1 port1.8
2          GROUP0002                          port1.2 port1.8
3          GROUP0003                          port1.3 port1.8
4          GROUP0004                          port1.4 port1.8
5          GROUP0005                          port1.5 port1.8
6          GROUP0006                          port1.6 port1.8
7          GROUP0007                          port1.7 port1.8
```

注意事項

本機能の注意事項は以下のとおりです。

- ・ プライベートVLANとの併用はできません。
- ・ 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 packets 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。
 - スパニングツリーのブロック状態
 - IGMPスヌーピング/MLDスヌーピングの状態
 - ループ検出のブロック状態
- ・ VLAN間ルーティングでは、ハードウェア処理でルーティングする packets のみがマルチプルVLANによる通信制限が適用されます。
CPUを介したVLAN間ルーティングには適用されません。
- ・ マルチプルVLANが設定されている場合、ヤマハ無線アクセスポイントの管理フレームであるYMPIフレームが透過されます。
そのため、複数のヤマハ無線アクセスポイントが異なるマルチプルVLANグループに所属していても、クラスター管理機能または無線LANコントローラー機能を利用することが可能です。

関連文書

- ・ [VLAN](#)

スパニングツリー

機能概要

スパニングツリーは、ネットワーク上の経路の冗長性を確保しつつ、ループを防止する機能です。

通常、L2スイッチは、ブロードキャスト packets を隣接するスイッチへフラッディングします。ループ状にネットワークが構成されていた場合、スイッチは互いにフラッディングし合うため、ループが発生してしまいます。

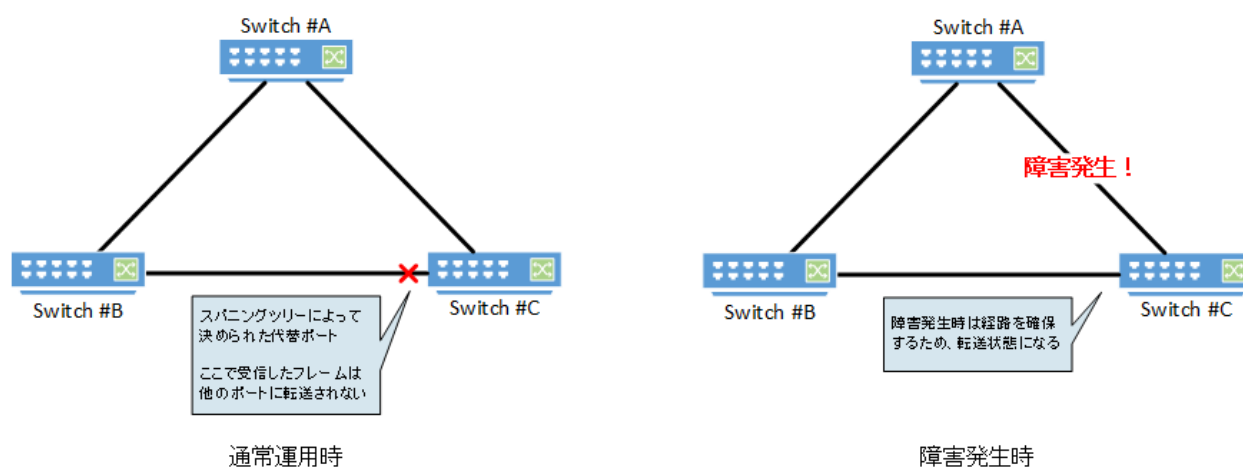
これにより帯域幅とスイッチのCPUリソースは大幅に減少してしまいます。

スパニングツリーは、このような物理的にループ状に構成された場合でも、論理的にはツリー構造になるように各ポートの役割を決め、ブロードキャスト packets が回り続けることのない構成にします。

またリンク障害が発生した場合でも、障害を検出しツリーを再構築することで回復します。

本製品では、STP, RSTP, MSTPをサポートしています。

・スパニングツリー機能概要



用語の定義

STP : Spanning Tree Protocol (802.1d)

スパニングツリープロトコル (STP) は、BPDU (ブリッジプロトコルデータユニット) メッセージを交換することで、ループを回避できるようにします。

本製品では、**IEEE802.1d** と **RFC4188** をサポートしています。

RSTP : Rapid Spanning Tree Protocol (802.1w)

ラピッドスパニングツリープロトコル (RSTP) は、STPを拡張したもので、構成の変更やリンク障害があった場合に、STPよりも高速にスパニングツリーを回復できます。

本製品では、**IEEE802.1w** と **RFC4318** をサポートしています。

MSTP : Multiple Spanning Tree Protocol (802.1s)

マルチプルスパニングツリープロトコル (MSTP) は、STPとRSTPを更に拡張したもので、VLANをインスタンスというグループにまとめ、そのグループ単位でスパニングツリーを構成します。

これにより経路の負荷を分散することができます。

本製品では、**IEEE802.1s** をサポートしています。

機能詳細

本製品は、MSTP によるルート構成を柔軟にするため、以下の機能に対応します。

- ・プライオリティの設定
 - ブリッジプライオリティの設定
 - ポートプライオリティの設定
- ・パスコストの設定
- ・タイムアウトの設定
 - 転送遅延時間の設定
 - 最大エージング時間の設定
- ・エッジポートの指定 (Port Fast設定)
- ・BPDU ガード
- ・BPDU フィルタリング
- ・ルートガード

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。

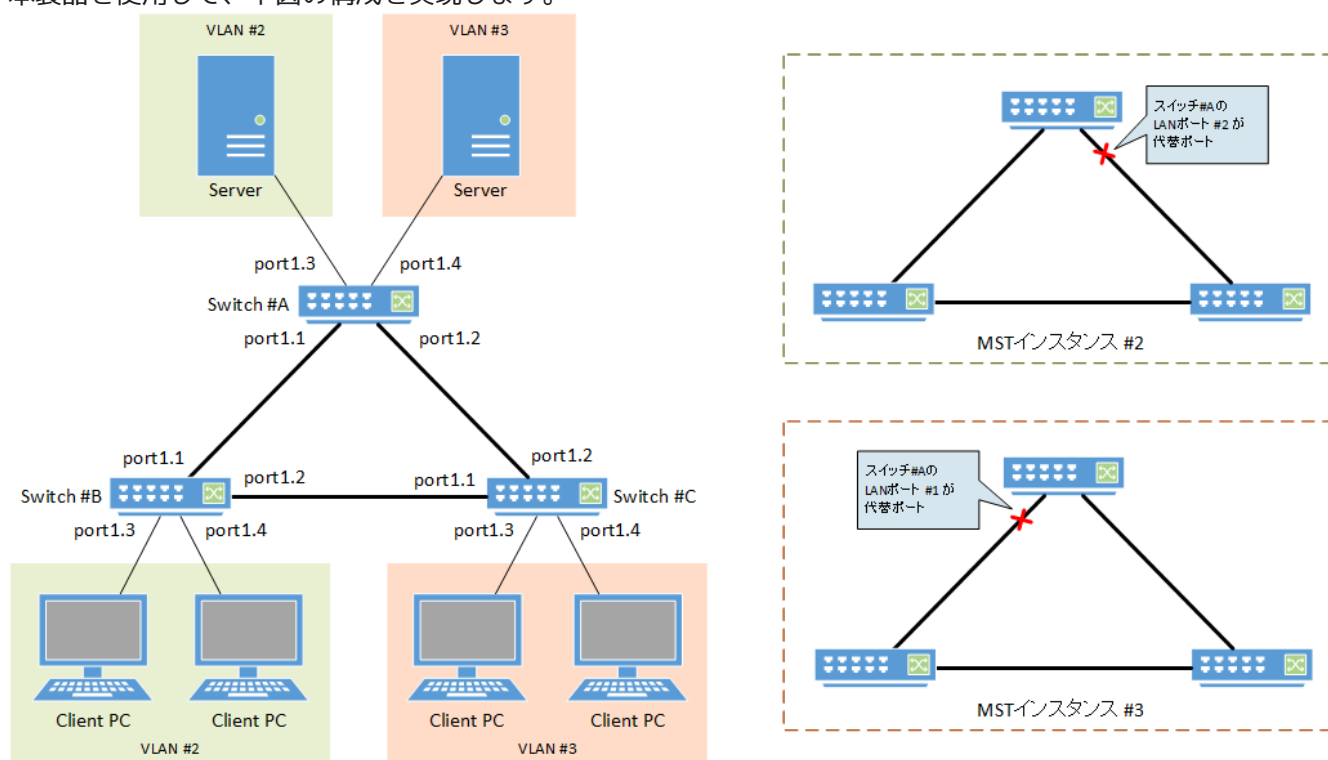
操作項目	操作コマンド
システムのスパニングツリーの設定	spanning-tree shutdown
転送遅延時間の設定	spanning-tree forward-time
最大エージング時間の設定	spanning-tree max-age
ブリッジのプライオリティ設定	spanning-tree priority
インターフェースのスパニングツリーの設定	spanning-tree
インターフェースのリンクタイプの設定	spanning-tree link-type
インターフェースのBPDUフィルタリングの設定	spanning-tree bpdu-filter
インターフェースのBPDUガードの設定	spanning-tree bpdu-guard
インターフェースのパスコストの設定	spanning-tree path-cost
インターフェースのプライオリティの設定	spanning-tree priority
インターフェースのエッジポートの設定	spanning-tree edgeport
スパニングツリーの状態の表示	show spanning-tree
スパニングツリーのBPDUの統計情報の表示	show spanning-tree statistics
プロトコル互換モードのクリア	clear spanning-tree detected protocols
MSTモードへの移行	spanning-tree mst configuration
MSTインスタンスの生成	instance

操作項目	操作コマンド
MSTインスタンスに対するVLANの設定	instance vlan
MSTインスタンスのプライオリティの設定	instance priority
MSTリージョン名の設定	region
MSTリージョンのリビジョン番号の設定	revision
インターフェースに対するMSTインスタンスの設定	spanning-tree instance
MSTインスタンスにおけるインターフェースのプライオリティの設定	spanning-tree instance priority
MSTインスタンスにおけるインターフェースのパスコストの設定	spanning-tree instance path-cost
MSTリージョン情報の表示	show spanning-tree mst config
MSTP情報の表示	show spanning-tree mst
MSTインスタンス情報の表示	show spanning-tree mst instance

コマンド実行例

MSTP 設定例

本製品を使用して、下図の構成を実現します。



- ・ MSTインスタンスを使用してスパニングツリーを構成します。
- ・ 負荷分散のため、MSTインスタンス(VLAN)ごとに経路が異なるように設定します。
- ・ PCが接続されるLANポートはエッジポートにします。

■ 設定手順

1. [スイッチ#A] VLAN #2 と VLAN #3 を定義します。

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

① VLAN #2 の定義

② VLAN #3 の定義

2. [スイッチ#A] CISTのプライオリティを設定します。

```
Yamaha(config)#spanning-tree priority 8192 ①
```

① CISTのプライオリティを8192にする

3. [スイッチ#A] MSTの設定を行います。

```
Yamaha(config)#spanning-tree mst configuration
Yamaha(config-mst)#region Sample ①
Yamaha(config-mst)#revision 1 ②
Yamaha(config-mst)#instance 2 vlan 2 ③
Yamaha(config-mst)#instance 3 vlan 3 ④
Yamaha(config-mst)#exit
```

① MSTリージョン名を「Sample」にする

② MSTリビジョン番号を1にする

③ MSTインスタンス #2 を定義し、VLAN #2 と関連付ける

④ MSTインスタンス #3 を定義し、VLAN #3 と関連付ける

4. [スイッチ#A] LANポート #1 ~ #2 をトランクポートに設定し、VLAN #2 ~ #3 に所属させます。
また、MSTインスタンス #2 ~ #3 を設定します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#switchport mode trunk ①
Yamaha(config-if)#switchport trunk allowed vlan add 2,3 ②
Yamaha(config-if)#spanning-tree instance 2 ③
Yamaha(config-if)#spanning-tree instance 3 ④
Yamaha(config-if)#exit
(上記設定をLANポート #2に対しても行います。)
```

① トランクポートに設定する

② VLAN #2 ~ #3 に所属させる

③ MSTインスタンス #2 を設定する

④ MSTインスタンス #3 を設定する

5. [スイッチ#A] LANポート #3 をアクセスポートに設定し、VLAN #2 に所属させます。
また、MSTインスタンス #2 を設定し、エッジポートにします。

```
Yamaha(config)#interface port1.3
```

```
Yamaha(config-if)#switchport mode access ①
Yamaha(config-if)#switchport access vlan 2 ②
Yamaha(config-if)#spanning-tree instance 2 ③
Yamaha(config-if)#spanning-tree edgeport ④
Yamaha(config-if)#exit
```

- ① アクセスポートに設定する
- ② VLAN #2 に所属させる
- ③ MSTインスタンス #2 を設定する
- ④ エッジポートに設定する

6. [スイッチ#A] LANポート #4 をアクセスポートに設定し、VLAN #3 に所属させます。
また、MSTインスタンス #3 を設定し、エッジポートにします。

```
Yamaha(config)#interface port1.4
Yamaha(config-if)#switchport mode access ①
Yamaha(config-if)#switchport access vlan 3 ②
Yamaha(config-if)#spanning-tree instance 3 ③
Yamaha(config-if)#spanning-tree edgeport ④
Yamaha(config-if)#exit
```

- ① アクセスポートに設定する
- ② VLAN #3 に所属させる
- ③ MSTインスタンス #3 を設定する
- ④ エッジポートに設定する

7. [スイッチ#B] VLAN #2 と VLAN #3 を定義します。

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

- ① VLAN #2 の定義
- ② VLAN #3 の定義

8. [スイッチ#B] CISTのプライオリティを設定します。

```
Yamaha(config)#spanning-tree priority 16384 ①
```

- ① CISTのプライオリティを16384にする

9. [スイッチ#B] MSTの設定を行います。

```
Yamaha(config)#spanning-tree mst configuration
Yamaha(config-mst)#region Sample ①
Yamaha(config-mst)#revision 1 ②
Yamaha(config-mst)#instance 2 vlan 2 ③
Yamaha(config-mst)#instance 2 priority 8192 ④
```

```
Yamaha(config-mst)#instance 3 vlan 3 ⑤  
Yamaha(config-mst)#instance 3 priority 16384 ⑥  
Yamaha(config-mst)#exit
```

- ① MSTリージョン名を「Sample」にする
- ② MSTリビジョン番号を1にする
- ③ MSTインスタンス #2 を定義し、VLAN #2 と関連付ける
- ④ MSTインスタンス #2 のプライオリティを8192にする
- ⑤ MSTインスタンス #3 を定義し、VLAN #3 と関連付ける
- ⑥ MSTインスタンス #3 のプライオリティを16384にする

10. [スイッチ#B] LANポート #1 ～ #2 をトランクポートに設定し、VLAN #2 ～ #3 に所属させます。
また、MSTインスタンス #2 ～ #3 を設定します。

```
Yamaha(config)#interface port1.1  
Yamaha(config-if)#switchport mode trunk ①  
Yamaha(config-if)#switchport trunk allowed vlan add 2,3 ②  
Yamaha(config-if)#spanning-tree instance 2 ③  
Yamaha(config-if)#spanning-tree instance 3 ④  
Yamaha(config-if)#exit  
(上記設定をLANポート #2に対しても行います。)
```

- ① トランクポートに設定する
- ② VLAN #2 ～ #3 に所属させる
- ③ MSTインスタンス #2 を設定する
- ④ MSTインスタンス #3 を設定する

11. [スイッチ#B] LANポート #3 をアクセスポートに設定し、VLAN #2 に所属させます。
また、MSTインスタンス #2 を設定し、エッジポートにします。

```
Yamaha(config)#interface port1.3  
Yamaha(config-if)#switchport mode access ①  
Yamaha(config-if)#switchport access vlan 2 ②  
Yamaha(config-if)#spanning-tree instance 2 ③  
Yamaha(config-if)#spanning-tree edgeport ④  
Yamaha(config-if)#exit  
⑤
```

- ① アクセスポートに設定する
- ② VLAN #2 に所属させる
- ③ MSTインスタンス #2 を設定する
- ④ エッジポートに設定する
- ⑤ 上記設定をLANポート #4に対しても行います。

12. [スイッチ#C] VLAN #2 と VLAN #3 を定義します。

```
Yamaha(config)#vlan database
```

```
Yamaha(config-vlan)#vlan 2 ①  
Yamaha(config-vlan)#vlan 3 ②  
Yamaha(config-vlan)#exit
```

① VLAN #2 の定義

② VLAN #3 の定義

13. [スイッチ#C] MSTの設定を行います。

```
Yamaha(config)#spanning-tree mst configuration  
Yamaha(config-mst)#region Sample ①  
Yamaha(config-mst)#revision 1 ②  
Yamaha(config-mst)#instance 2 vlan 2 ③  
Yamaha(config-mst)#instance 2 priority 16384 ④  
Yamaha(config-mst)#instance 3 vlan 3 ⑤  
Yamaha(config-mst)#instance 3 priority 8192 ⑥  
Yamaha(config-mst)#exit
```

① MSTリージョン名を「Sample」にする

② MSTリビジョン番号を1にする

③ MSTインスタンス #2 を定義し、VLAN #2 と関連付ける

④ MSTインスタンス #2 のプライオリティを16384にする

⑤ MSTインスタンス #3 を定義し、VLAN #3 と関連付ける

⑥ MSTインスタンス #3 のプライオリティを8192にする

14. [スイッチ#C] LANポート #1 ~ #2 をトランクポートに設定し、VLAN #2 ~ #3 に所属させます。
また、MSTインスタンス #2 ~ #3 を設定します。

```
Yamaha(config)#interface port1.1  
Yamaha(config-if)#switchport mode trunk ①  
Yamaha(config-if)#switchport trunk allowed vlan add 2,3 ②  
Yamaha(config-if)#spanning-tree instance 2 ③  
Yamaha(config-if)#spanning-tree instance 3 ④  
Yamaha(config-if)#exit  
(上記設定をLANポート #2に対しても行います。)
```

① トランクポートに設定する

② VLAN #2 ~ #3 に所属させる

③ MSTインスタンス #2 を設定する

④ MSTインスタンス #3 を設定する

15. [スイッチ#C] LANポート #3 をアクセスポートに設定し、VLAN #3 に所属させます。
また、MSTインスタンス #3 を設定し、エッジポートにします。

```
Yamaha(config)#interface port1.3  
Yamaha(config-if)#switchport mode access ①  
Yamaha(config-if)#switchport access vlan 3 ②  
Yamaha(config-if)#spanning-tree instance 3 ③  
Yamaha(config-if)#spanning-tree edgeport ④
```



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

⑤

- ① アクセスポートに設定する
- ② VLAN #3 に所属させる
- ③ MSTインスタンス #3 を設定する
- ④ エッジポートに設定する
- ⑤ 上記設定をLANポート #4に対しても行います。

16. LANケーブルを接続します。

17. [スイッチ#A] CISTの構成を確認します。

```
Yamaha>show spanning-tree |include Root Id
% Default: CIST Root Id 200100a0deaeb920 ①
% Default: CIST Reg Root Id 200100a0deaeb920

Yamaha>show spanning-tree |include Role
% port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated - State Forwarding
% port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State Forwarding
% port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State Forwarding
% port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State Forwarding
% port1.5: Port Number 909 - Ifindex 5005 - Port Id 0x838d - Role Disabled - State Discarding
% port1.6: Port Number 910 - Ifindex 5006 - Port Id 0x838e - Role Disabled - State Discarding
% port1.7: Port Number 911 - Ifindex 5007 - Port Id 0x838f - Role Disabled - State Discarding
% port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Disabled - State Discarding
% port1.9: Port Number 913 - Ifindex 5009 - Port Id 0x8391 - Role Disabled - State Discarding
% port1.10: Port Number 914 - Ifindex 5010 - Port Id 0x8392 - Role Disabled - State Discarding
```

① プライオリティが高いスイッチ #A がCISTのルートブリッジになる

18. [スイッチ#B] CISTの構成を確認します。

```
Yamaha>show spanning-tree |include Root Id
% Default: CIST Root Id 200100a0deaeb920 ①
% Default: CIST Reg Root Id 200100a0deaeb920

Yamaha>show spanning-tree |include Role
% port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State Forwarding
% port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State Forwarding
% port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State
```

```
Forwarding
% port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State Forwarding
% port1.5: Port Number 909 - Ifindex 5005 - Port Id 0x838d - Role Disabled - State Discarding
% port1.6: Port Number 910 - Ifindex 5006 - Port Id 0x838e - Role Disabled - State Discarding
% port1.7: Port Number 911 - Ifindex 5007 - Port Id 0x838f - Role Disabled - State Discarding
% port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Disabled - State Discarding
% port1.9: Port Number 913 - Ifindex 5009 - Port Id 0x8391 - Role Disabled - State Discarding
% port1.10: Port Number 914 - Ifindex 5010 - Port Id 0x8392 - Role Disabled - State Discarding
```

① プライオリティが高いスイッチ #A がCISTのルートブリッジになる

19. [スイッチ#C] CISTの構成を確認します。

```
Yamaha>show spanning-tree |include Root Id
% Default: CIST Root Id 200100a0deaeb920 ①
% Default: CIST Reg Root Id 200100a0deaeb920

Yamaha>show spanning-tree |include Role
% port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Alternate - State Discarding ②
% port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Rootport - State Forwarding
% port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State Forwarding
% port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State Forwarding
% port1.5: Port Number 909 - Ifindex 5005 - Port Id 0x838d - Role Disabled - State Discarding
% port1.6: Port Number 910 - Ifindex 5006 - Port Id 0x838e - Role Disabled - State Discarding
% port1.7: Port Number 911 - Ifindex 5007 - Port Id 0x838f - Role Disabled - State Discarding
% port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Disabled - State Discarding
% port1.9: Port Number 913 - Ifindex 5009 - Port Id 0x8391 - Role Disabled - State Discarding
% port1.10: Port Number 914 - Ifindex 5010 - Port Id 0x8392 - Role Disabled - State Discarding
```

① プライオリティが高いスイッチ #A がCISTのルートブリッジになる

② プライオリティが低いスイッチ #C のLAN #1 ポートがCISTの代替ポートになる

20. [スイッチ#A] MSTインスタンス #2 の構成を確認します。

```
Yamaha>show spanning-tree mst instance 2 |include Root Id
% Default: MSTI Root Id 200200a0deaeb879 ①
```

```
Yamaha>show spanning-tree mst instance 2 |include Role
% port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State Forwarding
% port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Alternate - State Discarding ②
% port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State Forwarding
```

- ① プライオリティが高いスイッチ #B がMSTインスタンス #2 のルートブリッジになる
- ② プライオリティが低いスイッチ #A のLAN #2 ポートがMSTインスタンス #2 の代替ポートになる

21. [スイッチ#B] MSTインスタンス #2 の構成を確認します。

```
Yamaha>show spanning-tree mst instance 2 |include Root Id
% Default: MSTI Root Id 200200a0deaeb879 ①

Yamaha>show spanning-tree mst instance 2 |include Role
% port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated - State Forwarding
% port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State Forwarding
% port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State Forwarding
% port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State Forwarding
```

- ① プライオリティが高いスイッチ #B がMSTインスタンス #2 のルートブリッジになる

22. [スイッチ#C] MSTインスタンス #2 の構成を確認します。

```
Yamaha>show spanning-tree mst instance 2 |include Root Id
% Default: MSTI Root Id 200200a0deaeb879 ①

Yamaha>show spanning-tree mst instance 2 |include Role
% port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport - State Forwarding
% port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State Forwarding
```

- ① プライオリティが高いスイッチ #B がMSTインスタンス #2 のルートブリッジになる

23. [スイッチ#A] MSTインスタンス #3 の構成を確認します。

```
Yamaha>show spanning-tree mst instance 3 |include Root Id
% Default: MSTI Root Id 200300a0deaeb83d ①

Yamaha>show spanning-tree mst instance 3 |include Role
% port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Alternate - State Discarding ②
% port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Rootport - State Forwarding
% port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State
```

Forwarding

- ① プライオリティが高いスイッチ #C がMSTインスタンス #3 のルートブリッジになる
- ② プライオリティが低いスイッチ #A のLAN #1 ポートがMSTインスタンス #3 の代替ポートになる

24. [スイッチ#B] MSTインスタンス #3 の構成を確認します。

```
Yamaha>show spanning-tree mst instance 3 |include Root Id
% Default: MSTI Root Id 200300a0deaeb83d ①

Yamaha>show spanning-tree mst instance 3 |include Role
% port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated - State Forwarding
% port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Rootport - State Forwarding
```

- ① プライオリティが高いスイッチ #C がMSTインスタンス #3 のルートブリッジになる

25. [スイッチ#C] MSTインスタンス #3 の構成を確認します。

```
Yamaha>show spanning-tree mst instance 3 |include Root Id
% Default: MSTI Root Id 200300a0deaeb83d ①

Yamaha>show spanning-tree mst instance 3 |include Role
% port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated - State Forwarding
% port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Designated - State Forwarding
% port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Designated - State Forwarding
% port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated - State Forwarding
```

- ① プライオリティが高いスイッチ #C がMSTインスタンス #3 のルートブリッジになる

注意事項

- ・ 本製品の **STP**、**RSTP** は、**MSTPの下位互換** により対応します。

関連文書

- ・ [Layer 2機能 : VLAN](#)
- ・ STP
 - IEEE802.1d
 - RFC4188
- ・ RSTP
 - IEEE802.1w
 - RFC4318
- ・ MSTP
 - IEEE802.1s

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/SFPポートおよび論理インターフェース (以降、「ループ検出対応インターフェース」という) 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、ループ検出対応インターフェースごとに有効・無効制御が行えます。
ループ検出対応インターフェース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。
 - ループ検出対応インターフェースごとの設定は、 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。(初期状態では機能していません)
 - システム全体の設定: 無効
 - ループ検出対応インターフェースの設定: 有効
3. ループ検出、スパニングツリープロトコルともにシステム全体の設定が **有効** に設定されている場合、ループ検出対応インターフェースの設定は、スパニングツリープロトコルを優先的に扱います。
4. 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」という) を、リンクアップしているループ検出対応インターフェースから **2秒間隔** で送信します。
ただし、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、LDFの受信ポートは以下の動作を行います。
 - **Port Shutdown**
 - 送信と受信のループ検出対応インターフェースが同じ場合、該当ポートをシャットダウンします。
 - シャットダウン後、5分後にリンクアップし、LDFの送信を再開します。(ループが発生している場合は、本動作が繰り返されます。)
 - 5分の監視時間内に該当ポートをリンクアップしたい場合は、 **no shutdown** コマンドを使用します。

■ Port Blocking

- 以下のいずれかに該当した場合、LDFの受信ポートはLDF以外のフレームを遮断します。
 - 論理インターフェースから送信したLDFを、LAN/SFPポートで受信した
 - スタティック論理インターフェースから送信したLDFを、LACP論理インターフェースで受信した
 - 送信と受信のインターフェース種別が同じで、インターフェース番号の大きいほうがLDFを受信した
- 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したループ検出対応インターフェースは、5秒間、自身が送信したLDFを検出できなかった場合、ループが解消したと判断し、通常の通信を再開します。

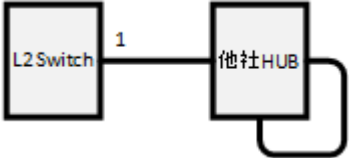
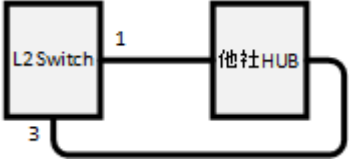
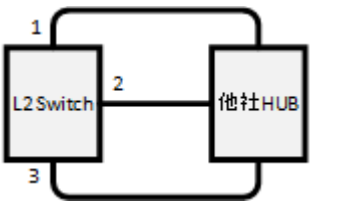
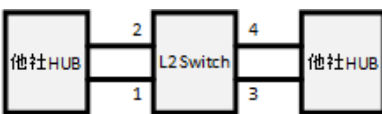
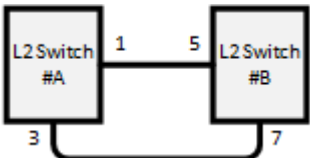
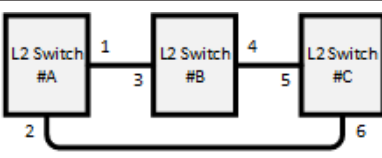
■ Port Detected

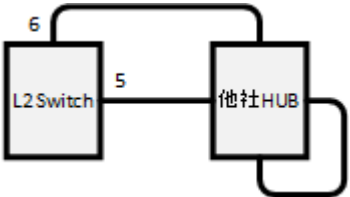
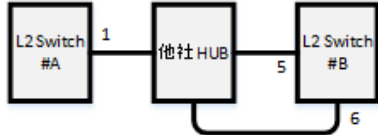
- 以下のいずれかに該当した場合、他のポートでブロッキングを行っているため、LDFの受信ポートは通常の通信を継続します。
 - LAN/SFPポートから送信したLDFを、論理インターフェースで受信した
 - LACP論理インターフェースから送信したLDFを、スタティック論理インターフェースで受信した
 - 送信と受信のインターフェース種別が同じで、インターフェース番号の小さいほうがLDFを受信した
 - 。ループを検出すると、本製品のポートランプ表示を専用の状態に変更し、以下のSYSLOGメッセージを出力します。
 - [LOOP]: inf: Detected Loop! : port1.1, 1.3 ..., sa1,3 ..., po1,3 <1>
 - 。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, 1.3 ..., sa1,3 ..., po1,3 ...
5. ループ検出したループ検出対応インターフェースで Shutdown / Blocking 動作を行わずに、強制的に Detected 動作にすることができます。
- 。本設定は、 **loop-detect blocking disable** コマンドを使用します。
 - 。本設定が有効な場合、次に大きな番号のポートでPort Blockingが実施されます。(Shutdown動作は行われません。)
6. 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。(MODEボタンのある機種では、MODEボタンの3秒間長押しでも可能。)
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。(ポートランプ表示を復旧し、SYSLOGメッセージを出力します。)
7. 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 (ループ検出対応インターフェース単位の状態)
8. ループ検出機能が無効な状態で、ループ検出対応インターフェースで 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、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。
9. 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

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。

・ループ検出例

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 : Shutdown
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

