ヤマハ L2 スイッチ

SWP2 シリーズ(SWP2-10SMF、SWP2-10MMF)

コマンドリファレンス

Rev.2.03.24

目次

序文 : はじめに 13

第 1 章 : コマンドリファレンスの見方 14

1.1 対応するプログラムのリビジョン 14
1.2 コマンドリファレンスの見方 14
1.3 インターフェース名について 14
1.4 no で始まるコマンドの入力形式について 15

第 2 章 : コマンドの使い方 16

2.1 コンソールによる操作 16
2.1.1 コンソールターミナルからのアクセス 16
2.1.2 TELNET クライアントからのアクセス 16
2.1.3 SSH クライアントからのアクセス 17
2.1.4 コンソールターミナル/VTY の設定 17
2.2 設定(Config)ファイルによる操作 18
2.2.1 TFTP クライアントからのアクセス 18
2.2.2 設定ファイルの読み出し/書き込み 18
2.3 ログイン 19
2.4 コマンド入力モードについて 20
2.4.1 コマンド入力モードの基本 20
2.4.2 個別コンフィグレーションモード 21
2.4.3 コマンドプロンプトのプレフィックス 22
2.4.4 異なる入力モードのコマンド実行 22
2.5 コンソール使用時のキーボード操作 22
2.5.1 コンソール入力の基本操作 22
2.5.2 コマンドヘルプ 23
2.5.3 入力コマンドの補完、キーワード候補一覧の表示 23
2.5.4 コマンドの省略入力 24
2.5.5 コマンドヒストリー 24
2.6 「show」で始まるコマンド 24
2.6.1 モディファイア 24

第 3 章 : コンフィグレーション 25

3.1 設定値の管理 25
3.2 デフォルト設定値 25

第 4 章 : 保守・運用機能 31

4.1 パスワード 31
4.1.1 特権パスワードの設定 31
4.1.2 パスワードの暗号化 31
4.2 ユーザーアカウント管理 32
4.2.1 ユーザーの設定 32
4.2.2 ユーザー権限の変更 33
4.2.3 ログインユーザー情報の表示 34
4.2.4 バナーの設定 34
4.3 コンフィグの管理 35
4.3.1 ランニングコンフィグの保存 35
4.3.2 ランニングコンフィグの保存 36
4.3.3 対象機能のバックアップを行う 36
4.3.4 ランニングコンフィグの表示 37
4.3.5 スタートアップコンフィグの表示 38

4.3.6 バックアップコンフィグの表示....38
4.3.7 スタートアップコンフィグの消去....39
4.3.8 対象機能のバックアップを削除する....39
4.4 起動情報の管理....39
4.4.1 起動情報の表示....39
4.4.2 起動情報のクリア....40
4.5 筐体情報表示....40
4.5.1 製品情報の表示....40
4.5.2 稼動情報の表示....41
4.5.3 ディスク使用状況....42
4.5.4 実行中のプロセスの表示....42
4.5.5 メモリ使用状況の表示....42
4.5.6 技術サポート情報の表示....43
4.6 システム自己診断....45
4.6.1 システム自己診断結果の表示....45
4.6.2 オンデマンド診断の実行....46
4.6.3 オンデマンド診断結果の削除....46
4.7 ケーブル診断....46
4.7.1 ケーブル診断の実行....46
4.7.2 ケーブル診断結果のクリア....47
4.7.3 ケーブル診断結果の表示....47
4.8 時刻管理....47
4.8.1 時刻の手動設定....47
4.8.2 タイムゾーンの設定....48
4.8.3 サマータイムの設定(繰り返し)....50
4.8.4 サマータイムの設定(日付指定)....50
4.8.5 現在時刻の表示....51
4.8.6 NTP サーバーの設定....52
4.8.7 NTP サーバーによる時刻同期(1 ショット更新)....53
4.8.8 NTP サーバーによる時刻同期(周期更新設定)....53
4.8.9 NTP サーバーによる時刻同期設定情報の表示....53
4.9 端末設定....54
4.9.1 ラインモード(コンソールターミナル)への移行....54
4.9.2 VTY ポートの設定およびラインモード(VTY ポート)への移行....54
4.9.3 端末ログインタイムアウト時間の設定....55
4.9.4 使用している端末 1 ページあたりの表示行数の変更....55
4.9.5 端末 1 ページあたりの表示行数の設定....56
4.10 保守....56
4.10.1 保守 VLAN の設定....56
4.11 SYSLOG....57
4.11.1 ログの通知先(SYSLOG サーバー)の設定....57
4.11.2 ログの通知フォーマットの設定....57
4.11.3 ログのファシリティ値の設定....58
4.11.4 ログの出力レベル(debug)の設定....58
4.11.5 ログの出力レベル(informational)の設定....59
4.11.6 ログの出力レベル(error)の設定....59
4.11.7 ログのコンソール出力設定....60
4.11.8 ログのバックアップ....60
4.11.9 ログの削除....60
4.11.10 ログの参照....60
4.12 SNMP....61
4.12.1 SNMP 通知メッセージの送信先ホストの設定....61
4.12.2 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....62
4.12.3 送信する通知メッセージタイプの設定....63
4.12.4 システムコンタクトの設定....64
4.12.5 システムロケーションの設定....64
4.12.6 SNMP コミュニティーの設定....65
4.12.7 SNMP ビューの設定....65
4.12.8 SNMP グループの設定....66
4.12.9 SNMP ユーザーの設定....67
4.12.10 SNMP サーバーへアクセスできるクライアントの IP アドレス制限....68

4.12.11 SNMP コミュニティーの情報の表示 69
4.12.12 SNMP ビューの設定内容の表示 69
4.12.13 SNMP グループの設定内容の表示 70
4.12.14 SNMP ユーザーの設定内容の表示 70
4.13 RMON 70
4.13.1 RMON 機能の設定 70
4.13.2 RMON イーサネット統計情報グループの設定 71
4.13.3 RMON 履歴グループの設定 72
4.13.4 RMON イベントグループの設定 73
4.13.5 RMON アラームグループの設定 74
4.13.6 RMON 機能の状態表示 76
4.13.7 RMON イーサネット統計情報グループの状態表示 76
4.13.8 RMON 履歴グループの状態表示 77
4.13.9 RMON イベントグループの状態表示 77
4.13.10 RMON アラームグループの状態表示 78
4.13.11 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 78
4.14 sFlow 79
4.14.1 sFlow 機能の設定 79
4.14.2 sFlow エージェントの設定 79
4.14.3 sFlow コレクターの設定 80
4.14.4 sFlow データグラムの最大サイズの設定 80
4.14.5 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 81
4.14.6 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 81
4.14.7 カウンターサンプリングのポーリング間隔の設定 81
4.14.8 sFlow の状態の表示 82
4.14.9 sFlow のサンプリング情報の表示 82
4.15 TELNET サーバー 83
4.15.1 TELNET サーバーの起動および受付ポート番号の変更 83
4.15.2 TELNET サーバーの設定状態の表示 84
4.15.3 TELNET サーバーへアクセスできるホストの設定 84
4.15.4 TELNET サーバーへアクセスできるクライアントの IP アドレス制限 84
4.16 TELNET クライアント 85
4.16.1 TELNET クライアントの起動 85
4.16.2 TELNET クライアントの有効化 86
4.17 TFTP サーバー 86
4.17.1 TFTP サーバーの起動および受付ポート番号の変更 86
4.17.2 TFTP サーバーの設定状態の表示 87
4.17.3 TFTP サーバーへアクセスできるホストの設定 87
4.18 HTTP サーバー 88
4.18.1 HTTP サーバーの起動および受付ポート番号の変更 88
4.18.2 セキュア HTTP サーバーの起動および受付ポート番号の変更 88
4.18.3 HTTP サーバーの設定状態の表示 89
4.18.4 HTTP サーバーへアクセスできるホストの設定 89
4.18.5 HTTP サーバーへアクセスできるクライアントの IP アドレス制限 90
4.18.6 Web GUI の言語設定 91
4.18.7 HTTP サーバーのログインタイムアウト時間の設定 91
4.19 SSH サーバー 92
4.19.1 SSH サーバーの起動および受付ポート番号の変更 92
4.19.2 SSH サーバーの設定状態の表示 92
4.19.3 SSH サーバーへアクセスできるホストの設定 93
4.19.4 SSH サーバーへアクセスできるクライアントの設定 93
4.19.5 SSH サーバーホスト鍵の作成 94
4.19.6 SSH サーバーホスト鍵のクリア 95
4.19.7 SSH サーバー公開鍵の表示 95
4.19.8 SSH クライアントの生存確認の設定 96
4.20 SSH クライアント 97
4.20.1 SSH クライアントの起動 97
4.20.2 SSH クライアントの有効化 97
4.20.3 SSH ホスト情報のクリア 98
4.21 メール通知 98
4.21.1 SMTP メールサーバーの設定 98

4.21.2 SMTP メールサーバー名の設定 99
4.21.3 メール通知のトリガー設定 100
4.21.4 メール送信のテンプレート設定モード 100
4.21.5 メール送信のサーバー ID の設定 101
4.21.6 メール送信の送信元メールアドレスの設定 101
4.21.7 メール送信の宛先メールアドレスの設定 101
4.21.8 メール送信の件名の設定 102
4.21.9 メール送信待ち時間の設定 102
4.21.10 証明書送付時のメール設定 103
4.21.11 証明書通知時のメール設定 103
4.21.12 証明書の有効期限切れ通知タイミングの設定 104
4.21.13 メール送信情報の表示 104
4.22 Yamaha Unified Network Operation Service (Y-UNOS) 105
4.22.1 Y-UNOS 機能の設定 105
4.22.2 Y-UNOS 情報の表示 106
4.23 LLDP 106
4.23.1 LLDP 機能の有効化 106
4.23.2 システムの説明文の設定 107
4.23.3 システムの名称の設定 107
4.23.4 LLDP エージェントの作成 108
4.23.5 LLDP による自動設定機能の設定 108
4.23.6 LLDP 送受信モードの設定 109
4.23.7 管理アドレスの種類の設定 109
4.23.8 基本管理 TLV の設定 110
4.23.9 IEEE-802.1 TLV の設定 111
4.23.10 IEEE-802.3 TLV の設定 111
4.23.11 LLDP-MED TLV の設定 112
4.23.12 LLDP フレームの送信間隔の設定 112
4.23.13 高速送信期間の LLDP フレーム送信間隔の設定 113
4.23.14 LLDP フレーム送信停止から再初期化までの時間の設定 113
4.23.15 機器情報の保持時間(TTL)を算出するための乗数の設定 114
4.23.16 高速送信期間の LLDP フレーム送信個数の設定 114
4.23.17 ポート単位で管理できる機器の最大接続台数の設定 115
4.23.18 LLDP 機能のインターフェース一括設定 115
4.23.19 インターフェースの状態表示 116
4.23.20 全てのインターフェースにおける接続機器の情報表示 118
4.23.21 LLDP フレームカウンターのクリア 120
4.24 L2MS (Layer 2 management service)の設定 120
4.24.1 L2MS 制御フレームの送受信設定 120
4.24.2 L2MS の情報の表示 121
4.25 スナップショット 121
4.25.1 スナップショット機能の設定 121
4.25.2 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 122
4.25.3 スナップショットの作成 122
4.25.4 スナップショットの削除 122
4.26 ファームウェア更新 123
4.26.1 ファームウェア更新サイトの設定 123
4.26.2 ファームウェア更新で使用する HTTP プロキシーサーバーの設定 123
4.26.3 ファームウェア更新の実行 124
4.26.4 ファームウェアダウンロードタイムアウト時間の設定 125
4.26.5 リビジョンダウンの許可 125
4.26.6 ファームウェア更新機能設定の表示 125
4.26.7 ファームウェア更新の再起動時刻の設定 126
4.27 スケジュール 126
4.27.1 スケジュールの設定 126
4.27.2 スケジュールテンプレートの説明文の設定 128
4.27.3 スケジュールテンプレートの有効/無効の設定 128
4.27.4 スケジュールテンプレートの設定 129
4.27.5 スケジュールテンプレートのコマンド実行の設定 129
4.28 保守運用一般 130
4.28.1 ホスト名の設定 130

4.28.2 システムの再起動.....131
4.28.3 設定の初期化.....131
4.28.4 初期 LED モードの設定.....131
4.28.5 LED モードの表示.....132
4.28.6 ポートエラー LED 状態の表示.....132
4.28.7 ディップスイッチの状態表示.....133
4.28.8 「このスイッチを探す」機能開始.....133
4.28.9 「このスイッチを探す」機能停止.....133
4.28.10 ProAV プロファイル種別の設定.....134

第 5 章 : インターフェース制御.....135
5.1 インターフェース基本設定.....135
5.1.1 説明文の設定.....135
5.1.2 シャットダウン.....135
5.1.3 通信速度・通信モードの設定.....136
5.1.4 MRU 設定.....136
5.1.5 クロス／ストレート自動判別設定.....137
5.1.6 EEE 設定.....137
5.1.7 EEE 対応可否を表示する.....138
5.1.8 EEE ステータス情報を表示する.....138
5.1.9 ポートミラーリングの設定.....139
5.1.10 ポートミラーリングの状態表示.....140
5.1.11 インターフェースの状態表示.....141
5.1.12 インターフェースの状態の簡易表示.....143
5.1.13 インターフェースのリセット.....144
5.1.14 フレームカウンター表示.....145
5.1.15 フレームカウンターのクリア.....146
5.1.16 SFP+モジュールの状態表示.....147
5.1.17 SFP+モジュールの受光レベル監視の設定.....148
5.1.18 送信キューの使用率監視の設定(システム).....148
5.1.19 送信キューの使用率監視の設定(インターフェース).....149
5.1.20 送信キューの使用率監視の設定表示.....149
5.2 リンクアグリゲーション.....150
5.2.1 スタティック論理インターフェースの設定.....150
5.2.2 スタティック論理インターフェースの状態表示.....150
5.2.3 LACP 論理インターフェースの設定.....151
5.2.4 LACP 論理インターフェースの状態表示.....152
5.2.5 LACP システム優先度の設定.....154
5.2.6 LACP システム優先度の表示.....154
5.2.7 LACP 異速度リンクアグリゲーションの設定.....155
5.2.8 LACP タイムアウトの設定.....155
5.2.9 LACP フレームカウンターのクリア.....156
5.2.10 LACP フレームカウンターの表示.....156
5.2.11 ロードバランス機能のルールの設定.....157
5.2.12 LACP 論理インターフェースのプロトコル状態表示.....158
5.2.13 LACP ポート優先度の設定.....160
5.3 ポート認証.....160
5.3.1 システム全体での IEEE 802.1X 認証機能の設定.....160
5.3.2 システム全体での MAC 認証機能の設定.....161
5.3.3 システム全体での Web 認証機能の設定.....161
5.3.4 IEEE 802.1X 認証機能の動作モード設定.....162
5.3.5 IEEE 802.1X 認証の未認証ポートでの転送制御の設定.....162
5.3.6 EAPOL パケットの送信回数の設定.....163
5.3.7 MAC 認証機能の設定.....163
5.3.8 MAC 認証時の MAC アドレス形式の設定.....164
5.3.9 MAC 認証のスタティック登録の設定.....165
5.3.10 Web 認証機能の設定.....165
5.3.11 ホストモードの設定.....166
5.3.12 認証順序の設定.....167
5.3.13 再認証の設定.....167

5.3.14 ダイナミック VLAN の設定....168
5.3.15 ゲスト VLAN の設定....168
5.3.16 認証失敗後の抑止期間の設定....169
5.3.17 再認証間隔の設定....169
5.3.18 RADIUS サーバー全体の応答待ち時間の設定....170
5.3.19 サプリカント応答待ち時間の設定....170
5.3.20 RADIUS サーバーホストの設定....171
5.3.21 RADIUS サーバー 1 台あたりの応答待ち時間の設定....172
5.3.22 RADIUS サーバーへの要求再送回数の設定....172
5.3.23 RADIUS サーバー共有パスワードの設定....173
5.3.24 RADIUS サーバー使用抑制時間の設定....173
5.3.25 RADIUS サーバーに通知する NAS-Identifier 属性の設定....174
5.3.26 RADIUS サーバー無応答時の認証の設定....174
5.3.27 ポート認証情報の表示....175
5.3.28 サプリカント情報の表示....176
5.3.29 統計情報の表示....176
5.3.30 統計情報のクリア....177
5.3.31 RADIUS サーバー設定情報の表示....177
5.3.32 Web 認証成功後のリダイレクト先 URL の設定....178
5.3.33 認証状態のクリア....178
5.3.34 認証状態のクリアする時刻の設定(システム)....179
5.3.35 認証状態のクリアする時刻の設定(インターフェース)....179
5.3.36 EAP パススルーの設定....180
5.4 ポートセキュリティー....180
5.4.1 ポートセキュリティー機能の設定....180
5.4.2 許可 MAC アドレス登録....181
5.4.3 セキュリティー違反時の動作の設定....181
5.4.4 ポートセキュリティー情報の表示....182
5.5 エラー検出機能....182
5.5.1 errdisable 状態からの自動復旧機能の設定....182
5.5.2 エラー検出機能の情報表示....183

第 6 章 : Layer 2 機能....184
6.1 FDB(フォワーディングデータベース)....184
6.1.1 MAC アドレス学習機能の設定....184
6.1.2 ダイナミックエントリーのエージングタイム設定....184
6.1.3 ダイナミックエントリーの削除....185
6.1.4 スタティックエントリーの設定....185
6.1.5 MAC アドレステーブルの表示....186
6.1.6 MAC アドレス数の表示....187
6.2 VLAN....187
6.2.1 VLAN モードへの移行....187
6.2.2 VLAN インターフェースの設定....188
6.2.3 プライベート VLAN の設定....188
6.2.4 プライマリー VLAN に対するセカンダリー VLAN の設定....189
6.2.5 アクセスポート(タグなしポート)の設定....190
6.2.6 アクセスポート(タグなしポート)の所属 VLAN の設定....191
6.2.7 トランクポート(タグ付きポート)の設定....191
6.2.8 トランクポート(タグ付きポート)の所属 VLAN の設定....192
6.2.9 トランクポート(タグ付きポート)のネイティブ VLAN の設定....193
6.2.10 プライベート VLAN のポート種別の設定....194
6.2.11 プライベート VLAN のホストポートの設定....194
6.2.12 プライベート VLAN のプロミスカスポートの設定....195
6.2.13 ボイス VLAN の設定....196
6.2.14 ボイス VLAN の CoS 値の設定....197
6.2.15 ボイス VLAN の DSCP 値の設定....197
6.2.16 マルチプル VLAN グループの設定....198
6.2.17 マルチプル VLAN グループの名前の設定....199
6.2.18 マルチプル VLAN 設定時の YMPI フレーム透過機能の設定....199
6.2.19 VLAN 情報の表示....200

6.2.20 プライベート VLAN 情報の表示....200
6.2.21 マルチプル VLAN グループ設定情報の表示....201
6.3 STP(スパニングツリープロトコル)....201
6.3.1 システムのスパニングツリーの設定....201
6.3.2 転送遅延時間の設定....202
6.3.3 最大エージング時間の設定....202
6.3.4 ブリッジプライオリティの設定....203
6.3.5 インターフェースのスパニングツリーの設定....203
6.3.6 インターフェースのリンクタイプの設定....204
6.3.7 インターフェースの BPDU フィルタリングの設定....204
6.3.8 インターフェースの BPDU ガードの設定....205
6.3.9 インターフェースのパスコストの設定....206
6.3.10 インターフェースのプライオリティの設定....206
6.3.11 インターフェースのエッジポートの設定....207
6.3.12 スパニングツリーの状態表示....207
6.3.13 スパニングツリーの BPDU の統計情報の表示....209
6.3.14 プロトコル互換モードのクリア....211
6.3.15 MST モードへの移行....211
6.3.16 MST インスタンスの生成....211
6.3.17 MST インスタンスに対する VLAN の設定....212
6.3.18 MST インスタンスのプライオリティの設定....213
6.3.19 MST リージョン名の設定....213
6.3.20 MST リージョンのリビジョン番号の設定....213
6.3.21 インターフェースに対する MST インスタンスの設定....214
6.3.22 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....214
6.3.23 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....215
6.3.24 MST リージョン情報の表示....216
6.3.25 MSTP 情報の表示....216
6.3.26 MST インスタンス情報の表示....217
6.4 ループ検出....218
6.4.1 ループ検出機能の設定(システム)....218
6.4.2 ループ検出機能の設定(インターフェース)....219
6.4.3 ループ検出時の Port Blocking の設定....220
6.4.4 Port Blocking のループ解消を一定間隔で確認する....221
6.4.5 ループ検出状態のリセット....221
6.4.6 ループ検出機能の状態表示....221
6.5 DHCP スヌーピング....222
6.5.1 DHCP スヌーピングの有効/無効設定 (システム)....222
6.5.2 DHCP スヌーピングの有効/無効設定 (VLAN)....223
6.5.3 DHCP スヌーピングのポート種別設定....224
6.5.4 MAC アドレス検証の有効/無効設定....224
6.5.5 Option 82 の有効/無効設定....225
6.5.6 Option 82 付きパケットの Untrusted ポート受信許可設定....226
6.5.7 Option 82 の Remote-ID の設定....226
6.5.8 Option 82 の Circuit-ID の設定....226
6.5.9 Option 82 の Subscriber-ID の設定....227
6.5.10 DHCP パケット受信レート制限の設定....228
6.5.11 DHCP パケット破棄時 SYSLOG 出力の有効/無効設定....228
6.5.12 DHCP スヌーピングのシステム設定情報の表示....229
6.5.13 DHCP スヌーピングのインターフェース設定情報の表示....229
6.5.14 バインディングデータベースの表示....230
6.5.15 DHCP スヌーピングの統計情報表示....230
6.5.16 バインディングデータベースのクリア....230
6.5.17 DHCP スヌーピングの統計情報のクリア....231

第 7 章 : Layer 3 機能....232
7.1 IPv4 アドレス管理....232
7.1.1 IPv4 アドレスの設定....232
7.1.2 IPv4 アドレスの表示....233
7.1.3 DHCP クライアントによる動的 IPv4 アドレスの設定....233

7.1.4 DHCP クライアントの状態の表示 234
7.1.5 Auto IP 機能の設定 235
7.2 IPv4 経路制御 235
7.2.1 IPv4 静的経路設定 235
7.2.2 IPv4 転送表の表示 236
7.2.3 IPv4 経路表の表示 237
7.2.4 IPv4 経路表に登録されている経路エントリーのサマリーの表示 237
7.3 ARP 237
7.3.1 ARP テーブルの表示 237
7.3.2 ARP テーブルの消去 238
7.3.3 静的 ARP エントリーの設定 238
7.3.4 ARP タイムアウトの設定 238
7.3.5 ARP タイムアウト時の ARP リクエスト送信方式の設定 239
7.4 IPv4 転送制御 239
7.4.1 IPv4 転送設定 239
7.4.2 IPv4 転送設定の表示 240
7.4.3 MTU の設定 240
7.5 IPv4 疎通確認 241
7.5.1 IPv4 疎通確認 241
7.5.2 IPv4 経路確認 242
7.6 IPv6 アドレス管理 242
7.6.1 IPv6 の設定 242
7.6.2 IPv6 アドレスの設定 243
7.6.3 IPv6 アドレスの RA 設定 243
7.6.4 DHCPv6 クライアントによる動的 IPv6 アドレスの設定 244
7.6.5 DHCPv6-PD を使用した IPv6 アドレスの設定 245
7.6.6 DHCPv6-PD クライアントの設定 246
7.6.7 RA によるデフォルトゲートウェイの自動登録設定 247
7.6.8 IPv6 アドレスの表示 248
7.6.9 DHCPv6 クライアントの状態の表示 249
7.6.10 DHCPv6 クライアントのリセット 250
7.6.11 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 250
7.7 IPv6 経路制御 251
7.7.1 IPv6 静的経路設定 251
7.7.2 IPv6 転送表の表示 252
7.7.3 IPv6 経路表の表示 252
7.7.4 IPv6 経路表に登録されている経路エントリーのサマリーの表示 253
7.8 Neighbor キャッシュ 253
7.8.1 静的 Neighbor キャッシュエントリーの設定 253
7.8.2 Neighbor キャッシュテーブルの表示 253
7.8.3 Neighbor キャッシュテーブルの消去 254
7.9 IPv6 転送制御 254
7.9.1 IPv6 転送設定 254
7.9.2 IPv6 転送設定の表示 254
7.10 IPv6 疎通確認 255
7.10.1 IPv6 疎通確認 255
7.10.2 IPv6 経路確認 256
7.11 DNS クライアント 256
7.11.1 DNS への問い合わせ機能の設定 256
7.11.2 DNS サーバーリストの設定 257
7.11.3 デフォルトドメイン名の設定 257
7.11.4 検索ドメインリストの設定 258
7.11.5 DNS クライアント情報の表示 258

第 8 章 : IP マルチキャスト制御 260
8.1 IP マルチキャスト基本設定 260
8.1.1 未知のマルチキャストフレームの処理方法の設定 260
8.1.2 未知のマルチキャストフレームの処理方法の設定(インターフェース) 260
8.1.3 リンクローカルマルチキャストフレームの転送設定 261
8.1.4 マルチキャストフレームの転送設定 261

8.1.5 トポロジー変更時の IGMP/MLD クエリー送信機能の有効／無効設定....262
8.2 IGMP スヌーピング....262
8.2.1 IGMP スヌーピングの有効／無効設定....262
8.2.2 IGMP スヌーピング高速脱退の設定....263
8.2.3 マルチキャストルーターの接続先の設定....264
8.2.4 クエリー送信機能の設定....264
8.2.5 IGMP クエリー送信間隔の設定....265
8.2.6 IGMP パケットの TTL 値検証機能の設定....265
8.2.7 IGMP パケットの RA 検証機能の設定....266
8.2.8 IGMP パケットの ToS 検証機能の設定....266
8.2.9 IGMP バージョンの設定....267
8.2.10 IGMP レポート抑制機能の設定....268
8.2.11 IGMP レポート転送機能の設定....268
8.2.12 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の設定....269
8.2.13 マルチキャストルーター接続ポート情報の表示....270
8.2.14 IGMP グループメンバーシップ情報の表示....270
8.2.15 インターフェースの IGMP 関連情報を表示....271
8.2.16 IGMP グループメンバーシップのエントリー削除....272
8.3 MLD スヌーピング....272
8.3.1 MLD スヌーピングの有効／無効設定....272
8.3.2 MLD スヌーピング高速脱退の設定....273
8.3.3 マルチキャストルーターの接続先の設定....273
8.3.4 クエリー送信機能の設定....274
8.3.5 MLD クエリー送信間隔の設定....274
8.3.6 MLD バージョンの設定....275
8.3.7 MLD レポート抑制機能の設定....276
8.3.8 マルチキャストルーター接続ポート情報の表示....276
8.3.9 MLD グループメンバーシップ情報の表示....277
8.3.10 インターフェースの MLD 関連情報を表示....277
8.3.11 MLD グループメンバーシップのエントリー削除....278

第 9 章 : トラフィック制御....279
9.1 ACL....279
9.1.1 IPv4 アクセスリストの生成....279
9.1.2 IPv4 アクセスリストの説明文追加....281
9.1.3 IPv4 アクセスリストの適用....281
9.1.4 IPv6 アクセスリストの生成....282
9.1.5 IPv6 アクセスリストの説明文追加....283
9.1.6 IPv6 アクセスリストの適用....283
9.1.7 MAC アクセスリストの生成....284
9.1.8 MAC アクセスリストの説明文追加....285
9.1.9 MAC アクセスリストの適用....286
9.1.10 生成したアクセスリストの表示....287
9.1.11 統計数のクリア....287
9.1.12 インターフェースに適用したアクセスリストの表示....288
9.1.13 VLAN アクセスマップの設定および VLAN アクセスマップモードへの移行....288
9.1.14 VLAN アクセスマップに対するアクセスリストの設定....288
9.1.15 VLAN アクセスマップフィルターの設定....289
9.1.16 VLAN アクセスマップの表示....290
9.1.17 VLAN アクセスマップフィルターの表示....290
9.2 QoS (Quality of Service)....290
9.2.1 QoS の有効・無効制御....290
9.2.2 デフォルト CoS の設定....291
9.2.3 トラストモードの設定....292
9.2.4 QoS 機能の設定状態の表示....293
9.2.5 インターフェースの QoS 情報の表示....293
9.2.6 送信キュー使用率の表示....294
9.2.7 CoS-送信キュー ID 変換テーブルの設定....295
9.2.8 DSCP-送信キュー ID 変換テーブルの設定....296
9.2.9 ポート優先度の設定....296

9.2.10 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....297
9.2.11 クラスマップ(トラフィックの分類条件)の生成....298
9.2.12 クラスマップの関連付け....298
9.2.13 トラフィック分類条件の設定(access-list)....299
9.2.14 トラフィック分類条件の設定(CoS)....300
9.2.15 トラフィック分類条件の設定(TOS 優先度)....300
9.2.16 トラフィック分類条件の設定(DSCP)....300
9.2.17 トラフィック分類条件の設定(Ethernet Type)....301
9.2.18 トラフィック分類条件の設定(VLAN ID)....302
9.2.19 トラフィック分類条件の設定(VLAN ID レンジ指定)....302
9.2.20 クラスマップ情報の表示....302
9.2.21 受信フレームに対するポリシーマップの生成....303
9.2.22 受信フレームに対するポリシーマップの適用....304
9.2.23 プレマーキングの設定(CoS)....305
9.2.24 プレマーキングの設定(TOS 優先度)....306
9.2.25 プレマーキングの設定(DSCP)....306
9.2.26 個別ポリサーの設定(シングルレート)....307
9.2.27 個別ポリサーの設定(ツインレート)....308
9.2.28 個別ポリサーのリマーキングの設定....310
9.2.29 集約ポリサーの生成....311
9.2.30 集約ポリサーの設定(シングルレート)....311
9.2.31 集約ポリサーの設定(ツインレート)....312
9.2.32 集約ポリサーのリマーキングの設定....313
9.2.33 集約ポリサーの表示....314
9.2.34 集約ポリサーの適用....315
9.2.35 メータリングカウンターの表示....316
9.2.36 メータリングカウンターのクリア....316
9.2.37 送信キューの指定(CoS-Queue)....317
9.2.38 送信キューの指定(DSCP-Queue)....317
9.2.39 ポリシーマップ情報の表示....318
9.2.40 マップステータスの表示....320
9.2.41 送信キューのスケジューリング設定....321
9.2.42 トラフィックシェーピング(ポート単位)の設定....321
9.2.43 トラフィックシェーピング(キュー単位)の設定....322
9.3 フロー制御....323
9.3.1 フロー制御(IEEE 802.3x PAUSE の送受信)の設定(システム)....323
9.3.2 フロー制御(IEEE 802.3x PAUSE の送受信)の設定(インターフェース)....323
9.3.3 フロー制御の動作状態の表示....324
9.4 ストーム制御....325
9.4.1 ストーム制御の設定....325
9.4.2 ストーム制御 受信上限値の表示....325

第 10 章 : アプリケーション....327
10.1 ローカル RADIUS サーバー....327
10.1.1 ローカル RADIUS サーバー機能の設定....327
10.1.2 アクセスインターフェースの設定....327
10.1.3 ルート認証局を生成....328
10.1.4 RADIUS コンフィグレーションモード....328
10.1.5 認証方式の設定....328
10.1.6 RADIUS クライアント(NAS)の設定....329
10.1.7 認証ユーザーの設定....330
10.1.8 再認証間隔の設定....332
10.1.9 ローカル RADIUS サーバーへの設定データ反映....332
10.1.10 クライアント証明書の発行....332
10.1.11 クライアント証明書の発行中断....333
10.1.12 クライアント証明書の失効....334
10.1.13 クライアント証明書のエクスポート(メール送信)....334
10.1.14 RADIUS クライアント(NAS)の表示....335
10.1.15 認証ユーザー情報の表示....336
10.1.16 クライアント証明書の発行状態表示....336

10.1.17 クライアント証明書のリスト表示.....337
10.1.18 クライアント証明書の失効リスト表示.....337

索引.....339

序文

はじめに

- 本書の記載内容の一部または全部を無断で転載することを禁じます。
- 本書の記載内容は将来予告なく変更されることがあります。
- 本製品を使用した結果発生した情報の消失等の損失については、当社では責任を負いかねます。
  保証は本製品物損の範囲に限ります。予めご了承ください。
- 本書の内容については万全を期して作成致しておりますが、記載漏れやご不審な点がございましたらご一報くださいますようお願い致します。
- 本書に記載されている会社名、製品名は各社の登録商標あるいは商標です。

第 1 章

コマンドリファレンスの見方

1.1 対応するプログラムのリビジョン

このコマンドリファレンスは、ヤマハ L2 スイッチ SWP2 のファームウェア、Rev.2.03.24 に対応しています。
このコマンドリファレンスの作成時より後にリリースされた最新のファームウェアや、マニュアル類および差分については以下に示す URL の WWW サーバーにある情報を参照してください。
https://www.yamaha.com/proaudio/

1.2 コマンドリファレンスの見方

このコマンドリファレンスは、ヤマハ L2 スイッチ SWP2 のコンソールから入力するコマンドを説明しています。

1 つ 1 つのコマンドは次の項目の組合せで説明します。

[書式]	コマンドの入力形式を説明します。キー入力時には大文字と小文字のどちらを使用しても構いません。
	コマンドの名称部分は太字 (**Bold face**) で示します。
	パラメーター部分は斜体 (*Italic face*) で示します。
	キーワードは標準文字で示します。
	括弧 ([ ]) で囲まれたパラメーターは省略可能であることを示します。
[キーワード]	コマンドに設定可能なキーワードの種類と意味を説明します。
[パラメーター]	コマンドに設定可能なパラメーターの種類とその意味を説明します。
[初期設定]	コマンドの初期設定値を示します。
[入力モード]	コマンド実行可能なモードを示します。
[説明]	コマンドの解説部分です。
[ノート]	コマンドを使用する場合に特に注意すべき事柄を示します。
[設定例]	コマンドの具体例を示します。
[適用モデル]	コマンドが適用できるモデル名称を示します。 モデルにより適用可否が異なるコマンドのみ明記しており、記載がないコマンドについてはシリーズ共通で適用可能です。

1.3 インターフェース名について

コマンドの入力形式において、スイッチの各インターフェースを指定するためにインターフェース名を利用します。
SWP2 で扱うインターフェース名には、以下があります。

インターフェース種別	プレフィックス	説明	指定例
LAN/SFP+ポート	port	物理ポートの指定に使用します。 指定する際は、port に続けて "1" + "." + "ポート番号"を指定します。	LAN ポート #1 を指定する場合:port1.1

インターフェース種別	プレフィックス	説明	指定例
VLAN インターフェース	vlan	VLAN の指定に使用します。指定する際は、vlan に続けて"VLAN ID"を指定します。	VLAN #1 を指定する場合 : vlan1
スタティック論理インターフェース	sa	複数の LAN/SFP+ポートを束ねたリンクアグリゲーションの指定に使用します。指定する際は、sa または po に続けて "論理インターフェース ID"を指定します	スタティック論理インターフェース #1 を指定する場合：sa1
LACP 論理インターフェース	po		LACP 論理インターフェース #2 を指定する場合：po2

1.4 no で始まるコマンドの入力形式について

コマンドの入力形式に **no** で始まる形のものが並記されているコマンドが多数あります。**no** で始まる形式を使うと、特別な記述がない限り、そのコマンドの設定を削除し、初期値に戻します。

第 2 章

コマンドの使い方

SWP2 のコマンド操作は、次の 2 種類の方法で行うことができます。

操作の種類	操作の方法	説明
コンソールによる操作	• コンソールターミナルからのアクセス • TELNET クライアントからのアクセス • SSH クライアントからのアクセス	コマンドを 1 つ 1 つ実行して対話的に設定や操作を行います。
Config ファイルによる操作	• TFTP によるファイル転送 • GUI 操作によるファイル転送	必要なコマンド一式を記述したファイル(これを Config ファイルと呼ぶ)により一括設定したり、SWP2 の設定を一括で取得します。

本章では、各操作方法について説明します。

2.1 コンソールによる操作

2.1.1 コンソールターミナルからのアクセス

SWP2 の CONSOLE ポートに接続した端末から設定を行う場合、RJ-45/DB-9 コンソールケーブル(YRC-RJ45)を使用してください。

パソコンをコンソールターミナル(シリアル端末)として使用する場合、パソコンのシリアル(COM)ポートを制御するターミナルソフトウェアが必要です。コンソールターミナルの通信設定は、次のとおりです。

設定項目	設定値
ボーレート	9600bps
データ	8bit
パリティ	なし
ストップビット	1bit
フロー制御	Xon/Xoff

なお、コンソールターミナルに関する設定は、**line con** コマンドでラインモードに移行して行います。

2.1.2 TELNET クライアントからのアクセス

パソコンなどの TELNET クライアントを使用して、SWP2 の TELNET サーバーに接続し、操作を行います。TELNET を使用した設定を行うためには、まず、接続環境(IP ネットワーク)の構築を行い、次に、TELNET サーバーの設定を行います。

SWP2 の IP アドレスの設定については、以下のとおりです。

- IPv4 アドレスの初期設定は、VLAN #1 に対して、ip address dhcp を設定しています。
- IPv4 アドレスの変更は、**ip address** コマンドで行います。

SWP2 の TELNET サーバー機能については、以下のとおりです。

- TELNET サーバー機能の初期設定は、デフォルトポート(TCP ポート 23 番)で起動していて、VLAN #1 からのアクセスのみ許可しています。
- 受信ポート番号の変更は、**telnet-server** コマンドで行います。
- TELNET サーバーへのアクセスは、VLAN 単位で制御でき、**telnet-server interface** コマンドで設定できます。

また、TELNET クライアントが接続する仮想的な通信ポートのことを"仮想端末(VTY: Virual TYpewriter)ポート"といいます。TELNET クライアントの最大同時接続数は、SWP2 の VTY ポート数に依存します。SWP2 の VTY ポートについては、以下のとおりです。

- VTY ポートの初期設定は、8 個の VTY ポート(ID:0～7)が使用可能となっています。
- VTY ポート数の確認は、**show running-config | include line vty** コマンドで行います。

- VTY ポート数の変更は、**line vty** コマンドで行います。(最大 8 個(ID:0～7))

なお、VTY ポートの設定は、**line vty** コマンドで対象 VTY ポートを指定した後、ラインモードに移行して行います。仮想端末ポートは SWP2 内部で ID 管理しますが、ログインセッションと ID の割り当ては接続タイミングに依存するため、通常はすべての VTY ポートに対して同じ設定を行ってください。

2.1.3 SSH クライアントからのアクセス

パソコンなどの SSH クライアントを使用して、SWP2 の SSH サーバーに接続し、操作を行います。SSH を使用した設定を行うためには、まず、接続環境(IP ネットワーク)の構築を行い、次に、SSH サーバーの設定を行います。

SWP2 の IP アドレスの設定については、以下のとおりです。

- IPv4 アドレスの初期設定は、VLAN #1 に対して、ip address dhcp を設定しています。
- IPv4 アドレスの変更は、**ip address** コマンドで行います。

SSH クライアントからアクセスする場合、事前に SWP2 の以下の設定が必要です。

- **ssh-server host key generate** コマンドで SSH サーバーのホスト鍵の生成をします。
- **ssh-server** コマンドで SSH サーバー機能を有効にします。
- **username** コマンドでユーザー名とパスワードの登録をします。

SWP2 の SSH サーバー機能については、以下のとおりです。

- SSH サーバーへのアクセスは、VLAN 単位で制御でき、**ssh-server interface** コマンドで設定できます。
- 以下の機能をサポートしていないのでご注意ください
- SSH プロトコルバージョン 1
- パスワード認証以外のユーザー認証 (ホストベース認証、公開鍵認証、チャレンジ・レスポンス認証、GSSAPI 認証)
- ポートフォワーディング (X11/TCP 転送)
- Gateway Ports (ポート中継)
- 空パスワードの許可

また、SSH クライアントが接続する仮想的な通信ポートのことを"仮想端末(VTY: Virual TYpewriter)ポート"といいます。SSH クライアントの最大同時接続数は、SWP2 の VTY ポート数に依存します。SWP2 の VTY ポートについては、以下のとおりです。

- VTY ポートの初期設定は、8 個の VTY ポート(ID:0～7)が使用可能となっています。
- VTY ポート数の確認は、**show running-config | include line vty** コマンドで行います。
- VTY ポート数の変更は、**line vty** コマンドで行います。(最大 8 個(ID:0～7))

なお、VTY ポートの設定は、**line vty** コマンドで対象 VTY ポートを指定した後、ラインモードに移行して行います。仮想端末ポートは SWP2 内部で ID 管理しますが、ログインセッションと ID の割り当ては接続タイミングに依存するため、通常はすべての VTY ポートに対して同じ設定を行ってください。

2.1.4 コンソールターミナル/VTY の設定

SWP2 は、コンソールターミナルおよび VTY に対して、以下を設定できます。

1. 無操作と判定するタイムアウト時間
2. 端末画面の 1 ページの表示行数

設定項目	設定内容
無操作と判定するタイムアウト時間	端末でキー入力がない場合にログインセッションを強制的に切断するまでの時間を設定します。 初期設定では、10 分で強制切断されます。 本設定は、ラインモードの **exec-timeout** コマンドで設定し、次のセッションから有効になります。

設定項目	設定内容
端末画面の 1 ページの表示行数	端末画面の 1 ページ当たりの行数を指定します。 0～512 行/1 ページ指定可能で、初期設定では、24 行/ページとなっています。 本状態で表示を行うと、23 行表示後、"--- More---" と表示され、キー入力待ちとなります。 本設定は、以下の 2 種類があり、上から順番にシステムに適用されます。 1) 非特権 EXEC モードの **terminal length** コマンド 2) グローバルコンフィグレーションモードの **service terminal-length** コマンド 1)の設定は端末を使用しているユーザーに一時的に有効にさせる機能で、コマンド実行後、即座に反映されます。 2)の設定は次のセッションから有効となります。