ループ検出ケース	構成例	ループ検出状況
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Shutdownします。 port1.5 : Shutdown port1.6 : Shutdown
8		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はShutdown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。 スイッチ#A port1.1 : Shutdown スイッチ#B port1.5 : Detected スイッチ#B port1.6 : Blocking

関連コマンド

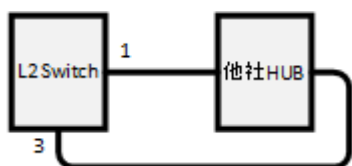
関連コマンドについて、以下に示します。
コマンドの詳細は、コマンドリファレンスを参照願います。

操作項目	操作コマンド
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(インターフェース)	loop-detect enable/disable
ループ検出時のPort Blockingの設定	loop-detect blocking enable/disable
ループ検出時のPort Blocking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

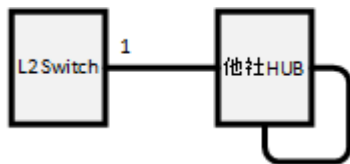
コマンド実行例

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)#spanning-tree disable ①
Yamaha(config-if)#loop-detect enable ②
Yamaha(config-if)#loop-detect blocking enable ③
(上記設定をLANポート #3 に対しても行います。)
```

- ① LANポートごとのスパニングツリー機能を無効にする

- ② LANポートごとのループ検出機能を有効にする

- ③ Blockingを有効にする

- ・ LANポートごとのループ検出機能の有効化、blockingの有効化は、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。

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	port-blocking	status
port1.1	enable(*)	enable	Normal
port1.2	enable	enable	Normal
port1.3	enable(*)	enable	Normal
port1.4	enable	enable	Normal
port1.5	enable	enable	Normal
port1.6	enable	enable	Normal
port1.7	enable	enable	Normal
port1.8	enable	enable	Normal
port1.9	enable	enable	Normal
:	:	:	:

(*): Indicates that the feature is enabled.

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	port-blocking	status
port1.1	enable(*)	enable	Detected ①
port1.2	enable	enable	Normal
port1.3	enable(*)	enable	Blocking ②
port1.4	enable	enable	Normal
port1.5	enable	enable	Normal
port1.6	enable	enable	Normal
port1.7	enable	enable	Normal
port1.8	enable	enable	Normal
port1.9	enable	enable	Normal
:	:	:	:

(*): Indicates that the feature is enabled.

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	port-blocking	status
port1.1	enable(*)	enable	Shutdown ①
port1.2	enable	enable	Normal
port1.3	enable(*)	enable	Normal
port1.4	enable	enable	Normal
port1.5	enable	enable	Normal
port1.6	enable	enable	Normal
port1.7	enable	enable	Normal
port1.8	enable	enable	Normal
port1.9	enable	enable	Normal
:	:	:	:

(*): Indicates that the feature is enabled.

① LANポート #1 はShutdown状態になる

注意事項

- ・ 論理インターフェースに束ねるLAN/SFPポートは、ループ検出の設定 (有効・無効、Port Blocking) が同じである必要があります。
 - ・ ループ検出の設定が異なるLAN/SFPポートは論理インターフェースとして束ねることはできません。
 - ・ ループ検出の設定は論理インターフェースに所属しているLAN/SFPポートに対して行うことができません。

関連文書

- ・ [スパニングツリー](#)
- ・ [LED制御](#)

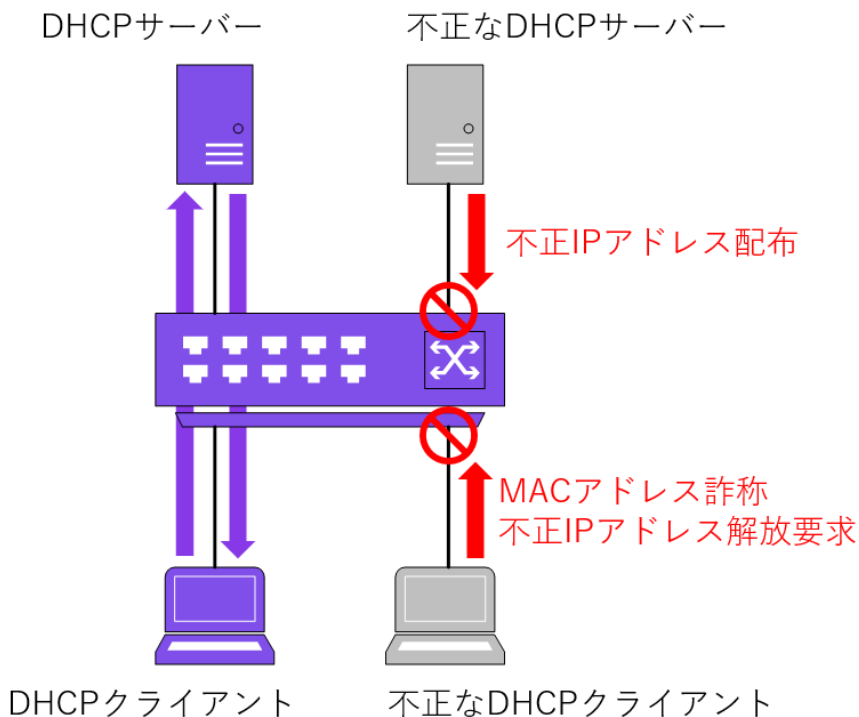
DHCPスヌーピング

機能概要

DHCPスヌーピングは、DHCPサーバーとクライアント間でやりとりされるDHCPメッセージを監視して、不正なDHCPメッセージをフィルタリングする機能です。

本機能を利用することで、以下のようなセキュリティ向上の効果が期待できます。

- ・ 不正なDHCPサーバーからのIPアドレスの配布を抑止する
- ・ 不正なDHCPクライアントからのIPアドレス解放やIPアドレス重複検出を抑止する
- ・ MACアドレスの詐称を抑止する
- ・ Option 82の詐称を抑止する



用語の定義

Trusted ポート

DHCPスヌーピングによるDHCPメッセージのフィルタリングが無効なポート。信頼されたDHCPサーバーを接続する。

Untrusted ポート

DHCPスヌーピングによるDHCPメッセージのフィルタリングが有効なポート。DHCPクライアントを接続する。

IfIndex

インターフェースの識別番号。IfIndexの割り当ては[インターフェース基本機能](#)を参照。

機能詳細

DHCPスヌーピングの有効化

DHCPスヌーピングを有効にするには、グローバルコンフィグレーションモードで **ip dhcp snooping enable** コマンドを実行したうえで、さらに、DHCPスヌーピングを有効にするVLANのインターフェースモードで **ip dhcp snooping enable** コマンドを実行する必要があります。

DHCPスヌーピング機能に関するシステムの設定状況は、**show ip dhcp snooping** コマンドで確認することができます。

DHCPスヌーピング機能に関するインターフェースの設定状況は、**show ip dhcp snooping interface** コマンドで確認することができます。

バインディングデータベース

DHCPスヌーピングを有効にすると、DHCPサーバーとDHCPクライアント間のメッセージを監視して、バインディングデータベースを構築します。

DHCPサーバーからIPアドレスが配布されたときに、以下のDHCPクライアントの情報がバインディングデータベースに登録されます。

- DHCPクライアントからDHCPメッセージを受信したVLAN ID
- DHCPクライアントからDHCPメッセージを受信したインターフェース情報
- DHCPクライアントのMACアドレス
- DHCPクライアントのIPアドレス
- リース時間

バインディングデータベースのエントリー情報は、**show ip dhcp snooping binding** コマンドで確認することができます。

登録されたエントリー情報は、エントリーのリース時間が満了するか、DHCPクライアントからDHCP RELEASEメッセージを受信したときに削除されます。

また、**clear ip dhcp snooping binding** コマンドでバインディングデータベースをクリアすることができます。

バインディングデータベースのエントリーは最大 **512** 件登録できます。

DHCPスヌーピングのポート種別

DHCPスヌーピングでは、**ip dhcp snooping trust** コマンドでLAN/SFPポートを「Trustedポート」と「Untrustedポート」の2つに分類します。

Trustedポートには信頼されたDHCPサーバーを接続し、UntrustedポートにはDHCPクライアントを接続します。

それぞれの動作仕様は以下のとおりです。

- Trustedポート
 - DHCPメッセージのフィルタリングを行わずに、そのまま転送します。
- Untrustedポート
 - DHCPサーバーから送信されるDHCPパケットを破棄します。
 - バインディングデータベースにMACアドレスが登録されていて、かつ登録インターフェースとは異なるインターフェースから以下のDHCPパケットを受信したとき、当該DHCPパケットを破棄します。
 - IPアドレス解放要求 (DHCP RELEASE)
 - IPアドレス重複検出通知 (DHCP DECLINE)
 - MACアドレス検証が有効の場合、DHCPパケットの送信元MACアドレスとクライアントハードウェアアドレス (chaddr) を比較し、一致しない場合は当該DHCPパケットを破棄します。

- Option 82が有効の場合、DHCPクライアントから受信したDHCPパケットに既にOption 82情報が付与されているとき、当該DHCPパケットを破棄します。

Untrustedポートでは、MACアドレス検証はデフォルトで **有効** になっており、**ip dhcp snooping verify mac-address** コマンドで無効にすることができます。

UntrustedポートにDHCPエージェントを接続する必要がある場合、DHCPエージェントはDHCPクライアントからのDHCPパケットの送信元MACアドレスを書き換えるため、MACアドレス検証を無効にする必要があります。

Option 82

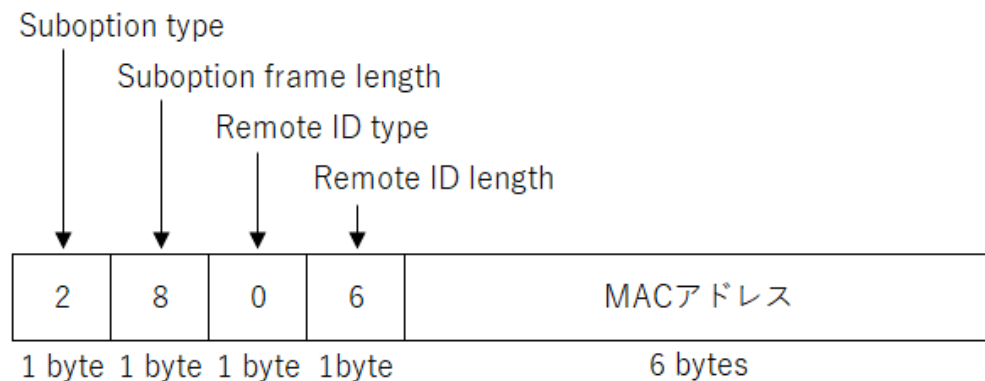
DHCPスヌーピングが有効のとき、Option 82を有効にすると、UntrustedポートでDHCPクライアントから受信したDHCPパケットにOption 82情報を付与します。

また、UntrustedポートにDHCPクライアントが直接接続されているとき、DHCPサーバーからDHCPクライアント宛てに送信された戻りパケットのOption 82情報を削除して転送します。

Option 82はデフォルトで **有効** です。Option 82情報として、以下の情報が付与されます。

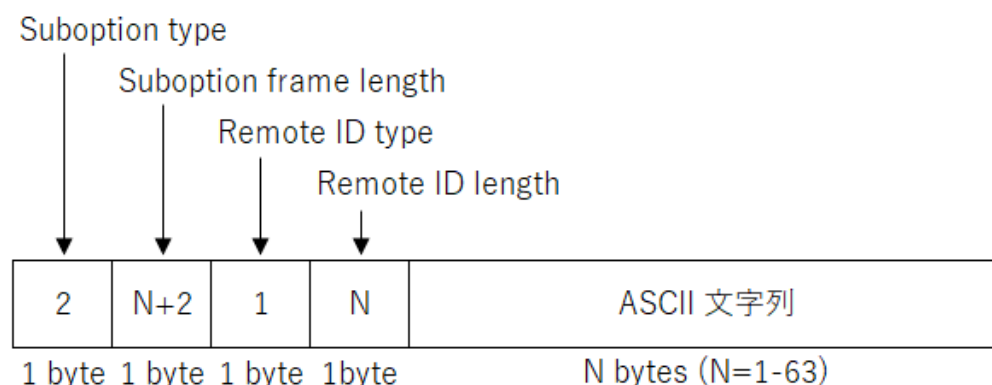
- Remote-ID

- デフォルトでは、本機のMACアドレスが付与されます。
 - フォーマット： Suboption type=2, Remote-ID type=0 (Default)



- **ip dhcp snooping information option format remote-id** コマンドで、Remote-IDに63文字以内の任意の文字列（半角英数字および半角記号）を付与することができます。

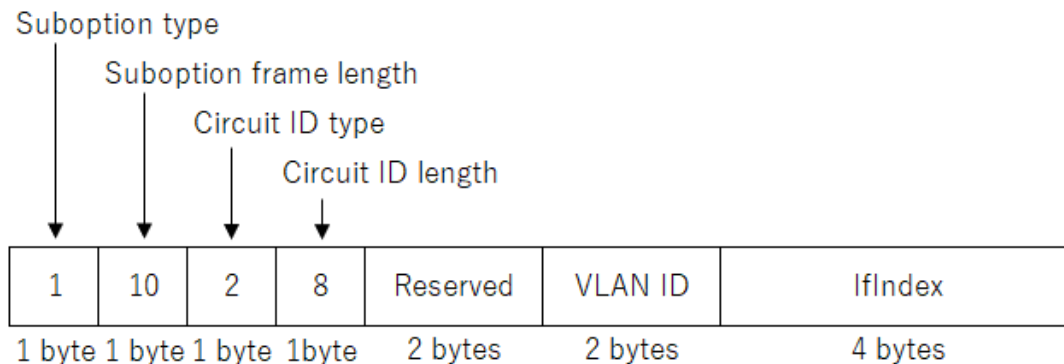
- フォーマット： Suboption type=2, Remote-ID type=1



- Circuit-ID

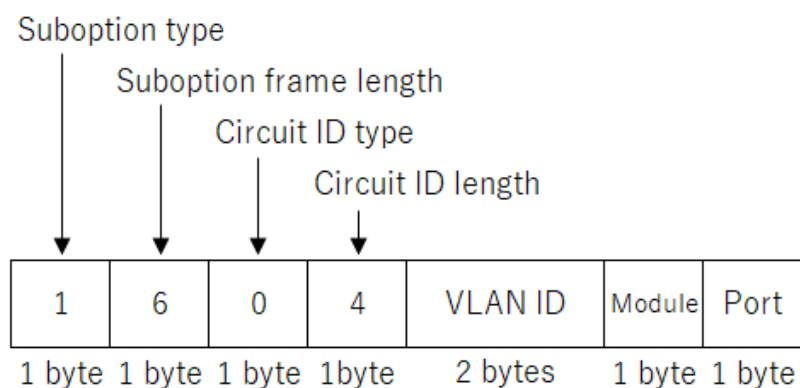
- デフォルトでは、DHCPクライアントからDHCPパケットを受信したVLAN IDとIfIndexが付与されます。

- フォーマット： Suboption type=1, Circuit-ID type=2 (Default)



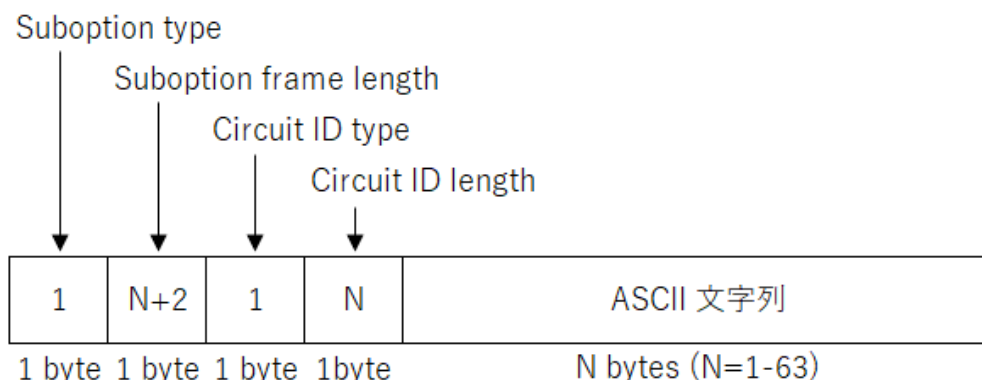
- **ip dhcp snooping information option format-type circuit-id** コマンドで、Circuit-IDの情報を、DHCPクライアントからDHCPパケットを受信したVLAN IDとポート番号に変更することができます。「Module」には物理ポートの場合はスタック番号が付与され、スタンドアロン時またはスタック非対応機種では、「1」が設定されます。論理ポートの場合は、スタティック「0x11」、LACP「0x12」が固定で設定されます。

- フォーマット： Suboption type=1, Circuit-ID type=0



- また、Circuit-IDに63文字以内の任意の文字列（半角英数字および半角記号）を指定することもできます。

- フォーマット： Suboption type=1, Circuit-ID type=1



• Subscriber-ID

- デフォルトでは付与されません。
- **ip dhcp snooping subscriber-id** コマンドで、対象ポートのSubscriber-IDに50文字以内の任意の文字列（半角英数字および半角記号）を設定することで、Option 82情報に含めることができます。

Option 82が有効のとき、Untrustedポートで既にOption 82情報が付与されたDHCPパケットを受信した場合、Option 82情報の詐称を抑止するために、そのDHCPパケットを破棄します。
UntrustedポートにOption 82を付与するDHCPリレーエージェントを接続する場合、**ip dhcp snooping information option allow-untrusted** コマンドで、UntrustedポートにおけるOption 82を含むDHCPパケットの転送を許可する必要があります。

DHCPパケットのレート制限

DHCPスヌーピングが有効のとき、**ip dhcp snooping limit rate** コマンドで、システム全体で1秒あたりに受信可能なDHCPパケット数を設定することができます。
受信レートの上限を超過した場合、受信レートを越えた受信DHCPパケットは破棄されます。デフォルトではレート制限は行いません。

DHCPスヌーピングの統計情報

DHCPスヌーピングにより破棄されたDHCPパケットの統計情報は、**show ip dhcp snooping statistics** コマンドで確認することができます。

ただし、DHCPパケットのレート制限により破棄されたパケットは本統計情報に含まれません。
統計情報は、**clear ip dhcp snooping statistics** コマンドで削除することができます。

SYSLOGへの出力

DHCPスヌーピングの受信DHCPパケット検査によりDHCPパケットが破棄された場合、INFOレベルのSYSLOGに破棄理由を出力することができます。
SYSLOGへの出力の有効/無効の設定は **ip dhcp snooping logging** コマンドで設定することができ、デフォルトではSYSLOGに出力します。
出力されるSYSLOGメッセージは以下のとおりです。

レベル	出力条件	SYSLOGメッセージ
INFO	UntrustedポートでDHCPサーバーパケットを受信した	2022/07/21 09:00:00: [DHCP SN]:inf: DHCP dropped due to prohibited message type, VLAN 1, port1.1, DHCP OFFER, 1234.4567.abcd
INFO	登録外インターフェースからDHCP RELEASE/DECLINEを受信した	2022/07/21 09:00:00: [DHCP SN]:inf: DHCP dropped due to source interface mismatch, VLAN 1, port1.1, DHCP RELEASE, 5c5a.c7d6.9e1e
INFO	送信元MACとchaddrが一致しない	2022/07/21 09:00:00: [DHCP SN]:inf: DHCP dropped due to source mac mismatch, VLAN 1, port1.1, DHCP INFORM, 001c.4321.abcd
INFO	UntrustedポートでOption 82付きパケットを受信した	2022/07/21 09:00:00: [DHCP SN]:inf: DHCP dropped due to option82 value, VLAN 1, port1.1, DHCP INFORM, 5c5a.c7d6.9e1e

関連コマンド

関連コマンドについて、以下に示します。

操作項目	操作コマンド
DHCPスヌーピングの有効/無効設定（システム）	ip dhcp snooping enable/disable
DHCPスヌーピングの有効/無効設定（VLAN）	ip dhcp snooping enable/disable

操作項目	操作コマンド
DHCPスヌーピングのポート種別設定	ip dhcp snooping trust
MACアドレス検証の有効/無効設定	ip dhcp snooping verify mac-address enable/disable
Option 82の有効/無効設定	ip dhcp snooping information option enable/disable
Option 82付きパケットのUntrustedポート受信許可設定	ip dhcp snooping information option allow-untrusted
Option 82のRemote-IDの設定	ip dhcp snooping information option format remote-id
Option 82のCircuit-IDの設定	ip dhcp snooping information option format-type circuit-id
Subscriber-IDの設定	ip dhcp snooping subscriber-id
DHCPパケット受信レート制限の設定	ip dhcp snooping limit rate
DHCPパケット破棄時SYSLOG出力の有効/無効設定	ip dhcp snooping logging enable/disable
DHCPスヌーピングのシステム設定情報表示	show ip dhcp snooping
DHCPスヌーピングのインターフェース設定情報表示	show ip dhcp snooping interface
バインディングデータベースの表示	show ip dhcp snooping binding
DHCPスヌーピングの統計情報表示	show ip dhcp snooping statistics
バインディングデータベースのクリア	clear ip dhcp snooping binding
DHCPスヌーピングの統計情報クリア	clear ip dhcp snooping statistics

コマンド実行例

信頼するインターフェースを指定

信頼されたDHCPサーバーを接続するインターフェース(LANポート #1)を指定する。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#ip dhcp snooping trust
Yamaha(config-if)#exit
```

DHCPスヌーピングの有効化

システム及びVLAN #1 のDHCPスヌーピングを有効にする。

```
Yamaha(config)#ip dhcp snooping enable
Yamaha(config)#interface vlan1
Yamaha(config-if)#ip dhcp snooping enable
Yamaha(config-if)#exit
```

注意事項

- ・ 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
2. 等コストマルチパスの設定

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サーバーに問合せを行うことで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
 - 複数の場合は、デフォルトゲートウェイの値が最も大きいものが優先。
- DHCPv6による自動設定
 - 複数の場合は、最新で取得したものが優先。
 - DHCPv6で通知されたアドレスがリンクローカルアドレスの場合は設定されない。
- DHCP、DHCPv6 の両方が使用されている場合は、DNSサーバーのアドレスを取得したときに、お互いの設定は上書きされる。

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
 - 複数の場合は、デフォルトゲートウェイの値が最も大きいものが優先。

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
- DHCPv6による自動設定
 - 複数の場合は、最新で取得したものが優先。

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256文字以内に収める必要があります** 。

等コストマルチパスの設定

本製品は、以下の機能において **等コストマルチパス** に対応します。

- IPv4 スタティックルーティング
- IPv6 スタティックルーティング
- RIPv1, RIPv2, RIPv3 (対応機種のみ)
- OSPFv2, OSPFv3 (対応機種のみ)

同一の宛先への経路がRIBに複数登録されている場合に、それらの複数の経路がFIBに反映されます。
同一の宛先への経路を **最大8経路** までFIBに登録することができます。初期設定では **4経路** となります。
等コストマルチパスの登録可能数は **maximum-paths** コマンドで変更することができます。
設定変更後は再起動するまで実動作には反映されません。

等コストマルチパスの宛先に対するロードバランスのルールの設定には、 **port-channel load-balance** コマンドを使用します。
port-channel load-balance コマンドによるロードバランスのルールの設定は、リンクアグリゲーションの動作にも影響するため変更する場合は注意が必要です。

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願います。

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
等コストマルチパスの設定	等コストマルチパスの登録可能数設定	maximum-paths
	等コストマルチパスの登録可能数表示	show ip route summary
		show ipv6 route summary
	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

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 or DHCPv6 Client.

等コストマルチパス

等コストマルチパスの登録可能数を5に変更します。

また、ロードバランスのルールとして送信元IPアドレスと送信先IPアドレスを使用します。

1. 等コストマルチパスの登録可能数設定

```
Yamaha(config)#maximum-paths 5
% System Reboot is required for new Maximum-Path value to take effect.
```

。設定を反映させるためには再起動が必要です。

2. ロードバランスのルールとして送信元IPアドレスと送信先IPアドレスを設定

```
Yamaha(config)#port-channel load-balance src-dst-ip
```

3. 現在の等コストマルチパスの登録可能数を確認します。

```
Yamaha(config)#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths   : 5
Route Source      Networks
connected         3
rip               2
Total             5
```

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
4. MTU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。
- 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 **no ip address** コマンドを実行すると、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、**プライマリアドレスを1個** と、**セカンダリーアドレスを4個** まで設定できます。

システム全体 で設定できるIPv4アドレスは **最大8個** までです。
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** を設定してあります。

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アドレスが割り当てられ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機能の有効化は、 **auto-ip enable** コマンドで行います。
- Auto IP機能は、 **1つの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インターフェイスのルート情報の設定
- デフォルトゲートウェイの設定
- スタティックルート情報の設定
- ルート情報の表示

VLANインターフェイスのルート情報

本製品は、VLANインターフェイスに対して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。

VLANインターフェイスに対して設定したIPv4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。

スタティックルート情報の設定

本製品は、 **宛先ネットワークアドレスへのルート(送信するゲートウェイのアドレス)** を静的に設定することができます。

- スタティックルート情報の設定は、 **ip route** コマンドで行います。
- スタティックルート情報の表示は、 **show ip route** コマンドで行います。

経路表と経路選択

ルート情報の設定では、以下に示す2種類のテーブル(表)を使用します。

- RIB (Routing Information Base : IP経路表)
- FIB (Forwarding Information Base : IP転送表)

それぞれの役割は以下のとおりです。

- **RIB**
RIB (Routing Information Base : IP経路表) は、各種経路設定の情報を蓄積するデータベースです。

- RIBに経路が登録されるのは以下の場合です。
 - VLANインターフェースにIPv4アドレスを設定したとき
 - 手動によりスタティックルート情報やデフォルトゲートウェイを設定したとき
 - DHCPメッセージによってデフォルトゲートウェイを学習したとき
- RIBの確認は、 **show ip route database** コマンドで行います。

• FIB

FIB (Forwarding Information Base : IP転送表) 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。

FIBには、RIBに登録されている経路のうち、「最適」と判断され実際にパケット転送に使用される経路だけが登録されます。

- 最適と判断する条件は以下のとおりです。
 - 該当のVLANインターフェースがリンクアップしていること
 - RIBに同一宛先への経路が複数登録されている場合は、以下の優先順位で1つだけ決定する
 1. DHCPメッセージにより学習した経路より、手動設定による経路を優先
 2. ゲートウェイのIPアドレスの値が最も大きい経路を優先
- FIBの確認は、 **show ip route** コマンドで行います。

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 テーブルは、動的/静的エントリーあわせて、 **最大508エントリー** 保存されます。
- 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 テーブルに対する静的エントリーの設定は、 **arp** コマンドで行います。最大255件まで登録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。

MTUの設定

本製品は、 **VLANインターフェース** に対して、MTUを設定することができます。

- MTU値の設定には、 **mtu** コマンドを使用します。
- MTUの初期値は **1500バイト** で、 **68バイト** から **9216バイト** までの範囲で設定することができます。ただし、ipv6 enableが設定されたVLANインターフェースでは、 **1280バイト** から **9216バイト** までの範囲となります。
- 初期値を除いて最大で7つまで異なるMTU値を設定することができます。

- ・ 受信したパケットをルーティングする場合、以下の動作となります。
 - IPv4パケットで、IPv4ヘッダーのTotal Lengthフィールドの値がMTU値を超える場合、分割 (IPフラグメント)して転送します。
DF (Don't Fragment)ビットが付加されたIPv4パケットは、分割 (IPフラグメント)して転送せず、ICMPエラー (Fragmentation needed)を返送してパケットを破棄します。
 - IPv6パケットで、IPv6ヘッダーのPayload Lengthフィールドの値がMTU値を超える場合、ICMPv6エラー (Packet too Big)を返送してパケットを破棄します。
 - **mru** コマンドで設定された受信可能な最大フレームサイズを超えるパケットはルーティングしません。ジャンボフレームを転送する場合、必要に応じて **mru** コマンドで受信可能な最大フレームサイズを調整してください。
 - **分割 (IPフラグメント)して転送する場合、ソフトウェアによる転送となるため転送速度が制限され、なおかつCPU使用率の高騰につながります。**
転送するジャンボフレームのサイズに応じてmtuコマンドを設定することで、分割 (IPフラグメント)が発生しないようにすることを推奨します。
- ・ 本製品がパケットを送信する場合、以下の動作となります。
 - パケットを送信するVLANインターフェースのMTU値に対して、送信するIPv4/IPv6パケットのサイズが大きい場合、MTU値に応じて分割 (IPフラグメント)して送信します。

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願います。

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
	Auto IP機能の有効／無効設定	auto-ip enable/disable
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
	スタティックルート情報の設定	ip route
	スタティックルート情報の表示	show ip route
	ルート情報の表示	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
	静的エントリーの設定	arp
MTUの設定	MTUの設定	mtu

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。

- ・ 本製品の保守は、デフォルトVLAN (VLAN #1) で行います。
 - ・ 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。
 - ・ VLAN #1 につながれたホストからの **Web / TFTP アクセスを許可** します。
1. 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
```

2. デフォルトVLAN (VLAN #1) に対して DHCP 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)#ip address dhcp
```

3. DHCPサーバー より払い出された情報を確認します。

```
Yamaha(config-if)#end
Yamaha#show dhcp lease
Interface vlan1
-----
IP Address:          192.168.1.3
Expires:             YYYY/MM/DD 05:08:41
Renew:               YYYY/MM/DD 19:08:41
Rebind:              YYYY/MM/DD 02:38:41
Server:
Options:
  subnet-mask        255.255.255.0
  default-gateway    192.168.1.1
  dhcp-lease-time    72000
  domain-name-servers 192.168.1.1
  dhcp-server-identifier 192.168.1.1
  domain-name        xxx.xxxxx.xx.xx
```

4. HTTPサーバー、TFTPサーバーに対してデフォルトVLAN (VLAN #1) からのアクセスを許可するように設定します。
設定後、リモートホストからWebアクセスをしてください。

```
Yamaha(config)#http-server interface vlan1 ①
Yamaha(config)#tftp-server interface vlan1 ②
```

① HTTPサーバーのアクセス許可

② TFTPサーバーのアクセス許可

注意事項

特になし

関連文書

- ・ [Layer 2機能 : VLAN](#)
- ・ [保守・運用機能 : 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
4. MTUの設定
5. DHCPv6-PDクライアントの設定