2.2 設定(Config)ファイルによる操作

必要なコマンド一式を記述したファイルを設定(Config)ファイルと呼びます。

SWP2 に設定した項目は、TFTP により LAN 上のホストから Config ファイルとして読み出すことができます。またホスト上の Config ファイルを SWP2 に読み込ませて設定を行うこともできます。

Config ファイルは全体の設定を記述したものであり、特定部分の設定だけを読み出したり差分点だけを書き込んだりすることはできません。Config ファイルは ASCII＋改行コード(CRLF または LF)で構成するテキストファイルとします。

なお、Config ファイルの内容は、コマンドの書式やパラメーターの指定などの内容が正しく記述されている必要があります。間違った書式や内容があった場合には、その内容は動作に反映されず無視されます。

2.2.1 TFTP クライアントからのアクセス

TFTP により Config ファイルをやりとりするためには、まず、接続環境(IP ネットワーク)の構築を行い、次に、TFTP サーバーの設定を行います。

SWP2 の IP アドレスの設定については、以下のとおりです。

- IPv4 アドレスの初期設定は、VLAN #1 に対して、ip address dhcp を設定しています。
- IPv4 アドレスの変更は、**ip address** コマンドで行います。

SWP2 の TFTP サーバー機能については、以下のとおりです。

- TFTP サーバー機能の初期設定は、デフォルトポート(UDP ポート 69 番)で起動していて、どこからのアクセスも許可されていません。
- 受信ポート番号の変更は、**tftp-server** コマンドで行います。
- TFTP サーバーへのアクセスは、VLAN 単位で制御でき、**tftp-server interface** コマンドで設定できます。アクセスを許可する VLAN ID を設定してください。

2.2.2 設定ファイルの読み出し/書き込み

設定ファイルの読み出し/書き込みは、LAN 上のホストから TFTP コマンドを実行します。

読み出し/書き込みを行う設定ファイルは以下の通りです。

- 設定ファイル

対象 CONFIG	対象ファイル	説明	備考
running-config	CONFIG ファイル (.txt)	現在運用中の設定値 (基本設定)	
startup-config (USER モード/DANTE モード)	CONFIG ファイル (.txt)	保存されている設定値 (基本設定)	USER モード : ディップスイッチ #1 ON DANTE モード : ディップスイッチ #1 OFF
	すべての設定 (.zip)	保存されている設定値 (すべての設定)	

設定ファイルの読み出し(GET)/書き込み(PUT)先のリモートパスとして、以下を指定します。

- 対象ファイルのリモートパス(自動再起動なし)

対象 CONFIG	対象ファイル	リモートパス	読み出し(GET)	書き込み(PUT)	自動再起動
running-config	CONFIG ファイル (.txt)	config	○	○	-
startup-config (USER モード)	CONFIG ファイル (.txt)	config0	○	○	-
	すべての設定 (.zip)	config0-all	○	○	-
startup-config (DANTE モード)	CONFIG ファイル (.txt)	config1	○	-	-
	すべての設定 (.zip)	config1-all	○	-	-

また、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。USER モードのみ有効です。

- 対象ファイルのリモートパス(自動再起動あり)

対象 CONFIG	対象ファイル	リモートパス	読み出し(GET)	書き込み(PUT)	自動再起動
startup-config (USER モード)	CONFIG ファイル (.txt)	reconfig	-	○	○
	すべての設定 (.zip)	reconfig-all	-	○	○

設定ファイルを書き込み(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。

使用するコマンドの形式は、そのホストの OS(TFTP クライアント)に依存します。次の点に注意して実行してください。

- SWP2 の IP アドレス
- 転送モードは"バイナリモード"で行います。
- リモートパスの後ろに"/PASSWORD"という形式で特権パスワードを指定する必要があります。
  特権パスワードが初期設定の状態では、設定ファイルの読み出し/書き込みをすることはできません。前もって特権パスワードを変更する必要があります。
- リモートパスに"config"を指定して PUT(書き込み)する場合、現在運用中の設定に対して、追加または上書きをします。
  設定を追加または変更しないものについては、現在運用している設定のままとなります。
  また、設定値は保存されないため、保存したい場合は **write** コマンド等で保存してください。
- 暗号化されたパスワード(**password 8** や **enable password 8** のコマンド形式)は、TFTP で running-config に PUT しても設定に反映されません。
  また、暗号化されたパスワードを含むユーザーの設定(**username** コマンド)は、ユーザーの登録自体が行われません。

2.3 ログイン

SWP2 の起動が完了すると、ログイン画面を表示します。

設定したユーザー名とパスワードを入力することでログインすることができます。

初期設定では、初期管理ユーザーが設定されており、ユーザー名:**admin**、パスワード:**admin** でログインすることができます。

- ログイン画面

```
Username:admin
Password:
```

- ログイン後のコンソール画面

```
SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
  Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.
```

```
SWP2>
```

初期管理ユーザーでログインした場合、初回のみパスワード変更画面が表示されますので、パスワードを変更してください。

- パスワード変更画面

```
Username:admin
Password:

SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
  Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.

Please change the default password for admin.
New Password:
New Password(Confirm):
Saving ...
Succeeded to write configuration
```

なお、パスワードを 3 回連続で間違えた場合、1 分間ログインが制限されます。1 分経過後、正しいパスワードを入力してください。

- ログイン制限画面

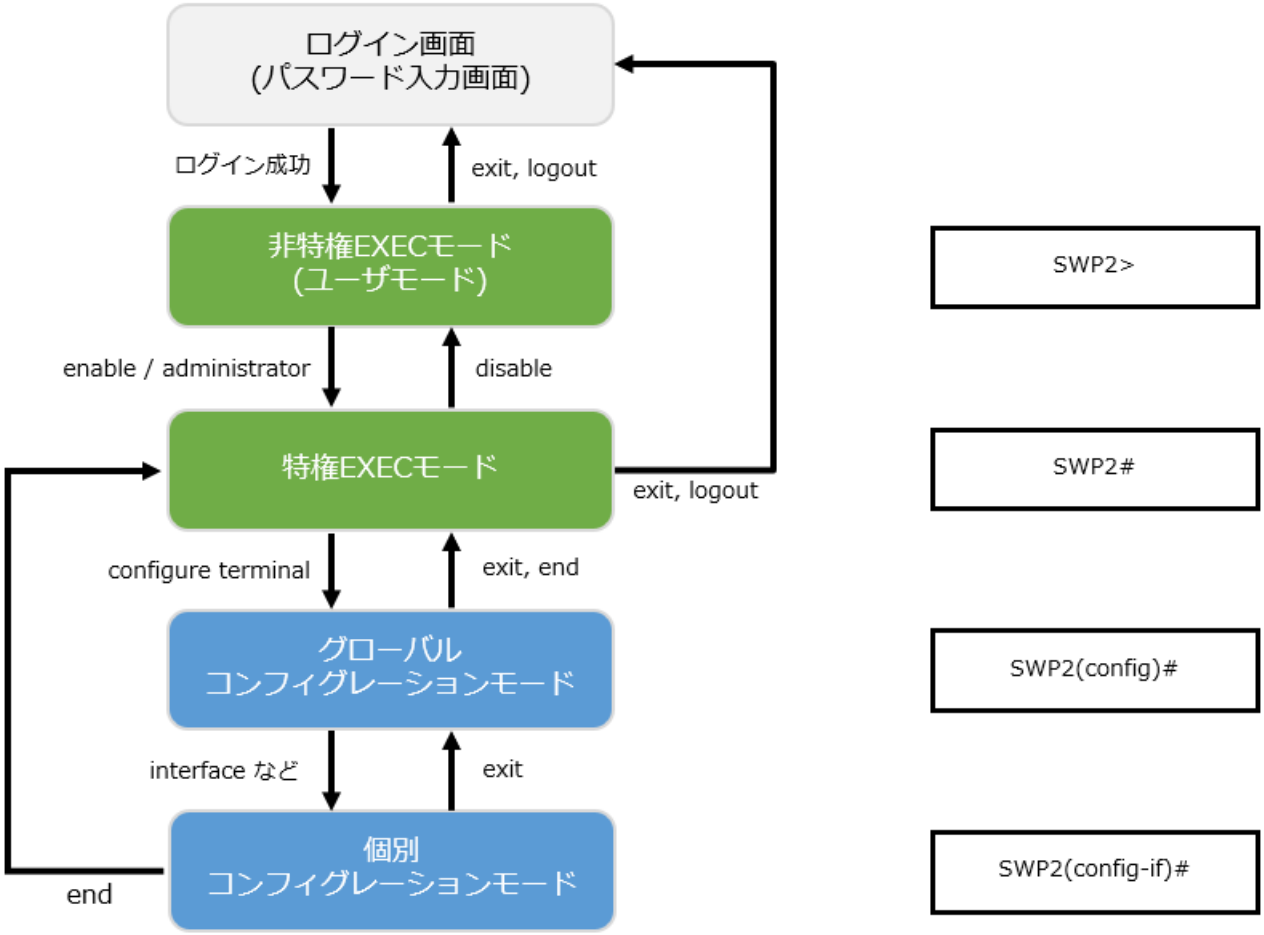
```
Username: user
Password:
% Incorrect username or password, or login as user is restricted.
Password:
% Incorrect username or password, or login as user is restricted.
Password:
% Incorrect username or password, or blocked upon 3 failed login attempts for user.
% Please try again later.
```

- ログイン制限されたユーザーが、再びパスワードを間違えると制限時間が更新されます。
- 制限時間経過後に正しいパスワードを入力することでログインできるようになります。

2.4 コマンド入力モードについて

2.4.1 コマンド入力モードの基本

SWP2 の設定変更や状態参照をする場合、適切なコマンド入力モードに遷移してから、コマンドを実行する必要があります。コマンドの入力モードは以下のような階層に分かれており、各々のモードで入力できるコマンドが異なります。ユーザーは、プロンプトを確認することで、現在、どのモードにいるのか確認することができます。



コマンド入力モードの遷移に関連する基本的なコマンドは、以下となります。 グローバルコンフィグレーションモードから個別コンフィグレーションモードへの遷移コマンドについては、「個別コンフィグレーションモード」を参照してください。

- **exit** コマンド
- **logout** コマンド
- **enable** コマンド / **administrator** コマンド
- **disable** コマンド
- **configure terminal** コマンド
- **end** コマンド

2.4.2 個別コンフィグレーションモード

個別コンフィグレーションモードとは、LAN/SFP+ポートや VLAN インターフェース、QoS など、特定の項目に対する詳細な設定を行うためのモードの総称です。個別コンフィグレーションモードに入るには、グローバルコンフィグレーションモードで各モードに移動するためのコマンドを実行します。

SWP2 の個別コンフィグレーションモードには次のものがあります。個別コンフィグレーションモードの中には階層化されているものもあります。例えば、ポリシーマップモード → ポリシーマップ・クラスモードです。

個別コンフィグレーションモード	遷移コマンド	プロンプト
インターフェースモード	**interface** コマンド	SWP2(config-if)#
ラインモード	**line con** コマンド **line vty** コマンド	SWP2(config-line)#
VLAN モード	**vlan database** コマンド	SWP2(config-vlan)#
VLAN アクセスマップモード	**vlan access-map** コマンド	SWP2(config-vlan-access-map)#
MST モード	**spanning-tree mst configuration** コマンド	SWP2(config-mst)#

個別コンフィグレーションモード	遷移コマンド	プロンプト
クラスマップモード	**class-map** コマンド	SWP2(config-cmap)#
ポリシーマップモード	**policy-map** コマンド	SWP2(config-pmap)#
ポリシーマップ・クラスモード	**class** コマンド	SWP2(config-pmap-c)#
集約ポリサーモード	**aggregate-police** コマンド	SWP2(config-agg-policer)#
LLDP エージェントモード	**lldp-agent** コマンド	SWP2(lldp-agent)#
メールテンプレートモード	**mail template** コマンド	SWP2(config-mail)#
スケジュールテンプレートモード	**schedule template** コマンド	SWP2(config-schedule)#
RADIUS コンフィグレーションモード	**radius-server local-profile** コマンド	SWP2(config-radius)#

2.4.3 コマンドプロンプトのプレフィックス

コマンドプロンプトのプレフィックスは、ホスト名を表示しています。初期状態ではホスト名として、モデル名である「SWP2」を表示しています。本表示は、**hostname** コマンドでホスト名を設定することで変更できます。SWP2 を複数使用している場合など、各スイッチに別々の名前を設定しておくことで、管理がしやすくなります。

ホスト名の変更

```
SWP2(config)# hostname Switch-012
Switch-012(config)#
```

2.4.4 異なる入力モードのコマンド実行

SWP2 では、モードごとに利用可能なコマンドが異なるため、実行可能なモードまで遷移してコマンドを実行しなければなりません。それを解消するコマンドとして、**do** コマンドを提供します。

do コマンドを使用すると、すべてのコンフィグレーションモードから特権 EXEC モードのコマンドを実行することができます。これにより、すべてのコンフィグレーションモードから特権 EXEC モードに移動することなく、設定中のコンフィグレーションを参照をしたり、設定の保存が可能となります。

ただし、**do** では補完機能は利用できないため、その後に続くコマンドをフルスペルまたは省略系で入力する必要があります。

- フルスペルで入力する場合

  ```
  SWP2(config)#do show running-config
  ```
- 省略形で入力する場合

  ```
  SWP2(config)#do sh ru
  ```

2.5 コンソール使用時のキーボード操作

2.5.1 コンソール入力の基本操作

SWP2 では、コマンドライン上で、以下の操作が可能です。

- カーソルの移動

キーボード操作	説明・備考
→	1 文字右に移動します
←	1 文字左に移動します
Esc 押下後に F	1 単語右に移動します(カーソル位置にある単語の最後の文字の次に移動します)
Esc 押下後に B	1 単語左に移動します(カーソル位置にある単語の先頭文字に移動します)
Ctrl + A	行の先頭に移動します
Ctrl + E	行の末尾に移動します

- 入力文字の削除

キーボード操作	説明・備考
Backspace	カーソルの左にある文字を削除します
Ctrl + H	
Ctrl + D	カーソル位置の文字を削除します。 コマンド行が空の状態で本操作をした場合は、**exit** コマンドと同じ動作となります。
Esc 押下後に D	カーソル位置以降、最初の空白の直前までを削除します
Ctrl + K	カーソル位置から行の末尾までを削除します
Ctrl + U	入力中の文字を全て削除します

- その他

キーボード操作	説明・備考
Ctrl + T	カーソル位置の文字とその直前の文字を入れ換えます。 カーソルが行の末尾にあるとき、直前の文字とその前の文字を入れ換えます。
Ctrl + C	非特権 EXEC モードと特権 EXEC モードでは、入力中のコマンドを破棄して次の行に移ります。 個別コンフィグレーションモードでは、入力中のコマンド行を破棄して特権 EXEC モードに遷移します。 現在実行中のコマンド処理を中断します。 (ex: **ping** コマンド)
Ctrl + Z	個別コンフィグレーションモードから特権 EXEC モードに遷移します。 **end** コマンドと同じ動作となります。

2.5.2 コマンドヘルプ

コマンドライン上で'?'を入力することで、指定できるコマンドまたはパラメーターを検索できます。

```
SWP2#show vlan ?
  <1-4094>      VLAN id
  access-map    Show VLAN Access Map
  brief         VLAN information for all bridges (static and dynamic)
  filter        Show VLAN Access Map Filter
  private-vlan  private-vlan information

SWP2#show vlan
```

2.5.3 入力コマンドの補完、キーワード候補一覧の表示

コンソール上でコマンド入力途中に、"Tab"キーを押すと、コマンド名が補完されます。また、キーワード入力後に"Tab"キーを押すと、次に入力可能なキーワードの候補一覧を表示します。本操作は、"Ctrl + I"キーを押しても同様な動作となります。

- コマンド名の補完

```
SWP2#con"<Tab>キーを押す"
       ↓
SWP2#configure
```

- キーワード候補一覧の表示

```
SWP2(config)#vlan "<Tab>キーを押す"
access-map  database    filter
SWP2(config)#vlan
```

2.5.4 コマンドの省略入力

コマンドまたはパラメーターを省略して入力した時、入力された文字が一意のコマンドまたはパラメーターとして認識できる場合は、そのコマンドが実行されます。

コマンドの省略入力例(show running-config)

```
SWP2# sh run
```

2.5.5 コマンドヒストリー

コマンドヒストリー機能を使用すると、過去に入力したコマンドを簡単な操作で再実行したり、過去に入力したコマンドの一部を変更して再実行することができます。コマンドヒストリーは、各モード共通の履歴として表示されます。

操作方法について、以下に示します。

キーボード操作	説明・備考
↑	コマンド履歴をさかのぼる
Ctrl + P	
↓	コマンド履歴を進める
Ctrl + N	

2.6 「show」で始まるコマンド

2.6.1 モディファイア

モディファイアは、**show** コマンドが出力する情報をフィルターに通し、必要な情報に内容を絞ることで端末画面に見やすく表示します。

SWP2 では、**show** コマンドのモディファイアとして、次の 3 種類を提供します。

モディファイア	説明
include	指定した文字列を含む行だけを出力する
grep	
exclude	指定した文字列を含まない行を出力する

なお、モディファイアは単一でのみ使用可能です。複数指定することはできません。

- (例) **show running-config** で VLAN #1 を含む情報を表示する。

```
SWP2#show running-config | grep vlan1
interface vlan1
http-server interface vlan1
telnet-server interface vlan1
```

- (例) **show spanning-tree** で Role を含む情報を表示する。

```
SWP2# show spanning-tree | include Role
%   po1: Port Number 505 - Ifindex 4601 - Port Id 0x81f9 - Role Disabled - State
Discarding
%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
State Forwarding
%   port1.2: Port Number 906 - Ifindex 5002 - Port Id 0x838a - Role Disabled -
State Forwarding
%   port1.3: Port Number 907 - Ifindex 5003 - Port Id 0x838b - Role Disabled -
State Forwarding
%   port1.4: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Disabled -
State Forwarding
%   port1.6: Port Number 910 - Ifindex 5006 - Port Id 0x838e - Role Disabled -
State Forwarding
%   port1.7: Port Number 911 - Ifindex 5007 - Port Id 0x838f - Role Disabled -
State Forwarding
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Disabled -
State Forwarding
%   port1.9: Port Number 913 - Ifindex 5009 - Port Id 0x8391 - Role Disabled -
State Forwarding
%   port1.10: Port Number 914 - Ifindex 5010 - Port Id 0x8392 - Role Disabled -
State Forwarding
```

第 3 章

コンフィグレーション

3.1 設定値の管理

SWP2 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 (USER モード時) 一部機能のバックアップコンフィグへの保存(DANTE モード時)
スタートアップコンフィグ (startup-config)	USER モードでは、Flash ROM 上に保存した設定値。 DANTE モードでは、デフォルトコンフィグと同様の設定値。	参照 ランニングコンフィグによる更新 (USER モード時)
バックアップコンフィグ (backup-config)	DANTE モード時に保存した、一部機能の設定値。Flash ROM 上で管理する。	ランニングコンフィグによる更新 (DANTE モード時)
デフォルトコンフィグ (default-config)	デフォルトの設定値。Flash ROM 上で管理する。 起動時のディップスイッチ #2/#3 の設定によって選択される VLAN プリセットを元に作成される。	操作不可

SWP2 のシステム起動時、以下の流れとなります。

1. ディップスイッチ #1 を参照し、CONFIG モードを決定する。
   - ディップスイッチ #1 が上(OFF)の場合、DANTE モードで起動する
   - ディップスイッチ #1 が下(ON)の場合、USER モードで起動する
2. 各 CONFIG モードごとに、スタートアップコンフィグを決定する。
   - DANTE モードの場合
     - ディップスイッチ #2/#3 の設定によって選択されるデフォルトコンフィグを使用する
   - USER モードの場合
     - USER モード用のスタートアップコンフィグが存在する場合、該当データを使用する
     - USER モード用のスタートアップコンフィグが存在しない場合、ディップスイッチ #2/#3 の設定によって選択されるデフォルトコンフィグを使用する
3. スタートアップコンフィグを RAM 上にランニングコンフィグとして展開する。
   - DANTE モード時にバックアップコンフィグが存在する場合、該当データをランニングコンフィグに上書き展開する

SWP2 運用中にコマンドなどで設定を変更すると、変更した内容はすぐにランニングコンフィグに反映されます。
ランニングコンフィグを変更した後、USER モードでは **write** または **copy** コマンドを実行することで、スタートアップコンフィグが更新されます。
また、DANTE モードでは **backup-config** コマンドを実行することで、バックアップコンフィグが更新されます。
設定・変更した内容を保存しないで再起動すると、設定・変更内容が失われます。ご注意ください。

3.2 デフォルト設定値

SWP2 では、ディップスイッチ #2/#3 によって指定された VLAN プリセットが、デフォルト設定値となります。ディップスイッチ #2/#3 の設定に対する VLAN プリセットタイプは以下のとおりです。

なお、工場出荷状態の設定は、本書に記載された各コマンドの初期値が適用されるわけではなく、以下のデフォルト設定値になっています。

- ディップスイッチ #2/#3 の設定

設定位置		VLAN プリセットタイプ
#2	#3	
上(OFF)	上(OFF)	Normal
下(ON)	上(OFF)	A
上(OFF)	下(ON)	B
下(ON)	下(ON)	C

まずモデルおよびプリセット共通の設定を表示し、次にモデルごとのプリセット固有の設定値を示します。

- モデルおよびプリセット共通のデフォルト設定(システム全体)

設定分類	設定項目	デフォルト設定値
端末設定	コンソールタイムアウト	600 sec
	VTY 数	8
	表示行数	24
ユーザーアカウント	初期管理ユーザー	ユーザー名:admin、パスワード:admin
	特権パスワード	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	UTC (±0)
	NTP サーバー	なし
	NTP 更新周期	1 時間に 1 回
RMON	動作	有効
sFlow	動作	無効
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/swp2.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	無効
	自動設定機能	無効
L2MS	動作	有効(変更不可)
	役割	エージェント(変更不可)
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

設定分類	設定項目	デフォルト設定値
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
L2 スイッチング	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	有効
DNS クライアント	動作	有効
トラフィック制御	QoS	有効
	QoS DSCP-送信キュー ID 変換テーブル	DSCP:8 → 送信キュー:2 DSCP:26 → 送信キュー:3 DSCP:34 → 送信キュー:4 DSCP:48 → 送信キュー:5 上記以外 → 送信キュー:0
	フロー制御 (IEEE 802.3x)	無効
Web GUI	言語設定	英語

- モデルおよびプリセット共通のデフォルト設定 (LAN/SFP+ポート)

設定分類	設定項目	デフォルト設定値
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	プリセットに依存
	所属 VLAN ID	プリセットに依存
L2MS	L2MS フィルター	プリセットに依存
L2 スイッチング	スパニングツリー	プリセットに依存
	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	DSCP
	フロー制御 (IEEE 802.3x)	無効
	ストーム制御	無効

- SWP2 の VLAN プリセット Normal のデフォルト設定 (システム全体)

設定分類	設定項目	デフォルト設定値
IP マルチキャスト制御	トポロジー変更時の IGMP/MLD クエリー送信機能	有効(待ち時間 5 sec)

- SWP2 の VLAN プリセット Normal のデフォルト設定 (LAN/SFP+ポート)

Interface	L2MS Filter	LAG(Static)	Port Mode	VLAN	STP
port1.1	Disable	-	Access	1(default)	×
port1.2	Disable	-	Access	1(default)	×
port1.3	Disable	-	Access	1(default)	×
port1.4	Disable	-	Access	1(default)	×
port1.5	Disable	-	Access	1(default)	×
port1.6	Disable	-	Access	1(default)	×
port1.7	Disable	-	Access	1(default)	×
port1.8	Disable	-	Access	1(default)	×
port1.9	Disable	-	Access	1(default)	×
port1.10	Disable	-	Access	1(default)	×
port1.11	Disable	-	Access	1(default)	○
port1.12	Disable	-	Access	1(default)	○

- SWP2 の VLAN プリセット Normal のデフォルト設定 (VLAN インターフェース)
  - VLAN #1(for Dante and Control)
    - IPv4 Address: DHCP
    - IGMP Snooping: Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
- SWP2 の VLAN プリセット A のデフォルト設定 (システム全体)

設定分類	設定項目	デフォルト設定値
IP マルチキャスト制御	トポロジー変更時の IGMP/MLD クエリー送信機能	有効(待ち時間 5 sec)

- SWP2 の VLAN プリセット A のデフォルト設定 (LAN/SFP+ポート)

Interface	L2MS Filter	LAG(static)	Port Mode	VLAN	STP
port1.1	Disable	-	Access	1(default)	×
port1.2	Disable	-	Access	1(default)	×
port1.3	Disable	-	Access	1(default)	×
port1.4	Disable	-	Access	1(default)	×
port1.5	Disable	-	Access	2	×
port1.6	Disable	-	Access	2	×
port1.7	Disable	-	Access	1(default)	×
port1.8	Disable	-	Access	1(default)	×
port1.9	Disable	-	Access	2	×
port1.10	Disable	-	Access	2	×
port1.11	Disable	sa1	Trunk	1(native), 2	○
port1.12	Disable				

- SWP2 の VLAN プリセット A のデフォルト設定 (VLAN インターフェース)
  - VLAN #1(for Dante)
    - IPv4 Address: DHCP
    - IGMP Snooping: Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-Leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Control)
    - IGMP Snooping: Disable
- SWP2 の VLAN プリセット B のデフォルト設定 (システム全体)

設定分類	設定項目	デフォルト設定値
IP マルチキャスト制御	トポロジー変更時の IGMP/MLD クエリー送信機能	有効(待ち時間 5 sec)

- SWP2 の VLAN プリセット B のデフォルト設定(LAN/SFP+ポート)

Interface	L2MS Filter	LAG(static)	Port Mode	VLAN	STP
port1.1	Disable	-	Access	1(default)	×
port1.2	Disable	-	Access	1(default)	×
port1.3	Disable	-	Access	1(default)	×
port1.4	Disable	-	Access	1(default)	×
port1.5	Disable	-	Access	2	×
port1.6	Disable	-	Access	2	×
port1.7	Disable	-	Access	1(default)	×
port1.8	Disable	-	Access	2	×
port1.9	Disable	sa1	Trunk	1(native), 2	○
port1.10	Disable				
port1.11	Disable	sa2	Trunk	1(native), 2	○
port1.12	Disable				

- SWP2 の VLAN プリセット B のデフォルト設定 (VLAN インターフェース)
  - VLAN #1(for Dante)
    - IPv4 Address: DHCP
    - IGMP Snooping: Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Control)
    - IGMP Snooping: Disable
- SWP2 の VLAN プリセット C のデフォルト設定 (LAN/SFP+ポート)

Interface	L2MS Filter	LAG(static)	Port Mode	VLAN	STP
port1.1	Disable	-	Access	1(default)	×
port1.2	Disable	-	Access	1(default)	×
port1.3	Disable	-	Access	1(default)	×
port1.4	Enable	-	Access	2	×
port1.5	Enable	-	Access	2	×

Interface	L2MS Filter	LAG(static)	Port Mode	VLAN	STP
port1.6	Enable	-	Access	2	×
port1.7	Disable	-	Access	1(default)	×
port1.8	Disable	-	Access	1(default)	×
port1.9	Enable	-	Access	2	×
port1.10	Enable	-	Access	2	×
port1.11	Disable	-	Access	1(default)	×
port1.12	Enable	-	Access	2	×

- SWP2 の VLAN プリセット C のデフォルト設定(VLAN インタフェース)
  - VLAN #1(for Dante)
    - IPv4 Address: DHCP
    - IGMP Snooping: Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-leave : Disable
      - Check TTL : Disable
  - VLAN #2(for Control)
    - IGMP Snooping: Enable
      - Querier : Enable
      - Query Interval : 30sec
      - Fast-leave : Disable
      - Check TTL : Disable

第 4 章

保守・運用機能

4.1 パスワード

4.1.1 特権パスワードの設定

[書式]

enable password *password*

[パラメーター]

password : 特権パスワード

半角英数字および " と ' と | と > と ? と空白文字を除く半角記号(8 文字以上 32 文字以内)
最初の文字は半角英数字でなければいけない

[初期設定]

enable password admin

[入力モード]

グローバルコンフィグレーションモード

[説明]

特権 EXEC モードへ移行するためのパスワードを設定する。

初期パスワードである admin に変更することはできない。

[ノート]

password-encryption コマンドにしたがって暗号化されたパスワードの場合、 コンフィグ上では"**enable password** 8 *password*"の形式で表示される。

ユーザーはコマンドラインからコンフィグ設定するとき、この形式で入力することはできない。また、8 は予約文字であるため、パスワードに 8 のみを指定することはできない。

起動時に、特権パスワードが設定されていない場合は、初期パスワード(admin)を自動的に設定する。

[設定例]

特権パスワードとして admin1234 を設定する。

```
SWP2(config)#enable password admin1234
```

4.1.2 パスワードの暗号化

[書式]

password-encryption *switch*
no password-encryption

[パラメーター]

switch : パスワードを暗号化するか否か

設定値	説明
enable	暗号化する
disable	暗号化しない

[初期設定]

password-encryption disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

パスワードの暗号化を有効にする。

有効にすると、**password** コマンド、**enable password** コマンド、**username** コマンドで入力したパスワードを、コンフィグ中では暗号化された形式で保存する。

no 形式で実行した場合は、パスワードの暗号化を無効し、**password** コマンド、**enable password** コマンド、**username** で入力したパスワードを、コンフィグ中では平文のまま保存する。

[ノート]

パスワードの暗号化を無効から有効に変更した場合は、既に設定済みのパスワードは平文から暗号化された形式に変更されるが、有効から無効に変更した場合は、既に暗号化されているコンフィグ中のパスワードは平文には戻らない。

[設定例]

パスワードの暗号化を有効にする。

```
SWP2(config)#password-encryption enable
```

パスワードの暗号化を無効にする。

```
SWP2(config)#no password-encryption
```

4.2 ユーザーアカウント管理

4.2.1 ユーザーの設定

[書式]

username *username* [privilege *privilege*] password *password*
no username *username*

[キーワード]

privilege	:	ユーザーの権限を指定する
password	:	ユーザーのパスワードを指定する

[パラメーター]

username : ユーザー名

半角英数字(32 文字以内)

privilege : 特権を付与するか否か

設定値	説明
on	特権 EXEC モード移行時にパスワードの入力が求められない Administrator 権限で Web GUI にアクセスできる
off	特権 EXEC モード移行時にパスワードの入力が求められる Guest 権限で Web GUI にアクセスできる

password : ユーザーのログインパスワード

半角英数字および " と ' と | と > と ? と空白文字を除く半角記号(8 文字以上 32 文字以内)

最初の文字は半角英数字でなければいけない

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

ユーザー情報を設定する。

ユーザー情報は最大で 33 件まで登録できる。 ただし、privilege off のユーザーは最大 32 件まで、privilege on のユーザーは 必ず 1 件必要となる。

以下の単語はユーザー名として登録できない。

lp, adm, bin, ftp, gdm, man, rpc, sys, xfs, halt, mail, news, nscd, sync, uucp, root, sshd, games, daemon, gopher, nobody, ftpuser, mtsuser, rpcuser, mailnull, operator, shutdown

デフォルトパスワードである admin はパスワードとして使用できない。

[ノート]

password-encryption コマンドが設定されていた場合、パスワードは暗号化されコンフィグ上では"**username** *username* password 8 *password*"の形式で表示される。

ユーザーはコマンドラインからコンフィグ設定するとき、この形式で入力することはできない。また、8 は予約文字であるため、パスワードに 8 のみを指定することはできない。

起動時に、privilege on のユーザーが 1 つも設定されていない場合は、初期管理ユーザー(admin/admin)を追加する。

起動時に、パスワードが設定されていないユーザーは、ユーザー名と同じ文字列をパスワードに自動設定する。

[設定例]

ユーザー **user1234** を設定する。

```
SWP2(config)#username user1234 password user_pass
```

特権を付与したユーザー **user1234** を設定する。

```
SWP2(config)#username user1234 privilege on password user_pass
```

4.2.2 ユーザー権限の変更

[書式]

username *username* privilege *privilege*

[キーワード]

privilege	:	ユーザーの権限を指定する

[パラメーター]

username	:	ユーザー名 半角英数字(32 文字以内)
privilege	:	特権を付与するか否か

設定値	説明
on	特権 EXEC モード移行時にパスワードの入力が求められない Administrator 権限で Web GUI にアクセスできる
off	特権 EXEC モード移行時にパスワードの入力が求められる Guest 権限で Web GUI にアクセスできる

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

登録済みのユーザーの権限を変更する。

[ノート]

未登録のユーザーには設定できない。

[設定例]

登録済みのユーザー **user1234** に特権を付与する。

```
SWP2(config)#username user1234 privilege on
```

4.2.3 ログインユーザー情報の表示

[書式]

show users

[入力モード]

非特権 EXEC モード, 特権 EXEC モード, グローバルコンフィグレーションモード

[説明]

ログイン中のユーザー情報を表示する。

以下の項目が表示される。

項目	説明
Line	ログイン手段を表示する。 **con 0** はシリアルコンソールポート **vty N** は VTY ポート **http N** は Web GUI
Own	自身の接続ポートの行に ***** を表示する。
User	ログイン中のユーザー名を表示する。
Status	ログイン状態を表示する。ユーザーが使用中の場合、**Login** を表示する。
Login time	ログイン時間を表示する。
IP address	接続ユーザーの IP アドレスを表示する。

[設定例]

ユーザーのログイン情報を表示する。

```
SWP2>show users

  Line    Own  User                                Status  Login time  IP address
-------------------------------------------------------------------------------
---------
  con  0       user1234                            Login   02:15:23
  vty  0  *    operators1                          Login   00:12:59    192.168.100.1
  vty  1       abcdefghijklmnopqrstuvwxyzabcdef    Login   00:00:50    192.168.100.24
  vty  2       -                                   Login   00:00:21    192.168.100.10
  vty  3       -                                   -       -
  vty  4       -                                   -       -
  vty  5       -                                   -       -
  vty  6       -                                   -       -
  vty  7       -                                   -       -
  http 0       user1234                            Login   01:12:25    192.168.100.4
  http 1       (noname)                            Login   00:18:04    192.168.100.102
  http 2       -                                   -       -
  http 3       -                                   -       -
```

4.2.4 バナーの設定

[書式]

banner motd *word*

no banner motd

[パラメーター]

word : 半角英数字および半角記号(256 文字以内)

[初期設定]

no banner motd

[入力モード]

グローバルコンフィグレーションモード

[説明]

コンソールログイン時に表示されるバナーを設定する。

[設定例]

バナー表示を「Hello World!」に設定する。

```
Username:
Password:

SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
  Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.

SWP2>enable
SWP2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWP2(config)#banner motd Hello World!
SWP2(config)#exit
SWP2#exit

Username:
Password:

Hello World!

SWP2>enable
SWP2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWP2(config)#no banner motd
SWP2(config)#exit
SWP2#exit

Username:
Password:

SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
  Copyright (c) 2018 Yamaha Corporation. All Rights Reserved.

SWP2>
```

4.3 コンフィグの管理

4.3.1 ランニングコンフィグの保存

[書式]

copy running-config startup-config

[入力モード]

特権 EXEC モード

[説明]

現在運用中の設定(ランニングコンフィグ)を起動時の設定(スタートアップコンフィグ) として保存する。

[ノート]

保存先のスタートアップコンフィグは、起動時の本体ディップスイッチ #1 で決定する。

ランニングコンフィグの保存は **write** コマンドや **save** コマンドでも行うことができる。

USER モードの場合のみ、本コマンドで設定を保存することができる。DANTE モードの場合は、**backup-config** コマンドで一部の設定を保存することができる。

[設定例]

ランニングコンフィグを保存する。

```
SWP2#copy running-config startup-config
Succeeded to write configuration
SWP2#
```

4.3.2 ランニングコンフィグの保存

[書式]

write

save

[入力モード]

特権 EXEC モード、個別コンフィグレーションモード

[説明]

現在運用中の設定(ランニングコンフィグ)を起動時の設定(スタートアップコンフィグ)として保存する。

[ノート]

保存先のスタートアップコンフィグは、起動時の本体ディップスイッチ #1 で決定する。

ランニングコンフィグの保存は **copy running-config startup-config** コマンドでも行うことができる。

USER モードの場合のみ、本コマンドで設定を保存することができる。DANTE モードの場合は、**backup-config** コマンドで一部の設定を保存することができる。

[設定例]

ランニングコンフィグを保存する。

```
SWP2#write
Succeeded to write configuration.
SWP2#
```

4.3.3 対象機能のバックアップを行う

[書式]

backup-config

[入力モード]

特権 EXEC モード

[説明]

特定機能の設定をバックアップする。

バックアップ対象機能は以下。

- IPv4 アドレス
- 時刻設定
- ユーザーアカウントの設定
- ファームウェア更新の設定
- SYSLOG の設定
- HTTP サーバーの設定
- TELNET サーバーの設定
- SSH サーバーの設定
- TFTP サーバの設定

本コマンドを実行すると、上記の特定機能の設定をバックアップコンフィグとして保存する。

DANTE モードで起動したときにバックアップコンフィグが存在する場合、その設定をリストアする。

[ノート]

USER モードで動作中に本コマンドを実行するとエラーとなる。

[設定例]

バックアップコンフィグを保存する。

```
SWP2#backup-config
Succeeded to write backup configuration
SWP2#
```

4.3.4 ランニングコンフィグの表示

[書式]

show running-config [*section*]

show config

[パラメーター]

section : 表示するセクション

設定値	説明
access-list	アクセスリスト関連
http-server	HTTP サーバー関連
interface	インターフェース関連
ip	IP 関連
ipv6	IPv6 関連
key	認証キー関連
l2ms	L2MS 関連
lldp	LLDP 関連
mail	メール通知関連
radius-server	RADIUS サーバー関連
schedule	スケジュール関連
sflow	sFlow 関連
snmp	SNMP 関連
spanning-tree	STP 関連
ssh-server	SSH サーバー関連
telnet-sever	TELNET サーバー関連

[入力モード]

特権 EXEC モード、個別コンフィグレーションモード

[説明]

現在運用中の設定(ランニングコンフィグ)を表示する。

section 指定省略時はすべての設定を表示する。

[設定例]

ランニングコンフィグを表示する。

```
SWP2#show running-config
!
interface port1.1
 switchport
...
!
line con 0
line vty 0 7
!
end

SWP2#
```

4.3.5 スタートアップコンフィグの表示

[書式]

show startup-config

[入力モード]

特権 EXEC モード

[説明]

起動時に使用する設定(スタートアップコンフィグ)を表示する。

[ノート]

表示するスタートアップコンフィグは、起動時の本体ディップスイッチ #1 で決定する。

[設定例]

次回起動時のスタートアップコンフィグを表示する。

```
SWP2#show startup-config
!
!  Last Modified: Mon Jan 01 00:00:00 UTC 2018
!
qos enable
qos dscp-queue 0 0
qos dscp-queue 1 0
qos dscp-queue 2 0
qos dscp-queue 3 0
qos dscp-queue 4 0

...

!
telnet-server enable
!
line con 0
line vty 0 7
!
end
SWP2#
```

4.3.6 バックアップコンフィグの表示

[書式]

show backup-config

[入力モード]

特権 EXEC モード

[説明]

バックアップコンフィグを表示する。

[ノート]

USER モードで動作中に本コマンドを実行するとエラーとなる。

[設定例]

バックアップコンフィグを表示する。

```
SWP2#show backup-config
!
!  Last backup: Fri Sep 7 00:00:00 UTC 2018
!
interface vlan1
 ip address dhcp
!
interface vlan2
!
http-server enable
http-server language english
!
telnet-server enable
```

```
!
end
SWP2#
```

4.3.7 スタートアップコンフィグの消去

[書式]

erase startup-config

[入力モード]

特権 EXEC モード

[説明]

起動時に使用する設定(スタートアップコンフィグ)とそれに付随する情報を消去する。

[ノート]

消去するスタートアップコンフィグは、起動時の本体ディップスイッチ #1 で決定する。

[設定例]

スタートアップコンフィグを消去する。

```
SWP2#erase startup-config
Succeeded to erase configuration.
SWP2#
```

4.3.8 対象機能のバックアップを削除する

[書式]

erase backup-config

[入力モード]

特権 EXEC モード

[説明]

バックアップコンフィグを削除する。

[ノート]

USER モードで動作中に本コマンドを実行するとエラーとなる。

[設定例]

バックアップコンフィグを削除する

```
SWP2#erase backup-config
Succeeded to erase backup configuration
SWP2#
```

4.4 起動情報の管理

4.4.1 起動情報の表示

[書式]

show boot *num*
show boot all
show boot list

[キーワード]

all	:	起動情報の履歴を最大で 5 件まで表示する
list	:	起動情報の履歴を最大で 5 件まで簡易表示する

[パラメーター]

num	:	<0-4> 指定した番号の履歴を表示する

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

起動情報を表示する。

[ノート]

cold start コマンド、**clear boot list** コマンドを実行すると、この履歴はクリアされる。

[設定例]

現在の起動情報を表示する。

```
SWP2>show boot 0
 Running EXEC: SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
Previous EXEC: SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
Restart by reload command
```

起動履歴の一覧を表示する。

```
SWP2>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
--- ---------- -------- --------------------------------------------------
```

4.4.2 起動情報のクリア

[書式]

clear boot list

[入力モード]

特権 EXEC モード

[説明]

起動情報の履歴を削除する。

[設定例]

起動情報をクリアする。

```
SWP2#clear boot list
```

4.5 筐体情報表示

4.5.1 製品情報の表示

[書式]

show inventory

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

本体および SFP+モジュールの製品情報を表示する。

以下の項目が表示される。

項目	説明
NAME	名称
DESCR	概要
Vendor	ベンダー名
PID	プロダクト ID
VID	バージョン ID、無効の場合は 0
SN	シリアル番号

[設定例]