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ります。

- **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**、**DHCPv6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。
- DHCPv6による自動設定を指定した際の動作は、以下となります。
 - **ipv6 address dhcp** コマンドを設定すると、DHCPv6のステートフル動作(IA_NA)が有効になります。
 - 自動設定されている状態で **no ipv6 address dhcp** コマンドを実行すると、取得していたIPv6アドレスの解放メッセージをDHCPv6サーバーに送ります。
 - DHCPv6サーバーより取得した情報は、 **show ipv6 dhcp interface** コマンドで確認します。
- RA (ルータ広告)による自動設定の **ipv6 address autoconfig** コマンドで、パラメーターに **stateless** を指定すると、DHCPv6のステートレス動作が有効になります。
- IPv6アドレスは **1つのVLANインターフェイス** に、 **グローバルアドレス(自動設定、DHCPv6クライアント、DHCPv6-PD を使用したIPv6アドレスの設定を含む)**を5個 までと、 **リンクローカルアドレス**を1個 設定できます。

システム全体 で設定できるIPv6アドレスは **最大8個** までです。

VLANインターフェイ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インターフェイスのルート情報の設定
- デフォルトゲートウェイの設定
- スタティックルート情報の設定
- ルート情報の表示

VLANインターフェイスのルート情報

本製品は、VLANインターフェイスに対して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インターフェイ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。
- **ipv6 address dhcp** コマンド、 **ipv6 dhcp client pd** コマンド、 **ipv6 address autoconfig** コマンド 設定時、RAを送信した機器のアドレスが自動的にデフォルトゲートウェイに追加されます。
 - **ipv6 nd accept-ra-default-routes** コマンドで、RAによるデフォルトゲートウェイ自動登録設定の有効/無効を設定できます。

スタティックルート情報の設定

本製品は、宛先ネットワークアドレスへのルート(送信するゲートウェイのアドレス)を静的に設定することができます。

- ・スタティックルート情報の設定は、**ipv6 route** コマンドで行います。
- ・スタティックルート情報の表示は、**show ipv6 route** コマンドで行います。

経路表と経路選択

ルート情報の設定では、次に示す2種類のテーブル(表)を使用します。

- ・RIB (Routing Information Base : IP経路表)
- ・FIB (Forwarding Information Base : IP転送表)

それぞれの役割は以下のとおりです。

- ・ **RIB**

RIB (Routing Information Base : IP経路表) は、各種経路設定の情報を蓄積するデータベースです。

- RIBに経路が登録されるのは以下の場合です。
 - VLANインターフェースにIPv6アドレスを設定したとき
 - 手動によりスタティックルート情報やデフォルトゲートウェイを設定したとき
- RIBの確認は、**show ipv6 route database** コマンドで行います。

- ・ **FIB**

FIB (Forwarding Information Base : IP転送表) 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。

FIBには、RIBに登録されている経路のうち、「最適」と判断され実際にパケット転送に使用される経路だけが登録されます。

- 最適と判断する条件は以下のとおりです。
 - 該当のVLANインターフェイスがリンクアップしていること
 - RIBに同一宛先への経路が複数登録されている場合は、以下の優先順位で1つだけ決定する
 1. ゲートウェイのIPアドレスの値が最も大きい経路を優先
- FIBの確認は、**show ipv6 route** コマンドで行います。

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** 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は、動的/静的エントリあわせて、**最大128エントリ** 保存されます。
- ・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に対する静的エントリの設定は、 **ipv6 neighbor** コマンドで行います。最大63件まで登録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。

MTUの設定

本製品は、 **VLANインターフェース** に対して、MTUを設定することができます。

- MTU値の設定には、 **mtu** コマンドを使用します。
- MTUの初期値は **1500バイト** で、 **68バイト** から **9216バイト** までの範囲で設定することができます。ただし、ipv6 enableが設定されたVLANインターフェースでは、 **1280バイト** から **9216バイト** までの範囲となります。
- 初期値を除いて最大で7つまで異なるMTU値を設定することができます。
- 受信したパケットをルーティングする場合、以下の動作となります。
 - IPv4パケットで、IPv4ヘッダーのTotal Lengthフィールドの値がMTU値を超える場合、分割 (IPフラグメント)して転送します。
DF (Don't Fragment)ビットが付加されたIPv4パケットは、分割 (IPフラグメント)して転送せず、ICMPエラー (Fragmentation needed)を返送してパケットを破棄します。
 - IPv6パケットで、IPv6ヘッダーのPayload Lengthフィールドの値がMTU値を超える場合、ICMPv6エラー (Packet too Big)を返送してパケットを破棄します。
 - **mru** コマンドで設定された受信可能な最大フレームサイズを超えるパケットはルーティングしません。ジャンボフレームを転送する場合、必要に応じて **mru** コマンドで受信可能な最大フレームサイズを調整してください。
 - **分割 (IPフラグメント)して転送する場合、ソフトウェアによる転送となるため転送速度が制限され、なおかつCPU使用率の高騰につながります。**
転送するジャンボフレームのサイズに応じてmtuコマンドを設定することで、分割 (IPフラグメント)が発生しないようにすることを推奨します。
- 本製品がパケットを送信する場合、以下の動作となります。
 - パケットを送信するVLANインターフェースのMTU値に対して、送信するIPv4/IPv6パケットのサイズが大きい場合、MTU値に応じて分割 (IPフラグメント)して送信します。

DHCPv6-PDクライアントの設定

本製品は、 **VLANインターフェース** に対して、DHCPv6-PDクライアントを設定できます。
DHCPv6-PDサーバーからプレフィックスを取得し、取得したプレフィックスを、アドレス設定や、自身のDHCPv6サーバーの再割り当てに使用できます。

- **ipv6 dhcp client pd prefixname** コマンドを設定すると、DHCPv6-PDのステートフル動作(IA_PD)が有効になります。
- **prefixname** で取得したプレフィックスは、以下で使用できます。
 - **ipv6 address pd** コマンドで、取得したプレフィックスを使用して、IPv6アドレスを設定する。
 - DHCPv6モードの **range** コマンドで、取得したプレフィックスを使用して、DHCPv6サーバーで動的に割り当てるIPv6アドレスの範囲を設定する。(DHCPv6サーバー対応モデルのみ)
 - DHCPv6モードの **prefix-delegation** コマンドで、取得したプレフィックスを使用して、DHCPv6サーバーでプレフィックスの再割り当てを設定する。(DHCPv6サーバー対応モデルのみ)
- DHCPv6サーバーより取得した情報は、 **show ipv6 dhcp interface** コマンドで確認します。

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願います。

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
	DHCPv6-PD を使用したIPv6アドレスの設定	ipv6 address pd
	IPv6アドレスの表示	show ipv6 interface
	IPv6アドレスのRA設定	ipv6 address autoconfig
	DHCPv6クライアントによる動的IPv6アドレスの設定	ipv6 address dhcp
	DHCPv6-PDクライアントの設定	ipv6 dhcp client pd
	RAによるデフォルトゲートウェイの自動登録設定	ipv6 nd accept-ra-default-routes
	DHCPv6クライアントの状態の表示	show ipv6 dhcp interface
	DHCPv6クライアントのリセット	clear ipv6 dhcp client
	DHCPv6クライアント設定時に受信するNDのプレフィックスの設定	ipv6 dhcp client nd-prefix
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
	スタティックルート情報の設定	ipv6 route
	スタティックルート情報の表示	show ipv6 route
	ルート情報の表示	show ipv6 route
Neighbor キャッシュの設定	静的Neighbor キャッシュエントリの設定	ipv6 neighbors
	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
MTUの設定	MTUの設定	mtu

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。

- ・ 本製品の保守は、デフォルトVLAN (VLAN #1) で行います。
- ・ 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。
- ・ VLAN #1 につながれたホストからの **Web / TFTP アクセスを許可** 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	up

3. HTTPサーバー、TFTPサーバーに対してデフォルトVLAN (VLAN #1) からのアクセスを許可するように設定します。

設定後、リモートホストからWebアクセスをしてください。

```
Yamaha(config)#http-server interface vlan1 ①
Yamaha(config)#tftp-server interface vlan1 ②
```

① HTTPサーバーのアクセス許可

② TFTPサーバーのアクセス許可

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。

- ・ 本製品の保守は、デフォルトVLAN (VLAN #1) で行います。
- ・ 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。
- ・ VLAN #1 につながれたホストからの **Web / TFTP アクセスを許可** します。

1. 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

2. 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
```

3. HTTPサーバー、TFTPサーバーに対してデフォルトVLAN (VLAN #1) からのアクセスを許可するように設定します。
設定後、リモートホストからWebアクセスをしてください。

```
Yamaha(config)#http-server interface vlan1 ①
Yamaha(config)#tftp-server interface vlan1 ②
```

- ① HTTPサーバーのアクセス許可
- ② TFTPサーバーのアクセス許可

IPv6ネットワーク環境の設定 (DHCPv6)

本製品にIPv6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。

- ・ 本製品の保守は、デフォルトVLAN (VLAN #1) で行います。
- ・ IPv6アドレスは、デフォルトVLAN (VLAN #1) に対して **DHCPv6** にて自動で設定します。
- ・ VLAN #1 につながれたホストからの **Web / TFTP アクセスを許可** します。

1. デフォルトVLAN (VLAN #1) に対して DHCPv6 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 dhcp ②
```

- ① IPv6を有効にする
- ② DHCPv6を設定する

2. DHCPv6 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          IPv6-Address          Admin-Status  Link-Status
vlan1              *2001:db8:1:aa10::dd37/128
                  fe80::ae44:f2ff:fe84:efdd/64    up            up
```

3. HTTPサーバー、TFTPサーバーに対してデフォルトVLAN (VLAN #1) からのアクセスを許可するように設定します。
設定後、リモートホストからWebアクセスをしてください。

```
Yamaha(config)#http-server interface vlan1 ①
```

```
Yamaha(config)#tftp-server interface vlan1 ②
```

- ① HTTPサーバーのアクセス許可
- ② TFTPサーバーのアクセス許可

IPv6ネットワーク環境の設定 (DHCPv6-PD)

本製品にIPv6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。

- ・ 本製品の保守は、デフォルトVLAN (VLAN #1)で行います。
- ・ VLAN #100 に対して **DHCPv6-PD** を設定して、プレフィックスを取得します。
- ・ IPv6アドレスは、デフォルトVLAN (VLAN #1) に対して、DHCPv6-PDで取得したプレフィックスを使用して設定します。
- ・ VLAN #1 につながれたホストからの **Web / TFTP アクセスを許可** します。

1. VLAN #100 に対して DHCPv6-PD を設定します。

```
Yamaha#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Yamaha(config)#interface vlan100
Yamaha(config-if)#ipv6 enable
Yamaha(config-if)#ipv6 dhcp client pd PD_VLAN100          ... (PD_VLAN100
という名前で、プレフィックスを取得)
Yamaha(config-if)#end
```

2. DHCPv6-PD により取得したプレフィックス情報を確認します。

```
Yamaha#show ipv6 dhcp interface
Interface vlan100
  Client Type      : IA_PD
  Prefix name      : PD_VLAN100
  prefix           : 2001:db8:1:aaf0::/60 ①
  IAID             : 0f28924a
  DUID             : 000100010000000000a0de000000
  preferred lifetime : 604800
  valid lifetime   : 2592000
  expires          : 2023/4/19 08:08:04
```

- ① 2001:db8:1:aaf0::/60 を取得

3. デフォルトVLAN (VLAN #1) に対してIPv6アドレスを設定します。
DHCPv6-PDで取得したプレフィックスを使用して、2001:db8:1:aaf2::1/64 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 pd PD_VLAN100 ::2:0:0:0:1/64 ②
```

- ① IPv6を有効にする

② IPv6アドレスを設定する

4. 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      Admin-Status  Link-Status
vlan1          *2001:db8:1:aaf2::1/64
                fe80::ae44:f2ff:fe84:efdd/64      up            up
```

5. HTTPサーバー、TFTPサーバーに対してデフォルトVLAN (VLAN #1) からのアクセスを許可するように設定します。 設定後、リモートホストからWebアクセスをしてください。

```
Yamaha(config)#http-server interface vlan1 ①
Yamaha(config)#tftp-server interface vlan1 ②
```

① HTTPサーバーのアクセス許可

② TFTPサーバーのアクセス許可

注意事項

- DHCPv6クライアント機能使用中に、対向のDHCPv6サーバーの設定が変更された場合、変更された設定がDHCPv6クライアントに正しく反映されないことがあります。その場合、**clear ipv6 dhcp client** コマンドを用いて、DHCPv6クライアントのリセットを行ってください。
- 本製品のDHCPv6クライアントでは、以下の動作には対応していません。
 - DHCPv6クライアントが送信する、Solicit メッセージの SOL_MAX_RT オプションの要求。
 - SOL_MAX_RT オプションを受信した場合の、DHCPv6クライアント内部の SOL_MAX_RT パラメーターの書き換え。
 - なお、DHCPv6クライアント内部の SOL_MAX_RT パラメーターは、120秒固定で動作します。
 - DHCPv6クライアントが送信する、Request メッセージの INF_MAX_RT オプションの要求。
 - INF_MAX_RT オプションを受信した場合の、DHCPv6クライアント内部の INF_MAX_RT パラメーターの書き換え。
 - なお、DHCPv6クライアント内部の INF_MAX_RT パラメーターは、120秒固定で動作します。

関連文書

- [Layer 2機能 : VLAN](#)
- [保守・運用機能 : リモートアクセス制御](#)
- [Yamaha rtpro: ARPって何？](#)

スタティックルーティング

機能概要

本製品では、IPネットワークでの経路制御としてスタティックルーティング(静的ルート情報)を使用することができます。

管理者がコマンド入力によって明示的にルート情報を登録することができます。

IPv4ネットワークの静的ルートとIPv6ネットワークの静的ルートの両方の設定が可能です。

静的ルート情報には、以下の2種類があります。

タイプ	説明
VLANインターフェースルート情報	ip/ipv6 address コマンドによるIPアドレス設定で自動登録されるルート情報
スタティックルート情報	ip/ipv6 route コマンドによるルート設定で登録されるルート情報

経路表の表示には、 **show ip/ipv6 route** コマンドを使用します。

用語の定義

特になし

機能詳細

VLANインターフェースルート情報

ip/ipv6 address コマンドによるIPアドレス設定で自動登録されるルート情報です。

本製品に直接接続されているネットワークのルート情報となり、インターフェースに関連付けられています。

VLAN1インターフェースにIPアドレスとして192.168.100.1/24を設定し、経路表を表示します。

```
Yamaha(config)# interface vlan1
Yamaha(config-if)# ip address 192.168.100.1/24
Yamaha(config-if)# exit
Yamaha(config)# exit
Yamaha#show ip route
Codes: C - connected, S - static
       * - candidate default

C       192.168.100.0/24 is directly connected, vlan1

Gateway of last resort is not set
```

スタティックルート情報

ip/ipv6 route コマンドによるルート設定で登録されるルート情報です。

特定のネットワーク宛のルートを静的に設定したり、デフォルトゲートウェイを設定することができます。

デフォルトゲートウェイを設定する場合は、宛先ネットワークとして **0.0.0.0/0** を指定します。

ip route コマンドによるIPv4スタティック経路は最大128個まで設定することができます。

ipv6 route コマンドによるIPv6スタティック経路は最大32個まで設定することができます。

172.16.0.0/16宛の経路のゲートウェイを192.168.100.254に設定し、経路表を表示します。

```
Yamaha(config)# ip route 172.16.0.0/24 192.168.100.254
Yamaha(config)# exit
Yamaha# show ip route
Codes: C - connected, S - static
       * - candidate default

S       172.16.0.0/24 [1/0] via 192.168.100.254, vlan1
C       192.168.100.0/24 is directly connected, vlan1

Gateway of last resort is not set
```

デフォルトゲートウェイとして192.168.100.200を設定し、経路表を表示します。

```
Yamaha(config)# ip route 0.0.0.0/0 192.168.100.200
Yamaha(config)# exit
Yamaha# show ip route
Codes: C - connected, S - static
       * - candidate default

Gateway of last resort is 192.168.100.200 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 192.168.100.200, vlan1
S       172.16.0.0/24 [1/0] via 192.168.100.254, vlan1
C       192.168.100.0/24 is directly connected, vlan1
```

経路表の表示

経路表には、実際にパケット転送で使用するルート情報のみが登録されているIP転送表(FIB)とすべてのルート情報が登録されているIP経路表(RIB)の2つがあります。
VLANインターフェースルート情報とスタティックルート情報は、すべてIP経路表に登録されます。そして、その中から実際にパケット転送処理で使用するルート情報のみがIP転送表に登録されます。

IP転送表とIP経路表を表示するには、**show ip/ipv6 route** コマンドを使用します。
経路表では、VLANインターフェースルート情報とスタティックルート情報は以下のように表示されます。

タイプ	表示
VLANインターフェースルート情報	C - connected
スタティックルート情報	S - static

show ip/ipv6 routeでオプションを指定しない場合、IP転送表が表示されます。
show ip/ipv6 routeでdatabaseオプションを指定することでIP経路表を表示することができます。
また、その他のオプションを指定することでサマリー情報や特定の経路の情報のみを表示することもできます。

オプション	説明
IPアドレス	指定したIPアドレス宛にパケットを転送するとき使用されるルート情報を表示する。

オプション	説明
IPアドレスとプレフィックス	指定した情報と一致するルート情報を表示する。
database	設定されている全てのルート情報(IP経路表)を表示する。
summary	IP経路表のサマリー情報を表示する

show ip route コマンドの詳しい使用方法については、コマンドリファレンスを参照してください。

ルート情報の優先度(管理距離)

ルート情報には、Administrative Distanceと一般的に呼ばれる優先度が存在します。これは、VLANインターフェースルート情報とスタティックルート情報で同じ宛先へのルート情報が登録されたとき、どちらを優先するか決めるために使用されます。ルート情報の優先度は、スタティックルーティングに限らずダイナミックルーティングも含めて適用することができます。スタティックルーティングのルート情報の優先度は、**ip route** コマンド末尾のオプションにより1～255の範囲で指定することができます。小さい値のほうが優先度が高くなり、初期状態では以下の優先度となります。

タイプ	優先度の初期値	優先度の変更方法
VLANインターフェースルート情報	なし(他のどのルート情報よりも優先)	設定変更不可。
スタティックルート情報	1	ip/ipv6 route コマンド末尾のオプションにより1～255の範囲で指定可能。

ルーティング機能の有効化

ip/ipv6 forwarding コマンドでルーティング機能の有効/無効を切り替えることができます。初期状態では、IPv4, IPv6ともにルーティング機能は無効となっています。

関連コマンド

関連コマンドについて、以下に示します。
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。

- ・ 関連コマンド一覧

機能種別	操作項目	操作コマンド
ルート情報の設定	スタティックルート情報の設定	ip route / ipv6 route
	スタティックルート情報の表示	show ip route / show ipv6 route
	ルート情報の表示	show ip route / show ipv6 route
ルーティング機能の設定	ルーティング機能の設定	ip forwarding / ipv6 forwarding
	ルーティング機能の状態表示	show ip forwarding / show ipv6 forwarding

注意事項

特になし

関連文書

特になし

IPマルチキャスト機能

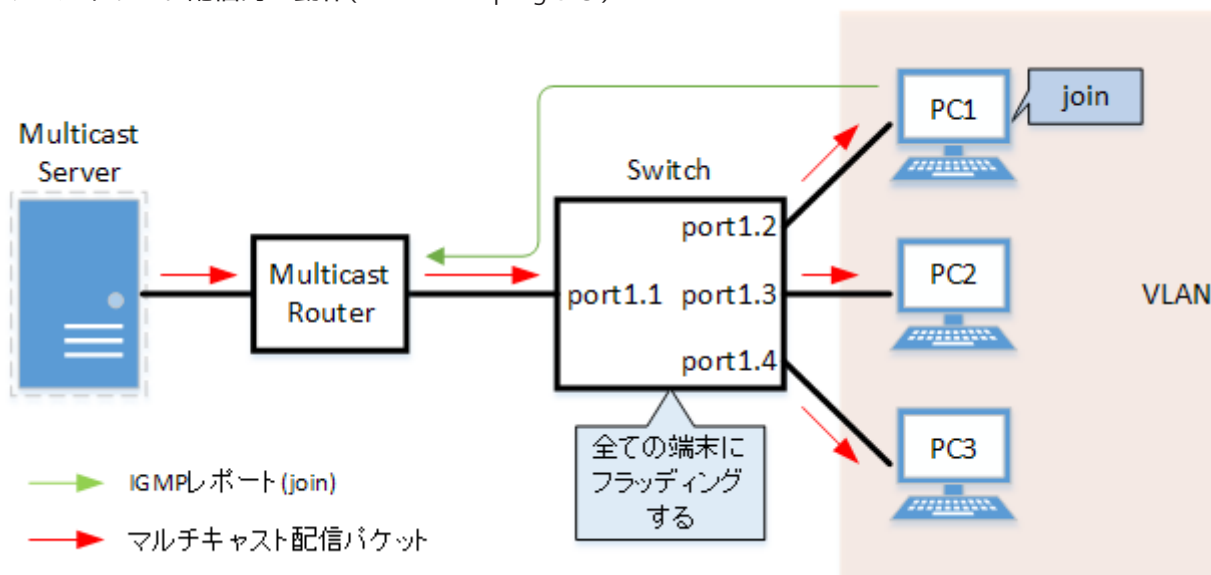
IGMP Snooping

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。

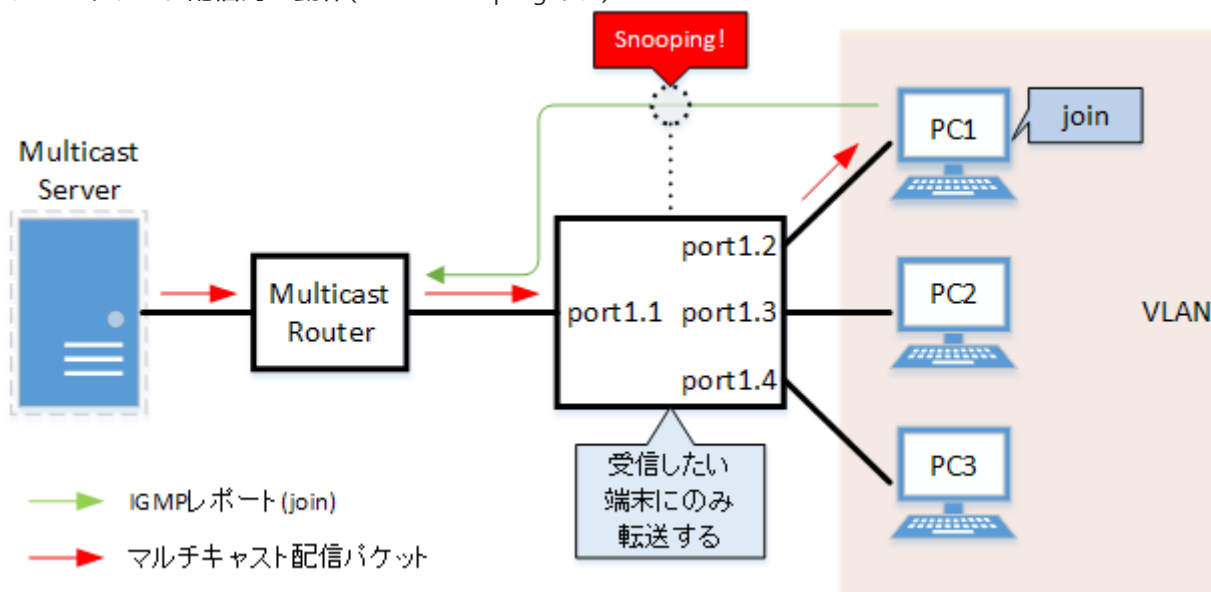
L2スイッチでは、マルチキャストパケットはVLAN単位で配送されるため、VLAN内に1つでもマルチキャストパケットを受信したい端末が存在すると、同一VLAN内のすべてのポートにパケットが配送されてしまいます。

- ・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、非クエリア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、設定バージョンに上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の送受信も有効にし、送信フレームに基本管理TLVを追加してください。

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。(すべてのVLANインターフェースにIPv4アドレスが割り当てられていない場合は、0.0.0.0を設定して送信します。)

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、送信フレームに基本管理TLVを追加してください。

関連コマンド

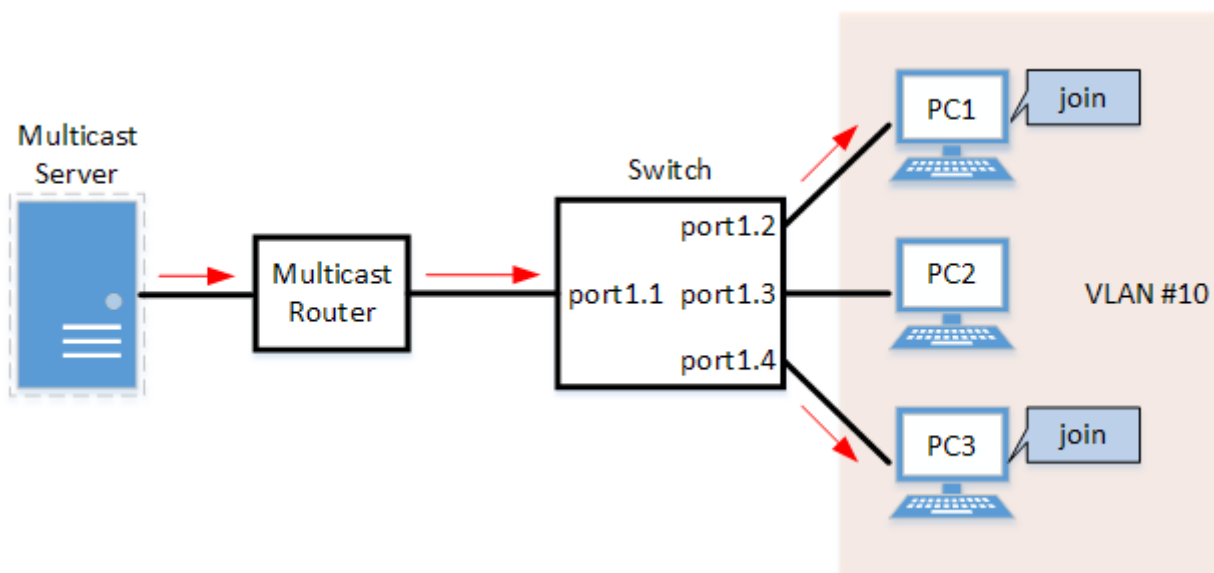
関連コマンドについて、以下に示します。
コマンドの詳細は、コマンドリファレンスを参照願います。

操作項目	操作コマンド
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	l2-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	l2-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	l2-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	l2-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トリー削除	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。)
- **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 Snoopingの有効化、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)

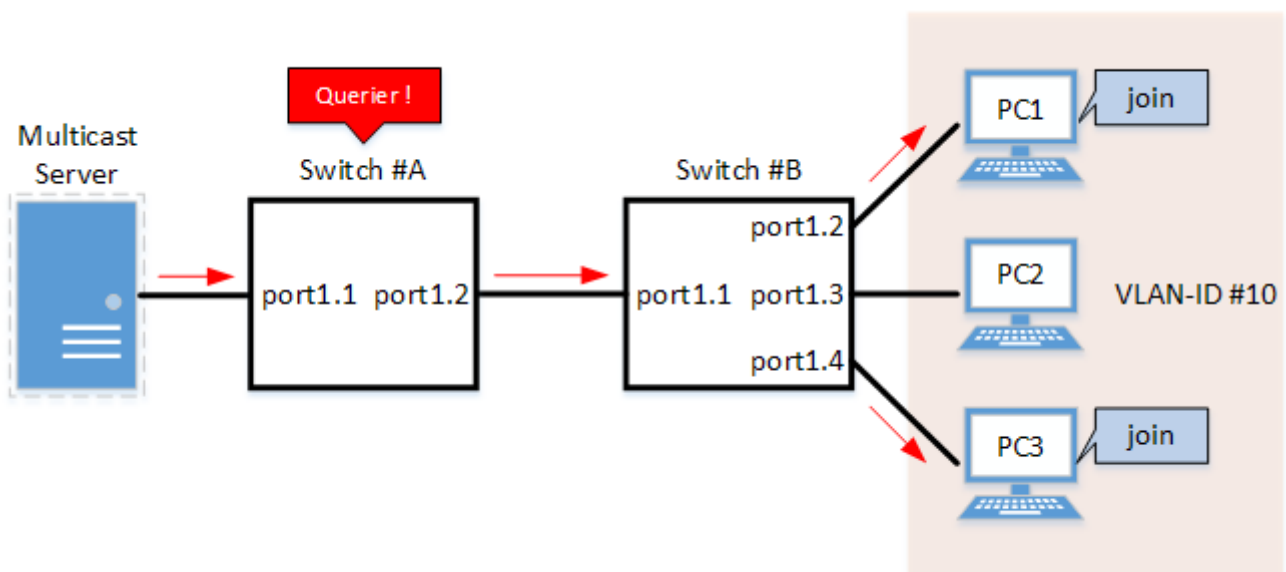

```
Yamaha#show ip igmp snooping mrouter vlan10
VLAN    Interface          IP-address    Expires
10      port1.1(dynamic)      192.168.100.216  00:00:49
```

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

・ IGMP Snoopingの有効化は、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. [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 Snoopingの有効化、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)

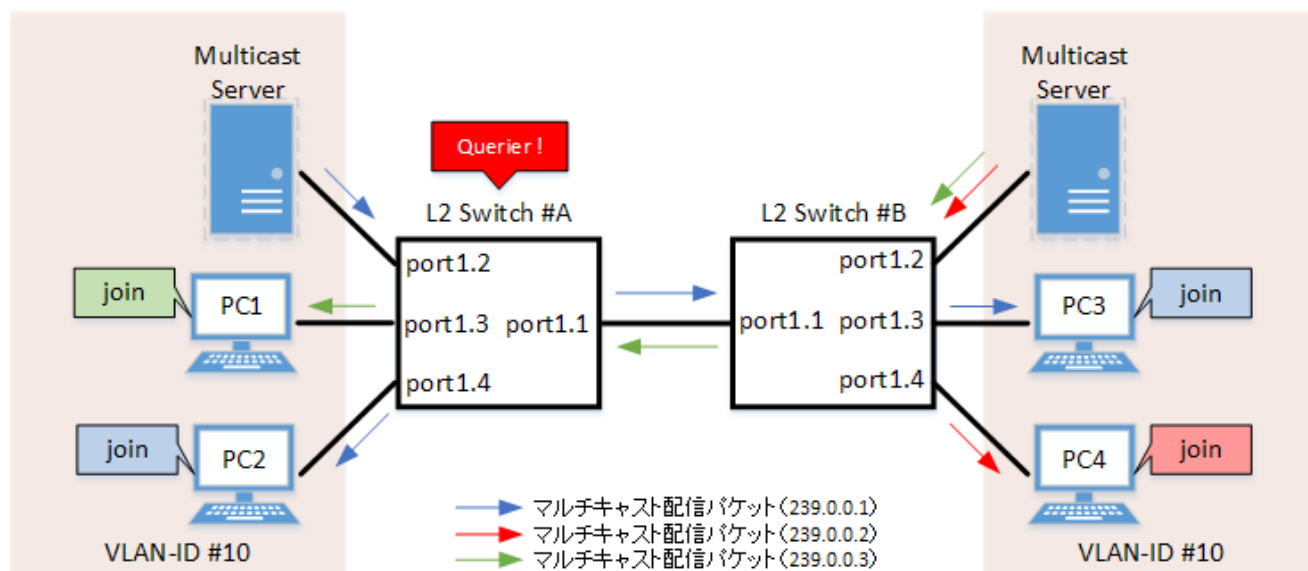
```
Yamaha#show ip igmp snooping mrouter vlan10
VLAN    Interface          IP-address    Expires
10      port1.1(dynamic)    192.168.100.216  00:00:49
```

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、以下を行います。

- LLDPの送受信を有効にし、送信フレームに基本管理TLVを追加 します。
- 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。
- 非クエリアへIGMPレポートを転送するため、以下を行います。
 - LLDPの送受信を有効にし、送信フレームに基本管理TLVを追加 します。
 - 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、以下を行います。
 - LLDPの送受信を有効にし、送信フレームに基本管理TLVを追加 します。
 - 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

- IGMP Snoopingの有効化は、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. [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、送信フレームに基本管理TLVを追加します。

```
Yamaha(config)# lldp run
Yamaha(config)# interface port1.1
Yamaha(config-if)# lldp-agent
Yamaha(lldp-agent)# set lldp enable txrx
Yamaha(lldp-agent)# tlv-select basic-mgmt
```

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 auto-assignment 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 Snoopingの有効化、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、送信フレームに基本管理TLVを追加します。

```
Yamaha(config)# lldp run
Yamaha(config)# interface port1.1
Yamaha(config-if)# lldp-agent
Yamaha(lldp-agent)# set lldp enable txrx
Yamaha(lldp-agent)# tlv-select basic-mgmt
```

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。

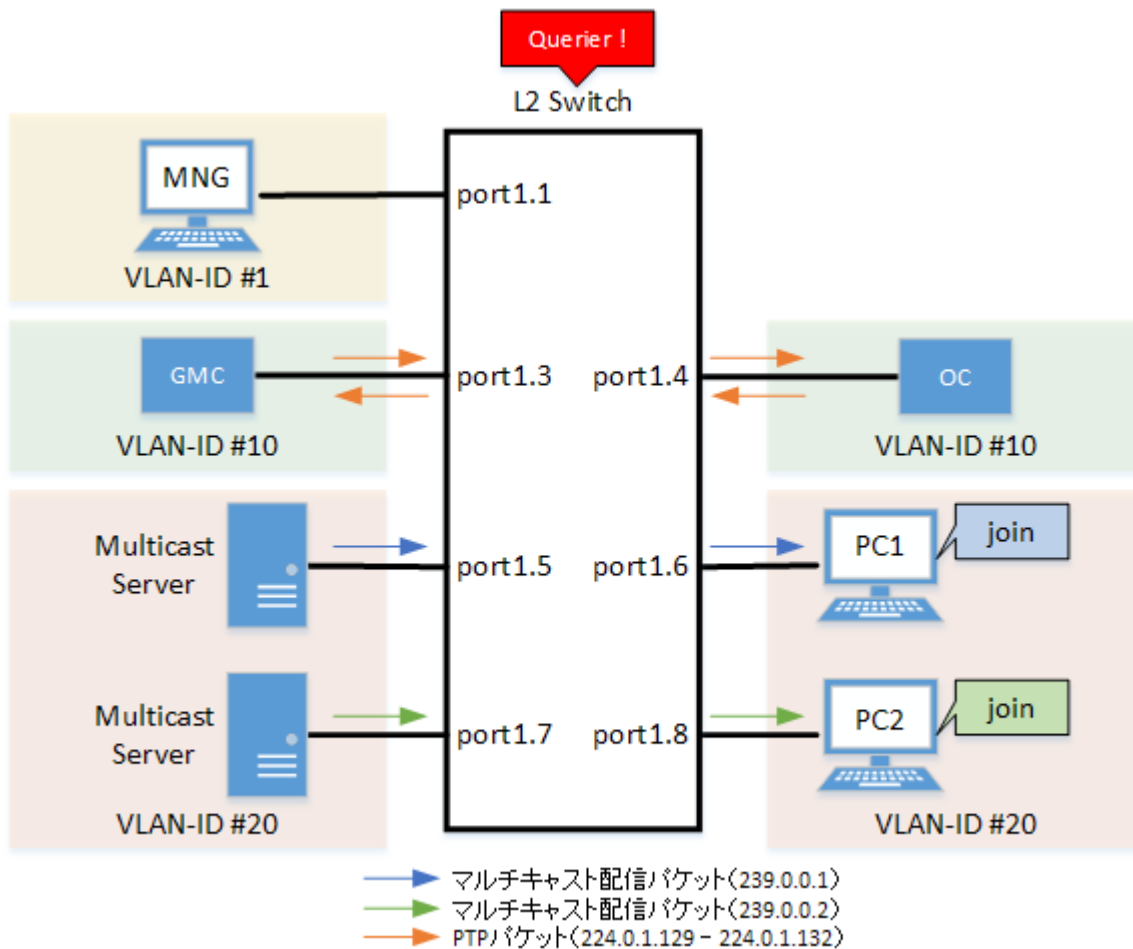
```
Yamaha#show ip igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan  Group/Source Address  Interface  Flags  Uptime  Expires  Last Reporter
Version
10    239.0.0.1               port1.1    R      00:00:03  00:00:47  192.168.100.2
```

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							

IGMP Snooping の設定(複数のマルチキャスト環境をVLANで分離する場合)

1つのスイッチで時刻同期とデータ配信をVLANで分離して構成します。

VLANは、**VLAN #1：管理用**、**VLAN #10：時刻同期用**、**VLAN #20：データ配信用** とします。



- ・システム全体
 - システム全体として **リンクローカルマルチキャストアドレスを常に転送する** ようにします。
- ・VLAN #1
 - LANポート #1 は、**アクセスポートに設定し、VLAN #1 に所属** させます。
 - **IGMP クエリー送信機能を有効** にします。
- ・VLAN #10
 - LANポート #3 ~ #4 は、**アクセスポートに設定し、VLAN #10 に所属** させます。
 - PTPパケット (224.0.1.129 ~ 224.0.1.132) はできるだけ途切れることがないようにするため、**常にフラッディングする** ようにします。
 - **IGMP クエリー送信機能を有効** にします。

- VLAN #20

- LANポート #5 ～ #8 は、 **アクセスポートに設定し、VLAN #20 に所属** させます。
- VLAN #20 で不要なマルチキャストにより帯域が逼迫しないように **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。
- **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** にします。

1. システム全体としてリンクローカルマルチキャストアドレスを常に転送するようにします。

```
Yamaha(config)#l2-unknown-mcast forward link-local
```

2. VLAN #1 にIGMP Snoopingの設定を行います。

```
Yamaha(config)#interface vlan1  
Yamaha(config-if)#ip igmp snooping enable ①  
Yamaha(config-if)#ip igmp snooping querier ②
```

① VLAN #1 のIGMP Snoopingを有効にする

② VLAN #1 のIGMP クエリー送信機能を有効にする

- IGMP Snoopingの有効化は、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。

3. VLAN #10 を定義して、IGMP Snoopingとマルチキャスト転送の設定を行います。

```
Yamaha(config)# vlan database  
Yamaha(config-vlan)#vlan 10 ①  
Yamaha(config-vlan)#exit  
Yamaha(config)#interface vlan10  
Yamaha(config-if)#l2-mcast flood 224.0.1.129 ②  
Yamaha(config-if)#l2-mcast flood 224.0.1.130 ③  
Yamaha(config-if)#l2-mcast flood 224.0.1.131 ④  
Yamaha(config-if)#l2-mcast flood 224.0.1.132 ⑤  
Yamaha(config-if)#ip igmp snooping enable ⑥  
Yamaha(config-if)#ip igmp snooping querier ⑦
```

① VLAN #10 の定義

② VLAN #10 で224.0.1.129を常にフラッディングする

③ VLAN #10 で224.0.1.130を常にフラッディングする

④ VLAN #10 で224.0.1.131を常にフラッディングする

⑤ VLAN #10 で224.0.1.132を常にフラッディングする

⑥ VLAN #10 のIGMP Snoopingを有効にする

⑦ VLAN #10 のIGMP クエリー送信機能を有効にする

- IGMP Snoopingの有効化は、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. LANポート #3 ～ #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 port1.3
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 10
①
```

① 上記設定をLANポート #4 に対しても行います。

5. VLAN #20 を定義して、IGMP Snoopingとマルチキャスト転送の設定を行います。

```
Yamaha(config)# vlan database
Yamaha(config-vlan)#vlan 20 ①
Yamaha(config-vlan)#exit
Yamaha(config)#interface vlan20
Yamaha(config-if)#l2-unknown-mcast discard ②
Yamaha(config-if)#ip igmp snooping enable ③
Yamaha(config-if)#ip igmp snooping query-interval 20 ④
Yamaha(config-if)#ip igmp snooping querier ⑤
Yamaha(config-if)#ip igmp snooping fast-leave ⑥
```

① VLAN #20 の定義

② VLAN #20 で未知のマルチキャストを破棄する

③ VLAN #20 のIGMP Snoopingを有効にする

④ VLAN #20 のIGMP クエリーの送信間隔を20秒にする

⑤ VLAN #20 のIGMP クエリー送信機能を有効にする

⑥ VLAN #20 のFast-Leave機能を有効にする

- IGMP Snoopingの有効化は、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#A] LANポート #5 ～ #8 を アクセスポートに設定し、VLAN #20 に所属させます。

```
Yamaha(config)# interface port1.5
Yamaha(config-if)# switchport mode access
Yamaha(config-if)# switchport access vlan 20
①
```

① 上記設定をLANポート #6 ～ #8 に対しても行います。

7. マルチキャスト受信者の情報を確認します。

このとき、PTPのパケット（224.0.1.129 ～ 224.0.1.132）は常にフラッディングされているのでリストにありません。

```
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
20    239.0.0.1                port1.6    R      00:00:02  00:00:48  192.168.100.1
V3
20    239.0.0.2                port1.8    R      00:00:02  00:00:48  192.168.100.2
```


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、**I2-unknown-mcast** コマンドで行ってください。
- ・ トポロジ変更を検出した場合に、通常の送信間隔にかかわらずクエリーを送信したい場合は、**I2-mcast snooping tcn-query** コマンドを設定してください。

関連文書

- ・ [Layer 2機能 : VLAN](#)

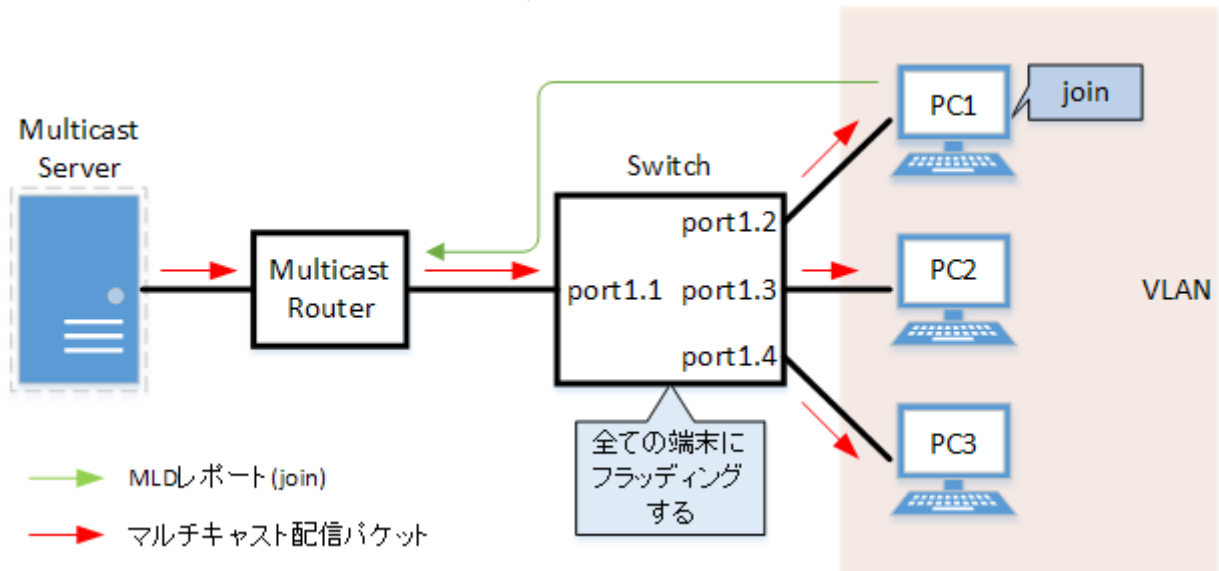
MLD Snooping

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。

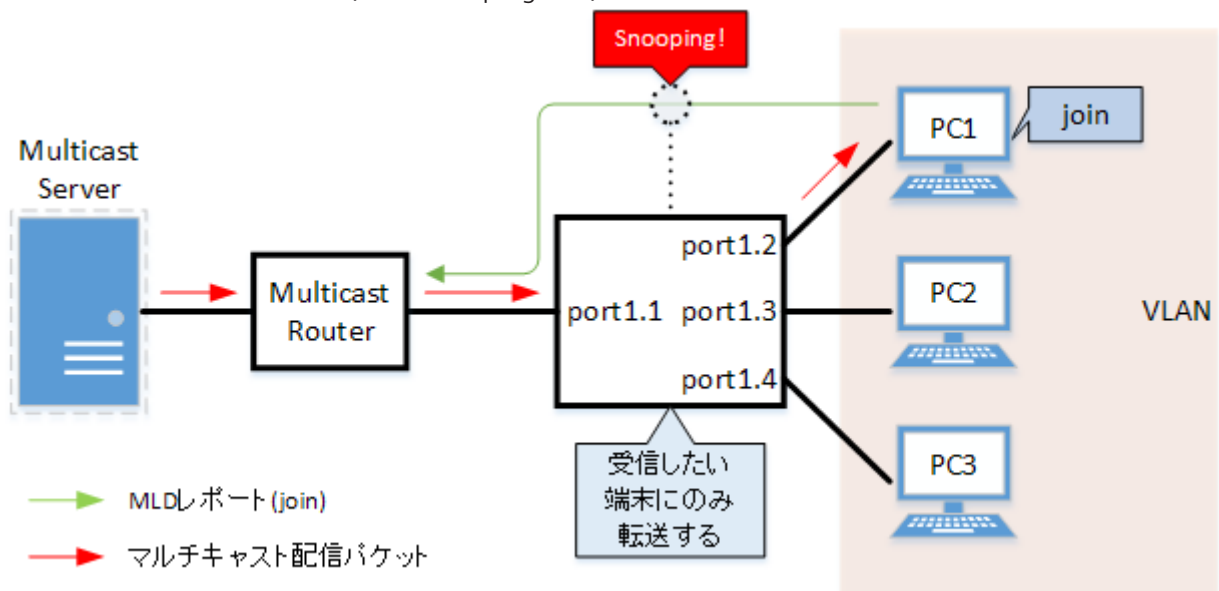
L2スイッチでは、マルチキャストパケットはVLAN単位で配送されるため、VLAN内に1つでもマルチキャストパケットを受信したい端末が存在すると、同一VLAN内のすべてのポートにパケットが配送されてしまいます。

- ・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パケットを破棄をします。
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パケットを破棄をします。

関連コマンド

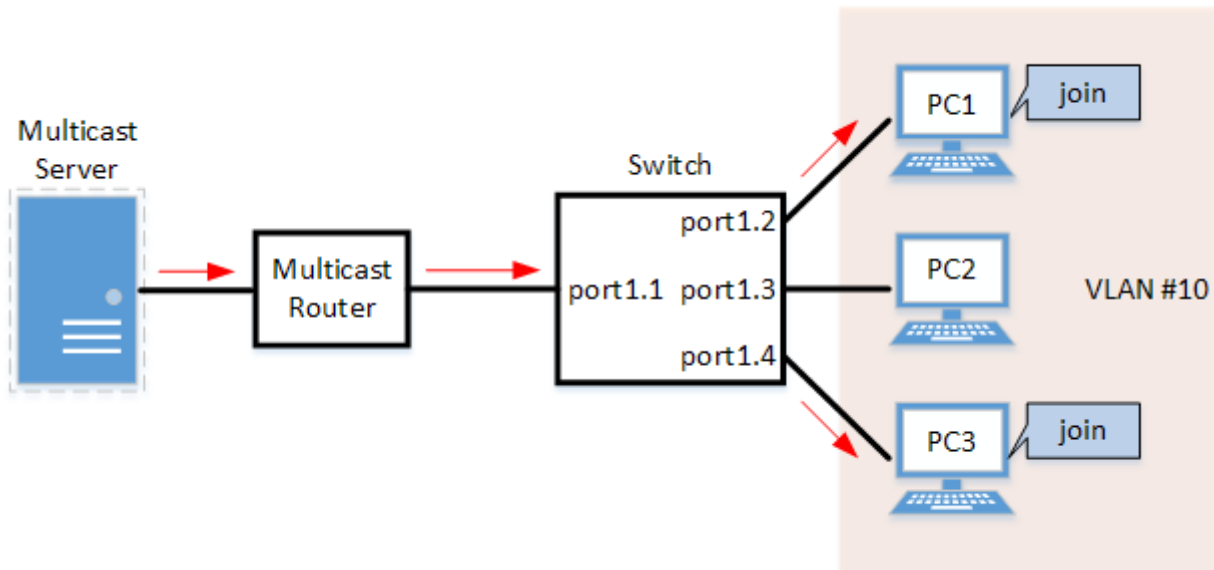
関連コマンドについて、以下に示します。
コマンドの詳細は、コマンドリファレンスを参照願います。

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 Snoopingの有効化、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。

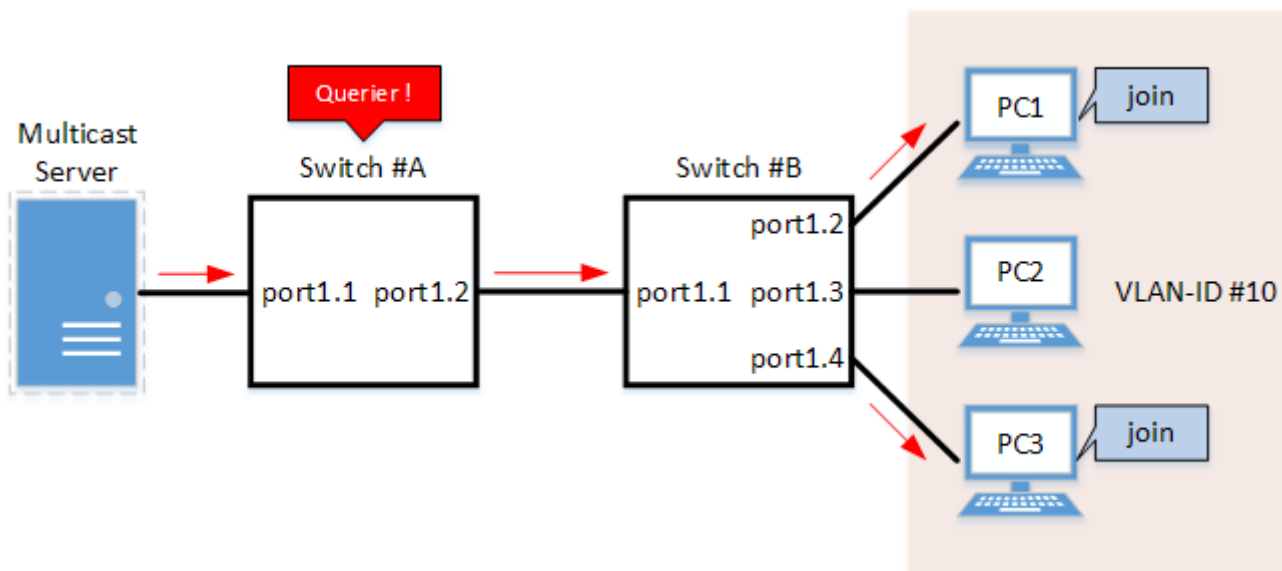
```

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

◦ MLD Snoopingの有効化は、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. [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にする

⑤ VLAN #10 のMLD Fast-leave機能を有効にする

- ・ MLD Snoopingの有効化、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、`I2-unknown-mcast` コマンドで行ってください。
- トポロジ変更を検出した場合に、通常の送信間隔にかかわらずクエリーを送信したい場合は、**`I2-mcast snooping tcn-query`** コマンドを設定してください。
- スタック機能が有効な場合、MLDスヌーピングは設定にかかわらず **無効** になります。

関連文書

- [Layer 2機能 : VLAN](#)
- [Layer 3機能 : 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、許可したフレームのみを転送し、拒否したフレームを破棄します。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 宛先IPv4アドレス IPプロトコル種別	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。また、TCP/UDPなどのIPプロトコル種別を特定して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 宛先MACアドレス	2001～3000	特定のデバイスからのアクセス、転送に対して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

機能詳細

アクセスリストの生成

アクセスリストは、各アクセスリストのID数の分、生成することができます。（**1 機能概要** の表を参照ください）

アクセスリストは、1つのリストに対して制御条件を **最大で256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

本製品の入力 (in) / 出力 (out) 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、in / out それぞれに対して **1つ** となっています。

- ・ インターフェースに対するアクセスリストの適用状況

アクセスリストの種類	LAN/SFPポート		VLANインターフェース		スタティック/LACP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	○	×	○	×	○	×

(*)制約事項として、ポート番号範囲を指定したIPv4アクセスリストは、インターフェースの出力 (out) 側に適用できません。

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。

本製品では、インターフェースに対して制御条件を **最大で512個** 登録することができます。
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。

ただし、システム内部でも制御条件を使用する場合があります、この時もリソースを消費します。

LAN/SFPポートおよび論理インターフェースに対する設定

LAN/SFPポートおよび論理インターフェース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、説明文を追加してください。
2. アクセスリストを確認します。
3. LAN/SFPポートおよび論理インターフェース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 (LAN/SFPポートおよび論理インターフェース適用時)

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	access-list	show access-list	access-group	show access-group
IPv6アクセスリスト	access-list	show access-list	access-group	show access-group
MACアクセスリスト	access-list	show access-list	access-group	show access-group

VLANインターフェースに対する設定

VLANインターフェース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、説明文を追加してください。
2. アクセスリストを確認します。
3. VLANアクセスマップを生成します。
4. VLANアクセスマップにアクセスリストを設定します。
5. VLANアクセスマップを確認します。
6. VLAN アクセスマップを VLAN に適用します。
7. 適用したVLANアクセスマップを確認します。

1. 2. の操作については、3.2 に示した操作と同じになります。
以下に 3. 以降の操作コマンドの一覧を示します。

- ・ VLANアクセスマップ操作コマンド

アクセスリストの種類	VLANアクセスマップの生成	VLANアクセスマップへのアクセスリストの設定	VLANアクセスマップの確認	VLANアクセスマップの適用	適用したVLANアクセスマップの確認
IPv4アクセスリスト	vlan access-map	match access-list	show vlan access-map	vlan filter	show vlan filter
IPv6アクセスリスト	vlan access-map	match access-list	show vlan access-map	vlan filter	show vlan filter
MACアクセスリスト	vlan access-map	match access-list	show vlan access-map	vlan filter	show vlan filter

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アクセスリストの適用	access-group
IPv4アクセスリストの生成	access-list

操作項目	操作コマンド
IPv4アクセスリストの説明文追加	access-list description
IPv4アクセスリストの適用	access-group
IPv6アクセスリストの生成	access-list
IPv6アクセスリストの説明文追加	access-list description
IPv6アクセスリストの適用	access-group
MACアクセスリストの生成	access-list
MACアクセスリストの説明文追加	access-list description
MACアクセスリストの適用	access-group
生成したアクセスリストの表示	show access-list
インターフェースに適用したアクセスリストの表示	show access-group
VLANアクセスマップの作成	vlan access-map
VLANアクセスマップへの条件設定	match
VLANアクセスマップのVLANへの割り当て	vlan filter
VLANアクセスマップの表示	show vlan access-map
VLANアクセスマップフィルタの表示	show vlan filter

コマンド実行例

IPv4アクセスリストの設定

LANポートへの適用例

■ホスト指定

LANポート #1 に対して、ホスト: **192.168.1.1** から ホスト: **10.1.1.1** へのアクセスのみを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、アクセスリストの説明文 **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 any host 192.168.1.1 host 10.1.1.1 ①
Yamaha(config)#access-list 123 deny any 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 any host 192.168.1.1 host 10.1.1.1
  20 deny any any any
Yamaha#
```

- ① アクセスリストの生成

- ② アクセスリストの説明文追加
- 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 #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

アクセスリストを変更(設定の削除や追加)したい場合は、一旦LANポートへの適用を解除する必要があります。上記設定に対して、ホスト: **192.168.1.1** から ホスト: **10.1.1.1** へのアクセスを許可する設定を削除し、ホスト: **192.168.1.1** から ホスト: **10.1.1.2** へのアクセスを許可する設定を追加します。

1. LANポート #1 から アクセスリスト #123 の適用を一旦解除します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#no access-group 123 in ①
```

- ① アクセスリストの適用解除

2. アクセスリスト #123 に設定の削除と追加を行い、確認します。

```
Yamaha(config)#no access-list 123 10 ①
Yamaha(config)#access-list 123 10 permit any host 192.168.1.1 host 10.1.1.2 ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ③
IPv4 access list 123
  10 permit any host 192.168.1.1 host 10.1.1.2
  20 deny any any any
```

- ① アクセスリストから削除
- ② アクセスリストに追加
- ③ アクセスリストの確認

3. LANポート #1 に アクセスリスト #123 を再度適用します。

```
Yamaha(config)#interface port1.1
Yamaha(config-if)#access-group 123 in ①
```

- ① アクセスリストの適用

■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 ホスト: **10.1.1.1** へのアクセスのみを許可す

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、アクセスリストの説明文 **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 any 192.168.1.0 0.0.0.255 host 10.1.1.1 ①
Yamaha(config)#access-list 123 deny any any 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 any 192.168.1.0/24 host 10.1.1.1
    20 deny any any any
Yamaha#
```

① アクセスリストの生成

② アクセスリストの説明文追加

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

アクセスリストを変更(設定の削除や追加)したい場合は、一旦LANポートへの適用を解除する必要があります。具体的な手順については、ホスト指定の場合と同様です。

VLANインターフェースへの適用例

■ホスト指定

VLAN #1000 に対して、ホスト: **192.168.1.1** から ホスト: **10.1.1.1** へのアクセスのみを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** とします。

使用するVLANアクセスマップは、**VAM-002** とし、**アクセスリスト #123** を設定します。

1. **アクセスリスト #123** を生成し、確認します。

```
Yamaha(config)#access-list 123 permit any host 192.168.1.1 host 10.1.1.1 ①
Yamaha(config)#access-list 123 deny any any any
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ②
IPv4 access list 123
```

```
10 permit any host 192.168.1.1 host 10.1.1.1
20 deny any any any
```

- ① アクセスリストの生成
- ② アクセスリストの確認

2. **VLANアクセスマップ VAM-002** を生成し、 **アクセスリスト #123** を設定します。

```
Yamaha(config)#vlan access-map VAM-002 ①
Yamaha(config-vlan-access-map)#match access-list 123 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-002
  match ipv4 access-list 123
```

- ① VLANアクセスマップの生成
- ② アクセスリストの登録
- ③ VLANアクセスマップとアクセスリストの設定を確認

3. **VLAN #1000** に **VLANアクセスマップ VAM-002** を適用し、状態を確認します。

```
Yamaha(config)#vlan filter VAM-002 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-002 is applied to vlan 1000 in
```

- ① VLANにVLANアクセスマップを適用
- ② VLANアクセスマップの設定確認

アクセスリストを変更(設定の削除や追加)したい場合は、一旦VLANインターフェースへの適用やVLANアクセスマップへの設定を解除する必要があります。

上記設定に対して、ホスト: **192.168.1.1** から ホスト: **10.1.1.1** へのアクセスを許可する設定を削除し、ホスト: **192.168.1.1** から ホスト: **10.1.1.2** へのアクセスを許可する設定を追加します。

1. **VLAN #1000** から **VLANアクセスマップ VAM-002** の適用を一旦解除します。

```
Yamaha(config)#no vlan filter VAM-002 1000 in ①
```

- ① VLANからVLANアクセスマップの適用解除

2. **VLANアクセスマップ VAM-002** から、 **アクセスリスト #123** の設定を一旦解除します。

```
Yamaha(config)#vlan access-map VAM-002 ①
Yamaha(config-vlan-access-map)#no match access-list 123 ②
```

- ① VLANアクセスマップの変更
- ② アクセスリストの登録解除

3. **アクセスリスト #123** に設定の削除と追加を行い、確認します。

```
Yamaha(config)#no access-list 123 10 ①
Yamaha(config)#access-list 123 10 permit any host 192.168.1.1 host 10.1.1.2 ②
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ③
IPv4 access list 123
  10 permit any host 192.168.1.1 host 10.1.1.2
  20 deny any any any
```

- ① アクセスリストから削除
- ② アクセスリストに追加
- ③ アクセスリストの確認

4. **VLANアクセスマップ VAM-002** に、**アクセスリスト #123** を再設定します。

```
Yamaha(config)#vlan access-map VAM-002 ①
Yamaha(config-vlan-access-map)#match access-list 123 ②
```