製品情報を表示する。

```
SWP2>show inventory
NAME  : L2 switch
DESCR : SWP2
Vendor: Yamaha
PID   : SWP2
VID   : 0000
SN    : SMF00000

NAME  : SFP1
DESCR : 10G Base-LR
Vendor: Yamaha
PID   : YSFP-10G-LR
VID   : V1.0
SN    : Z5H00000YJ

NAME  : SFP2
DESCR : 10G Base-LR
Vendor: Yamaha
PID   : YSFP-10G-LR
VID   : V1.0
SN    : Z5H00001YJ

SWP2>
```

4.5.2 稼動情報の表示

[書式]

show environment

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

システムの稼動情報を表示する。

以下の項目が表示される。

- モデル名
- ブートバージョン
- ファームウェアリビジョン
- ボードバージョン
- 仕向け情報
- シリアル番号
- デバイス ID
- MAC アドレス
- CPU 使用率
- メモリ使用率
- ファームウェアファイル
- CONFIG モード
- VLAN プリセット(DANTE モード時のみ)
- 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

[設定例]

稼動情報を表示する。

```
SWP2>show environment
[Device]
  Model               : SWP2
  BootROM version     : 1.01
  Firmware version    : Rev.2.03.24 (Mon Sep  1 00:00:00 2025)
```

```
  Board version      : 00
  Destination        : 00 (-)
  Serial             : S00000000
  Device ID          : 0000000-0000000-0000000-00000
  MAC-Address        : ac44.f200.0000

[Status]
  CPU                : 8%(5sec)  4%(1min)  4%(5min)
  Memory             : 27% used

[Configuration]
  Startup firmware           : exec0
  Configration mode          : USER
  Serial Baudrate            : 9600

[Time]
  Boot time                  : 2025/07/07 07:11:33 +00:00
  Current time               : 2025/07/07 07:23:01 +00:00
  Elapsed time from boot     : 0days 00:11:32
```

4.5.3 ディスク使用状況

[書式]

show disk-usage

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

システムで使用しているディスクの使用状況を表示する。

- System : システム使用エリア(設定情報含む)
- Temporary : 一時エリア

[設定例]

ディスクの使用状況を表示する。

```
SWP2#show disk-usage
  Category    Total    Used     Free     Used (%)
  ----------- -------- -------- -------- --------
  System       160.6M     1.1M   154.8M       1%
  Temporary     80.0M     2.4M    77.6M       3%
```

4.5.4 実行中のプロセスの表示

[書式]

show process

[入力モード]

特権 EXEC モード

[説明]

実行中のプロセスを一括表示する。

[設定例]

実行中のプロセスを表示する。

```
SWP2#show process
```

4.5.5 メモリ使用状況の表示

[書式]

show memory

[入力モード]

特権 EXEC モード

[説明]

プロセス毎のメモリ使用量を表示する。

以下の項目を表示する。

項目	説明
PID	プロセス ID
NAME	プロセス名
%MEM	物理メモリの占有率
SIZE	物理メモリの使用量(現在値)
PEAK	物理メモリの使用量(これまでの最大値)
DATA	動的仮想メモリー領域サイズ
STK	スタックサイズ

[設定例]

プロセス毎のメモリ使用量を表示する。

```
SWP2#show memory
```

4.5.6 技術サポート情報の表示

[書式]

show tech-support

[入力モード]

特権 EXEC モード

[説明]

技術サポート情報を表示する。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る。

コマンド	実行可否
show running-config	○
show startup-config	○
show environment	○
show system-diagnostics	○
show clock detail	○
show disk-usage	○
show dipsw	○
show inventory	○
show boot all	○
show logging	○
show process	○
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	○

コマンド	実行可否
show qos queue-counters	○
show ddm status	○
show errdisable	○
show auth status	○
show auth supplicant	○
show error port-led	○
show ip interface brief	○
show ip forwarding	○
show ipv6 interface brief	○
show ipv6 dhcp interface	○
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 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	○

[設定例]

技術サポート情報を表示する。

```
SWP2#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 environment ***
...

*** show disk-usage ***
...

*** show dipsw ***
...
...
...

#
# End of Information for Yamaha Technical Support
#

SWP2#
```

4.6 システム自己診断

4.6.1 システム自己診断結果の表示

[書式]

show system-diagnostics

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

すべてのシステム自己診断結果（ブートアップ診断結果、オンデマンド診断結果、ヘルスモニタリング診断結果）を表示する。

[設定例]

システム自己診断結果を表示する。

```
SWP2#show system-diagnostics
Test results:
  P = Pass, F = Fail, U = Untested
  N = Normal, W = Warning

- Bootup
  Loading Test: Pass

  RTC Test: Pass

   . . .

- On-demand
  Last on-demand diagnostics information:
    Date     : 2025/01/01 09:00:00 +09:00
    BootROM  : Ver.1.00
     . . .

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

   . . .

- Health monitoring
   . . .

  SFP Test:
```

```
Port  13  14  15  16
------------------
       N   N   N   N
```

4.6.2 オンデマンド診断の実行

[書式]

system-diagnostics on-demand execute [no-confirm]

[キーワード]

no-confirm　：　オンデマンド診断の実行確認（y or n）を行わず即時実行する

[入力モード]

特権 EXEC モード

[説明]

オンデマンド診断を実行する。

診断中はすべての LAN/SFP+ポートをシャットダウンする。診断終了時には簡易診断結果を表示し、自動的にシステムを再起動する。

パラメーターを指定しない場合は、オンデマンド診断を実行するかどうかの確認を求められる。

診断を実行する場合は "y" を、実行しない場合は "n" を入力する必要がある。

[ノート]

オンデマンド診断結果の詳細は再起動後に **show system-diagnostics** コマンドで確認できる。

[設定例]

オンデマンド診断を実行する。

```
SWP2#system-diagnostics on-demand execute
The system will be rebooted after diagnostics. Continue ? (y/n) y
on-demand diagnostics completed (pass). reboot immediately...
```

4.6.3 オンデマンド診断結果の削除

[書式]

clear system-diagnostics on-demand

[入力モード]

特権 EXEC モード

[説明]

オンデマンド診断結果を削除する。

[設定例]

オンデマンド診断結果を削除する。

```
SWP2#clear system-diagnostics on-demand
```

4.7 ケーブル診断

4.7.1 ケーブル診断の実行

[書式]

cable-diagnostics tdr execute interface *ifname*
test cable-diagnostics tdr interface *ifname*

[パラメーター]

ifname　：　LAN ポートのインターフェース名
　　対象のインターフェース

[入力モード]

特権 EXEC モード

[説明]

ケーブル診断を実行する。前回の診断結果は show cable-diagnostics tdr コマンドで確認できる。

[ノート]

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る。

[設定例]

port1.1 に接続されている LAN ケーブルの診断を実行する。

```
SWP2#cable-diagnostics tdr execute interface port1.1
The port will be temporarily down during test. Continue? (y/n): y
% To check result, enter "show cable-diagnostics tdr"
```

4.7.2 ケーブル診断結果のクリア

[書式]

clear cable-diagnostics tdr
clear test cable-diagnostics tdr

[入力モード]

特権 EXEC モード

[説明]

前回の cable-diagnostics tdr execute interface コマンドの実行結果をクリアする。

[設定例]

前回のケーブル診断の実行結果をクリアする。

```
SWP2#clear cable-diagnostics tdr
SWP2#
```

4.7.3 ケーブル診断結果の表示

[書式]

show cable-diagnostics tdr
show test cable-diagnostics tdr

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

前回の cable-diagnostics tdr execute interface コマンドの実行結果を表示する。

[設定例]

前回のケーブル診断の実行結果を表示する。

```
SWP2#show cable-diagnostics tdr
Last run on Tue May 31 14:29:35 2022
Port      Pair  Status  Fault distance
-----------------------------------------
port1.8   1     OK      -
          2     OK      -
          3     Open    15   m
          4     Open    15   m
```

4.8 時刻管理

4.8.1 時刻の手動設定

[書式]

clock set *time month day year*

[パラメーター]

time : hh:mm:ss
時刻

month : <1-12> または Jan, Feb, Mar, ... , Dec
月 または 月名

day : <1-31>
日

year : 年(西暦 4 桁)

[入力モード]

特権 EXEC モード

[説明]

システム時計を設定する。

[設定例]

時刻を 2015 年 1 月 1 日 0 時 0 分 0 秒に設定する。

```
SWP2#clock set 00:00:00 Jan 1 2015
```

4.8.2 タイムゾーンの設定

[書式]

clock timezone *zone*
clock timezone *offset*
no clock timezone

[パラメーター]

zone : タイムゾーン名

設定値	説明
UTC	協定世界時
JST	日本標準時

offset : UTC からの時差を設定

設定値	説明
-12:00	GMT-12:00
-11:00	GMT-11:00
-10:00	GMT-10:00
-9:00	GMT-9:00
-8:00	GMT-8:00
-7:00	GMT-7:00
-6:00	GMT-6:00
-5:00	GMT-5:00
-4:30	GMT-4:30
-4:00	GMT-4:00
-3:30	GMT-3:30
-3:00	GMT-3:00
-2:00	GMT-2:00
-1:00	GMT-1:00
+0:00	GMT+0:00
+1:00	GMT+1:00
+2:00	GMT+2:00
+3:00	GMT+3:00
+3:30	GMT+3:30
+4:00	GMT+4:00
+4:30	GMT+4:30
+5:00	GMT+5:00
+5:30	GMT+5:30
+5:45	GMT+5:45
+6:00	GMT+6:00
+6:30	GMT+6:30
+7:00	GMT+7:00
+8:00	GMT+8:00
+9:00	GMT+9:00
+9:30	GMT+9:30
+10:00	GMT+10:00
+11:00	GMT+11:00
+12:00	GMT+12:00
+13:00	GMT+13:00

[初期設定]

clock timezone UTC

[入力モード]

グローバルコンフィグレーションモード

[説明]

タイムゾーンを設定する。

no 形式で実行すると、UTC になる。

[設定例]

タイムゾーンを JST に設定する。

```
SWP2(config)#clock timezone JST
```

タイムゾーンを UTC+9 時間に設定する。

```
SWP2(config)#clock timezone +9:00
```

4.8.3 サマータイムの設定(繰り返し)

[書式]

clock summer-time *name* **recurring** *week wday month time week wday month time* [*offset*]
no clock summer-time

[パラメーター]

name	:	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 半角英数字(7 文字以内)
week	:	<1-4> または first, last 月の何週目かを指定する
wday	:	Sun, Mon, Tue, ... , Sat 曜日
month	:	<1-12> または Jan, Feb, Mar, ... , Dec 月 または 月名
time	:	hh:mm 時刻
offset	:	<1-1440> サマータイムの間に追加する時間。分で指定する。デフォルト値は 60。

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

サマータイムを設定する。
毎年指定した週と曜日で開始および終了するようにサマータイムを設定する。
最初の部分でサマータイムの開始時期を、2 番めの部分で終了時期を指定する。
no 形式で実行すると、設定が削除される。

[ノート]

サマータイムは重複設定できない。

[設定例]

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する。

```
SWP2(config)#clock summer-time JDT recurring 2 Sun Mar 2:00 1 Sun Nov 2:00
```

4.8.4 サマータイムの設定(日付指定)

[書式]

clock summer-time *name* **date** *month day year time month day year time* [*offset*]
no clock summer-time

[パラメーター]

name	:	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

半角英数字(7 文字以内)

month : <1-12> または Jan, Feb, Mar, ... , Dec

月 または 月名

day : <1-31>

日

year : 年(西暦 4 桁)

time : hh:mm

時刻

offset : <1-1440>

サマータイムの間に追加する時間。分で指定する。デフォルト値は 60。

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

サマータイムを設定する。

指定した日付で開始および終了するようにサマータイムを設定する。

最初の部分でサマータイムの開始日付を、2 番めの部分で終了日付を指定する。

no 形式で実行すると、設定が削除される。

[ノート]

サマータイムは重複設定できない。

[設定例]

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する。

```
SWP2(config)#clock summer-time JDT date Mar 14 2021 2:00 Nov 7 2021 2:00
```

4.8.5 現在時刻の表示

[書式]

show clock [detail]

[キーワード]

detail : 詳細情報も表示する

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

現在の時刻、年月日を表示する。

detail を指定した場合は、詳細情報(現在の時刻とサマータイム)を表示する。

サマータイムは繰り返し(recurring)の場合、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する。

[設定例]

現在の時刻を表示する。

```
SWP2>show clock
Thu Jan 1 00:00:00 JST 2015
```

現在の時刻の詳細情報を表示する。(サマータイムの設定がある場合)

```
SWP2>show clock detail
Thu Jan 1 00:00:00 JST 2021

Summer Time
```

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

現在の時刻の詳細情報を表示する。(サマータイムの設定がない場合)

```
SWP2>show clock detail
SWX3220>show clock detail
Thu Jan 1 00:00:00 JST 2021

Summer Time Disabled
```

4.8.6 NTP サーバーの設定

[書式]

ntpdate server ipv4 *ipv4_addr*
ntpdate server ipv6 *ipv6_addr*
ntpdate server name *fqdn*
no ntpdate server

[キーワード]

ipv4	:	NTP サーバーを IPv4 アドレスで指定する
ipv6	:	NTP サーバーを IPv6 アドレスで指定する
name	:	NTP サーバーをホスト名で指定する

[パラメーター]

ipv4_addr	:	NTP サーバーの IPv4 アドレス
ipv6_addr	:	NTP サーバーの IPv6 アドレス IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)
fqdn	:	NTP サーバーのホスト名 文字種として英字(大文字/小文字)、数字、.(ピリオド)、-(ハイフン)が使用可能

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

NTP サーバーのアドレスまたはホスト名を登録する。

本コマンドは最大で 2 つまで設定できる。

no 形式で実行すると、設定が削除される。

NTP 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う。

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る。

[設定例]

NTP サーバーに 192.168.1.1 を設定する。

```
SWP2(config)#ntpdate server ipv4 192.168.1.1
```

NTP サーバーに fe80::2a0:deff:fe11:2233%vlan1 を設定する。

```
SWP2(config)#ntpdate server ipv6 fe80::2a0:deff:fe11:2233%vlan1
```

NTP サーバーに ntp.example.com を設定する。

```
SWP2(config)#ntpdate server name ntp.example.com
```

4.8.7 NTP サーバーによる時刻同期(1 ショット更新)

[書式]

ntpdate oneshot

[入力モード]

特権 EXEC モード

[説明]

登録されている NTP サーバーから時刻情報の取得を試みる。

本コマンド実行時に 1 度だけ行う。

[設定例]

NTP サーバーから時刻情報を取得する。

```
SWP2#ntpdate oneshot
```

4.8.8 NTP サーバーによる時刻同期(周期更新設定)

[書式]

ntpdate interval *interval-time*
no ntpdate interval

[パラメーター]

interval-time : <0-24>
時刻合わせの周期(時間)。0 時間を指定した場合は、周期更新を行わない

[初期設定]

ntpdate interval 1

[入力モード]

グローバルコンフィグレーションモード

[説明]

登録されている NTP サーバーから周期的に時刻情報を取得する間隔を 1 時間単位で設定する。

no 形式で実行すると、初期設定に戻る。

本コマンド実行時、即座に時刻の更新を行い、以降、設定した周期で更新を行う。

[設定例]

時刻の問い合わせを 2 時間おきに行う。

```
SWP2(config)#ntpdate interval 2
```

時刻の周期更新を行わないようにする。

```
SWP2(config)#ntpdate interval 0
```

4.8.9 NTP サーバーによる時刻同期設定情報の表示

[書式]

show ntpdate

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

NTP サーバーによる時刻同期に関する設定情報を表示する。

[設定例]

時刻同期設定情報を表示する。※更新周期 1 時間の場合

```
SWP2#show ntpdate
NTP Server 1 : ntp.nict.jp
```

```
NTP Server 2 : none
adjust time : Thu Jan 1 09:00:00 2015 + interval 1 hour
sync server : ntp.nict.jp
```

時刻同期設定情報を表示する。※周期更新なしの場合

```
SWP2#show ntpdate
NTP Server 1 : ntp.nict.jp
NTP Server 2 : none
adjust time : Thu Jan 1 09:00:00 2015
sync server : ntp.nict.jp
```

4.9 端末設定

4.9.1 ラインモード(コンソールターミナル)への移行

[書式]

line con *port*

[パラメーター]

port : 0

シリアルコンソールポート番号

[初期設定]

line con 0

[入力モード]

グローバルコンフィグレーションモード

[説明]

コンソールターミナルの設定を行うためのラインモードに移行する。

[ノート]

ラインモードからグローバルコンフィグレーションモードに戻るには **exit** コマンドを使用し、特権 EXEC モードに戻るには **end** コマンドを使用する。

[設定例]

コンソールターミナルを設定するためのラインモードに移行する。

```
SWP2(config)#line con 0
SWP2(config-line)#
```

4.9.2 VTY ポートの設定およびラインモード(VTY ポート)への移行

[書式]

line vty *port1* [*port2*]
no line vty *port1* [*port2*]

[パラメーター]

port1 : <0-7>

VTY ポート番号

port2 : <0-7>

範囲指定時の最終 VTY ポート番号

[初期設定]

no line vty 0 7

[入力モード]

グローバルコンフィグレーションモード

[説明]

指定した VTY ポートを有効にしたのち、VTY ポートの設定を行うためのラインモードに移行する。

no 形式で実行した場合は、指定した VTY ポートを無効にする。

port2 を指定した場合は、範囲指定となり、*port1* から *port2* までのすべての VTY ポートを指定したことになる。*port2* は *port1* 以上の番号にしなければならない。

[ノート]

TELNET クライアントの最大同時接続数は、有効な VTY ポートの数に依存する。

ラインモードからグローバルコンフィグレーションモードに戻るには **exit** コマンドを使用し、特権 EXEC モードに戻るには **end** コマンドを使用する。

[設定例]

VTY ポート #0 を有効にしたのち、ラインモードに移行する。

```
SWP2(config)#line vty 0
SWP2(config-line)#
```

4.9.3 端末ログインタイムアウト時間の設定

[書式]

exec-timeout *min* [*sec*]

no exec-timeout

[パラメーター]

min	:	<0-35791>
		タイムアウト時間(分)
sec	:	<0-2147483>
		タイムアウト時間(秒)

[初期設定]

exec-timeout 10

[入力モード]

ラインモード

[説明]

コンソールターミナルおよび VTY で、キー入力がない場合に自動的にログアウト するまでの時間を設定する。

sec を省略した場合は、0 が設定される。 *min*、*sec* ともに 0 に設定した場合は、 自動的にログアウトしない。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンド設定後、次のログイン時から設定が適用される。

[設定例]

コンソールのタイムアウト時間を 5 分に設定する。

```
SWP2(config)#line con 0
SWP2(config-line)#exec-timeout 5 0
SWP2(config-line)#
```

4.9.4 使用している端末 1 ページあたりの表示行数の変更

[書式]

terminal length *line*

terminal no length

[パラメーター]

line	:	<0-512>
		端末 1 ページあたりの表示行数

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

使用している端末 1 ページあたりの表示行数を変更する。

line に 0 を指定した場合、ページ単位で表示を一時停止しない。

terminal no length コマンドを実行した場合は、 表示行数がシリアルコンソールの場合は 24、VTY の場合は接続時の ウィンドウサイズとなる。

[ノート]

本コマンドは、実行後、即座に変更が反映される。

service terminal-length コマンドの設定より、 本コマンドの実行結果の方が優先して適用される。

[設定例]

使用している端末 1 ページあたりの表示行数を 100 行に変更する。

```
SWP2>terminal length 100
SWP2>
```

4.9.5 端末 1 ページあたりの表示行数の設定

[書式]

service terminal-length *line*
no service terminal-length

[パラメーター]

line : <0-512>
端末 1 ページあたりの表示行数

[初期設定]

no service terminal-length

[入力モード]

グローバルコンフィグレーションモード

[説明]

端末 1 ページあたりの表示行数を設定する。

line を 0 に設定した場合、ページ単位で表示を一時停止しない。

no 形式で実行した場合は、表示行数がシリアルコンソールの場合は 24、 VTY の場合は接続時のウィンドウサイズとなる。

[ノート]

本コマンド設定後、次のログイン時から設定が適用される。

terminal length コマンドが実行された場合、 **terminal length** コマンドの実行結果の方が 優先して適用される。

[設定例]

端末 1 ページあたりの表示行数を 100 行に設定する。

```
SWP2(config)#service terminal-length 100
SWP2(config)#
```

4.10 保守

4.10.1 保守 VLAN の設定

[書式]

management interface *interface*
no management interface

[パラメーター]

interface : VLAN インターフェース名

[初期設定]

management interface vlan1

[入力モード]

グローバルコンフィグレーションモード

[説明]