- ① VLANアクセスマップの変更
- ② アクセスリストの登録

5. **VLAN #1000** に **VLANアクセスマップ VAM-002** を再度適用します。

```
Yamaha(config)#vlan filter VAM-002 1000 in ①
```

- ① VLANにVLANアクセスマップを適用

■ネットワーク指定

VLAN #1000 に対して、ネットワーク: **192.168.1.0/24** から ホスト: **10.1.1.1** へのアクセスのみを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** とします。

使用するVLANアクセスマップは、**VAM-002** とし、**アクセスリスト #123** を設定します。

1. **アクセスリスト #123** を生成し、確認します。

```
Yamaha(config)#access-list 123 permit any 192.168.1.0 0.0.0.255 host 10.1.1.1 ①
Yamaha(config)#access-list 123 deny any any any
Yamaha(config)#end
Yamaha#
Yamaha#show access-list 123 ②
IPv4 access list 123
  10 permit any 192.168.1.0/24 host 10.1.1.1
  20 deny any any any
```

- ① アクセスリストの生成
- ② アクセスリストの確認

2. VLANアクセスマップ VAM-002 を生成し、アクセスリスト #123 を設定します。

```
Yamaha(config)#vlan access-map VAM-002 ①
Yamaha(config-vlan-access-map)#match access-list 123 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-002
    match ipv4 access-list 123
```

- ① VLANアクセスマップの生成
- ② アクセスリストの登録
- ③ VLANアクセスマップとアクセスリストの設定を確認

3. VLAN #1000 に VLANアクセスマップ VAM-002 を適用し、状態を確認します。

```
Yamaha(config)#vlan filter VAM-002 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-002 is applied to vlan 1000 in
```

- ① VLANにVLANアクセスマップを適用
- ② VLANアクセスマップの設定確認

アクセスリストを変更(設定の削除や追加)したい場合は、一旦VLANインターフェースへの適用やVLANアクセスマップへの設定を解除する必要があります。
具体的な手順については、ホスト指定の場合と同様です。

片方向からのTCP通信のみ許可する (TCPフラグの使用例)

VLAN10 と VLAN20 がありTCPの片方向通信制御を実現します。

- VLAN10 → VLAN20 は Telnet 等による通信が可能
- VLAN20 → VLAN10 は Telnet 等による通信は不可

1. アクセスリスト #1 を生成します。

ACK または **RST** フラグが立っているIPv4 TCPパケットのみを許可するように設定します。

```
Yamaha(config)#access-list 1 permit tcp any any ack ①
Yamaha(config)#access-list 1 permit tcp any any rst
Yamaha(config)#access-list 1 deny any any any
Yamaha(config)#end
Yamaha#
Yamaha#show access-list ②
IPv4 access list 1
    10 permit tcp any any ack
    20 permit tcp any any rst
    30 deny any any any
```

- ① アクセスリストの設定

② アクセスリストの設定確認

2. VLANアクセスマップ VAM-ESTABLISHED を生成し、アクセスリスト #1 を設定します。

```
Yamaha(config)#vlan access-map VAM-ESTABLISHED ①
Yamaha(config-vlan-access-map)#match access-list 1 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-ESTABLISHED
    match ipv4 access-list 1
```

① VLANアクセスマップの生成

② アクセスリストの登録

③ VLANアクセスマップの設定確認

3. VLAN #20 に VLANアクセスマップ VAM-ESTABLISHED を適用します。

```
Yamaha(config)#vlan filter VAM-ESTABLISHED 20 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-ESTABLISHED is applied to vlan 20 in
```

① VLANにVLANアクセスマップを適用

② VLANへの適用状態の確認

IPv6アクセスリストの設定

LANポートへの適用例

■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を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、アクセスリストの説明文 **IPV6-ACL-EX** を追加します。

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#
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 アクセスリストの説明文追加

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

アクセスリストを変更(設定の削除や追加)したい場合は、一旦LANポートへの適用を解除する必要があります。具体的な手順については、[IPv4アクセスリストの設定](#) の [LANポートへの適用例](#) を参考にしてください。

■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を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、アクセスリストの説明文 **IPV6-ACL-EX** を追加します。

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 アクセスリストの説明文追加

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

アクセスリストを変更(設定の削除や追加)したい場合は、一旦LANポートへの適用を解除する必要があります。具体的な手順については、[IPv4アクセスリストの設定](#) の [LANポートへの適用例](#) を参考にしてください。

■ホスト指定

VLAN #1000 に対して、ホスト: **2001:db8::1** からのアクセスのみを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** とします。
使用するVLANアクセスマップは、**VAM-001** とし、**アクセスリスト #3001** を設定します。

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)#end
Yamaha#
Yamaha#show access-list 3001 ②
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 アクセスリストの確認

2. **VLANアクセスマップ VAM-001** を生成し、**アクセスリスト #3001** を設定します。

```
Yamaha(config)#vlan access-map VAM-001 ①
Yamaha(config-vlan-access-map)#match access-list 3001 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-001
  match ipv6 access-list 3001
```

- ① VLANアクセスマップの生成
- ② アクセスリストの設定
- ③ VLANアクセスマップとアクセスリストの設定を確認

3. **VLAN #1000** に **VLANアクセスマップ VAM-001** を適用し、状態を確認します。

```
Yamaha(config)#vlan filter VAM-001 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-001 is applied to vlan 1000 in
```

- ① VLANにVLANアクセスマップを適用
- ② VLANアクセスマップの設定確認

アクセスリストを変更(設定の削除や追加)したい場合は、一旦VLANインターフェースへの適用やVLANアクセスマップへの設定を解除する必要があります。
具体的な手順については、[IPv4アクセスリストの設定](#) の [VLANインターフェースへの適用例](#) を参考にしてください。

■ネットワーク指定

VLAN #1000 に対して、ネットワーク: **2001:db8::/64** からのアクセスのみを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** とします。
使用するVLANアクセスマップは、**VAM-001** とし、**アクセスリスト #3001** を設定します。

1. **アクセスリスト #2** 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)#end
Yamaha#
Yamaha#show access-list 3001 ②
IPv6 access list 3001
  10 permit 2001:db8::/64
  20 deny any
```

- ① アクセスリストの生成
- ② アクセスリストの確認

2. **VLANアクセスマップ VAM-001** を生成し、**アクセスリスト #3001** を設定します。

```
Yamaha(config)#vlan access-map VAM-001 ①
Yamaha(config-vlan-access-map)#match access-list 3001 ②
Yamaha(config-vlan-access-map)#end
Yamaha#
Yamaha#show vlan access-map ③
Vlan access-map VAM-001
  match ipv6 access-list 3001
```

- ① VLANアクセスマップの生成
- ② アクセスリストの設定
- ③ VLANアクセスマップとアクセスリストの設定を確認

3. **VLAN #1000** に **VLANアクセスマップ VAM-001** を適用し、状態を確認します。

```
Yamaha(config)#vlan filter VAM-001 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-001 is applied to vlan 1000 in
```

- ① VLANにVLANアクセスマップを適用
- ② VLANアクセスマップの設定確認

アクセスリストを変更(設定の削除や追加)したい場合は、一旦VLANインターフェースへの適用やVLANアクセスマップへの設定を解除する必要があります。
具体的な手順については、[IPv4アクセスリストの設定](#) の [VLANインターフェースへの適用例](#) を参考にしてください。

MACアクセスリストの設定

LANポートへの適用例

■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を拒否するように設定します。使用するアクセスリストのIDは、**#2001** とし、アクセスリストの説明文 **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 any 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 any
```

- ① アクセスリストの生成
- ② アクセスリストの説明文追加
- 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

アクセスリストを変更(設定の削除や追加)したい場合は、一旦LANポートへの適用を解除する必要があります。具体的な手順については、[IPv4アクセスリストの設定](#) の [LANポートへの適用例](#) を参考にしてください。

■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を拒否するように設定します。使用するアクセスリストのIDは、**#2001** とし、アクセスリストの説明文 **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 any 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 any
```

- ① アクセスリストの生成
- ② アクセスリストの説明文追加
- 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

アクセスリストを変更(設定の削除や追加)したい場合は、一旦VLANインターフェースへの適用やVLANアクセスマップへの設定を解除する必要があります。

具体的な手順については、[IPv4アクセスリストの設定](#) の [LANポートへの適用例](#) を参考にしてください。

VLANインターフェースへの適用例

■ホスト指定

VLAN #1000 に対して、ホスト: **00-A0-DE-12-34-56** からのアクセスのみ拒否するように設定します。
使用するアクセスリストのIDは、**#2001** とし、アクセスリストの説明文 **MAC-ACL-EX** を追加します。
使用するVLANアクセスマップは、**VAM-003** とし、**アクセスリスト #2001** を設定します。

1. アクセスリスト #2000 を生成し、確認します。

```
Yamaha(config)#access-list 2001 deny host 00a0.de12.3456 any ①  
Yamaha(config)#access-list 2001 description MAC-ACL-EX ②  
Yamaha(config)#end  
Yamaha#  
Yamaha#show access-list ③  
MAC access list 2001  
10 deny host 00A0.DE12.3456 any
```

- ① アクセスリスト #2001 の生成
- ② アクセスリストの説明文追加
- ③ アクセスリストの確認

2. VLANアクセスマップ VAM-003 を生成し、 アクセスリスト #2001 を設定します。

```
Yamaha(config)# vlan access-map VAM-003 ①  
Yamaha(config-vlan-access-map)# match access-list 2001 ②  
Yamaha(config-vlan-access-map)# end  
Yamaha#  
Yamaha#show vlan access-map ③
```



```
Vlan access-map VAM-003
match mac access-list 2001
```

- ① VLANアクセスマップの生成
- ② アクセスリストの登録
- ③ VLANアクセスマップとアクセスリストの設定を確認

3. **VLAN #1000** に **VLANアクセスマップ VAM-003** を適用し、状態を確認します。

```
Yamaha(config)#vlan filter VAM-003 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-003 is applied to vlan 1000 in
```

- ① VLANにVLANアクセスマップを適用
- ② VLANアクセスマップの設定確認

アクセスリストを変更(設定の削除や追加)したい場合は、一旦VLANインターフェースへの適用やVLANアクセスマップへの設定を解除する必要があります。

具体的な手順については、[IPv4アクセスリストの設定](#) の [VLANインターフェースへの適用例](#) を参考にしてください。

■ベンダー指定

VLAN #1000 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を拒否するように設定します。

使用するアクセスリストのIDは、**#2001** とし、アクセスリストの説明文 **MAC-ACL-EX** を追加します。
使用するVLANアクセスマップは、**VAM-003** とし、**アクセスリスト #2001** を設定します。

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 any 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 any
```

- ① アクセスリスト #2001 の生成
- ② アクセスリストの説明文追加
- ③ アクセスリストの確認

2. **VLANアクセスマップ VAM-003** を生成し、**アクセスリスト #2001** を設定します。

```
Yamaha(config)# vlan access-map VAM-003 ①
Yamaha(config-vlan-access-map)# match access-list 2001 ②
Yamaha(config-vlan-access-map)# end
Yamaha#
Yamaha#show vlan access-map ③
```

```
Vlan access-map VAM-003
match mac access-list 2001
```

- ① VLANアクセスマップの生成
- ② アクセスリストの登録
- ③ VLANアクセスマップとアクセスリストの設定を確認

3. **VLAN #1000** に **VLANアクセスマップ VAM-003** を適用し、状態を確認します。

```
Yamaha(config)#vlan filter VAM-003 1000 in ①
Yamaha(config)#end
Yamaha#
Yamaha#show vlan filter ②
Vlan filter VAM-003 is applied to vlan 1000 in
```

- ① VLANにVLANアクセスマップを適用
- ② VLANアクセスマップの設定確認

アクセスリストを変更(設定の削除や追加)したい場合は、一旦VLANインターフェースへの適用やVLANアクセスマップへの設定を解除する必要があります。

具体的な手順については、[IPv4アクセスリストの設定](#) の [VLANインターフェースへの適用例](#) を参考にしてください。

注意事項

- ・ 受信フレームに対するアクセスリストが設定されたLAN/SFPポートは論理インターフェースに所属できません。
- ・ インターフェースの受信フレームに対するアクセスリスト設定は、論理インターフェースに所属しているLAN/SFPポートに対して適用できません。ただし、スタートアップコンフィグ上に論理インターフェースに所属しているLAN/SFPポートの受信フレームに対するアクセスリスト設定がある場合、最若番ポートの設定が論理インターフェースに適用されます。
- ・ フラグメントパケットは正しく条件判定できない場合があります。具体的には、条件にレイヤー 4 の情報(送信元ポート番号、宛先ポート番号、TCP の各種フラグ)が含まれる場合、2 番目以降のフラグメントパケットにそれらの情報が含まれないため正しい判定ができません。フラグメントパケットを処理する可能性がある場合には条件にレイヤー 4 の情報を含めないようにしてください。

関連文書

- ・ [Layer 2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。
受信フレームの CoS 値や DSCP 値を使用して振り分けたり、受信ポート毎に設定された優先度を適用させることができる。

LAN/SFPポートおよび論理インターフェース単位で設定が可能である。ただし、論理インターフェースに所属しているLAN/SFPポートは設定変更できない。

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。

クラスマップ

パケットをトラフィッククラスに分類するための条件を定義したもの。
ポリシーマップに関連付けて使用し、トラフィッククラス毎の QoS 処理(プレマーキング、送信キュー指定、メータリング・ポリシング・リマーキング)を定義することができる。

ポリシーマップ

受信ポートに対する一連の QoS 処理を行うための要素。単体では使用せず、1つ ～ 8つのクラスマップを関連付けて使用する。

ポリシーマップを LAN/SFP ポートおよび論理インターフェースに適用すると、該当ポートで受信したパケットに対し、ポリシーマップに関連付けられたクラスマップ単位でトラフィック分類が行われる。

また、トラフィッククラス毎に設定されたQoS処理(プレマーキング、送信キュー指定、メータリング・ポリシング・リマーキング)が行われるようになる。

ポリサー

メータリング、ポリシング、リマーキングの一連の設定の集まり。

1つのトラフィッククラスを対象としてメータリングを行う個別ポリサーと、複数のトラフィッククラスをひとまとめにしてメータリングを行う集約ポリサーの2種類がある。

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。

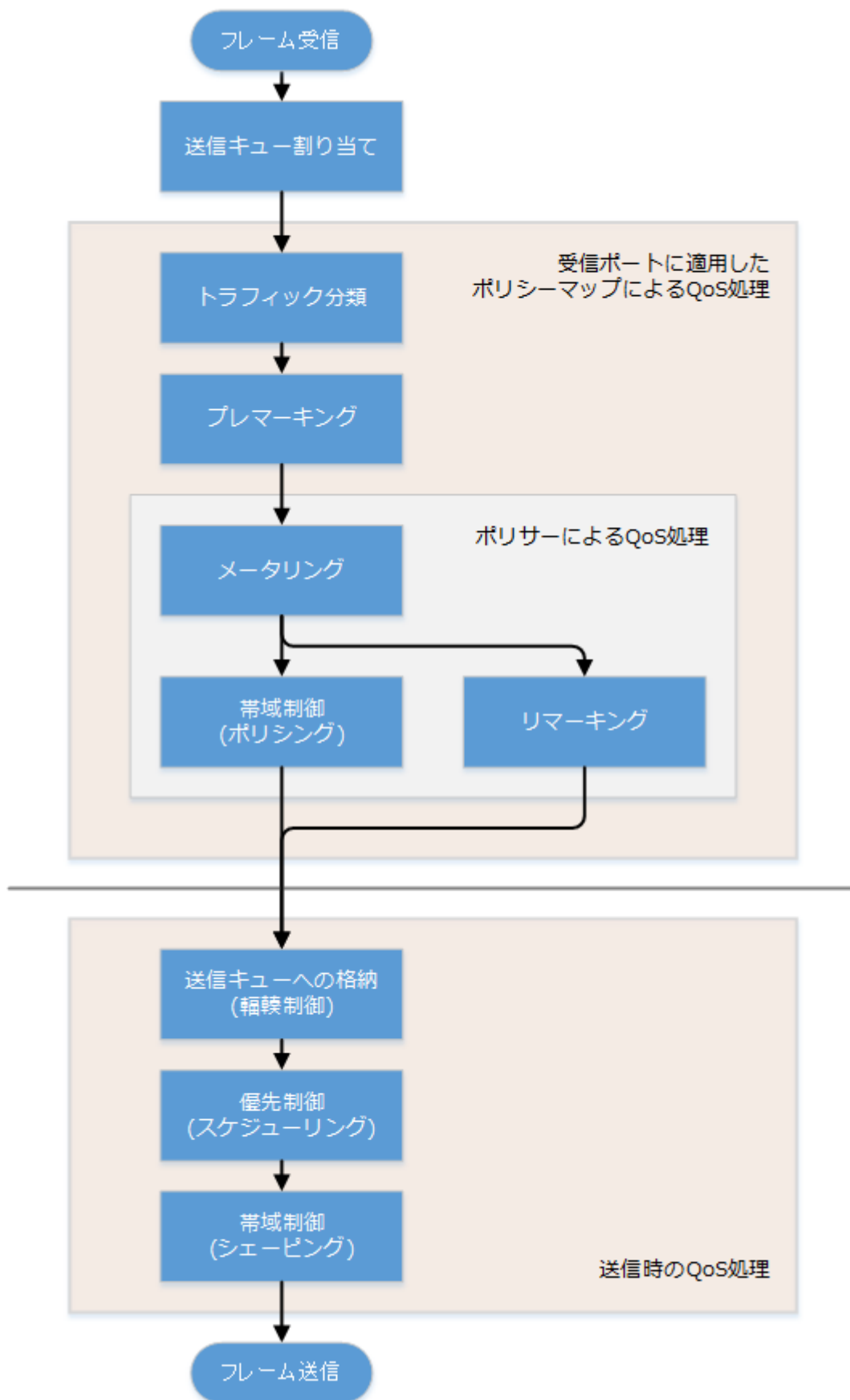
QoS 制御コマンドのほとんどは、QoS が有効化されていないと実行することができません。

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 制御を有効化するにはシステムのフロー制御が無効である必要があります。

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 値やDSCP 値、ポートの優先度のうち、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

DSCP 値	送信キューID	Traffic Type
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。

トラストモードが "CoS" または "DSCP" の場合、ポリシーマップによる QoS 処理 (以下) により、送信キューID の再割り当てが行われる場合があります。
この場合は、ポートのトラストモードに対応する送信キューID変換テーブルに基づいて、新しい送信キューID が再度割り当てられます。

- ・ プレマーキング
 - 詳細は **プレマーキング** を参照
- ・ 送信キュー指定
 - トラストモードが "CoS" の場合、**set cos-queue** コマンドにて送信キューID に対応した CoS 値を指定します。
 - トラストモードが "DSCP" の場合、**set dscp-queue** コマンドにて送信キューID に対応した DSCP 値を指定します。
- ・ リマーキング
 - 詳細は **メータリング・ポリシング・リマーキング** を参照

トラストモードが "ポート優先" の場合は、ポリシーマップの QoS 処理によって送信キューID を変更することはできません。(プレマーキング、送信キュー指定、リマーキングの設定を含むポリシーマップを適用することはできません)

送信キューの割り当て(スイッチ本体から送信されるフレーム)

送信キューの割り当ての例外として、スイッチ本体(CPU)から送信されるフレームは、**システムで決められた送信キュー** が自動的に割り当てられます。(**トラストモード** に基づく送信キュー割り当てはされません) どの送信キューを割り当てるかは、**qos queue sent-from-cpu** コマンドで変更することができ、初期設定では送信キューID は **7** が設定されています。

トラフィック分類

トラフィックの分類は、IP ヘッダや TCP ヘッダなどの条件を定義した **クラスマップ** に基づいて、受信フレームを分類する機能です。
分類可能な条件と、設定コマンドは下表のとおりです。

- ・ 分類可能な条件と、設定コマンド

分類条件	条件設定コマンド	クラスマップ設定コマンド	クラスマップあたりの登録可能数
送信元/宛先 MAC アドレス	access-list (*注3)	match access-list	1
送信元/宛先 IP アドレス			1
IP プロトコルタイプ (*注1)			1

分類条件	条件設定コマンド	クラスマップ設定コマンド	クラスマップあたりの登録可能数
Ethernet フレームタイプ番号	<code>match ethertype</code>		1
VLAN タグヘッダの CoS 値	<code>match cos</code>		8
IP ヘッダの Precedence 値	<code>match ip-precedence</code>		8
IP ヘッダの DSCP 値	<code>match ip-dscp</code>		8
VLAN ID (*注2)	<code>match vlan, match vlan-range</code>		30

(*注1) IP プロトコルタイプによる分類は、IPv6 は対象外となります。

(*注2) プライベート VLAN のアイソレート VLAN、コミュニティ VLAN は対象外となります。

(*注3) トラフィックの分類でアクセスリストに設定できる条件は **最大39件** までとなります。

- ・トラフィックの分類は **クラスマップ** 単位で行います。
- ・分類条件は 1 つの **クラスマップ** に対して **1 種類** 設定することができ、条件にマッチしたフレームは、ポリサーによる QoS 処理（メータリング・ポリシング・リマーキング）やプレマーキング、送信キューの指定を行うことができます。
- ・分類条件を指定しなかった場合は、すべてのフレームが該当のトラフィッククラスに分類されます。
- ・CoS, IP Precedence, DSCP, VLAN ID による分類は、1 つのクラスマップで複数個を登録することができます。
- ・**ポリシーマップ** に複数の **クラスマップ** を関連付けることで、受信ポートに対して複合的なトラフィックの分類を実現することができます。1 つの **ポリシーマップ** に関連付けられる **クラスマップ** は、**最大で 8 個** です。
- ・設定されている **クラスマップ** の情報は、`show class-map` コマンドで確認できます。
- ・設定されている **ポリシーマップ** の情報は、`show policy-map` コマンドで確認できます。
- ・**ポリシーマップ** がどのポートに適用されているか、**クラスマップ** がどのポリシーマップに関連付けられているかは、`show qos map-status` コマンドで確認できます。

プレマーキング

プレマーキングとは、トラフィッククラスに分類された受信フレームに対して、CoS 値、IP Precedence 値、DSCP 値を変更する（割り当てる）機能です。

プレマーキングは、ポリシーマップ・クラスモードの以下のコマンドで設定します。

- ・プレマーキング設定コマンド

プレマーキング対象	設定コマンド
CoS	<code>set cos</code>
IP Precedence	<code>set ip-precedence</code>
DSCP	<code>set ip-dscp</code>

- ・プレマーキング可能な DSCP 値は、**RFCで推奨されている値** とそれ以外に **4 個まで** を扱うことができます。（リマーキングで扱う DSCP 値についても、本ルールが適用されます。）
- ・プレマーキングの設定は、**クラスマップ** に対して **1 つだけ** 設定することができます。また、送信キュー指定（`set cos-queue, set ip-dscp-queue`）との併用はできません。

- ・ プレマーキングを行うと、変更後の値とトラストモードに対応する **送信キューID変換テーブル** に基づいて、送信キューの再割り当てが行われます。

メータリング・ポリシング・リマーキング

帯域使用量を計測し、得られた結果に応じてパケットの破棄や優先度の変更を行うことにより、帯域制御を実現します。

メータリング、ポリシング、リマーキングの一連の処理は **ポリサー** と呼ばれる単位で行います。

- ・ 帯域制御の処理概要

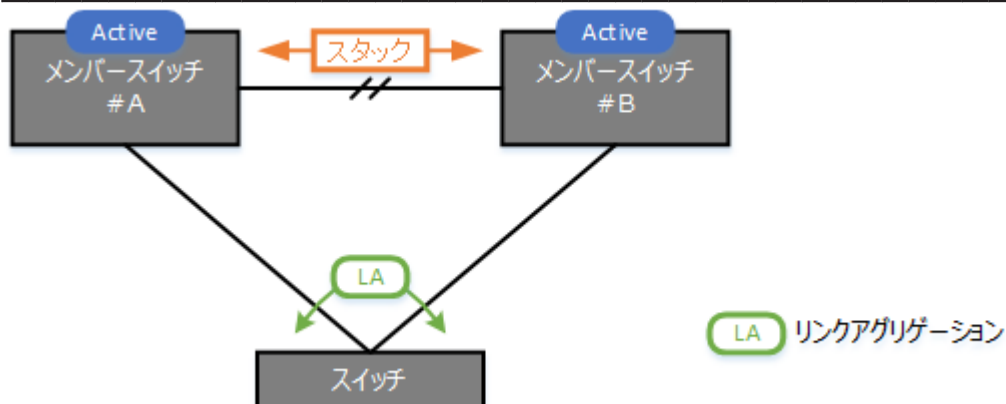
処理名	概要
メータリング	トラフィックレートとバーストサイズを基準に、分類したトラフィックがどの程度帯域を占有しているかを計測し、 3つの帯域クラス(Green, Yellow, Red)に分類します。 分類された帯域クラス毎に、破棄(ポリシング)やリマーキングなどの動作を指定することができます。
ポリシング	帯域クラスの情報をを用いて、フレームを破棄することで、帯域使用量を一定量に抑止します。
リマーキング	帯域クラスの情報をを用いて、フレームの CoS 値、IP Precedence 値、DSCP 値を変更します。

メータリング、ポリシング、リマーキングは、以下の論理インターフェースに対して動作させることはできません。

1. SWX3200-52GT にて Port1～24, 49, 50 (下図、青枠内のポート) と Port 25～48, 51, 52 (下図、緑枠内のポート) でグルーピングした論理インターフェース



2. スタックを構成するメンバースイッチを跨いでグルーピングした論理インターフェース(下図、緑のI/F)



ポリサーの種類

ポリサーには、メータリング・ポリシング・リマーキングを1つのトラフィッククラスを対象として行う **個別ポリサー** と、複数のトラフィッククラスをひとまとめにして行う **集約ポリサー** の2種類があります。

- ・ **個別ポリサー**

トラフィッククラス毎にメータリング・ポリシング・リマーキングを行います。
設定は、ポリシーマップ・クラスモードの **police** コマンドと **remark-map** コマンドを使用します。

- ・ **集約ポリサー**

複数のトラフィッククラスをひとまとめにして、メータリング・ポリシング・リマーキングを行います。

集約ポリサーは、 **aggregate-police** コマンドで生成し、集約ポリサーモードの **police** コマンドと **remark-map** コマンドで内容を設定します。

生成した集約ポリサーをトラフィッククラスに適用するには、 **police-aggregate** コマンドを使用します。

- ・ **個別ポリサー と 個別ポリサー** それぞれの設定において使用するコマンドは以下のとおりです。

設定内容	個別ポリサー	集約ポリサー
ポリサーの生成	-	aggregate-police
ポリサーの設定 (メータリング・ポリシング・リマーキング)	police single-rate, police twin-rate (ポリシーマップ・クラスモード)	police single-rate, police twin-rate (集約ポリサーモード)
トラフィッククラスへのポリサーの適用		police-aggregate
リマーキングの詳細設定	remark-map (ポリシーマップ・クラスモード)	remark-map (集約ポリサーモード)

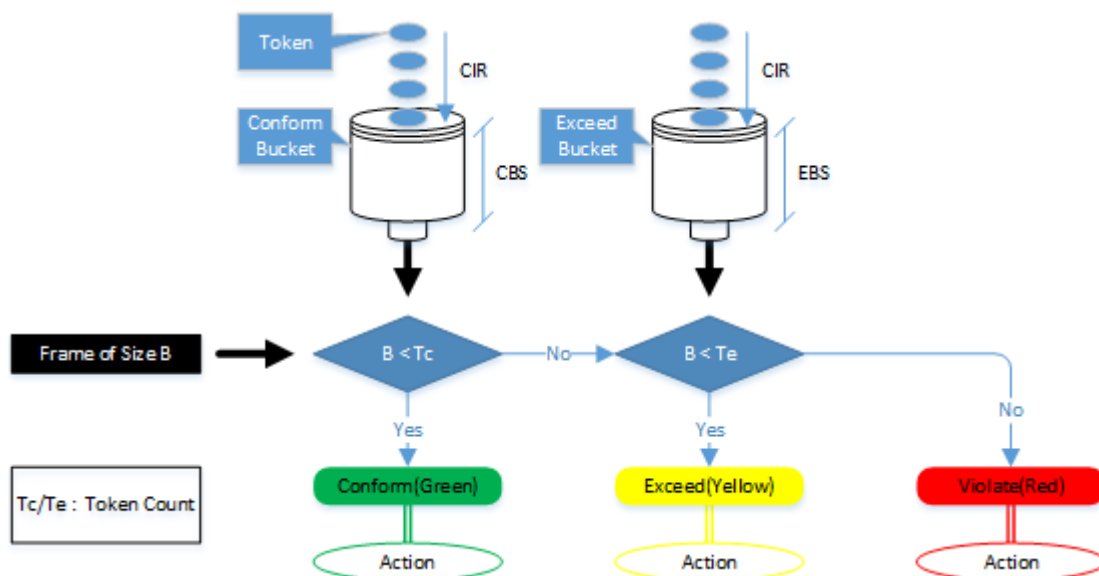
メータリングの設定

メータリングには、 **シングルレートポリサー** (RFC2697)と **ツインレートポリサー** (RFC2698)の2種類があります。

使用するメータリングの種類と制御パラメータは、 **police** コマンド(ポリシーマップ・クラスモードまたは集約ポリサーモード)で設定します。

- ・ **シングルレートポリサー(RFC2697)**

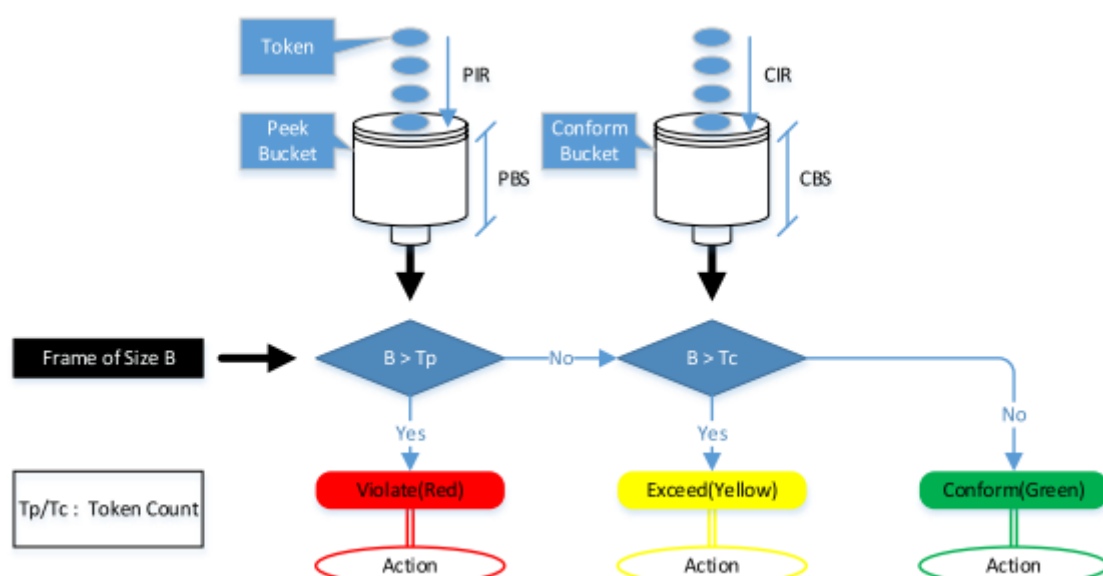
シングルレートポリサーは、 **トラフィックレート(CIR)** と **バーストサイズ(CBS, EBS)** に基づいて、トラフィッククラス内のフレームを **Green(適合)**、**Yellow(超過)**、**Red(違反)** の3つの帯域クラスに分類します。



- ° シングルレートポリサー 制御パラメータ
バーストサイズが適切に設定されていない場合、スループットが低下することがあります。

パラメータ	説 明
CIR (Committed Information Rate)	定期的にバケットに貯められるトークンの流量。 1 ～ 102,300,000 kbps で指定することができます。
CBS (Committed Burst Size)	一つ目のトークンバケット(適合トークンバケット)から一度に取り除けるトークンのトラフィック量。 11 ～ 2,097,120 kByteで指定することができます。
EBS (Exceed Burst Size)	二つ目のトークンバケット(超過トークンバケット)から一度に取り除けるトークンのトラフィック量。 11 ～ 2,097,120 kByteで指定することができます。

- ・ ツインレートポリサー(RFC2698)
ツインレートポリサーは、**トラフィックレート(CIR, PIR)**と**バーストサイズ(CBS, PBS)**に基づいて、トラフィッククラス内のフレームを**Green(適合)**、**Yellow(超過)**、**Red(違反)**の3つの帯域クラスに分類します。



- ° ツインレートポリサー 制御パラメータ
バーストサイズが適切に設定されていない場合、スループットが低下することがあります。

パラメータ	説 明
CIR (Committed Information Rate)	二つ目のトークンバケット(適合トークンバケット) に定期的に貯められるトークンの流量。 1 ～ 102,300,000 kbps で指定することができます。
PIR (Peak Information Rate)	一つ目のトークンバケット(ピークトークンバケット) に定期的に貯められるトークンの流量。 1 ～ 102,300,000 kbps で指定することができます。 ただし、CIR より小さな値は設定できません。

パラメータ	説 明
CBS (Committed Burst Size)	適合トークンバケットから一度に取り除けるトークンのトラフィック量。 11 ~ 2,097,120 kByteで指定することができます。
PBS (Peak Burst Size)	ピークトークンバケットから一度に取り除けるトークンのトラフィック量。 11 ~ 2,097,120 kByteで指定することができます。

メータリングアクション(ポリシング・リマーキング)の設定

メータリングで分類された帯域クラスに対する動作の指定は、**police** コマンド(ポリシーマップ・クラスモードまたは集約ポリサーモード)で行います。

本製品では、帯域クラス毎に以下の動作を定義することができます。

- ・帯域クラスに対する動作の指定

帯域クラス	転送	破棄	リマーキング
Green	○	×	×
Yellow	○	○	○
Red	×	○	(どちらか片方のみ)

- ・リマーキングの詳細の設定に関しては、**remark-map** コマンド(ポリシーマップ・クラスモードまたは集約ポリサーモード)で行います。
DSCP 値へのリマーキングは、プレマーキングと同じく、**RFCで推奨されている値** (別表1. 標準 PHB (RFC 推奨値)参照) とそれ以外に **4 個まで** を扱うことができます。
また、リマーキングを行うと、変更後の値とトラストモードに対応する **送信キューID変換テーブル** に基づいて、送信キューの再割り当てが行われます。
- ・メータリングを行わない場合、トラフィッククラスに分類された全てのフレームは、帯域クラス **Green** として扱われます。

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。

メータリングで分類された帯域クラスに対して、以下のしきい値を超えた場合に、該当フレームの破棄を行います。

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。

帯域クラス	テールドロップしきい値(%)
Green + Yellow	100%
Red	60%

- ・スタック機能が無効かつ、フロー制御が有効な場合のみテールドロップが無効になります。
しきい値を変更することはできません。

- ・送信キューの混雑度合いは、**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。)

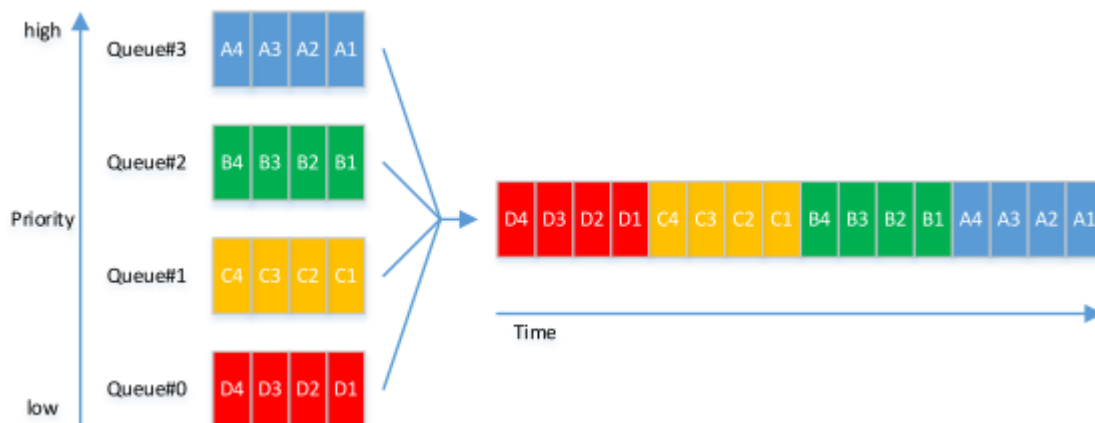
本製品は、送信キューのスケジューリング方式として、**絶対優先方式(SP)** と **重み付きラウンドロビン方式(WRR)** の2種類をサポートします。

また、SP と WRR をインターフェース内で組み合わせて使用することも可能です。(この場合、SPが優先的に処理されます。)

・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。

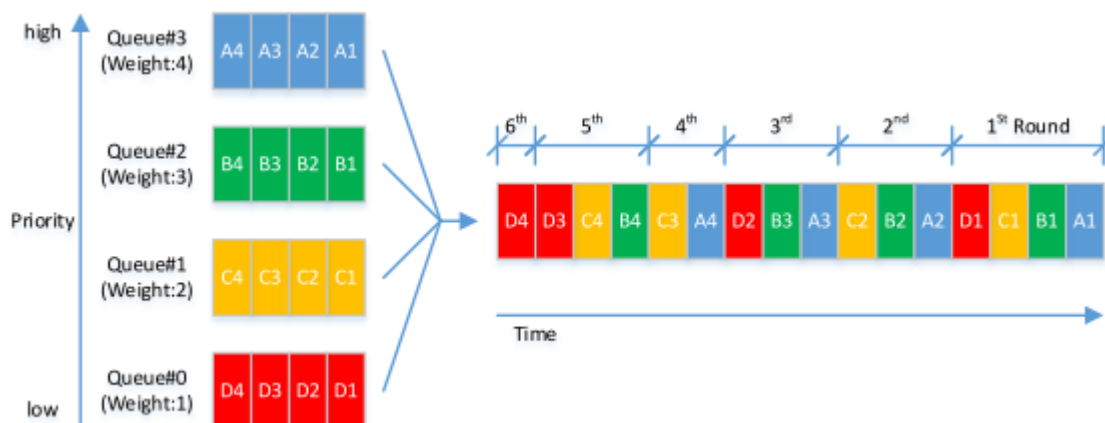
優先度の高いキューにフレームが格納されている場合には、それより優先度の低いキューからは全く送信することができなくなります。



・重み付きラウンドロビン方式 (WRR : Weighted Round Robin)

各キューに **重み** を設定し、その比率によってフレームを送信します。重みは、**1~32** の範囲で設定することができます。

優先度の低いキューからも、ある一定の割合にて送信をすることができます。



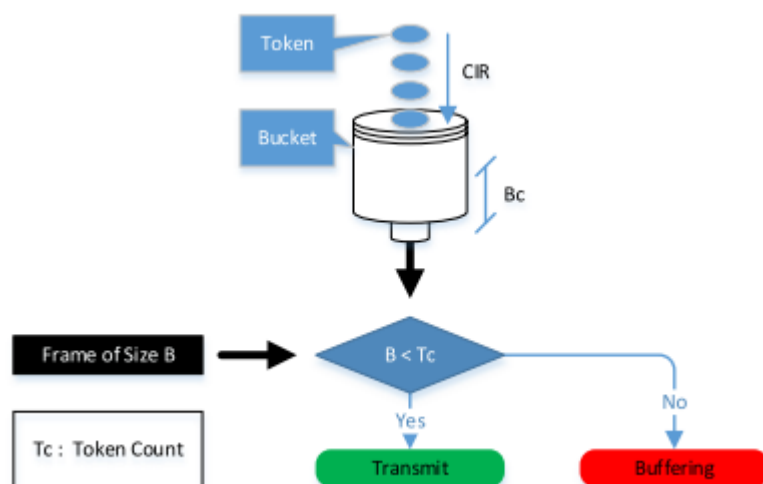
送信キューに対するスケジューリングの設定は、インターフェース単位ではなく、システムで一つの設定となります。

重みの設定は、**qos wrr-weight** コマンドを使用します。
初期設定(QoS 有効化時)、スケジューリング設定は全てのキューで **SP** となっています。

シェーピング

帯域の異なるネットワークを接続している場合、広帯域のネットワークから狭帯域のネットワークにそのままの転送速度でフレームを転送すると、フレームが転送しきれなくなり、帯域不足を招きます。
シェーピングは、フレーム送信時の速度を監視し、速度超過を見つけた場合にフレームを一時的にバッファリングしてから送信することにより、転送レートを一定に抑止する機能です。
本製品のシェーピングは、シングルトークンバケットにより実現されています。

- ・ シングルトークンバケット



- ・ シェーピングは、ポート単位とキュー単位で設定することができ、それぞれ以下のコマンドを使用します。

シェーピング対象	設定コマンド
ポート単位	traffic-shape rate
送信キュー単位	traffic-shape queue rate

- ・ 送信レートの上限(CIR)とバーストサイズ(BC)を指定します。
 - 送信レートの上限(CIR) : **18 - 1,000,000 kbps** で指定可能。
 - バーストサイズ(BC) : **4 - 16,000 kbyte** で指定可能。ただし、4Kbyte単位での設定となります。
 - キュー単位とポート単位のシェーピングを併用した場合、キュー単位のシェーピングの後にポート単位のシェーピングが適用されます。
- ・ 初期設定(QoS 有効化時)、シェーピング設定はすべてのポート、すべてのキューで **無効** 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 値は以下のとおりです。
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願います。

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
受信フレームに対するポリシーマップの生成	policy-map
受信フレームに対するポリシーマップの適用	service-policy input
QoS 機能の設定状態の表示	show qos

操作項目	操作コマンド
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
ポリシーマップ情報の表示	show policy-map
マップステータスの表示	show qos map-status
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
スイッチ本体から送信されるフレームの優先度設定	qos queue sent-from-cpu
クラスマップ(トラフィックの分類条件)の生成	class-map
クラスマップの関連付け	class
トラフィック分類条件の設定(access-group)	match access-list
トラフィック分類条件の設定(CoS)	match cos
トラフィック分類条件の設定(TOS優先度)	match ip-precedence
トラフィック分類条件の設定(DSCP)	match ip-dscp
トラフィック分類条件の設定(Ethernet Type)	match ethertype
トラフィック分類条件の設定(VLAN ID)	match vlan
トラフィック分類条件の設定(VLAN ID レンジ指定)	match vlan-range
クラスマップ情報の表示	show class-map
プレマーキングの設定(CoS)	set cos
プレマーキングの設定(TOS優先度)	set ip-precedence
プレマーキングの設定(DSCP)	set ip-dscp
個別ポリサー/集約ポリサーの設定(シングルレート)	police single-rate
個別ポリサー/集約ポリサーの設定(ツインレート)	police twin-rate
個別ポリサー/集約ポリサーのリマーキングの設定	remark-map
集約ポリサーの作成	aggregate-police
集約ポリサーの表示	show aggregate-police
集約ポリサーの適用	police-aggregate
メータリングカウンターの表示	show qos metering-counters
メータリングカウンターのクリア	clear qos metering-counters
送信キューの指定(CoS-Queue)	set cos-queue
送信キューの指定(DSCP-Queue)	set ip-dscp-queue
送信キューのスケジューリング設定	qos wrr-weight

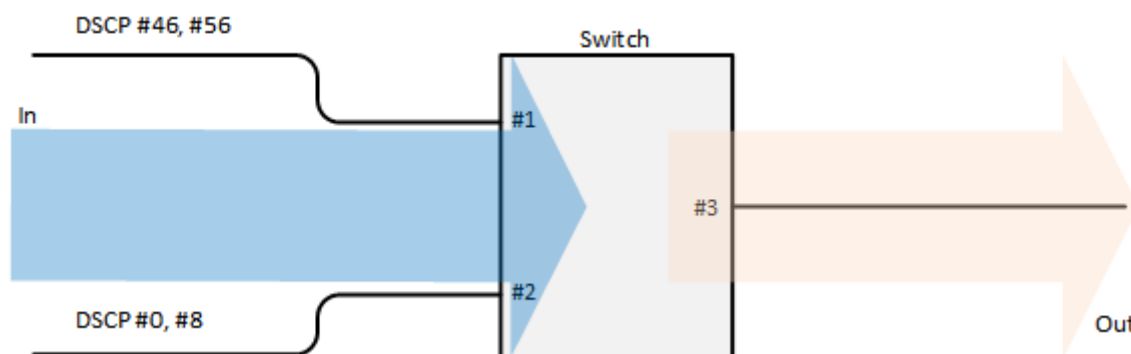
操作項目	操作コマンド
トラフィックシェーピング(ポート単位)の設定	traffic-shape rate
トラフィックシェーピング(キュー単位)の設定	traffic-shape queue rate

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。
DSCP = 56, 46, 8, 0 のフレームを受信するとき、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 (SP) 設定例



- ・ 入力フレームの優先度付けは以下とします。
 - DSCP = 56 のフレームを優先度 7 に設定
 - DSCP = 46 のフレームを優先度 5 に設定
 - DSCP = 8 のフレームを優先度 1 に設定
 - DSCP = 0 のフレームを優先度 0 に設定

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. DSCP - 送信キューID変換テーブルの設定をする。
DSCP値 = 46, 56 に対応する送信キューID はデフォルト値のため、特に設定の必要はありませんが、明示的に記載しています。

```
Yamaha(config)#qos dscp-queue 56 7 ①  
Yamaha(config)#qos dscp-queue 46 5 ②  
Yamaha(config)#qos dscp-queue 8 1 ③  
Yamaha(config)#qos dscp-queue 0 0 ④
```

- ① DSCP = 56 のフレームを送信キュー#7 へ格納
- ② DSCP = 46 のフレームを送信キュー#5 へ格納
- ③ DSCP = 8 のフレームを送信キュー#1 へ格納
- ④ DSCP = 0 のフレームを送信キュー#0 へ格納

3. 送信キューごとのスケジューリング方式を設定する。
デフォルト値のため、特に設定の必要はありませんが、明示的に記載しています。

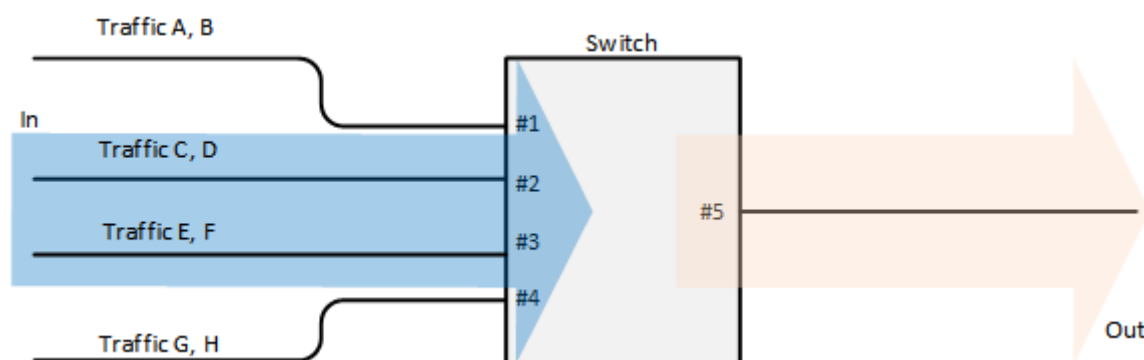
```
Yamaha(config)# no qos wrr-weight 7 ①  
Yamaha(config)# no qos wrr-weight 5 ②  
Yamaha(config)# no qos wrr-weight 1 ③  
Yamaha(config)# no qos wrr-weight 0 ④
```

- ① Queue:7 SP 方式
- ② Queue:5 SP 方式
- ③ Queue:1 SP 方式
- ④ Queue:0 SP 方式

アクセスリストを使用した優先制御(SP+WRR)

送信元 IP アドレスを使用してトラフィックを分類し、優先制御(WRR)を設定します。

- ・ 優先制御 (SP+WRR) 設定例



- ・ 入力フレームの分類条件と優先度付け
 - 192.168.10.2 からのパケットを **トラフィックA** に分類し、パケット送信時の 優先順位 7 に設定する
 - 192.168.20.2 からのパケットを **トラフィックB** に分類し、パケット送信時の 優先順位 6 に設定する
 - 192.168.30.2 からのパケットを **トラフィックC** に分類し、パケット送信時の 優先順位 5 に設定する
 - 192.168.40.2 からのパケットを **トラフィックD** に分類し、パケット送信時の 優先順位 4 に設定する
 - 192.168.50.2 からのパケットを **トラフィックE** に分類し、パケット送信時の 優先順位 3 に設定する

する

- 192.168.60.2 からのパケットを **トラフィックF** に分類し、パケット送信時の 優先順位 2 に設定する
 - 192.168.70.2 からのパケットを **トラフィックG** に分類し、パケット送信時の 優先順位 1 に設定する
 - 192.168.80.2 からのパケットを **トラフィックH** に分類し、パケット送信時の 優先順位 0 に設定する
- スケジューリング方式
SP と WRR を組み合わせた設定を行う。

キューID	方式	重み(%)
7	SP	-
6	SP	-
5	SP	-
4	WRR	8 (40.0%)
3	WRR	6 (30.0%)
2	WRR	3 (15.0%)
1	WRR	2 (10.0%)
0	WRR	1 (5.0%)

1. QoS を有効にして、トラフィック A～H のアクセスリストを定義し、LAN ポートに設定するトラフィッククラスを定義します。

```
Yamaha(config)#qos enable ①
Yamaha(config)#access-list 1 permit any 192.168.10.2 0.0.0.0 any ②
Yamaha(config)#class-map cmap-A
Yamaha(config-cmap)#match access-list 1
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 2 permit any 192.168.20.2 0.0.0.0 any ③
Yamaha(config)#class-map cmap-B
Yamaha(config-cmap)#match access-list 2
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 3 permit any 192.168.30.2 0.0.0.0 any ④
Yamaha(config)#class-map cmap-C
Yamaha(config-cmap)#match access-list 3
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 4 permit any 192.168.40.2 0.0.0.0 any ④
Yamaha(config)#class-map cmap-D
Yamaha(config-cmap)#match access-list 4
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 5 permit any 192.168.50.2 0.0.0.0 any ⑤
Yamaha(config)#class-map cmap-E
Yamaha(config-cmap)#match access-list 5
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 6 permit any 192.168.60.2 0.0.0.0 any ⑥
Yamaha(config)#class-map cmap-F
Yamaha(config-cmap)#match access-list 6
```

```

Yamaha(config-cmap)#exit
Yamaha(config)#access-list 7 permit any 192.168.70.2 0.0.0.0 any ⑦
Yamaha(config)#class-map cmap-G
Yamaha(config-cmap)#match access-list 7
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 8 permit any 192.168.80.2 0.0.0.0 any ⑧
Yamaha(config)#class-map cmap-H
Yamaha(config-cmap)#match access-list 8
Yamaha(config-cmap)#exit

```

- ① QoS を有効にする
- ② トラフィックA
- ③ トラフィックB
- ④ トラフィックC
- ⑤ トラフィックD
- ⑥ トラフィックE
- ⑦ トラフィックF
- ⑧ トラフィックG
- ⑨ トラフィックH

2. CoS - 送信キューID変換テーブルを初期設定に戻します。

```

Yamaha(config)#no qos cos-queue 0
Yamaha(config)#no qos cos-queue 1
Yamaha(config)#no qos cos-queue 2
Yamaha(config)#no qos cos-queue 3
Yamaha(config)#no qos cos-queue 4
Yamaha(config)#no qos cos-queue 5
Yamaha(config)#no qos cos-queue 6
Yamaha(config)#no qos cos-queue 7

```

3. LAN ポート #1 (port1.1) に対するポリシーを生成し、適用します。

Traffic-A に対して CoS 値 7 の送信キューを、Traffic-B に対して CoS 値 6 の送信キューを設定します。

```

Yamaha(config)#policy-map pmap1
Yamaha(config-pmap)#class cmap-A
Yamaha(config-pmap-c)#set cos-queue 7 ①
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-B
Yamaha(config-pmap-c)#set cos-queue 6 ②
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.1 ③
Yamaha(config-if)#service-policy input pmap1 ④
Yamaha(config-if)# exit

```

- ① Traffic-A はローカル優先順位 7
- ② Traffic-B はローカル優先順位 6

③ LAN ポート #1

④ 受信フレームに対しポリシーを適用

4. LAN ポート #2 (port1.2) に対するポリシーを生成し、適用します。
Traffic-C に対して CoS 値 5 の送信キューを、Traffic-D に対して CoS 値 4 の送信キューを設定します。

```
Yamaha(config)#policy-map pmap2
Yamaha(config-pmap)#class cmap-C
Yamaha(config-pmap-c)#set cos-queue 5 ①
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-D
Yamaha(config-pmap-c)#set cos-queue 4 ②
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.2 ③
Yamaha(config-if)#service-policy input pmap2 ④
Yamaha(config-if)# exit
```

① Traffic-C はローカル優先順位 5

② Traffic-D はローカル優先順位 4

③ LAN ポート #2

④ 受信フレームに対しポリシーを適用

5. LAN ポート #3 (port1.3) に対するポリシーを生成し、適用します。
Traffic-E に対して CoS 値 3 の送信キューを、Traffic-F に対して CoS 値 0 の送信キューを設定します。

```
Yamaha(config)#policy-map pmap3
Yamaha(config-pmap)#class cmap-E
Yamaha(config-pmap-c)#set cos-queue 3 ①
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-F
Yamaha(config-pmap-c)#set cos-queue 0 ②
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.3 ③
Yamaha(config-if)#service-policy input pmap3 ④
Yamaha(config-if)# exit
```

① Traffic-E はローカル優先順位 3

② Traffic-F はローカル優先順位 2

③ LAN ポート #3

④ 受信フレームに対しポリシーを適用

6. LAN ポート #4 (port1.4) に対するポリシーを生成し、適用します。
Traffic-G に対して CoS 値 2 の送信キューを、Traffic-H に対して CoS 値 1 の送信キューを設定します。

```
Yamaha(config)#policy-map pmap4
```

```
Yamaha(config-pmap)#class cmap-G  
Yamaha(config-pmap-c)#set cos-queue 2 ①  
Yamaha(config-pmap-c)#exit  
Yamaha(config-pmap)#class cmap-H  
Yamaha(config-pmap-c)#set cos-queue 1 ②  
Yamaha(config-pmap-c)#exit  
Yamaha(config-pmap)#exit  
Yamaha(config)#interface port1.4 ③  
Yamaha(config-if)#service-policy input pmap4 ④  
Yamaha(config-if)#exit
```

- ① Traffic-G はローカル優先順位 1
- ② Traffic-H はローカル優先順位 0
- ③ LAN ポート #4
- ④ 受信フレームに対しポリシーを適用

7. 送信キューのスケジューリング方式を設定します。

キューID 5, 6, 7 は、デフォルト設定のため、特に設定の必要はありませんが、明示的に記載しています。

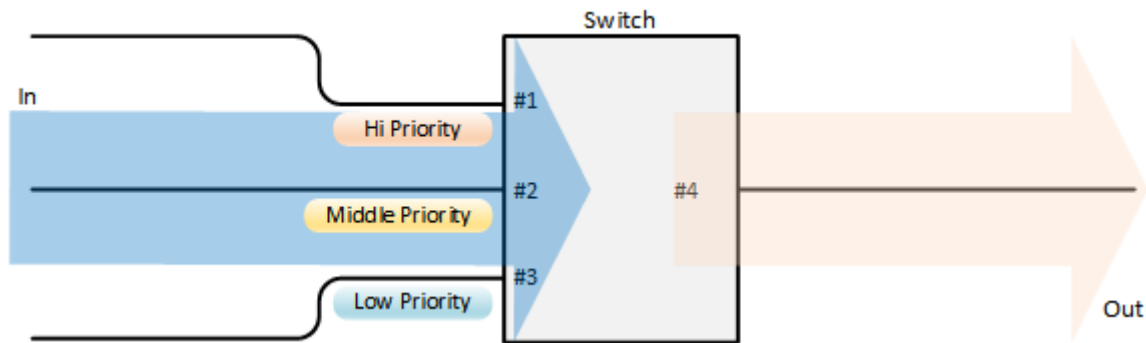
```
Yamaha(config)#qos wrr-weight 0 1 ①  
Yamaha(config)#qos wrr-weight 1 2 ②  
Yamaha(config)#qos wrr-weight 2 3 ③  
Yamaha(config)#qos wrr-weight 3 6 ④  
Yamaha(config)#qos wrr-weight 4 8 ⑤  
Yamaha(config)#no qos wrr-weight 5 ⑥  
Yamaha(config)#no qos wrr-weight 6 ⑦  
Yamaha(config)#no qos wrr-weight 7 ⑧
```

- ① 送信キュー0: WRR 方式、重み付け 1
- ② 送信キュー1: WRR 方式、重み付け 2
- ③ 送信キュー2: WRR 方式、重み付け 3
- ④ 送信キュー3: WRR 方式、重み付け 6
- ⑤ 送信キュー4: WRR 方式、重み付け 8
- ⑥ 送信キュー5: SP 方式
- ⑦ 送信キュー6: SP 方式
- ⑧ 送信キュー7: SP 方式

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

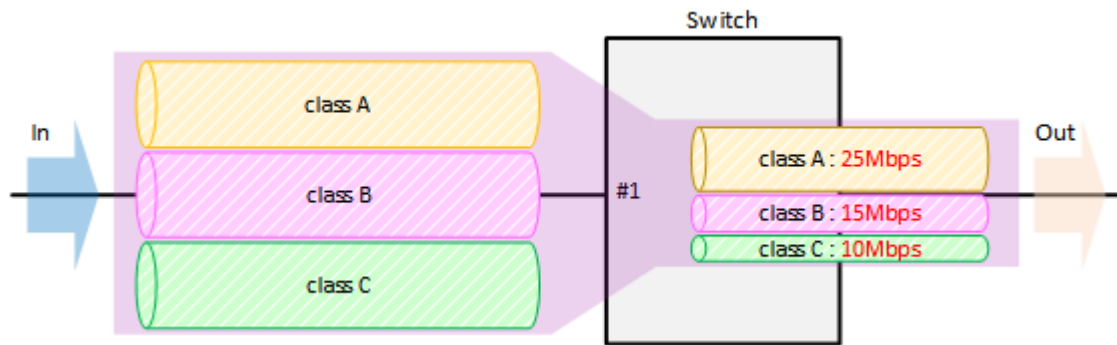
```
Yamaha(config)#qos enable ①
Yamaha(config)#interface port1.1 ②
Yamaha(config-if)#qos trust port-priority ③
Yamaha(config-if)#qos port-priority-queue 6 ④
Yamaha(config-if)#exit
Yamaha(config)#interface port1.2 ⑤
Yamaha(config-if)#qos trust port-priority ⑥
Yamaha(config-if)#qos port-priority-queue 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

アクセスリストを使用した帯域制御(ツインレート・個別ポリサー)

送信元 IP アドレスを使用して帯域制御を設定します。メータリングはツインレートポリサー、個別ポリサーを使用します。

- ・ 帯域制御 設定例



・ 入力フレームの分類条件と帯域制限の設定

- 192.168.10.2 からのパケットを **トラフィックA** に分類し、受信レート (CIR) 25Mbps を保証する
- 192.168.20.2 からのパケットを **トラフィックB** に分類し、受信レート (CIR) 15Mbps を保証する
- 192.168.30.2 からのパケットを **トラフィックC** に分類し、受信レート (CIR) 10Mbps を保証する

1. QoS を有効にして、トラフィック A～C のアクセスリストを定義し、LAN ポートに設定するトラフィッククラスを定義します。

```
Yamaha(config)#qos enable ①
Yamaha(config)#access-list 1 permit any 192.168.10.2 0.0.0.0 any ②
Yamaha(config)#class-map cmap-A
Yamaha(config-cmap)#match access-list 1
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 2 permit any 192.168.20.2 0.0.0.0 any ③
Yamaha(config)#class-map cmap-B
Yamaha(config-cmap)#match access-list 2
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 3 permit any 192.168.30.2 0.0.0.0 any ④
Yamaha(config)#class-map cmap-C
Yamaha(config-cmap)#match access-list 3
Yamaha(config-cmap)#exit
```

① QoS を有効にする

② トラフィックA

③ トラフィックB

④ トラフィックC

2. LAN ポート #1 (port1.1) に対するポリシーを生成し、適用します。

トラフィックA からトラフィックC に対して、個別にメータリングを設定します。

ツインレートポリサーにおいて Yellow, Red を破棄することにより、Green の帯域を確保（保証）することができます。