保守で利用する VLAN を設定する。

本コマンドを設定することで、L2MS エージェントで動作するとき、L2MS マネージャーから該当 VLAN に割り当てられた IP アドレスを設定・取得できる。

no 形式で実行した場合、もしくは VLAN を削除した場合、本コマンドも初期設定に戻る。

[設定例]

保守 VLAN を VLAN #2 に設定する。

```
SWP2(config)#management interface vlan2
```

4.11 SYSLOG

4.11.1 ログの通知先(SYSLOG サーバー)の設定

[書式]

logging host *host*
no logging host *host*

[パラメーター]

host : A.B.C.D

SYSLOG サーバーの IPv4 アドレス

: X:X::X:X

SYSLOG サーバーの IPv6 アドレス

IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)

[初期設定]

no logging host

[入力モード]

グローバルコンフィグレーションモード

[説明]

ログの通知先である SYSLOG サーバーの IP アドレスを設定する。

最大エントリー数は 2 である。

no 形式で実行した場合は初期設定に戻り、通知は行わない。

[設定例]

SYSLOG サーバーの IPv4 アドレスを、192.168.100.1 に設定する。

```
SWP2(config)#logging host 192.168.100.1
```

SYSLOG サーバーの IPv6 アドレスを、fe80::2a0:deff:fe11:2233 に設定する。

```
SWP2(config)#logging host fe80::2a0:deff:fe11:2233%vlan1
```

4.11.2 ログの通知フォーマットの設定

[書式]

logging format *type*
no logging format

[パラメーター]

type : ログのフォーマット種別

設定値	説明
legacy	ヘッダー部（タイムスタンプ、ホスト名）を含めない独自フォーマット

[初期設定]

no logging format

[入力モード]

グローバルコンフィグレーションモード

[説明]

SYSLOG サーバーへ通知するメッセージのフォーマットを変更する。

no 形式で実行した場合は SYSLOG メッセージにヘッダー部（タイムスタンプ、ホスト名）を含める。

[設定例]

SYSLOG メッセージのフォーマットをヘッダーなしに設定する。

```
SWP2(config)#logging format legacy
```

4.11.3 ログのファシリティ値の設定

[書式]

logging facility *facility*
no logging facility

[パラメーター]

facility : ログのファシリティ値

設定値	説明
0..23	facility 値
user	1
local0..local7	16..23

[初期設定]

logging facility local0

[入力モード]

グローバルコンフィグレーションモード

[説明]

SYSLOG サーバーへ通知するメッセージのファシリティ値を変更する。

[ノート]

ファシリティ値の意味づけは、各 SYSLOG サーバーで独自に行う。

[設定例]

SYSLOG メッセージのファシリティ値を 10 に設定する。

```
SWP2(config)#logging facility 10
```

4.11.4 ログの出力レベル(debug)の設定

[書式]

logging trap debug
no logging trap debug

[初期設定]

no logging trap debug

[入力モード]

グローバルコンフィグレーションモード

[説明]

debug レベルのログを SYSLOG に出力する。no 形式で実行した場合は出力しない。

debug レベルを有効にすると大量のログが出力されるため、必要な場合のみ有効にする。

logging host コマンドで SYSYLOG サーバーに通知する場合、ホスト側には十分なディスク領域を確保しておくことが望ましい。デフォルト設定は出力しない。

[設定例]

debug レベルのログを SYSLOG に出力する。

```
SWP2(config)#logging trap debug
```

4.11.5 ログの出力レベル(informational)の設定

[書式]

logging trap informational
no logging trap informational

[初期設定]

logging trap informational

[入力モード]

グローバルコンフィグレーションモード

[説明]

informational レベルのログを SYSLOG に出力する。

no 形式で実行した場合は出力しない。

[ノート]

logging stdout info コマンドでコンソールに出力させることが可能である。

[設定例]

informational レベルのログを SYSLOG に出力する。

```
SWP2(config)#logging trap informational
```

4.11.6 ログの出力レベル(error)の設定

[書式]

logging trap error
no logging trap error

[初期設定]

logging trap error

[入力モード]

グローバルコンフィグレーションモード

[説明]

error レベルのログを SYSLOG に出力する。

no 形式で実行した場合は出力しない。

[設定例]

error レベルのログを SYSLOG に出力する。

```
SWP2(config)#logging trap error
```

4.11.7 ログのコンソール出力設定

[書式]

logging stdout info
no logging stdout info

[初期設定]

no logging stdout info

[入力モード]

グローバルコンフィグレーションモード

[説明]

informational レベルの SYSLOG をコンソールに出力する。

no 形式で実行した場合は出力しない。

[設定例]

informational レベルの SYSLOG をコンソールに出力する。

```
SWP2(config)#logging stdout info
```

4.11.8 ログのバックアップ

[書式]

save logging

[入力モード]

非特権 EXEC モード, 特権 EXEC モード

[説明]

RAM 上に蓄積されたログを全て Flash ROM に保存する。

ログの蓄積は RAM 上で行われ、定期的に自動で Flash ROM にバックアップしているが、本コマンドにより、手動でバックアップすることができる。

[設定例]

ログのバックアップを行う。

```
SWP2#save logging
```

4.11.9 ログの削除

[書式]

clear logging

[入力モード]

特権 EXEC モード

[説明]

ログを削除する。

[設定例]

ログを削除する。

```
SWP2#clear logging
```

4.11.10 ログの参照

[書式]

show logging [reverse]

[キーワード]

reverse	:	ログを逆順に表示する

[入力モード]

非特権 EXEC モード, 特権 EXEC モード

[説明]

本機器の動作状況を記録したログを表示する。通常は発生時刻の古いものからログを順に表示するが、reverse が指定された場合は逆順に表示する。

ログの最大保持件数は 10,000 件である。最大数を越えた場合には、発生時刻の古いものから消去されていく。最大数以上のログを保存する場合には、**logging host** コマンドでログを SYSLOG サーバーに転送して、ホスト側で保存する必要がある。

出力するログのレベルは **logging trap** コマンドで設定可能である。

[ノート]

ログの蓄積は RAM 上で行われ、定期的に自動で Flash ROM にバックアップしている。電源を切るとバックアップされていないログは保存されないので、ログを保存したい場合は手動でバックアップする必要がある。

reload コマンドやファームウェアのバージョンアップなどによる再起動を行った場合は、ログを保持している。

[設定例]

ログを表示する。

```
SWP2#show logging
```

4.12 SNMP

4.12.1 SNMP 通知メッセージの送信先ホストの設定

[書式]

snmp-server host *host_address type* **version** *version community*
snmp-server host *host_address type* **version** *version seclevel user*
no snmp-server host *host_address*
no snmp-server host *host_address type* **version** *version community*
no snmp-server host *host_address type* **version** *version seclevel user*

[パラメーター]

host_address : 通知メッセージの送信先 IPv4 または IPv6 アドレス

IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)

type : 通知メッセージ

設定値	説明
traps	通知メッセージをトラップ形式(応答確認なし)で送信する
informs	通知メッセージを inform リクエスト形式(応答確認あり)で送信する。*version* が'2c'または'3'のとき指定できる

version : SNMP バージョン

設定値	説明
1	SNMPv1 を使用
2c	SNMPv2c を使用
3	SNMPv3 を使用

community : コミュニティー名(32 文字以内)

version が'1'または'2c'のとき指定できる
両端が、"" または " で囲まれていたとき、両端の ""、" は文字数に含まれない

seclevel : 通知メッセージの認証において求められるセキュリティーレベル

version が'3'のときのみ指定できる

設定値	説明
noauth	認証なし・暗号化なし(noAuthNoPriv)
auth	認証あり・暗号化なし(authNoPriv)
priv	認証あり・暗号化あり(authPriv)

user : ユーザー名(32 文字以内)

version が'3'のときのみ指定できる

両端が、"" または " で囲まれていたとき、両端の ""、" は文字数に含まれない

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

SNMP 通知メッセージの送信先を設定する。

最大エントリー数は 8 である。

no 形式で実行した場合は、指定送信先ホストの設定を削除する。

[ノート]

IPv6 リンクローカルアドレスで設定している場合、同一アドレスに対し異なる送出インターフェースを指定した設定を追加すると、 アドレスと送出インターフェースの組み合わせが変更されたとみなし、古い組み合わせの設定がすべて削除されるので注意すること。 例えば、"fe80::10%vlan1" を指定した設定が複数ある場合に、新たに "fe80::10%vlan2" の設定を追加すると、"fe80::10%vlan1" の設定はすべて削除され、 追加した "fe80::10%vlan2" の設定のみが残ることになる。

[設定例]

SNMPv1 を使用し、トラップの送信先を 192.168.100.11 に設定する。トラップのコミュニティー名を snmptrapname に指定する。

```
SWP2(config)#snmp-server host 192.168.100.11 traps version 1 snmptrapname
```

SNMPv2c を使用し、通知メッセージの送信先を 192.168.100.12 に設定する。通知タイプを informs、通知先のコミュニティー名を snmpinformsname に指定する。

```
SWP2(config)#snmp-server host 192.168.100.12 informs version 2c snmpinformsname
```

SNMPv3 を使用し、通知メッセージの送信先を 192.168.10.13 に設定する。通知タイプを traps、送信する時のセキュリティーレベルを priv に、ユーザー名を admin1 に指定する。

```
SWP2(config)#snmp-server host 192.168.10.13 traps version 3 priv admin1
```

4.12.2 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

[書式]

snmp-server startup-trap-delay *sec*
no snmp-server startup-trap-delay

[パラメーター]

sec : <10-600>

待機時間(秒)

[初期設定]

snmp-server startup-trap-delay 10

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム起動時に、SNMP 通知メッセージ（トラップ）を送信するまでの待機時間を設定する。

システム起動後、待機時間が経過するまでに生成された SNMP 通知メッセージは、待機時間経過後に送信される。

no 形式で実行した場合は、設定を削除する。

[ノート]

待機時間の計測開始、終了は、以下のログが出力されたタイミング。

```
[    SNMP]:dbg: SNMP startup trap delay timer start (delay_sec : XX)
[    SNMP]:dbg: SNMP startup trap delay timer end (delay_sec : XX)
```

[設定例]

システム起動時に、SNMP 通知メッセージを送信するまでの待機時間を 30 秒に設定する。

```
SWP2(config)#snmp-server startup-trap-delay 30
```

4.12.3 送信する通知メッセージタイプの設定

[書式]

snmp-server enable trap *trap_type* [*trap_type*]

no snmp-server enable trap

[パラメーター]

trap_type : トラップの種類

設定値	説明
coldstart	電源 OFF/ON、ファームウェア更新時
warmstart	reload コマンド実行時
linkdown	リンクダウン時
linkup	リンクアップ時
authentication	認証失敗時
l2ms	L2MS のエージェント検出／喪失時
errdisable	ErrorDisable 検出／解除時
rmon	RMON イベント実行時
termmonitor	端末監視検知時
bridge	スパニングツリー ルート検出／トポロジー変更時
loopdetect	ループ検出/解消時
all	すべてのトラップ種類。コンフィグ上では、上記すべてのトラップ種類が設定される。

[初期設定]

no snmp-server enable trap

[入力モード]

グローバルコンフィグレーションモード

[説明]

送信するトラップの通知タイプを指定する。

no 形式で実行した場合は、トラップを無効にする。

[設定例]

coldstart トラップを有効にする。

```
SWP2(config)#snmp-server enable trap coldstart
```

トラップを無効にする。

```
SWP2(config)#no snmp-server enable trap
```

4.12.4 システムコンタクトの設定

[書式]

snmp-server contact *contact*
no snmp-server contact

[パラメーター]

contact : システムコンタクトとして登録する名称(255 文字以内)

[初期設定]

no snmp-server contact

[入力モード]

グローバルコンフィグレーションモード

[説明]

MIB 変数 sysContact を設定する。
sysContact は一般的に、管理者の名前や連絡先を記入しておく変数である。
no 形式で実行した場合は、設定を削除する。

[設定例]

システムコンタクトを swx_admin@sample.com に設定する。

```
SWP2(config)#snmp-server contact swx_admin@sample.com
```

4.12.5 システムロケーションの設定

[書式]

snmp-server location *location*
no snmp-server location

[パラメーター]

location : システムロケーションとして登録する名称(255 文字以内)

[初期設定]

no snmp-server location

[入力モード]

グローバルコンフィグレーションモード

[説明]

MIB 変数 sysLocation を設定する。
sysLocation は一般的に、機器の設置場所を記入しておく変数である。
no 形式で実行した場合は、設定を削除する。

[設定例]

システムロケーションを MainOffice-1F に設定する。

```
SWP2(config)#snmp-server location MainOffice-1F
```

4.12.6 SNMP コミュニティーの設定

[書式]

snmp-server community *community ro_rw*
no snmp-server community *community*

[パラメーター]

community : コミュニティー名(32 文字以内)

両端が、"" または " で囲まれていたとき、両端の ""、" は文字数に含まれない

ro_rw : アクセス制限

設定値	説明
ro	読み出し専用
rw	書き込み可能

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

SNMP コミュニティーを設定する。
登録できるコミュニティーの最大数は 16 である。
no 形式で実行した場合、指定コミュニティーを削除する。

[設定例]

読み出し専用のコミュニティー名 public を設定する。

```
SWP2(config)#snmp-server community public ro
```

public コミュニティーを削除する。

```
SWP2(config)#no snmp-server community public
```

4.12.7 SNMP ビューの設定

[書式]

snmp-server view *view oid type*
no snmp-server view *view*

[パラメーター]

view : ビュー名(32 文字以内)

oid : MIB オブジェクト ID

type : タイプ

設定値	説明
include	指定したオブジェクト ID を管理対象にする
exclude	指定したオブジェクト ID を管理対象から除外する

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

SNMP MIB ビューを設定する。

MIB ビューとは、アクセス権を許可する際に指定する MIB オブジェクトの集合である。

登録できる MIB ビューの最大数は 16 である。

oid パラメーターと *type* パラメーターの組は、指定のオブジェクト ID 以降の MIB サブツリーを管理対象とする／しないことを意味する。*oid* パラメーターと *type* パラメーターの組を 1 つのエントリーとして、各々の MIB ビューに対して複数のエントリーを指定することができ、その最大数は 8 である。

複数のエントリーを指定した際に、それぞれ指定したオブジェクト ID の中で包含関係にあるものは、より下位の階層まで指定したオブジェクト ID に対応する *type* パラメーターが優先される。

no 形式でコマンドを実行した場合は、MIB ビューを削除する。エントリー単位の削除はできない。

[設定例]

internet ノード(1.3.6.1)以下を表す most ビューを設定する。

```
SWP2(config)#snmp-server view most 1.3.6.1 include
```

mib-2 ノード(1.3.6.1.2.1)以下を表す standard ビューを設定する。

```
SWP2(config)#snmp-server view standard 1.3.6.1.2.1 include
```

4.12.8 SNMP グループの設定

[書式]

snmp-server group *group seclevel* read *read_view* [write *write_view*]
snmp-server group *group seclevel* write *write_view* [read *read_view*]
no snmp-server group *group*

[キーワード]

read	:	本グループに所属するユーザーが読み出し可能な MIB ビューを指定する
write	:	本グループに所属するユーザーが書き込み可能な MIB ビューを指定する

[パラメーター]

group : グループ名(32 文字以内)

seclevel : 本グループに所属するユーザーに求められるセキュリティーレベル

設定値	説明
noauth	認証なし・暗号化なし(noAuthNoPriv)
auth	認証あり・暗号化なし(authNoPriv)
priv	認証あり・暗号化あり(authPriv)

read_view : 本グループに所属するユーザーが読み出し可能な MIB ビューの名前(32 文字以内)

write_view : 本グループに所属するユーザーが書き込み可能な MIB ビューの名前(32 文字以内)

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

ユーザーグループを設定する。

このコマンドで設定される MIB ビューに含まれない MIB オブジェクトへのアクセスは禁止される。

MIB ビューは **snmp-server view** コマンドによって定義される。

最大エントリー数は 16 である。

no 形式でコマンドを実行した場合は、指定グループの設定を削除する。

[設定例]

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は most ビューへのフルアクセス権を与える。

```
SWP2(config)#snmp-server group admins priv read most write most
```

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は standard ビューへの読み出しアクセス権を与える。

```
SWP2(config)#snmp-server group users auth read standard
```

4.12.9 SNMP ユーザーの設定

[書式]

snmp-server user *user group* [auth *auth auth_pass* [priv *priv priv_pass*]]

no snmp-server user *user*

[キーワード]

auth : 認証アルゴリズムを設定する

priv : 暗号化アルゴリズムを設定する

[パラメーター]

user : ユーザー名(32 文字以内)

両端が、"" または " で囲まれていたとき、両端の ""、" は文字数に含まれない

group : グループ名(32 文字以内)

両端が、"" または " で囲まれていたとき、両端の ""、" は文字数に含まれない

auth : 認証アルゴリズム

設定値	説明
md5	HMAC-MD5-96
sha	HMAC-SHA-96

auth_pass : 認証パスワード(8 文字以上、32 文字以内)

両端が、"" または " で囲まれていたとき、両端の ""、" は文字数に含まれない

priv : 暗号化アルゴリズム

設定値	説明
des	DES-CBC
aes	AES128-CFB

priv_pass : 暗号パスワード(8 文字以上、32 文字以内)

両端が、"" または " で囲まれていたとき、両端の ""、" は文字数に含まれない

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

ユーザーを設定する。

本コマンドのグループ名は **snmp-server group** コマンドで定義した名前を指定し、グループ設定で指定したセキュリティーレベルに応じて、通信内容の認証と暗号化で使用するアルゴリズムとパスワードを設定する。

なお、認証を行わず暗号化のみを行うことはできない。

最大エントリー数は 16 である。

認証や暗号化の有無、アルゴリズムおよびパスワードは、対向となる SNMP マネージャー側のユーザー設定と一致させておく必要がある。

no 形式でコマンドを実行した場合は、指定ユーザーの設定を削除する。

[設定例]

ユーザーとして admin1 を作成する。所属グループの指定と所属グループで定められたセキュリティーレベルに合わせて、認証・暗号化で使用するプロトコル(SHA, AES)とパスワード(passwd1234)を指定する。

```
SWP2(config)#snmp-server user admin1 admins auth sha passwd1234 priv aes passwd1234
```

ユーザーとして user1 を作成する。所属グループの指定と所属グループで定められたセキュリティーレベルに合わせて、認証・暗号化で使用するプロトコル(SHA)とパスワード(passwd5678)を指定する。

```
SWP2(config)#snmp-server user user1 users auth sha passwd5678
```

4.12.10 SNMP サーバーへアクセスできるクライアントの IP アドレス制限

[書式]

snmp-server access *action info* [community *community*]
no snmp-server access [*action info* [community *community*]]

[キーワード]

community : コミュニティーを指定する

[パラメーター]

action : アクセス条件に対する動作を指定する

設定値	説明
permit	条件を"許可"する

info : 条件とする送信元 IPv4/IPv6 アドレス情報を設定する

設定値	説明
A.B.C.D	IPv4 アドレス(A.B.C.D)を指定する
A.B.C.D/M	サブネットマスク長(Mbit)付きの IPv4 アドレス(A.B.C.D)を指定する
X:X::X:X	IPv6 アドレス(X:X::X:X)を指定する
X:X::X:X/M	サブネットマスク長(Mbit)付きの IPv6 アドレス(X:X::X:X)を指定する
any	すべての IPv4/IPv6 アドレスを指定する

community : コミュニティー名(32 文字以内)

アクセス条件を適用するコミュニティー

コミュニティーの指定を省略した場合、アクセス条件はすべてのコミュニティーに対して適用される

両端が、""または"で囲まれていたとき、両端の""、"は文字数に含まれない。

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

SNMP サーバーへのアクセスを許可するクライアント端末を IPv4/IPv6 アドレスで制限する。

本コマンドは最大 32 件まで設定が可能であり、先に設定されたものが優先して適用される。

本コマンドを設定した場合、登録した条件を満たさないアクセスはすべて拒否する。

ただし、本コマンドを設定していない場合は、すべてのアクセスを許可する。

no 形式で実行した場合は、指定した設定を削除する。

no 形式で community を省略した場合、指定した info のすべての設定を削除する。

no 形式ですべてのパラメーターを省略した場合、すべての設定を削除する。

[ノート]

本コマンドでのアクセスの制限は、SNMPv1, SNMPv2c のアクセスのみ適用される。

SNMPv3 のアクセスには適用されない。

[設定例]

SNMP サーバーへのアクセスを 192.168.100.0/24 のセグメントからのみ許可する。

```
SWP2(config)#snmp-server access permit 192.168.100.0/24
```

コミュニティー名'public'でアクセス可能なホストを 192.168.100.0/24 のみに、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 のみに制限する。

```
SWP2(config)#snmp-server access permit 192.168.100.0/24 community public
SWP2(config)#snmp-server access permit 192.168.100.12 community private
```

4.12.11 SNMP コミュニティーの情報の表示

[書式]

show snmp community

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

SNMP コミュニティーの情報を表示する。

コミュニティー名、アクセスモードを表示する。

[設定例]

SNMP コミュニティーの情報を表示する。

```
SWP2#show snmp community
SNMP Community information
  Community Name: public
  Access: Read-Only


  Community Name: private
  Access: Read-Write
```