```
Yamaha(config)#policy-map pmap1
Yamaha(config-pmap)#class cmap-A ①
Yamaha(config-pmap-c)#police twin-rate 25000 25000 156 50 yellow-action drop red-action drop
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-B ②
```

```

Yamaha(config-pmap-c)#police twin-rate 15000 15000 93 50 yellow-action drop red-action
drop
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-C ③
Yamaha(config-pmap-c)#police twin-rate 10000 10000 62 50 yellow-action drop red-action
drop
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.1... (LAN ポート 1)
Yamaha(config-if)#service-policy input pmap1 ⑤
Yamaha(config-if)#exit

```

① Traffic-A メータリング設定

② Traffic-B メータリング設定

③ Traffic-C メータリング設定

④ LAN ポート 1

⑤ 受信フレームに対しポリシーを適用

。メータリングの設定値は、以下となります。

- メータリング種別: ツインレートポリサー
- Traffic-A : CIR, PIR (25,000 kbps)、CBS (156 kbyte)、PBS (50 kbyte)
- Traffic-B : CIR, PIR (15,000 kbps)、CBS (93 kbyte)、PBS (50 kbyte)
- Traffic-C : CIR, PIR (10,000 kbps)、CBS (62 kbyte)、PBS (50 kbyte)

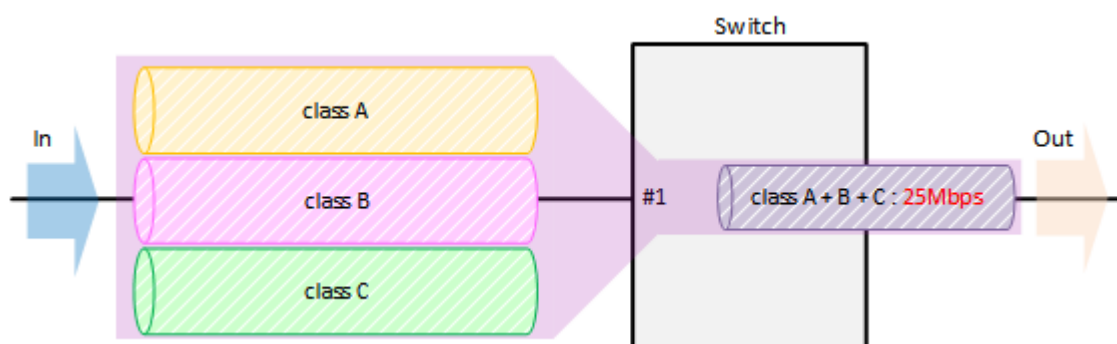
CBS は 往復時間を 0.05 秒とし、以下の算出式により求めています。

$CBS = CIR (bps) \div 8 (bit) \times 0.05 (second)$

アクセスリストを使用した帯域制御(シングルレート・集約ポリサー)

送信元 IP アドレスを使用して帯域制御を設定します。メータリングはシングルレートポリサー、集約ポリサーを使用します。

・ 帯域制御 設定例



・ 入力フレームの分類条件と帯域制限の設定

- 。 192.168.10.2 からのパケットを **トラフィックA** に分類する。
- 。 192.168.20.2 からのパケットを **トラフィックB** に分類する。
- 。 192.168.30.2 からのパケットを **トラフィックC** に分類する。
- 。 トラフィックA, B, C の受信レートを、併せて 25Mbps に制限する。
- 。 帯域クラス Yellow は DSCP = 0 にリマーケティングして、低優先度で送信する。

1. QoS を有効にして、トラフィック A～C のアクセスリストを定義し、LAN ポートに設定するトラフィッククラスを定義します。

```
Yamaha(config)#qos enable ①
Yamaha(config)#access-list 1 permit any 192.168.10.2 0.0.0.0 any ②
Yamaha(config)#class-map cmap-A
Yamaha(config-cmap)#match access-list 1
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 2 permit any 192.168.20.2 0.0.0.0 any ③
Yamaha(config)#class-map cmap-B
Yamaha(config-cmap)#match access-list 2
Yamaha(config-cmap)#exit
Yamaha(config)#access-list 3 permit any 192.168.30.2 0.0.0.0 any ④
Yamaha(config)#class-map cmap-C
Yamaha(config-cmap)#match access-list 3
Yamaha(config-cmap)#exit
```

① QoS を有効にする

② トラフィックA

③ トラフィックB

④ トラフィックC

2. DSCP-送信キューID変換テーブルを設定します。
Yellow のリマーケティングで使用する DSCP値 (0) に対して、最低優先度の送信キューを割り当てます。

```
Yamaha(config)#qos dscp-queue 0 0
```

3. 集約ポリサーを作成します。

```
Yamaha(config)#aggregate-police agp1 ①
Yamaha(config-agg-policer)#police single-rate 25000 156 50 yellow-action remark red-
action drop
Yamaha(config-agg-policer)#remark-map yellow ip-dscp 0
Yamaha(config-agg-policer)#exit
```

① 集約ポリサーを作成

- ・ 集約ポリサーのメータリングの設定値は、以下となります。

- メータリング種別: シングルレートポリサー
- Yellow は DSCP値 = 0 にリマーケティング
- CIR (25,000 kbps)、CBS (156 kbyte)、EBS (50 kbyte)

CBS は 往復時間を 0.05 秒とし、以下の算出式により求めています。

$$CBS = CIR (bps) \div 8 (bit) \times 0.05 (second)$$

4. LAN ポート #1 (port1.1) に対するポリシーを生成し、適用します。
トラフィックA から トラフィックC を一つに集約したメータリング (集約ポリサー) を設定します。

```
Yamaha(config)#policy-map pmap1
```

```
Yamaha(config-pmap)#class cmap-A ①
Yamaha(config-pmap-c)#police-aggregate agp1
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-B ②
Yamaha(config-pmap-c)#police-aggregate agp1
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#class cmap-C ③
Yamaha(config-pmap-c)#police-aggregate agp1
Yamaha(config-pmap-c)#exit
Yamaha(config-pmap)#exit
Yamaha(config)#interface port1.1 ④
Yamaha(config-if)#service-policy input pmap1 ⑤
Yamaha(config-if)#exit
```

- ① Traffic-A メータリング設定
- ② Traffic-B メータリング設定
- ③ Traffic-C メータリング設定
- ④ LAN ポート 1
- ⑤ 受信フレームに対しポリシーを適用

注意事項

- ・ 以下の設定が異なるLAN/SFPポートは論理インターフェースとして束ねることはできません。また、スタートアップコンフィグ上の論理インターフェースに所属しているLAN/SFPポートの以下の設定は、最若番ポートの設定が論理インターフェースに適用されます。
 - トラストモード
 - デフォルトCoS
 - ポート優先度
- ・ ポリシーマップが適用されたLAN/SFPポートは、論理インターフェースに所属できません。
- ・ ポリシーマップは論理インターフェースに所属しているLAN/SFPポートに対して適用できません。ただし、スタートアップコンフィグ上に論理インターフェースに所属しているLAN/SFPポートにポリシーマップがある場合、最若番ポートの設定が論理インターフェースに適用されます。
- ・ フラグメントパケットは正しく条件判定できない場合があります。具体的には、条件にレイヤー 4 の情報（送信元ポート番号、宛先ポート番号、TCP の各種フラグ）が含まれる場合、2 番目以降のフラグメントパケットにそれらの情報が含まれないため正しい判定ができません。フラグメントパケットを処理する可能性がある場合には条件にレイヤー 4 の情報を含めないようにしてください。

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

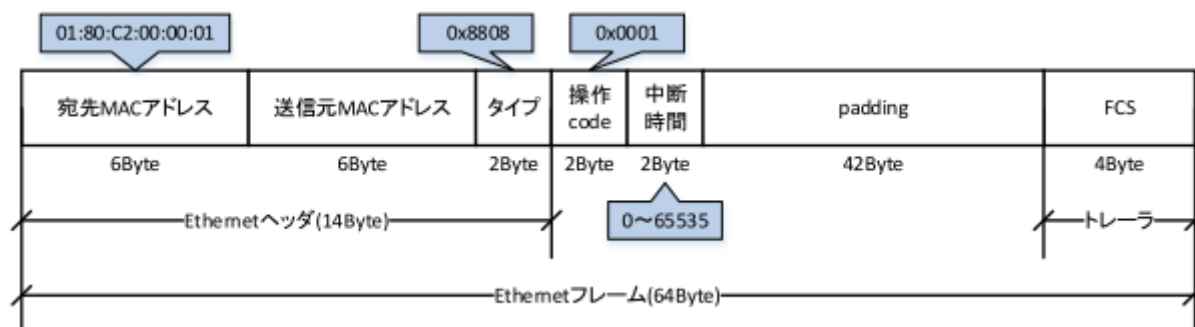
データの送信と受信を同時に行うことができない半二重通信では、データの衝突が発生する可能性がある。送信側の端末は、データ送信中に衝突の発生を監視しており、衝突を検出すると、送信を停止してジャム信号を送信する。ジャム信号送信後はランダムな待ち時間待機し、再度送信処理を行う。なお、IEEE では、ジャム信号について定義されていないが「10101010101010101010101010101010」のように、1 と 0 が交互に 32 個並んだビット列になっていることが多い。

機能詳細

IEEE 802.3x フロー制御

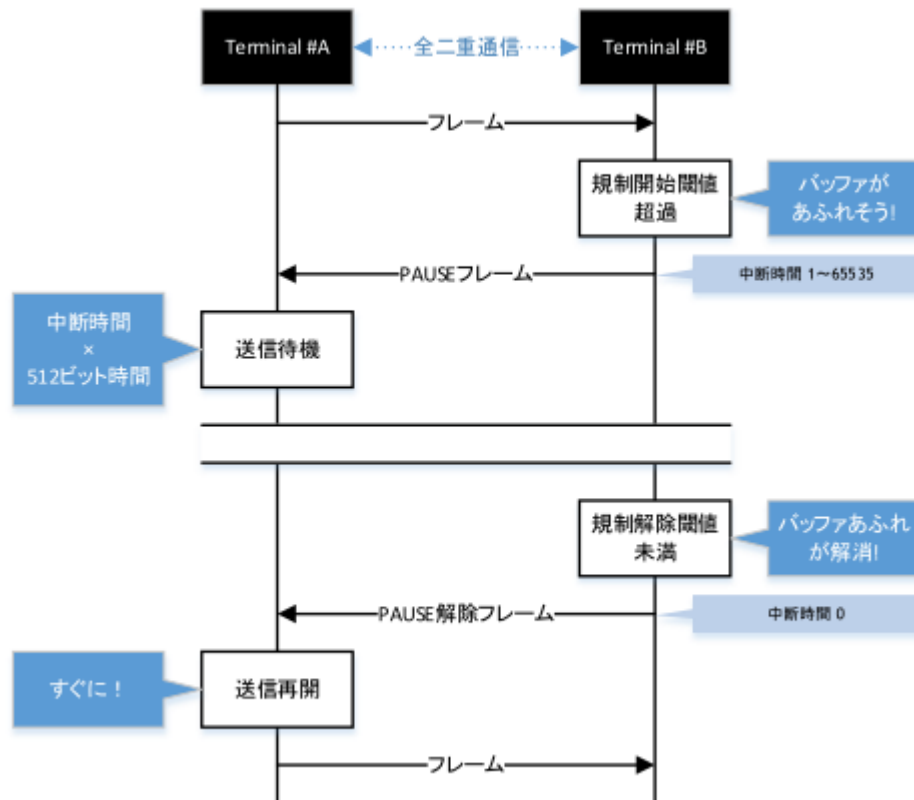
全二重通信の場合、IEEE802.3x オプションの MAC 制御プロトコルを使用することができます。フロー制御には、下図の **MAC 制御フレーム** が使われます。

- ・ MAC 制御フレーム



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
 - 受信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。
 - 受信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/SFP 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。

スタック機能が有効な場合を除き、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。

Qos機能を有効にしているとき、**フロー制御を有効にすることはできません**。

スタック機能を有効にしているとき、**Pauseフレームの受信のみ** 可能です。

バックプレッシャー

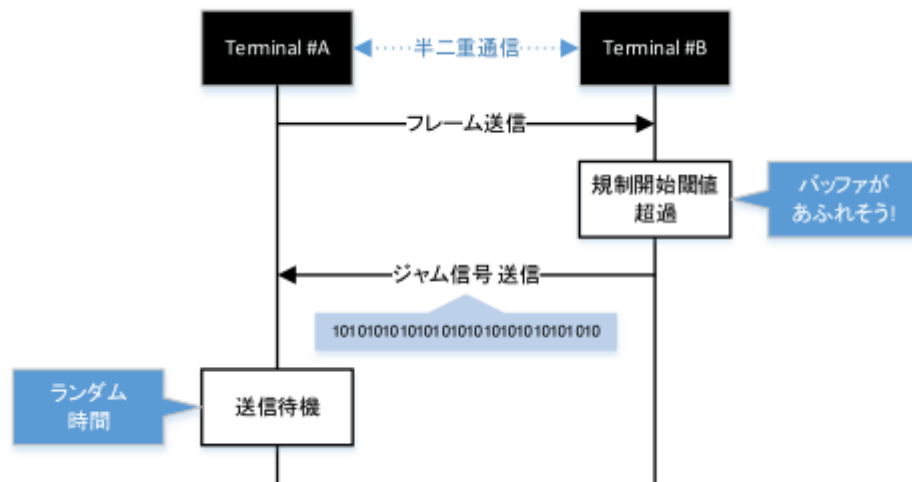
本製品は、LANポートの受信バッファがあふれそうになると、**ジャム信号** を送信します。

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。

スタック有効時にはスタックポートを経由した通信の場合、ジャム信号を送信しません。

・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願います。

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/SFP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/SFP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。

なお、**独自ループ検出** 機能と **ストーム制御** 機能を併用して使うと、**ループ検出の精度を高める (未然に防ぐ)** ことができます。

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/SFP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/SFP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. ストーム制御の **有効・無効のタイミング** で以下の **SYSLOG** を出力します。
 - ・有効時： [STORM]:inf: storm-control ENABLE (port:port1.1, type:B M U, level:50. 0%)
 - ・無効時： [STORM]:inf: storm-control DISABLE (port:port1.1)
4. 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。
5. LAN/SFP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

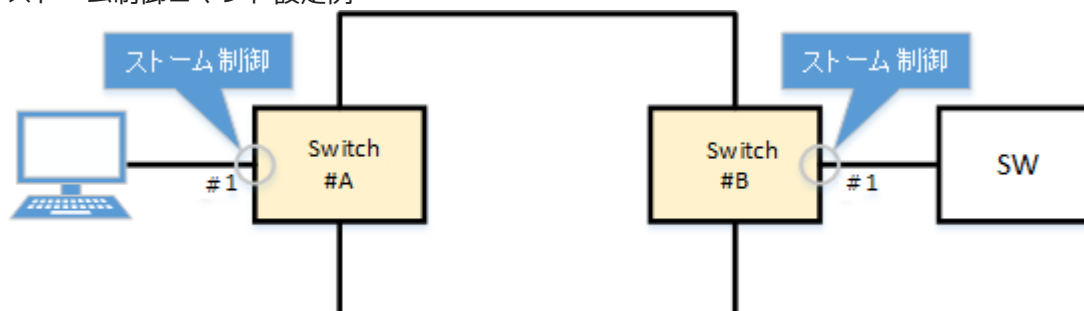
関連コマンドについて、以下に示します。
コマンドの詳細は、コマンドリファレンスを参照願います。

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。

- ・ ストーム制御コマンド設定例



```
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%
```

① broadcastを帯域の30%までに制限

注意事項

特になし

関連文書

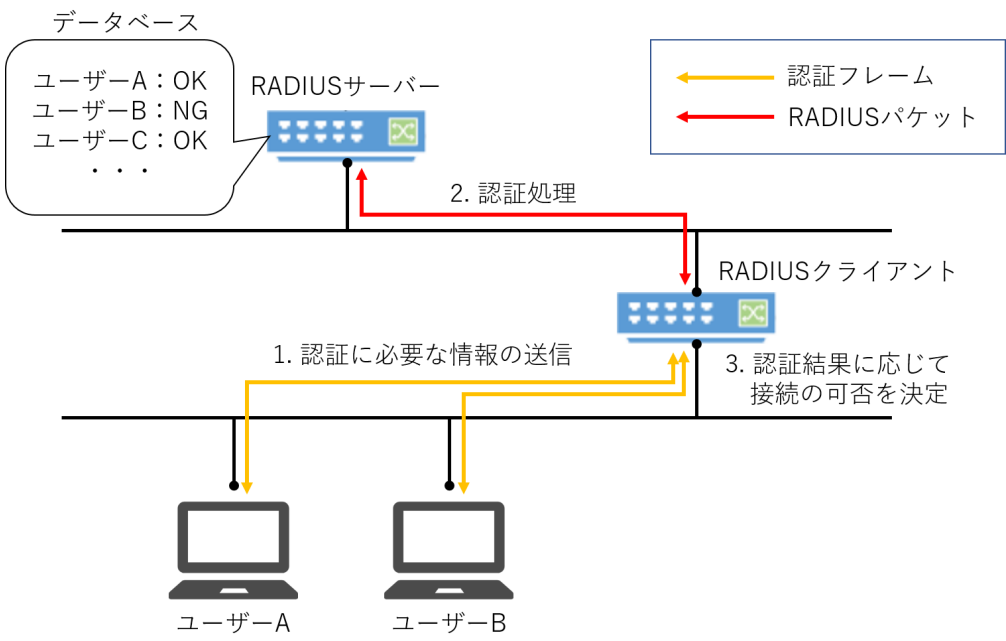
- ・ [Layer 2機能 : 独自ループ検出](#)

アプリケーション層機能

RADIUSサーバー

機能概要

RADIUSサーバー機能とは、ユーザー情報や証明書を管理し、クライアントから通知される情報を基にして認証を行う機能です。
本機のMAC認証・802.1X認証・Web認証と組み合わせることで、本機単体で認証機能を実現することができます。
また、本機以外の機器での認証時に本機を認証サーバーとして動作させることができます。



RADIUSサーバー機能の基本性能および対応する認証方式は以下のとおりです。

・基本性能

項目	性能
登録可能RADIUSクライアント数	100件
登録可能ユーザー数	2000件
鍵強度	2048ビット
署名アルゴリズム	SHA256
認証局名(デフォルト値)	swx-radius

・対応する認証方式

認証方式	用途
PAP	MAC認証
EAP-MD5	IEEE802.1X認証、MAC認証、WEB認証

認証方式	用途
EAP-TLS	IEEE802.1X認証
EAP-TTLS	IEEE802.1X認証
PEAP	IEEE802.1X認証

用語の定義

PKI (Public Key Infrastructure)

公開鍵基盤。公開鍵暗号を使用した、デジタル証明書、認証局(CA)などが含まれます。

認証局(CA)

信頼性を担保する機関。ルート認証局と中間認証局に分けられます。
ルート認証局を最上位に配置し、その配下に中間認証局がある木構造をなしています。

中間認証局

認証局(CA)の中でも、その信頼性がより上位の認証局(CA)によって担保されている認証局のことを指します。

ルート認証局

認証局(CA)の中でも、その信頼性が、自局自身によって担保されている認証局のことを指します。

ルート認証局証明書

発行者と主体者が同じであり、かつ自分自身の秘密鍵で、それに対応する自らの公開鍵に署名した公開鍵証明書のことで、木構造をなす証明書のルートとなるものです。

デジタル証明書

認証局が発行する公開鍵が、真正の発行者の公開鍵であることを証明するデータのことで、
発行者が、公開鍵と共に認証局(CA)に対して、証明書発行要求をおこなうと、認証局(CA)は精査し確認したのちにデジタル証明書を発行します。

EAP-MD5認証方式 (Message digest algorithm 5)

ユーザー名とパスワードを使う認証方式ですが、パスワード平文の代わりにMD5ハッシュ値を交換して認証します。

EAP-TLS認証方式 (Transport Layer Security)

IEEE 802.1Xで用いられる認証方式EAP実装の一種で、ユーザーIDとパスワードによる認証ではなくユーザーとRADIUSサーバー間のトランスポート層を暗号化した上で電子証明書を交換して認証します。RFC2716、RFC5216で規定されます。

EAP-TTLS認証方式 (Tunneled TLS)

IEEE 802.1Xで用いられる認証方式EAP実装の一種で、サーバーの電子証明書を用いてTLS通信路を構築し、その暗号化された通信路内でパスワードによりユーザーを認証します。RFC5281で規定されます。

PEAP認証方式 (Protected EAP)

動作原理はEAP-TTLSと同等(暗号トンネル内のプロトコルの違いのみ)で、サーバーの電子証明書を用いてTLS

通信路を構築し、その暗号化された通信路内でパスワードによりユーザーを認証します。

信頼されるということ

信頼性のある第三者機関によって、公開鍵が発行者のものであることの証明書が、発行されていること。

RADIUSサーバー

RADIUSサーバー機能を提供するホスト機器、ここでは本機のことを指します。

RADIUSサーバーを介して、接続されたユーザーを認証し、ユーザーID、パスワード、MACアドレス、所属VLAN等の認証・認可情報を管理します。

サーバー証明書

上記、RADIUSサーバーが信頼されていることを認証局(CA)が証明した証書です。

RADIUSクライアント

NAS、オーセンティケーターとも言われ、LAN/SFPポートに接続されたユーザーと認証サーバーの間を中継し、認証の成否によりLANへのアクセスを制御します。

ユーザー

RADIUSクライアントに接続して認証を要求する機器、又はソフトウェアであるサブリカントを指します。

認証する個人を特定するための最小単位となります。ユニークなユーザーIDと、パスワード、など認証や認可に必要なデータがあります。

クライアント証明書(ユーザー証明書)

上記、ユーザーが信頼されていることを認証局(CA)が証明した証書です。

機能詳細

ルート認証局

RADIUSサーバー機能を使用するためには、最初にルート認証局を作成する必要があります。

ルート認証局は、デジタル証明書の発行・管理に利用されるものであり、**crypto pki generate ca** コマンドで作成することができます。

認証局名は、**crypto pki generate ca** コマンドの引数で指定することができ、省略した場合は **swx-radius** となります。

ルート認証局をもとにして発行・管理される証明書には以下のものがあります。

すべての証明書で、鍵強度は2048ビット、署名アルゴリズムはSHA256となります。

ルート認証局証明書	本機が信頼されたルート認証局であることを証明します。 ルート認証局の作成と同時に発行されます。 有効期限は証明書作成から2037年12月31日 23時59分59秒 (JST)が適用されます。
サーバー証明書	本機が信頼されたサーバーであることを証明します。 ルート認証局の作成と同時に発行されます。 有効期限は証明書作成から2037年12月31日 23時59分59秒 (JST)が適用されます。
クライアント(ユーザー)証明書	ユーザーが信頼されていることを証明します。

クライアント失効証明書	クライアント証明書が無効になったことを証明します。

ルート認証局は以下の操作によって削除または上書きされます。

- **cold start** コマンドを実行したとき削除されます。
- **no crypto pki generate ca** コマンドを実行したとき削除されます。
- **stack enable** コマンドを実行したとき削除されます。
- **stack disable** コマンドを実行したとき削除されます。
- **erase startup-config** コマンドを実行したとき削除されます。
- **crypto pki generate ca** コマンドを再度実行したとき上書きされます。
- **restore system** コマンドを実行したとき上書きされます。
- **copy radius-server local** コマンドを実行したとき上書きされます。

最初に設置したルート認証局を一貫して保持し続ける必要がありますので、不用意に削除してしまわないようご注意ください。

また万一削除してしまった場合に備えて、後述のバックアップを予め行っておくよう対策をお願いします。

ひとたびルート認証局を削除してしまうと、同じ認証局名を設定したとしても以前とは異なる認証局になります。

もしバックアップ前にルート認証局を削除してしまった場合、それ以降は証明書の追加/失効はできません。証明書の発行を最初から全てやり直すことになります。

crypto pki generate ca コマンドによってルート認証局が作成されると、自動的に内部領域に保存されるため **write** コマンドを実行する必要はありません。

RADIUSクライアントの設定

RADIUSサーバーにアクセスすることを許可するRADIUSクライアントを **nas** コマンドで指定します。

個別のIPアドレスまたはネットワークアドレスで指定することができ、最大で **100件** を設定することができます。

RADIUSクライアントとして、以下の製品で動作を確認しています。

- ヤマハスイッチ(SWXシリーズ)
- ヤマハルーター(RTXシリーズ、NVRシリーズ)
- ヤマハ無線アクセスポイント(WLXシリーズ)

nas コマンドで設定したRADIUSクライアントの設定は、**show running-config** 等でコンフィグに表示されません。

コンフィグとは別の領域に自動保存されるため **write** コマンドを実行する必要はありませんが、実際の動作に反映させるためには **radius-server local refresh** コマンドを実行する必要があります。

設定内容を確認するには、**show radius-server local nas** コマンドを使用します。

ユーザーの登録

認証を行うユーザー情報は、**user** コマンドで登録します。

ユーザー情報は最大で **2000件** 登録することができます。

user コマンドで設定可能な項目は以下のとおりです。

タイプ	項目	概要・備考

必須	ユーザーID	ユーザー情報を一意に識別するためのID
パスワード	ユーザーIDと組み合わせて使用されるパスワード クライアント証明書が圧縮されている場合には、解凍にこのパスワードを使用します。	オプション
ユーザー名称	ユーザーの識別のため、任意の文字列を設定することができます。	
MACアドレス	RADIUSクライアントがCalling-Station-Idを通知してきたときに比較され、一致しないと認証されません。	
SSID	RADIUSクライアントがCalled-Station-Idを通知してきたときに比較され、一致しないと認証されません。	
メールアドレス	証明書をメールで送付するときの宛先となります。	
認証方式	デフォルトではEAP-TLSとなるため、他の認証方式とする場合には指定する必要があります。	
証明書有効期限	認証方式がEAP-TLSのときのみ有効で、省略した場合は2037年12月31日23時59分59秒となります。	

user コマンドで設定したユーザー設定は、**show running-config** 等でコンフィグに表示されません。コンフィグとは別の領域に自動保存されるため **write** コマンドを実行する必要はありませんが、実際の動作に反映させるためには **radius-server local refresh** コマンドを実行する必要があります。設定内容を確認するには、**show radius-server local user** コマンドを使用します。

認証方式の制限

authentication コマンドで認証方式を制限することができます。初期設定では認証方式は制限されていませんが、一時的に特定の認証方式を無効にしたい場合などで使用することができます。

RADIUSサーバー機能の有効化

RADIUSサーバー機能を有効にするには、**radius-server local enable** コマンドを使用します。RADIUSクライアントやユーザー情報の設定を行い、必要な準備が整ってからRADIUSサーバー機能を有効にしてください。

設定内容の動作への反映

RADIUSサーバーに関連した設定を追加・変更・削除した場合、**radius-server local refresh** コマンドを実行することで実動作に反映されます。**radius-server local refresh** コマンドによって実動作に反映されるコマンドは以下のとおりです。

- **authentication** コマンド

- **nas** コマンド
- **reauth interval** コマンド
- **user** コマンド

WebGUIでRADIUSサーバーに関連した設定を追加・変更・削除した場合には、自動的に **radius-server local refresh** コマンドに相当する処理が行われます。

クライアント証明書の発行

証明書を使った認証を行うユーザー(**user** コマンドで認証方式をEAP-TLSとしたユーザー)に対してクライアント証明書を発行する場合には、**certificate user** コマンドを使用します。
1ユーザーにつき、最大2通までクライアント証明書を保持することができ、3通目のクライアント証明書を発行すると既存のクライアント証明書の中で古いほうのクライアント証明書が失効します。

certificate user コマンドで個別のユーザーIDを指定した場合、指定したユーザーのクライアント証明書が発行されます。

certificate user コマンドで個別のユーザーIDを指定しない場合、以下の条件のどちらかに合致するすべてのユーザーのクライアント証明書が発行されます。

クライアント証明書の一括発行の対象条件

- 一度もクライアント証明書が発行されていない
- クライアント証明書が発行されたあと、パスワードまたは有効期限が変更されている

クライアント証明書の発行には、1通あたりおおよそ **15秒** 程度かかります。**certificate user** コマンドではバックグラウンドでクライアント証明書の発行処理が行われますが、複数のユーザーのクライアント証明書を一括発行する場合には時間がかかる可能性があるため注意してください。

クライアント証明書の発行を途中でキャンセルするには、**certificate abort** コマンドを使用します。

発行したクライアント証明書を取り出す方法は以下の通りです。

- **certificate user** コマンドでのmailオプション指定
クライアント証明書の発行と同時に指定したメールアドレスに対してクライアント証明書を送付することができます。
クライアント証明書はZIP圧縮されており、**user** コマンドのパスワードで解凍することができます。
クライアント証明書のメール送信の詳細については [証明書のメール送信](#) を参照してください。
- **certificate export sd** コマンド
任意のユーザーまたはすべてのユーザーのクライアント証明書を microSD にコピーして取り出すことができます。
compressオプションによって任意のユーザーのクライアント証明書を圧縮して取り出した場合、**user** コマンドのパスワードで解凍することができます。
compressオプションによってすべてのユーザーのクライアント証明書をまとめて圧縮して取り出した場合、パスワード不要で解凍することができます。
- **certificate export mail** コマンド
任意のユーザーまたはすべてのユーザーのクライアント証明書を **user** コマンドで設定したメールアドレス宛に送信することができます。
クライアント証明書はZIP圧縮されており、**user** コマンドのパスワードで解凍することができます。
- [Web GUIで本機にアクセス](#)
任意のユーザーまたはすべてのユーザーのクライアント証明書をダウンロードすることができます。
ZIP圧縮されていますが、解凍にパスワードは不要です。

クライアント証明書の失効

クライアント証明書を発行したユーザーに対して認証できないようにするには、失効証明書を発行する必要があります。

任意のユーザーに対して失効証明書が発行されると、認証処理において失効証明書が参照され、認証結果に反映されます。

失効証明書は以下の処理によって発行されます。

- **certificate revoke id** コマンドの実行
指定された証明書IDのクライアント証明書に対して失効証明書が発行されます。
- **certificate revoke user** コマンドの実行
指定されたユーザーのすべてのクライアント証明書に対して失効証明書が発行されます。
- **user** コマンドで認証方式をEAP-TLSからその他(PAP,PEAP,EAP-MD5,EAP-TTLS)に変更
対象ユーザーのすべてのクライアント証明書に対して失効証明書が発行されます。
対象ユーザーの認証方式を再度EAP-TLSに変更した場合は、**クライアント証明書の発行**の対象となります。
- **user** コマンドの削除
対象ユーザーのすべてのクライアント証明書に対して失効証明書が発行されます。
対象ユーザーと同じユーザーIDで再度ユーザーを登録した場合、**クライアント証明書の発行**の対象となります。
- **certificate user** コマンドで3通目のクライアント証明書を発行
対象ユーザーの古い方のクライアント証明書に対して失効証明書が発行されます。
- **ユーザー情報のインポートとエクスポート** でのインポート
インポートによってユーザーが削除された場合には、削除されたユーザーのすべてのクライアント証明書に対して失効証明書が発行されます。

証明書のメール送信

クライアント証明書の発行に記載されているクライアント証明書のメール送信を使用する場合には、事前に以下の準備が必要です。

ここで記載する設定は最低限のものであり、使用状況にあわせて必要な設定を行ってください。

1. SMTPサーバーの設定

1. **mail server smtp host** コマンドでSMTPサーバーを指定します。

2. メールテンプレートの設定

1. **mail template** コマンドでテンプレートIDを指定し、テンプレート設定モードに移行します。
2. **mail server smtp host** コマンドで設定したSMTPサーバーのメールサーバーIDを、**send server** コマンドで指定します。
3. **send from** コマンドで送信元メールアドレスを指定します。

3. 証明書のメール送信で使用するメールテンプレートの指定

1. **mail send certificate** コマンドで、上記で作成したメールテンプレートのIDを指定します。

メールの件名および本文は以下のとおりです。フォーマットを変更することはできません。

件名	Certification Publishment

本文	Certification is published. Name : [userコマンドの NAME/パラメーター] Account : [userコマンドの USERID/パラメーター] MAC address : XX:XX:XX:XX:XX:XX Expire : YYYY/MM/DD

設定および証明書の確認

- ・ **RADIUSクライアントの設定の確認**

show radius-server local nas コマンドを使用します。