4.12.12 SNMP ビューの設定内容の表示

[書式]

show snmp view

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

SNMP ビューの設定内容を表示する。

ビュー名、オブジェクト ID、タイプを表示する。

[設定例]

SNMP ビューの設定内容を表示する。

```
SWP2#show snmp view
SNMP View information
  View Name: most
  OID: 1.6.1
  Type: include
```

```
  View Name: standard
  OID: 1.3.6.1.2.1
  Type: include
```

4.12.13 SNMP グループの設定内容の表示

[書式]

show snmp group

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

SNMP グループの設定内容を表示する。

グループ名、セキュリティーレベル、読み込み用ビュー、書き込み用ビューを表示する。

[設定例]

SNMP グループの設定内容を表示する。

```
SWP2#show snmp group
SNMP Group information
  Group Name: admins
  Security Level: priv
  Read View: most
  Write View: most

  Group Name: users
  Security Level: auth
  Read View: standard
  Write View: standard
```

4.12.14 SNMP ユーザーの設定内容の表示

[書式]

show snmp user

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

SNMP ユーザーの設定内容を表示する。

エンジン ID、ユーザー名、所属するグループ名、認証方式、暗号化方式を表示する。

[設定例]

SNMP ユーザーの設定内容を表示する。

```
SWP2#show snmp user
SNMP User information
  EngineID: 0x8000049e0300a0deaeb90e

  User Name: admin1
  Group Name: admins
  Auth: sha
  Priv: aes

  User Name: user1
  Group Name: users
  Auth: sha
  Priv: none
```

4.13 RMON

4.13.1 RMON 機能の設定

[書式]

rmon *switch*

no rmon

[パラメーター]

switch : RMON 機能の動作

設定値	説明
enable	RMON 機能を有効にする
disable	RMON 機能を無効にする

[初期設定]

rmon enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体の RMON 機能の動作を設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドでシステム全体の RMON 機能が無効とした場合、以下の RMON グループの動作が無効となる。

- 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

本コマンドは、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が可能。

[設定例]

RMON 機能を有効にする。

```
SWP2(config)#rmon enable
```

RMON 機能を無効にする。

```
SWP2(config)#rmon disable
```

4.13.2 RMON イーサネット統計情報グループの設定

[書式]

rmon statistics *index* [owner *owner*]

no rmon statistics *index*

[パラメーター]

index : <1 - 65535>

イーサネット統計情報グループのインデックス(etherStatsIndex)

owner : イーサネット統計情報グループのオーナー名(etherStatsOwner)

127 文字以内

(省略した場合 : RMON_SNMP)

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースで、RMON のイーサネット統計情報グループの設定を有効にする。

本コマンドを設定した場合、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る。

同一インターフェースに対する、本コマンドの設定数の上限は 8 である。

no 形式で実行した場合は、設定と収集した統計情報を削除する。

[ノート]

RMON 機能でイーサネット統計情報グループの設定を有効にするためには、本コマンドに加えて、システム全体でも RMON 機能を有効にする必要がある。

本コマンドを上書きした場合、これまで収集した統計情報を削除したうえで、再度収集を開始する。

システム全体の RMON 機能を無効にした場合、統計情報の収集が中断される。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、再度収集を開始する。

[設定例]

port1.1 で RMON のイーサネット統計情報グループの設定を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#rmon statistics 1
```

4.13.3 RMON 履歴グループの設定

[書式]

rmon history *index* [buckets *buckets*] [interval *interval*] [owner *owner*]
no rmon history *index*

[パラメーター]

index	:	<1 - 65535>
		履歴グループのインデックス(historyControlIndex)
buckets	:	<1 - 65535>
		履歴グループの履歴保持数(historyControlBucketsRequested)
		(省略した場合 : 50)
interval	:	<1 - 3600>
		履歴グループの履歴保存間隔(秒)(historyControlInterval)
		(省略した場合 : 1800)
owner	:	履歴グループのオーナー名(historyControlOwner)
		127 文字以内
		(省略した場合 : RMON_SNMP)

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースで、RMON の履歴グループの設定を有効にする。

本コマンドを設定した場合、RMON MIB の historyControlTable が取得できるようになる。本コマンド設定後、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る。

同一インターフェースに対する、本コマンドの設定数の上限は 8 である。

no 形式で実行した場合は、設定と収集した履歴情報を削除する。

[ノート]

RMON 機能で履歴グループの設定を有効にするためには、本コマンドに加えて、システム全体でも RMON 機能を有効にする必要がある。

本コマンドを上書きした場合、これまで収集した履歴情報を削除したうえで、再度収集を開始する。

システム全体の RMON 機能を無効にした場合、履歴情報の収集が中断される。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、再度収集を開始する。

[設定例]

port1.1 で RMON の履歴グループの設定を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#rmon history 1
```

4.13.4 RMON イベントグループの設定

[書式]

rmon event *index type community* [description *description*] [owner *owner*]
no rmon event *index*

[パラメーター]

index : <1 - 65535>
イベントグループのインデックス(eventIndex)

type : イベント種別(eventType)

設定値	説明
log	ログに記録する
trap	SNMP トラップを送信
log-trap	ログに記録し、SNMP トラップを送信

community : コミュニティー名(eventCommunity)
127 文字以内
type が"trap"または"log-trap"のとき指定できる

description : イベントの説明(eventDescription)
127 文字以内
(省略した場合 : RMON_SNMP)

owner : イベントグループのオーナー名(eventOwner)
127 文字以内
(省略した場合 : RMON_SNMP)

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

RMON のイベントグループの設定を有効にする。

本コマンドを設定した場合、RMON MIB の eventTable が取得できるようになる。本コマンドのイベントグループの設定は、**rmon alarm** コマンドで使用する。

no 形式で実行した場合は、設定値を削除する。

[ノート]

RMON 機能でイベントグループの設定を有効にするためには、本コマンドに加えて、システム全体でも RMON 機能を有効にする必要がある。

RMON の SNMP トラップを送信する場合、SNMP のトラップ送信の設定が行われている必要がある。

[設定例]

SNMP トラップの設定を行ってから、RMON のイベントグループの設定を有効にする。イベント種別は"log-trap"、トラップのコミュニティ名は「public」とする。

```
SWP2(config)#snmp-server host 192.168.100.3 traps version 2c public
SWP2(config)#snmp-server enable trap rmon
SWP2(config)#rmon event 1 log-trap public
```

4.13.5 RMON アラームグループの設定

[書式]

rmon alarm *index variable* interval *interval* [*type*] rising-threshold *rising_threshold* event *rising_event-index* falling-threshold *falling_threshold* event *falling_event_index* [alarmstartup *startup*] [owner *owner*]

rmon alarm *index variable* interval *interval* [*type*] rising-threshold *rising_threshold* event *rising_event-index* [owner *owner*]

rmon alarm *index variable* interval *interval* [*type*] falling-threshold *falling_threshold* event *falling_event_index* [owner *owner*]

no rmon alarm *index*

[パラメーター]

index : <1-65535>

アラームグループのインデックス(alarmIndex)

variable : 監視対象 MIB オブジェクト(alarmVariable)

interval : <1-2147483647>

サンプリング間隔(秒)(alarmInterval)

type : サンプリング種別(alarmSampleType)

設定値	説明
absolute	絶対値による比較。サンプル値としきい値を直接比較する
delta	相対値による比較。最新サンプル値と前回サンプル値の差をしきい値と比較する

(省略した場合 : absolute)

rising_threshold : <1-2147483647>

上限しきい値(alarmRisingThreshold)

rising_event_index : <1-65535>

イベントインデックス(alarmRisingEventIndex)

falling_threshold : <1-2147483647>

下限しきい値(alarmFallingThreshold)

falling_event_index : <1-65535>

イベントインデックス(alarmFallingEventIndex)

startup : <1-3>

アラームの最初の判定で使用するしきい値(alarmStartupAlarm)

設定値	説明
1	上限しきい値のみ使用する(risingAlarm)
2	下限しきい値のみ使用する(fallingAlarm)
3	上限しきい値、下限しきい値の両方を使用する(risingOrFallingAlarm)

(省略した場合 : 3)

owner : アラームグループのオーナー名(alarmOwner)

127 文字以内

(省略した場合 : RMON_SNMP)

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

RMON のアラームグループの設定を有効にする。

variable には、RMON のアラームグループの監視対象 MIB オブジェクトを設定する。*variable* 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。以下の 3 つの形式で指定が可能。

- etherStatsEntry.X.Y
- (etherStatsEntry 下の OID 名).Y
- .1.3.6.1.2.1.16.1.1.1.X.Y

例えば、etherStatsPkts.1(.1.3.6.1.2.1.16.1.1.1.5.1)を設定する場合、以下のいずれの形式でも設定可能。

形式	説明
etherStatsEntry.X.Y	etherStatsEntry.5.1
(etherStatsEntry 下の OID 名).Y	etherStatsPkts.1
.1.3.6.1.2.1.16.1.1.1.X.Y	.1.3.6.1.2.1.16.1.1.1.5.1

rising_threshold または、*falling_threshold* のどちらかのみを設定する形式を使用可能。この場合、設定が省略されているパラメータには、以下の値が設定される。

- *rising_threshold* のみ使用
  - *falling_threshold* : *rising_threshold* と同じ値
  - *falling_event_index* : *rising_event_index* と同じ値
  - *startup* : 1(上限しきい値のみ使用する)
- *falling_threshold* のみ使用
  - *rising_threshold* : *falling_threshold* と同じ値
  - *rising_event_index* : *falling_event_index* と同じ値
  - *startup* : 2(下限しきい値のみ使用する)

本コマンドを設定した場合、RMON MIB の alarmTable が取得できるようになる。

no 形式で実行した場合は、設定値を削除する。

[ノート]

RMON 機能でアラームグループの設定を有効にするためには、本コマンドに加えて、システム全体でも RMON 機能を有効にする必要がある。

variable に指定する MIB オブジェクトは、イーサネット統計情報グループの MIB オブジェクトである。対象のインデックスを持つイーサネット統計情報グループが作成されていない場合、本コマンドはエラーとなる。

イーサネット統計情報グループは、**rmon statistics** コマンドにて作成可能。本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、本コマンドも削除される。

イベントのインデックスは、**rmon event** コマンドで設定したインデックスを指定する。本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、本コマンドも削除される。

rising_threshold のしきい値は、*falling_threshold* のしきい値以上の値でなければならない。

本コマンドを上書きした場合、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する。

システム全体の RMON 機能を無効にした場合、サンプリングが中断される。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する。

[設定例]

以下の条件で、RMON のアラームグループの設定を有効にする。

- 監視対象 MIB オブジェクトは、etherStatsPkts.1。
- サンプリング間隔は、180 秒。
- サンプリング種別は、delta。
- 上限しきい値は 3000、上限しきい値を上回ったときのイベントは 1。
- 下限しきい値は 2000、下限しきい値を下回ったときのイベントは 1。

```
SWP2(config)#rmon alarm 1 etherStatsPkts.1 interval 180 delta rising-threshold 3000
event 1 falling-threshold 2000 event 1
```

4.13.6 RMON 機能の状態表示

[書式]

show rmon

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

RMON 機能の設定や状態を表示する。

以下の項目が表示される。

- システム全体の RMON 機能の設定
- RMON 機能のグループごとの設定
  - 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

[設定例]

```
SWP2>show rmon
rmon: Enable

statistics:
    rmon collection index 1
    stats->ifindex = 5001
    input packets 7, bytes 600, drop events 0, multicast packets 4
    output packets 17, bytes 2091, multicast packets 17 broadcast packets 0

history:
    history index = 1
    data source ifindex = 5001
    buckets requested = 50
    buckets granted = 50
    Interval = 1800
    Owner RMON_SNMP

event:
    event Index = 1
       Description RMON_SNMP
       Event type Log
       Event community name RMON_SNMP
       Last Time Sent = 00:00:58
       Owner  RMON_SNMP

alarm:
    alarm Index = 1
      alarm status = VALID
        alarm Interval = 15
        alarm Type is Absolute
        alarm Value  = 0
        alarm Rising Threshold = 10
        alarm Rising Event = 1
        alarm Falling Threshold = 7
        alarm Falling Event = 1
        alarm Startup Alarm = 3
        alarm Owner is RMON_SNMP
```

4.13.7 RMON イーサネット統計情報グループの状態表示

[書式]

show rmon statistics

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

RMON イーサネット統計情報グループの設定や状態を表示する。

以下の項目が表示される。

- インデックス
- 対象インターフェース
- input パケット
- output パケット

[設定例]

```
SWP2>show rmon statistics
    rmon collection index 1
    stats->ifindex = 5001
    input packets 7, bytes 600, drop events 0, multicast packets 4
    output packets 17, bytes 2091, multicast packets 17 broadcast packets 0
```

4.13.8 RMON 履歴グループの状態表示

[書式]

show rmon history

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

RMON 履歴グループの設定や状態を表示する。

以下の項目が表示される。

- インデックス
- 対象インターフェース
- 履歴情報の保持数
- 履歴保存間隔
- オーナー名

[設定例]

```
SWP2>show rmon history
        history index = 1
        data source ifindex = 5001
        buckets requested = 50
        buckets granted = 50
        Interval = 1800
        Owner RMON_SNMP
```

4.13.9 RMON イベントグループの状態表示

[書式]

show rmon event

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

RMON イベントグループの設定や状態を表示する。

以下の項目が表示される。

- インデックス
- イベントの説明
- イベント種別
- トラップ送信時のコミュニティ名
- イベント実行時
- オーナー名

[設定例]

```
SWP2>show rmon event
    event Index = 1
       Description RMON_SNMP
```

```
       Event type Log
       Event community name RMON_SNMP
       Last Time Sent = 00:00:58
       Owner  RMON_SNMP
```

4.13.10 RMON アラームグループの状態表示

[書式]

show rmon alarm

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

RMON アラームグループの設定や状態を表示する。

以下の項目が表示される。

- インデックス
- アラームの状態
- 監視対象 MIB オブジェクト
- サンプリング間隔
- サンプリング種別
- 測定値
- 上限しきい値
- 上限しきい値のイベント
- 下限しきい値
- 下限しきい値のイベント
- 開始アラーム
- オーナー名

[設定例]

```
SWP2>show rmon alarm
      alarm Index = 1
        alarm status = VALID
          alarm Interval = 15
          alarm Type is Absolute
          alarm Value  = 0
          alarm Rising Threshold = 10
          alarm Rising Event = 1
          alarm Falling Threshold = 7
          alarm Falling Event = 1
          alarm Startup Alarm = 3
          alarm Owner is RMON_SNMP
```

4.13.11 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

[書式]

rmon clear counters

[入力モード]

インターフェースモード

[説明]

対象インターフェースの、RMON イーサネット統計情報グループのカウンターをクリアする。

[設定例]

port1.1 の RMON のイーサネット統計情報グループのカウンターをクリアする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#rmon clear counters
```

4.14 sFlow

4.14.1 sFlow 機能の設定

[書式]

sflow *switch*
no sflow

[パラメーター]

switch : sFlow 機能の動作

設定値	説明
enable	sFlow 機能を有効にする
disable	sFlow 機能を無効にする

[初期設定]

sflow disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

sFlow 機能の動作を設定する。
no 形式で実行した場合は初期設定に戻る。

[設定例]

sFlow 機能を有効にする。

```
SWP2(config)#sflow enable
```

4.14.2 sFlow エージェントの設定

[書式]

sflow agent *address*
no sflow agent

[パラメーター]

address : A.B.C.D
IPv4 アドレス
: X:X::X:X
IPv6 アドレス

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

sFlow エージェントの IP アドレスを設定する。
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る。
no 形式で実行した場合は初期設定に戻る。

[ノート]

スタック機能が有効な場合、IPv6 アドレスは指定できない。

[設定例]

sFlow エージェントの IP アドレスを「192.168.100.240」に設定する。

```
SWP2(config)#sflow agent 192.168.100.240
```

4.14.3 sFlow コレクターの設定

[書式]

sflow collector *address* [*port*]
no sflow collector

[パラメーター]

address	:	A.B.C.D
		IPv4 アドレス
	:	X:X::X:X
		IPv6 アドレス
port	:	<1 - 65535>
		sFlow コレクターの宛先 UDP ポート番号
		初期値は、6343

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

sFlow コレクターの IP アドレスと宛先 UDP ポート番号を設定する。
no 形式で実行した場合は初期設定に戻る。

[ノート]

スタック機能が有効な場合、IPv6 アドレスは指定できない。

[設定例]

sFlow コレクターの IP アドレスを「192.168.100.240」に設定する。

```
SWP2(config)#sflow collector 192.168.100.240
```

4.14.4 sFlow データグラムの最大サイズの設定

[書式]

sflow collector max-datagram-size *size*
no sflow collector max-datagram-size

[パラメーター]

size	:	<512 - 1452>(バイト)

[初期設定]

sflow collector max-datagram-size 1400

[入力モード]

グローバルコンフィグレーションモード

[説明]

sFlow エージェントから sFlow コレクターに送信されるデータグラムの最大サイズを設定する。
no 形式で実行した場合は初期設定に戻る。

[設定例]

sFlow データグラムの最大サイズを 1000 バイトに設定する。

```
SWP2(config)#sflow collector max-datagram-size 1000
```

4.14.5 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

[書式]

sflow sampling-rate *rate*
no sflow sampling-rate

[パラメーター]

rate : <256 - 1000000000>

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象ポートにて、パケットフローサンプリングを行う際の、サンプリングレートを設定する。
本コマンドが設定されていない場合は、パケットフローサンプリングは行われない。
LAN/SFP+ポートにだけ設定可能。
no 形式で実行した場合は初期設定に戻る。

[設定例]

パケットフローサンプリングのサンプリングレートを 10000 に設定する。

```
SWP2(config-if)#sflow sampling-rate 10000
```

4.14.6 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

[書式]

sflow max-header-size *size*
no sflow max-header-size

[パラメーター]

size : <14 - 256>(バイト)

[初期設定]

sflow max-header-size 128

[入力モード]

インターフェースモード

[説明]

対象ポートにて、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する。
no 形式で実行した場合は初期設定に戻る。
LAN/SFP+ポートにだけ設定可能。

[設定例]

パケットフローサンプリングの最大ヘッダーサイズを 100 に設定する。

```
SWP2(config-if)#sflow max-header-size 100
```

4.14.7 カウンターサンプリングのポーリング間隔の設定

[書式]

sflow polling-interval *interval*
no sflow polling-interval

[パラメーター]

interval : <1 - 86400>(秒)

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象ポートにて、カウンターサンプリングを行う際の、ポーリング間隔を設定する。

本コマンドが設定されていない場合は、カウンターサンプリングは行われない。

LAN/SFP+ポートにだけ設定可能。

no 形式で実行した場合は初期設定に戻る。

[設定例]

カウンターサンプリングのポーリング間隔を 100 秒 に設定する。

```
SWP2(config-if)#sflow polling-interval 100
```

4.14.8 sFlow の状態の表示

[書式]

show sflow

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

sFlow の状態を表示する。

[設定例]

sFlow の状態を表示する。

```
SWP2#show sflow
sFlow Global Configuration:
  sFlow Feature      : Enabled
  Agent Address      : 192.168.100.240
  Collector Address  : 192.168.100.2
  Collector UDP Port : 6343
  Max Datagram Size  : 1400(bytes)

sFlow Port Configuration:

            Sampling-Rate    Polling-Interval
  Port      (1 in N pkts)    (secs)
  ------------------------------------------------------------
  port1.1   300              30
  port1.5   500              (NOT SET)

sFlow Drop Sampling Count : 0
```

4.14.9 sFlow のサンプリング情報の表示

[書式]

show sflow sampling [*ifname*]

[パラメーター]

ifname : LAN/SFP+ポートのインターフェース名
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

ifname で指定したインターフェースの sFlow のサンプリング情報を表示する。

ifname を省略した場合は、全てのインターフェースの情報を表示する。

[ノート]

スタック機能が有効のとき、メインではないメンバースイッチで本コマンドは実行できない。

スタック機能が有効のとき、メイン、メンバー間で本情報は同期されない。

[設定例]

sFlow のサンプリング情報を表示する。

```
SWP2#show sflow sampling
sFlow sampling information:

  Interface port1.1:
    Packet-Flow-Sampling:
      Sampling count : 40
      Number of packets remaining until next sampling:
        Ingress : 208
        Egress  : 590
    Counter-Sampling:
      Sampling count : 65
      Number of seconds remaining until next sampling : 15

  Interface port1.5:
    Packet-Flow-Sampling:
      Sampling count : 15
      Number of packets remaining until next sampling:
        Ingress : 876
        Egress  : 870
    Counter-Sampling:
      (NOT SET)
```

4.15 TELNET サーバー

4.15.1 TELNET サーバーの起動および受付ポート番号の変更

[書式]

telnet-server enable [*port*]

telnet-server disable

no telnet-server

[キーワード]

enable	:	TELNET サーバーを有効にする
disable	:	TELNET サーバーを無効にする

[パラメーター]

port	:	<1-65535> TELNET サーバーのリスニングポート番号（省略した場合：23）

[初期設定]

telnet-server disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

TELNET サーバーを有効にする。また、リスニング TCP ポート番号を指定することができる。

no 形式で実行した場合は無効にする。

[設定例]

リスニングポート番号を 12345 にして TELNET サーバーを起動する。