```
Yamaha# show radius-server local nas 192.168.100.0/24
host                                     key
-----
192.168.100.0/24                       abcde
```

- ・ **ユーザーの設定の確認**

show radius-server local user コマンドを使用します。

```
Yamaha# show radius-server local user

Total      1

userid          name          vlan mode
-----
00a0de000000    Yamaha          1 eap-md5
```

```
Yamaha# show radius-server local user detail 00a0de000000

Total      1

userid      : 00a0de000000
password    : secretpassword
mode        : eap-md5
name        : Yamaha
vlan        : 1
```

- ・ **クライアント証明書の発行処理の状況確認**

show radius-server local certificate status コマンドを使用します。

```
Yamaha# show radius-server local certificate status
certificate process: xxxx/ zzzz processing...
```

- ・ **クライアント証明書の一覧確認**

show radius-server local certificate list コマンドを使用します。

```
Yamaha# show radius-server local certificate list detail Taro
```

userid	certificate number
-----	-----
----	----
Yamaha	Yamaha-DF598EE9B44D22CC
2018/12/31	
	Yamaha-DF598EE9B44D22CD
2019/12/31	

・失効証明書の確認

show radius-server local certificate revoke コマンドを使用します。

```
Yamaha# show radius-server local certificate revoke
```

userid	certificate number	reason
-----	-----	-----
----	----	----
Yamaha	Yamaha-DF598EE9B44D22CC	
expired		
Yamaha	Yamaha-DF598EE9B44D22CD	
revoked		

クライアント証明書の期限切れ事前メール通知

クライアント証明書の有効期限が切れる前にメールで通知を行うことができます。

事前メール通知を利用するには事前に以下の準備が必要です。

ここで記載する設定は最低限のものであり、使用状況にあわせて必要な設定を行ってください。

1. SMTPサーバーの設定

1. **mail server smtp host** コマンドでSMTPサーバーを指定します。

2. メールテンプレートの設定

1. **mail template** コマンドでテンプレートIDを指定し、テンプレート設定モードに移行します。

2. **mail server smtp host** コマンドで設定したSMTPサーバーのメールサーバーIDを、**send server** コマンドで指定します。

3. **send from** コマンドで送信元メールアドレスを指定します。

3. 証明書の期限切れ事前メール通知で使用するメールテンプレートの指定

1. **mail send certificate-notify** コマンドで、上記で作成したメールテンプレートのIDを指定します。

4. 証明書の期限切れ事前メール通知を行うタイミングの指定

1. **mail certificate expire-notify** コマンドで、有効期限切れの何日前にメール通知を行うか指定します。

クライアント証明書の期限切れ事前メール通知の対象となる証明書の確認は、**毎日23時59分59秒** に実施されます。

メールの件名および本文は以下のとおりです。フォーマットを変更することはできません。

件名	Certification expiration
本文	Your certificate will expire in [残り日数] days. Name : [userコマンドのNAME/パラメーター] Account : [userコマンドのUSERID/パラメーター] MAC address : XX:XX:XX:XX:XX:XX Expire : YYYY/MM/DD

ユーザー情報のインポートとエクスポート

・エクスポート

Web GUIからユーザー情報をCSV形式ファイルとしてエクスポートすることができます。

エクスポートしたCSV形式ファイルに追記することでユーザーをまとめて登録することができます。

本機でエクスポートしたユーザー情報をヤマハ無線アクセスポイント(WLXシリーズ)でインポートすることはできません。

・インポート

Web GUIからユーザー情報をインポートすることができます。

ユーザー情報をインポートするとき、インポートに伴ってクライアント証明書の発行対象となったユーザーに対して、一括でクライアント証明書を発行することができます。

ユーザーが多数含まれるユーザー情報をインポートする場合、実動作に反映されるまで時間がかかることがあります。

ヤマハ無線アクセスポイント(WLXシリーズ)でエクスポートしたユーザー情報を本機にインポートすることができます。

ただし、本機で使用できない文字が含まれていた場合、そのユーザーはインポートすることはできません。別途個別にユーザーの追加を行ってください。

本機で使用できない文字については、[注意事項](#)を参照してください。

すべてのRADIUSサーバー関連情報のバックアップとリストア

本機では、ルート認証局を含むすべてのRADIUSサーバー関連情報のバックアップ・リストアを行うことができます。

・バックアップ

copy radius-server local コマンドでエクスポート先としてmicroSDを指定することで、すべてのRADIUSサーバー関連情報をmicroSDにバックアップすることができます。

また、Web GUIからも同等のバックアップを行うことができます。機器の故障等に備えてバックアップしておくことを勧めます。

バックアップファイルには、以下の3つのコマンドの設定情報は含まれますが、それ以外のRADIUSサーバー機能に関わる設定情報は含まれません。バックアップファイルと併せてコンフィグファイルもバックアップしておくことを勧めます。

- **crypto pki generate ca** コマンド
- **user** コマンド
- **nas** コマンド

本機でバックアップしたすべてのRADIUSサーバー関連情報をヤマハ無線アクセスポイント(WLXシリーズ)でリストアすることはできません。

・ リストア

copy radius-server local コマンドでエクスポート先として内部のコンフィグ番号を指定することで、上記でバックアップしたデータをmicroSDからリストアすることができます。
また、Web GUIからも同様のリストアを行うことができ、SWXシリーズであればどのモデルで取得したデータであってもリストアすることができます。
ルート認証局が作成されている状態でリストアを行う場合には、ルート認証局が上書きされるため注意してください。

ヤマハ無線アクセスポイント(WLXシリーズ)でバックアップしたRADIUSサーバー関連情報のリストア

本機では、ヤマハ無線アクセスポイント(WLXシリーズ)でバックアップしたRADIUSサーバー関連情報をリストアすることができます。リストアはWeb GUIでのみ行うことができます。

ヤマハ無線アクセスポイント(WLXシリーズ)で動作させていたRADIUSサーバー機能を本機に移行する場合には、以下の手順を実施してください。

1. ヤマハ無線アクセスポイント(WLXシリーズ)でバックアップしたデータを本機にリストアします。
WLX402では、Web GUIのRADIUSサーバー設定ページからバックアップデータ(ZIPファイル)を取得することができます。
WLX313では、Web GUIの設定(保存/復元)ページからバックアップデータ(ZIPファイル)を取得することができます。
2. **nas** コマンドまたはWeb GUIでRADIUSクライアントを指定します。
3. **radius-server local interface** コマンドまたはWeb GUIでRADIUS認証を動作させるVLANインターフェースを指定します。
4. 証明書のメール送信や証明書の期限切れ事前メール通知を使用する場合はメール関連の設定を行います。
5. **radius-server local enable** コマンドまたはWeb GUIでRADIUSサーバー機能を有効にします。
6. **radius-server local refresh** コマンドでRADIUSの情報を実動作に反映させます。

上記の手順により、クライアント証明書を再発行する必要無く、ヤマハ無線アクセスポイント(WLXシリーズ)から本機にRADIUSサーバー機能を移行することができます。

ヤマハ無線アクセスポイント(WLXシリーズ)から本機にRADIUSサーバー機能を移行した場合、失効証明書の有効期限は取り込んだ日時から20年間に自動更新されます。

ヤマハ無線アクセスポイント(WLXシリーズ)でバックアップしたデータをリストアする場合、以下の情報を復元することができます。

- ・ ルート認証局
- ・ ルート証明書
- ・ サーバー証明書
- ・ クライアント証明書
- ・ 失効証明書
- ・ ユーザー情報

RADIUSクライアントの設定など上記以外の情報は復元されませんので、別途設定する必要があります。
本機で使用できない文字が含まれていた場合、そのユーザーはリストアすることはできません。別途個別にユーザーの追加を行ってください。

本機で使用できない文字については、[注意事項](#)を参照してください。

認証局名に本機で使用できない文字が含まれていたとしてもリストアすることができます。ただし、使用できない文字がアンダースコア(_)に変換されてコンフィグに表示されます。

SYSLOGの出力情報

RADIUSサーバー機能として、SYSLOGに出力する情報には以下のものがあります。
プレフィックスは、[**RADIUSD**] です。

タイプ	メッセージ	説明
INFO	RADIUS server started.	RADIUSサーバー機能のプロセスを開始しました。
INFO	RADIUS server stopped.	RADIUSサーバー機能のプロセスが停止しました。
INFO	Authentication succeeded.: [{ ユーザーID }/<via Auth-Type = { 認証方式 }>] (from client port { ポート番号 } cli { MACアドレス })	ユーザー認証に成功しました。
INFO	Authentication failed.: [{ ユーザーID }/<via Auth-Type = { 認証方式 }>] (from client port { ポート番号 } cli { MACアドレス })	ユーザー認証に失敗しました。
INFO	MAC address is not allowed.User-ID:{ ユーザーID } MAC:{ MACアドレス }	MACアドレスが適切でないため、ユーザー認証に失敗しました。
INFO	Connected NAS is not allowed.IP:{ IPアドレス }	許可していないRADIUSクライアントから認証要求を受信しました。

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。

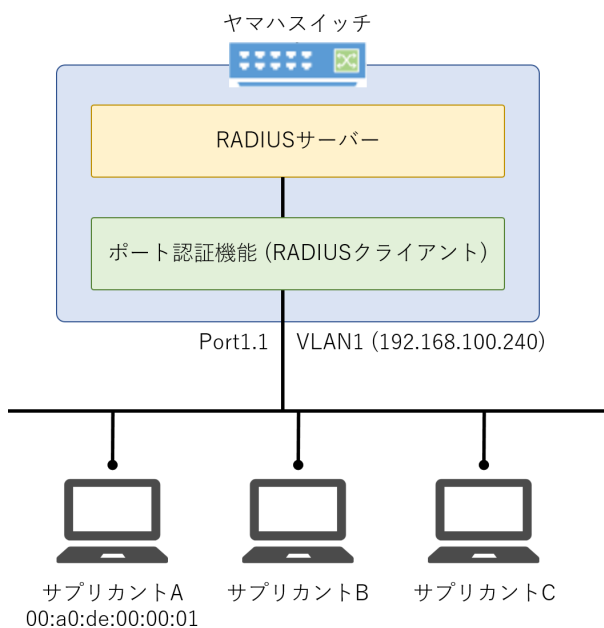
操作項目	操作コマンド
radius-server local enable	ローカルRADIUSサーバー機能の設定
radius-server local interface	アクセスインターフェースの設定
crypto pki generate ca	ルート認証局を生成
radius-server local-profile	RADIUSコンフィグレーションモード
authentication	認証方式の設定
nas	RADIUSクライアント(NAS)の設定
user	認証ユーザーの設定
reauth interval	再認証間隔の設定
radius-server local refresh	ローカルRADIUSサーバーへの設定データ反映
certificate user	クライアント証明書の発行
certificate abort	クライアント証明書の発行中断
certificate revoke id	指定した証明書IDのクライアント証明書の失効
certificate revoke user	指定したユーザーのクライアント証明書の失効
certificate export sd	クライアント証明書のエクスポート(SDコピー)

操作項目	操作コマンド
certificate export mail	クライアント証明書のエクスポート(メール送信)
copy radius-server local	RADIUSデータのコピー
show radius-server local nas	RADIUSクライアント(NAS)の表示
show radius-server local user	認証ユーザー情報の表示
show radius-server local certificate status	クライアント証明書の発行状態表示
show radius-server local certificate list	クライアント証明書のリスト表示
show radius-server local certificate revoke	クライアント証明書の失効リスト表示

設定例

RADIUSサーバー機能とポート認証機能を同時に利用する場合

ローカルRADIUSサーバーを使用して、サブリカントA、B、CをそれぞれMAC認証、IEEE802.1X認証、及びWeb認証で認証できるように設定します。



1. スイッチでローカルRADIUSサーバーを有効にし、ユーザーを登録します。

```
Yamaha# configure terminal
Yamaha(config)# crypto pki generate ca
Generate CA? (y/n): y
Finished
Yamaha(config)# radius-server local-profile
Yamaha(config-radius)# user 00a0de000001 00a0de000001 auth peap
Yamaha(config-radius)# user 8021xuser 8021xpass auth peap
Yamaha(config-radius)# user webuser webpass auth peap
Yamaha(config-radius)# exit
Yamaha(config)# radius-server local enable
Yamaha(config)# exit
Yamaha# radius-server local refresh
```

2. Web認証を行うためにVLAN #1 へIPアドレスを割り当てます

```
Yamaha# configure terminal
Yamaha(config)# interface vlan1
Yamaha(config-if)# ip-address 192.168.100.240/24
```

3. LANポート #1 でMAC認証、IEEE802.1X認証、及びWeb認証を有効化します。

```
Yamaha# configure terminal
Yamaha(config)# aaa authentication auth-mac
Yamaha(config)# auth-mac auth-user unformatted lower-case
Yamaha(config)# aaa authentication dot1x
Yamaha(config)# aaa authentication auth-web
Yamaha(config)# interface port1.1
Yamaha(config-if)# auth host-mode multi-supplicant
Yamaha(config-if)# auth-mac enable
Yamaha(config-if)# dot1x port-control auto
Yamaha(config-if)# auth-web enable
```

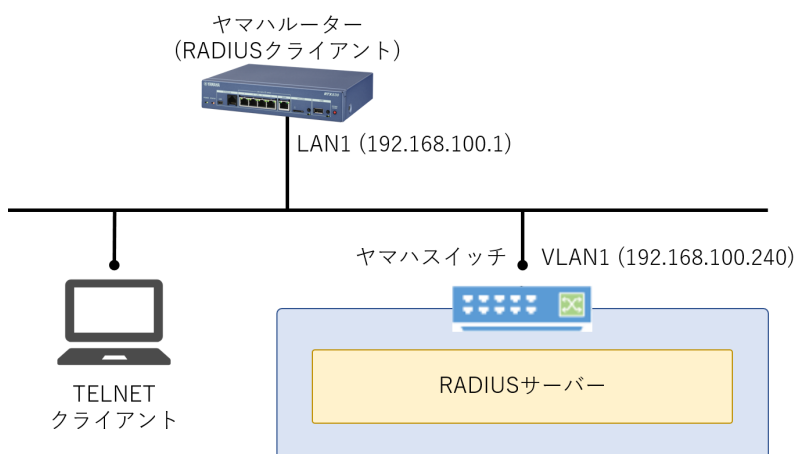
4. 認証機能で使用するRADIUSサーバーを設定します。

```
Yamaha# configure terminal
Yamaha(config)# radius-server host 127.0.0.1 key secret_local
```

ヤマハルーターのログインユーザーの認証でRADIUSサーバー機能を利用する場合

TELNETクライアントからヤマハルーターにアクセスするとき、ログインユーザーの認証と管理者権限の認証をヤマハスイッチのRADIUSサーバーで行います。

ログインユーザーとしては、ユーザーID: **user1**、パスワード: **password1** でログインできるようにします。管理者には、パスワード: **admin** で昇格できるようにします。



■ヤマハスイッチの設定

1. インターフェースにIPアドレスを設定します。

```
Yamaha# configure terminal
Yamaha(config)# interface vlan1
```

```
Yamaha(config-if)# ip address 192.168.100.240/24
Yamaha(config-if)# exit
```

2. ルート認証局を作成します。

```
Yamaha(config)#crypto pki generate ca
Generate CA? (y/n): y
Finished
```

3. RADIUSサーバーを設定します。

```
Yamaha(config)# radius-server local-profile
Yamaha(config-radius)# nas 192.168.100.1 key yamaha
Yamaha(config-radius)# user user1 password1 auth pap
Yamaha(config-radius)# user *administrator admin auth pap
Yamaha(config-radius)# exit
```

4. RADIUSクライアントの接続可能インターフェースを指定します。

```
Yamaha(config)# radius-server local interface vlan1
```

5. RADIUSサーバー機能を有効にします。

```
Yamaha(config)# radius-server local enable
Yamaha(config)#exit
```

6. RADIUSサーバーの設定を実動作に反映させます。

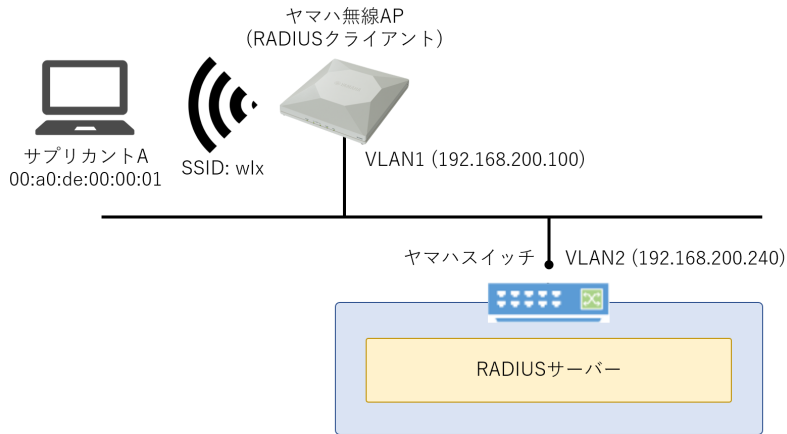
```
Yamaha#radius-server local refresh
Yamaha#
```

■ヤマハルーターの設定

```
login radius use on
administrator radius auth on
ip lan1 address 192.168.100.1/24
radius auth on
radius auth server 192.168.100.240
radius auth port 1812
radius secret yamaha
```

ヤマハ無線アクセスポイント(WLXシリーズ)のMAC認証でRADIUSサーバー機能を利用する場合

ヤマハ無線アクセスポイントに接続するサブリカントのMACアドレス認証をヤマハスイッチのRADIUSサーバーで行います。



■ヤマハスイッチの設定

1. インターフェースにIPアドレスを設定します。

```
Yamaha# configure terminal
Yamaha(config)# interface vlan2
Yamaha(config-if)# ip address 192.168.200.240/24
Yamaha(config-if)# exit
```

2. ルート認証局を作成します。

```
Yamaha(config)#crypto pki generate ca
Generate CA? (y/n): y
Finished
```

3. RADIUSサーバーを設定します。

```
Yamaha(config)# radius-server local-profile
Yamaha(config-radius)# nas 192.168.200.100 key yamaha
Yamaha(config-radius)# user 00a0de000001 00a0de000001 auth pap ssid wlx
Yamaha(config-radius)# exit
```

4. RADIUSクライアントの接続を許可するインターフェースを指定します。

```
Yamaha(config)# radius-server local interface vlan2
```

5. RADIUSサーバー機能を有効にします。

```
Yamaha(config)# radius-server local enable
Yamaha(config)#exit
```

6. RADIUSサーバーの設定を実動作に反映させます。

```
Yamaha#radius-server local refresh
Yamaha#
```

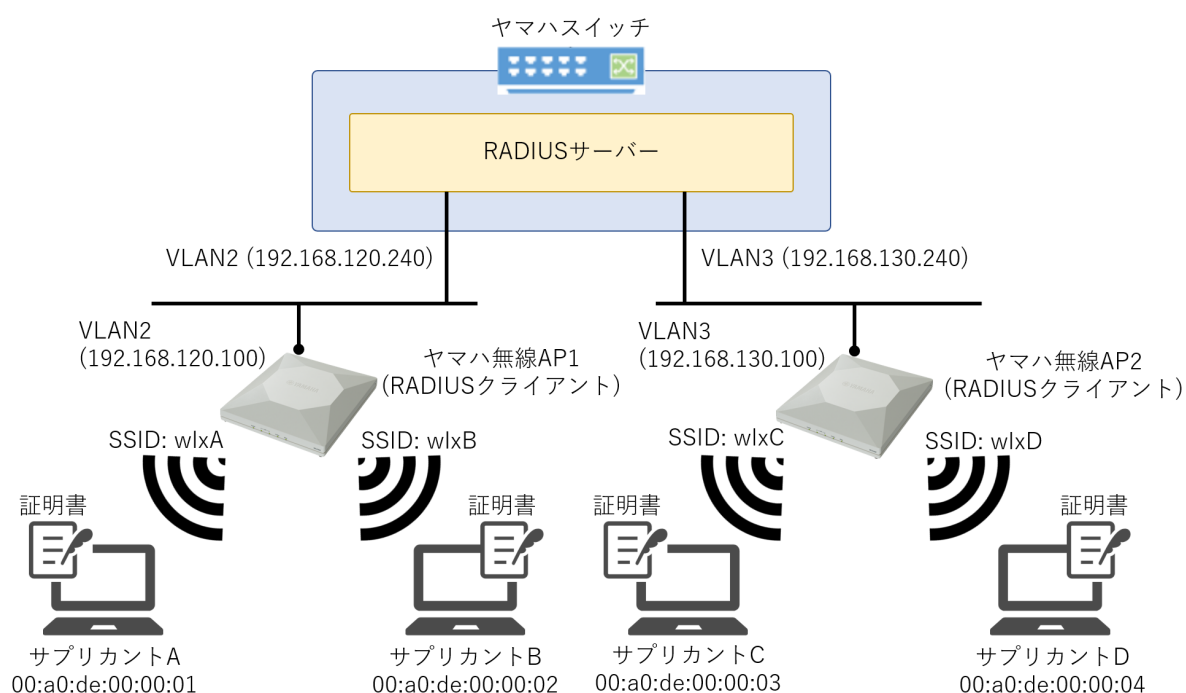
■ヤマハ無線AP(WLX402)の設定

※認証に関連した部分のみの設定となります。別途無線機能等の設定を環境にあわせて行ってください。

```
ip vlan-id 1 address 192.168.200.100/24
airlink slect 1
airlink ssid wlx
airlink radius auth on
airlink radius server 192.168.200.240
airlink radius secret yamaha
airlink enable 1
```

証明書を使ってヤマハ無線アクセスポイント(WLXシリーズ)に接続するためにRADIUSサーバー機能を利用する場合

ヤマハスイッチで発行した証明書をインストールしたサブリカントが、ヤマハ無線アクセスポイントに接続するときに認証を行います。



■ヤマハスイッチの設定

1. インターフェースにIPアドレスを設定します。

```
Yamaha(config)# interface vlan2
Yamaha(config-if)# ip address 192.168.120.240/24
Yamaha(config-if)# exit
```

2. ルート認証局を作成します。

```
Yamaha(config)#crypto pki generate ca
Generate CA? (y/n): y
Finished
```

3. RADIUSサーバーを設定します。

```
Yamaha(config)# radius-server local-profile
Yamaha(config-radius)# nas 192.168.120.100 key yamaha1
Yamaha(config-radius)# nas 192.168.130.100 key yamaha2
Yamaha(config-radius)# user user1 pass1 ssid wlxA
Yamaha(config-radius)# user user2 pass2 ssid wlxB
Yamaha(config-radius)# user user3 pass3 ssid wlxC
Yamaha(config-radius)# user user4 pass4 ssid wlxD
Yamaha(config-radius)# exit
```

4. RADIUSクライアントの接続を許可するインターフェースを指定します。

```
Yamaha(config)# radius-server local interface vlan2
Yamaha(config)# radius-server local interface vlan3
```

5. RADIUSサーバー機能を有効にします。

```
Yamaha(config)# radius-server local enable
Yamaha(config)# exit
```

6. クライアント証明書を発行します。

発行した証明書をサブリカントA～Dでそれぞれインストールします。

```
Yamaha# certificate user user1
Yamaha# certificate user user2
Yamaha# certificate user user3
Yamaha# certificate user user4
```

7. RADIUSサーバーの設定を実動作に反映させます。

```
Yamaha# radius-server local refresh
```

■ヤマハ無線AP1(WLX402)の設定

※認証に関連した部分のみの設定となります。別途無線機能等の設定を環境にあわせて行ってください。

```
ip vlan-id 2 address 192.168.120.100/24
airlink select 1
airlink ssid wlxA
airlink vlan-id 2
airlink radius auth on
airlink radius server 192.168.120.240
airlink radius secret yamaha1
airlink enable 1
airlink select 2
airlink ssid wlxB
airlink vlan-id 2
airlink radius auth on
airlink radius server 192.168.120.240
```

```
airlink radius secret yamaha1
airlink enable 2
```

■ヤマハ無線AP2(WLX402)の設定

※認証に関連した部分のみの設定となります。別途無線機能等の設定を環境にあわせて行ってください。

```
ip vlan-id 3 address 192.168.130.100/24
airlink select 1
airlink ssid wlxC
airlink vlan-id 3
airlink radius auth on
airlink radius server 192.168.130.240
airlink radius secret yamaha2
airlink enable 1
airlink select 2
airlink ssid wlxD
airlink vlan-id 3
airlink radius auth on
airlink radius server 192.168.130.240
airlink radius secret yamaha2
airlink enable 2
```

注意事項

- RADIUSサーバー機能では認証処理や証明書の発行等の処理において、本機の内蔵時計の時刻が使用されます。
そのため、本機の内蔵時計を常に正確な時刻に保つ必要があります。NTPサーバーとの時刻同期を推奨します。
- ルート認証局は、作成から一貫して保持し続ける必要がありますので、不用意に削除してしまわないようご注意ください。
削除してしまうと発行済みのクライアント証明書が使えなくなるため、すべてのユーザーに対してクライアント証明書の再発行が必要になります。
また、RADIUSサーバー機能に関連するほぼすべての設定が削除されます。
- 同じ型番のヤマハスイッチで同じ名前のルート認証局を作成したとしても、そのルート認証局は別物です。
クライアント証明書は、生成時に使用したルート認証局が存在するヤマハスイッチの認証でしか使用することはできません。
複数の機器で同一のルート認証局を保持するためには [すべてのRADIUSサーバー関連情報のバックアップとリストア](#) を参照してください。
- IPv6リンクローカルアドレスに対してRADIUSクライアントから接続しても認証を行うことはできません。
- ヤマハスイッチとヤマハ無線アクセスポイント(WLXシリーズ)では、ユーザー情報等に使用できる文字に違いがあります。違いは以下のとおりです。
(赤字がヤマハスイッチでのみ使用できない文字となります)

項目	ヤマハスイッチの制限	ヤマハ無線アクセスポイントの制限

ルート 認証局名 (crypto pki generate ca コマンドのCA-NAMEオプション)	半角英数字・半角記号のうち以下が使用できません。 \' (バックスラッシュ) '/' '[' ']' '?' ' ' (スペース) "" (ダブルクォート)	半角英数字・半角記号のうち以下が使用できません。 \' (バックスラッシュ) '/' '[' ']'
RADIUSクライアントの共有パスワード (nas コマンドのSECRETパラメーター)	半角英数字・半角記号のうち以下が使用できません。 \' (バックスラッシュ) '[' ']' '?' ' ' (スペース) "" (ダブルクォート)	半角英数字・半角記号のうち以下が使用できません。 \' (バックスラッシュ) '[' ']'
ユーザー情報のユーザーID (user コマンドのUSERIDパラメーター) 認証方式がEAP-TLSの場合	半角英数字・半角記号のうち以下が使用できません。 \' (バックスラッシュ) '/' '[' ']' ':' '< '*' '> ' ' '?' ' ' (スペース) "" (ダブルクォート)	半角英数字・半角記号のうち以下が使用できません。 \' (バックスラッシュ) '/' '[' ']'
ユーザー情報のユーザーID (user コマンドのUSERIDパラメーター) 認証方式がPAP,PEAPの場合	半角英数字・半角記号のうち以下が使用できません。 \' (バックスラッシュ) '[' ']' '?' ' ' (スペース) "" (ダブルクォート)	半角英数字・半角記号のうち以下が使用できません。 \' (バックスラッシュ) '[' ']'

ユーザー情報のパスワード (user コマンドのPASSWORDパラメーター)	半角英数字・半角記号のうち以下が使用できません。 '\' (バックスラッシュ) '[' ']' '?' ' ' (スペース) '"' (ダブルクォート)	半角英数字・半角記号のうち以下が使用できません。 '\' (バックスラッシュ) '[' ']'
ユーザー情報の名前 (user コマンドのNAMEオプション)	半角英数字・半角記号のうち以下が使用できません。 '?' ' ' (スペース) '"' (ダブルクォート)	半角英数字・半角記号すべて使用できます。

関連文書

- ・ [インターフェース制御機能: ポート認証](#)

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](#)include::license.adoc[ライセンスについて, leveloffset = 2]