```
SWP2(config)#telnet-server enable 12345
```

4.15.2 TELNET サーバーの設定状態の表示

[書式]

show telnet-server

[入力モード]

特権 EXEC モード

[説明]

TELNET サーバーの設定状況を表示する。以下の項目が表示される。

- TELNET サーバー機能の有効/無効
- リスニングポートの番号
- TELNET サーバーへのアクセスを許可する VLAN インターフェース
- TELNET サーバーへのアクセスを制限するフィルター

[設定例]

TELNET サーバーの設定状況を表示する。

```
SWP2#show telnet-server
Service:Enable
Port:23
Management interface(vlan): 1
Interface(vlan):1, 2, 3
Access:
    deny   192.168.100.5
    permit 192.168.100.0/24
```

4.15.3 TELNET サーバーへアクセスできるホストの設定

[書式]

telnet-server interface *interface*
no telnet-server interface *interface*

[パラメーター]

interface : VLAN インターフェース名

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

TELNET サーバーへのアクセスを許可する VLAN インターフェースを設定する。

no 形式で実行した場合は、指定したインターフェースを削除する。

本コマンドは最大 8 件まで設定でき、設定した順に適用する。

本コマンドを設定していない場合は、保守 VLAN のみアクセスできる。

[ノート]

telnet-server enable が設定されていない場合、本コマンドは機能しない。

[設定例]

VLAN #1、VLAN #2 に接続しているホストからの TELNET サーバーへのアクセスを許可する。

```
SWP2(config)#telnet-server interface vlan1
SWP2(config)#telnet-server interface vlan2
```

4.15.4 TELNET サーバーへアクセスできるクライアントの IP アドレス制限

[書式]

telnet-server access *action info*
no telnet-server access [*action info*]

[パラメーター]

action : アクセス条件に対する動作を指定する

設定値	説明
deny	条件を"拒否"する
permit	条件を"許可"する

info : 条件とする送信元 IPv4/IPv6 アドレス情報を設定する。

設定値	説明
A.B.C.D	IPv4 アドレス(A.B.C.D)を指定する
A.B.C.D/M	サブネットマスク長(Mbit)付きの IPv4 アドレス(A.B.C.D)を指定する
X:X::X:X	IPv6 アドレス(X:X::X:X)を指定する
X:X::X:X/M	サブネットマスク長(Mbit)付きの IPv6 アドレス(X:X::X:X)を指定する
any	すべての IPv4/IPv6 アドレスを指定する

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

TELNET サーバーへのアクセスを許可するクライアント端末を IPv4/IPv6 アドレスで制限する。

本コマンドは最大 8 件まで設定が可能であり、先に設定されたものが優先して適用される。

本コマンドを設定した場合、登録した条件を満たさないアクセスはすべて拒否する。

ただし、本コマンドを設定していない場合は、すべてのアクセスを許可する。

no 形式で実行した場合は、指定した設定を削除する。

no 形式でパラメーターを省略した場合、すべての設定を削除する。

[ノート]

telnet-server enable が設定されていない場合、本コマンドは機能しない。

[設定例]

192.168.1.1 と 192.168.10.0/24 のセグメントからの TELNET サーバーへのアクセスのみを許可する。

```
SWP2(config)#telnet-server access permit 192.168.1.1
SWP2(config)#telnet-server access permit 192.168.10.0/24
```

192.168.10.0/24 のセグメントからの TELNET サーバーへのアクセスのみを拒否する。

```
SWP2(config)#telnet-server access deny 192.168.10.0/24
SWP2(config)#telnet-server access permit any
```

4.16 TELNET クライアント

4.16.1 TELNET クライアントの起動

[書式]

telnet *host* [*port*]

[パラメーター]

host : リモートホスト名、または、IPv4 アドレス(A.B.C.D)、または、IPv6 アドレス(X:X::X:X)

IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)

port : <1-65535>

使用するポート番号（省略した場合：23）

[初期設定]

なし

[入力モード]

特権 EXEC モード

[説明]

指定したホストへ TELNET で接続する。

[設定例]

IPv4 アドレス 192.168.100.1 のホストに、ポート番号 12345 で TELNET 接続する。

```
SWP2#telnet 192.168.100.1 12345
```

IPv6 アドレス fe80::2a0:deff:fe11:2233 のホストに、ポート番号 12345 で TELNET 接続する。

```
SWP2#telnet fe80::2a0:deff:fe11:2233%vlan1 12345
```

4.16.2 TELNET クライアントの有効化

[書式]

telnet-client *switch*
no telnet-client

[パラメーター]

switch : TELNET クライアントを有効にするか否か

設定値	説明
enable	有効にする
disable	無効にする

[初期設定]

telnet-client disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

TELNET クライアントとして telnet コマンドを使用できるようにする。

no 形式で実行した場合は TELNET クライアントを無効にする。

[設定例]

TELNET クライアントを有効にする。

```
SWP2(config)#telnet-client enable
```

4.17 TFTP サーバー

4.17.1 TFTP サーバーの起動および受付ポート番号の変更

[書式]

tftp-server enable [*port*]
tftp-server disable
no tftp-server

[キーワード]

enable : TFTP サーバーを有効にする

disable : TFTP サーバーを無効にする

[パラメーター]

port : <1-65535>

TFTP サーバーのリスニングポート番号（省略した場合：69）

[初期設定]

tftp-server disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

TFTP サーバーを有効にする。また、リスニングポート番号を指定することができる。

no 形式で実行した場合は TFTP サーバーを無効にする。

[設定例]

リスニングポート番号を 12345 にして TFTP サーバーを起動する。

```
SWP2(config)#tftp-server enable 12345
```

4.17.2 TFTP サーバーの設定状態の表示

[書式]

show tftp-server

[入力モード]

特権 EXEC モード

[説明]

TFTP サーバーの設定状況を表示する。以下の項目が表示される。

- TFTP サーバー機能の有効/無効
- リスニングポートの番号
- TFTP サーバーへのアクセスを許可する VLAN インターフェース

[設定例]

TFTP サーバーの設定状況を表示する。

```
SWP2#show tftp-server
Service:Enable
Port:69
Management interface(vlan): 1
Interface(vlan):1, 2, 3
```

4.17.3 TFTP サーバーへアクセスできるホストの設定

[書式]

tftp-server interface *interface*

no tftp-server interface *interface*

[パラメーター]

interface : VLAN インターフェース名

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

TFTP サーバーへのアクセスを許可する VLAN インターフェースを設定する。

no 形式で実行した場合は、指定したインターフェースを削除する。

本コマンドは最大 8 件まで設定でき、設定した順に適用する。

本コマンドを設定していない場合は、保守 VLAN のみアクセスできる。

[設定例]

VLAN #1、VLAN #2 に接続しているホストからの TFTP サーバーへのアクセスを許可する。

```
SWP2(config)#tftp-server interface vlan1
SWP2(config)#tftp-server interface vlan2
```

4.18 HTTP サーバー

4.18.1 HTTP サーバーの起動および受付ポート番号の変更

[書式]

http-server enable [*port*]
http-server disable
no http-server

[キーワード]

enable	:	HTTP サーバーを有効にする
disable	:	HTTP サーバーを無効にする

[パラメーター]

port	:	<1-65535> HTTP サーバーのリスニングポート番号（省略した場合：80）

[初期設定]

http-server disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

HTTP サーバーを有効にする。また、リスニング TCP ポート番号を指定することができる。

no 形式で実行した場合は無効にする。

[設定例]

リスニングポート番号を 8080 にして HTTP サーバーを起動する。

```
SWP2(config)#http-server enable 8080
```

4.18.2 セキュア HTTP サーバーの起動および受付ポート番号の変更

[書式]

http-server secure enable [*port*]
http-server secure disable
no http-server secure

[キーワード]

enable	:	セキュア HTTP サーバーを有効にする
disable	:	セキュア HTTP サーバーを無効にする

[パラメーター]

port	:	<1-65535> セキュア HTTP サーバーのリスニングポート番号（省略した場合：443）

[初期設定]

http-server secure disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

セキュア HTTP サーバーを有効にする。また、リスニング TCP ポート番号を指定することができる。

no 形式で実行した場合は無効にする。

セキュア HTTP サーバを有効にした場合、暗号化はソフトウェアによって行われるため、トラフィック量に応じて CPU 使用率が高くなる。

高使用率を避けるために、ダッシュボードや LAN マップなど自動で更新される Web ページを複数ユーザーでアクセスする事は避けるのが好ましい。

[設定例]

リスニングポート番号を 8080 にしてセキュア HTTP サーバーを起動する。

```
SWP2(config)#http-server secure enable 8080
```

4.18.3 HTTP サーバーの設定状態の表示

[書式]

show http-server

[入力モード]

特権 EXEC モード

[説明]

HTTP サーバーの設定状況を表示する。以下の項目が表示される。

- HTTP サーバー機能の有効/無効
- HTTP サーバーのリスニングポートの番号
- HTTP サーバーへのアクセスを許可する VLAN インターフェース
- HTTP サーバーへのアクセスを制限するフィルター
- セキュア HTTP サーバー機能の有効/無効
- ログインタイムアウト時間

[設定例]

HTTP サーバーの設定状況を表示する。

```
SWP2#show http-server
HTTP :Enable(80)
HTTPS:Disable
Management interface(vlan): 1
Interface(vlan):1
Access:None
Login timeout:30 min 51 sec
```

4.18.4 HTTP サーバーへアクセスできるホストの設定

[書式]

http-server interface *interface*
no http-server interface *interface*

[パラメーター]

interface : VLAN インターフェース名

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

HTTP サーバーへのアクセスを許可する VLAN インターフェースを設定する。

no 形式で実行した場合は、指定したインターフェースを削除する。

本コマンドは最大 8 件まで設定でき、設定した順に適用する。

本コマンドを設定していない場合は、保守 VLAN のみアクセスできる。

[設定例]

VLAN #1、VLAN #2 に接続しているホストからの HTTP サーバーへのアクセスを許可する。

```
SWP2(config)#http-server interface vlan1
SWP2(config)#http-server interface vlan2
```

4.18.5 HTTP サーバーへアクセスできるクライアントの IP アドレス制限

[書式]

http-server access *action info*

no http-server access [*action info*]

[パラメーター]

action : アクセス条件に対する動作を指定する

設定値	説明
deny	条件を"拒否"する
permit	条件を"許可"する

info : 条件とする送信元 IPv4/IPv6 アドレス情報を設定する。

設定値	説明
A.B.C.D	IPv4 アドレス(A.B.C.D)を指定する
A.B.C.D/M	サブネットマスク長(Mbit)付きの IPv4 アドレス(A.B.C.D)を指定する
X:X::X:X	IPv6 アドレス(X:X::X:X)を指定する
X:X::X:X/M	サブネットマスク長(Mbit)付きの IPv6 アドレス(X:X::X:X)を指定する
any	すべての IPv4/IPv6 アドレスを指定する

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

HTTP サーバーへのアクセスを許可するクライアント端末を IPv4/IPv6 アドレスで制限する。

本コマンドは最大 8 件まで設定が可能であり、先に設定されたものが優先して適用される。

本コマンドを設定した場合、登録した条件を満たさないアクセスはすべて拒否する。

ただし、本コマンドを設定していない場合は、すべてのアクセスを許可する。

no 形式で実行した場合は、指定した設定を削除する。

no 形式でパラメーターを省略した場合、すべての設定を削除する。

[ノート]

http-server enable もしくは **http-server secure enable** が設定されていない場合、本コマンドは機能しない。

[設定例]

192.168.1.1 と 192.168.10.0/24 のセグメントからの HTTP サーバーへのアクセスのみを許可する。

```
SWP2(config)#http-server access permit 192.168.1.1
SWP2(config)#http-server access permit 192.168.10.0/24
```

192.168.10.0/24 のセグメントからの HTTP サーバーへのアクセスのみを拒否する。

```
SWP2(config)#http-server access deny 192.168.10.0/24
SWP2(config)#http-server access permit any
```

4.18.6 Web GUI の言語設定

[書式]

http-server language *lang*
no http-server language

[パラメーター]

lang : 言語を指定する

設定値	説明
japanese	日本語
english	英語

[初期設定]

http-server language japanese

[入力モード]

グローバルコンフィグレーションモード

[説明]

Web GUI の言語を設定する。

no 形式で実行した場合は、初期設定に戻る。

[設定例]

Web GUI の言語を英語にする。

```
SWP2(config)#http-server language english
```

4.18.7 HTTP サーバーのログインタイムアウト時間の設定

[書式]

http-server login-timeout *min* [*sec*]
no http-server login-timeout

[パラメーター]

min : <0-35791>
タイムアウト時間(分)

sec : <0-2147483>
タイムアウト時間(秒)

[初期設定]

http-server login-timeout 5

[入力モード]

グローバルコンフィグレーションモード

[説明]

HTTP サーバーへのアクセスがない場合に自動的にログアウトするまでの時間を設定する。

sec を省略した場合は、0 が設定される。

no 形式で実行した場合は初期設定に戻る。

[ノート]

設定可能な最小値は 1 分。

[設定例]

HTTP サーバーのタイムアウト時間を 2 分 30 秒に設定する。

```
SWP2(config)#http-server login-timeout 2 30
```

4.19 SSH サーバー

4.19.1 SSH サーバーの起動および受付ポート番号の変更

[書式]

ssh-server enable [*port*]
ssh-server disable
no ssh-server

[キーワード]

enable	:	SSH サーバーを有効にする
disable	:	SSH サーバーを無効にする

[パラメーター]

port	:	<1-65535>
		SSH サーバーのリスニングポート番号（省略した場合：22）

[初期設定]

ssh-server disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

SSH サーバーを有効にする。また、リスニング TCP ポート番号を指定することができる。

SSH サーバーを有効にする場合は、事前にホスト鍵の作成（ssh-server host key generate)を行っておく必要がある。

no 形式で実行した場合は SSH サーバーを無効にする。

[ノート]

SSH クライアントからログインする場合は、事前にユーザー名とパスワードの登録(username)をしておく必要がある。

[設定例]

リスニングポート番号を 12345 にして SSH サーバーを起動する。

```
SWP2#ssh-server host key generate
SWP2#configure terminal
SWP2(config)#ssh-server enable 12345
```

4.19.2 SSH サーバーの設定状態の表示

[書式]

show ssh-server

[入力モード]

特権 EXEC モード

[説明]

SSH サーバーの設定状況を表示する。

以下の項目が表示される。

- SSH サーバー機能の有効/無効
- リスニングポートの番号
- SSH サーバーホスト鍵の有無
- SSH サーバーへのアクセスを許可する VLAN インターフェース
- SSH サーバーへのアクセスを制限するフィルター

[設定例]

SSH サーバーの設定状況を表示する。

```
SWP2#show ssh-server
Service:Enable
Port:23
Hostkey:Generated
Management interface(vlan): 1
Interface(vlan):1, 2, 3
Access:
    deny   192.168.100.5
    permit 192.168.100.0/24
```

4.19.3 SSH サーバーへアクセスできるホストの設定

[書式]

ssh-server interface *ifname*
no ssh-server interface *ifname*

[パラメーター]

ifname : VLAN インターフェース名

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

SSH サーバーへのアクセスを許可する VLAN インターフェースを設定する。

no 形式で実行した場合は、指定したインターフェースを削除する。

本コマンドは最大 8 件まで設定でき、設定した順に適用する。

本コマンドを設定していない場合は、保守 VLAN のみアクセスできる。

[設定例]

VLAN #1, VLAN #2 に接続しているホストからの SSH サーバーへのアクセスを許可する。

```
SWP2(config)#ssh-server interface vlan1
SWP2(config)#ssh-server interface vlan2
```

4.19.4 SSH サーバーへアクセスできるクライアントの設定

[書式]

ssh-server access *action info*
no ssh-server access [*action info*]

[パラメーター]

action : アクセス条件に対する動作を指定する

設定値	説明
deny	条件を"拒否"する
permit	条件を"許可"する

info : 条件とする送信元 IPv4/IPv6 アドレス情報を設定する。

設定値	説明
A.B.C.D	IPv4 アドレス(A.B.C.D)を指定する
A.B.C.D/M	サブネットマスク長(Mbit)付きの IPv4 アドレス(A.B.C.D)を指定する
X:X::X:X	IPv6 アドレス(X:X::X:X)を指定する
X:X::X:X/M	サブネットマスク長(Mbit)付きの IPv6 アドレス(X:X::X:X)を指定する
any	すべての IPv4/IPv6 アドレスを指定する

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

SSH で接続するクライアント端末を IPv4/IPv6 アドレスで制限する。

本コマンドは最大 8 件まで設定が可能であり、先に設定されたものが優先して適用される。

本コマンドを設定した場合、登録した条件を満たさないアクセスはすべて拒否する。

ただし、本コマンドを設定していない場合は、すべてのアクセスを許可する。

no 形式で実行した場合は、指定した設定を削除する。

no 形式でパラメーターを省略した場合、すべての設定を削除する。

[ノート]

ssh-server enable コマンドが設定されていない場合、本コマンドは機能しない。

[設定例]

192.168.1.1 と 192.168.10.0/24 のセグメントからの SSH サーバーへのアクセスのみを許可する。

```
SWP2(config)#ssh-server access permit 192.168.1.1
SWP2(config)#ssh-server access permit 192.168.10.0/24
```

192.168.10.0/24 のセグメントからの SSH サーバーへのアクセスのみを拒否する。

```
SWP2(config)#ssh-server access deny 192.168.10.0/24
SWP2(config)#ssh-server access permit any
```

4.19.5 SSH サーバーホスト鍵の作成

[書式]

ssh-server host key generate [bit *bit*]

[パラメーター]

bit : 1024, 2048

RSA 鍵のビット長

[初期設定]

なし

[入力モード]

特権 EXEC モード

[説明]

SSH サーバーのホスト RSA 鍵とホスト DSA 鍵を設定する。

RSA 鍵は *bit* パラメータによって生成する鍵のビット数を指定できる。DSA 鍵は 1024 ビットの鍵を生成する。

[ノート]

SSH サーバー機能を利用する場合は、事前に本コマンドを実行してホスト鍵を生成する必要がある。

既にホスト鍵が設定されている状態で本コマンドを実行した場合、ユーザーに対してホスト鍵を更新するか否かを確認する。

ホスト鍵の生成には、数分程度の時間がかかる場合がある。

本コマンドは、SSH サーバーが無効の場合にのみ実行できる。

[設定例]

2048 ビットの RSA 鍵と、DSA 鍵を生成する。

```
SWP2#ssh-server host key generate bit 2048
```

4.19.6 SSH サーバーホスト鍵のクリア

[書式]

clear ssh-server host key

[入力モード]

特権 EXEC モード

[説明]

SSH サーバーのホスト RSA 鍵とホスト DSA 鍵を削除する。

[ノート]

本コマンドは、SSH サーバーが無効の場合にのみ実行できる。

[設定例]

ホスト RSA 鍵とホスト DSA 鍵を削除する。

```
SWP2#clear ssh-server host key
```

4.19.7 SSH サーバー公開鍵の表示

[書式]

show ssh-server host key [fingerprint]

[キーワード]

fingerprint　　:　鍵指紋を表示する

[入力モード]

特権 EXEC モード

[説明]

SSH サーバーの公開鍵を表示する。

fingerprint キーワードを指定した場合は、公開鍵の鍵長と鍵指紋、アスキーアートを表示する。

[ノート]

鍵指紋のハッシュアルゴリズムは、MD5 と SHA256 の両方を表示する。

[設定例]

公開鍵を表示する。

```
SWP2#show ssh-server host key
ssh-dss XXXXXXXXXX1kc3MAAAEBAPTB9YYdgvE+4bbhF4mtoIJri+ujdAIfgr4hL/0w7Jlvc50eXg
sXJoCqlPlsLRGHOOzxVYbOouPCUV/jPFCatgOIii8eJNzUqSB1e6MOFtGjmESrdYiafyIUhps+YWqd
TlIo0AFnVUKMqAbYODA3Cy7kNVptYRK8rcKWk1ChbatWnT/Z7RcmEVEou0qlOyp79b3DcpFM7ofa4d
9ySb6mj06Y/Ok8lL5qFhCHmGOGtqJTKZsqb5VnPz8FYC8t1s6/tpyrUa5aG2af/yTEa5U5BDYAuc88
wNIUG9alGo/8WIHiBJAm432o7UPqTHWO/5nYEQu44gmEPQrPGJ65GT8AAAAVAOpjE0Jyei+4c5qWSF
PXUgrLf5HAAABAQCnnPO+ZjWZcZwGa6LxTGMczAjDy5uwD4DWBbRxsPKaXlsicJGC0aridnTthIGa8
ARypDjhpL1a37SDezx8yClQ5vh+4SPLdS1hdSSzXXE+MXIICXnOVPdiKC4ia10n81tMxW/EPw4SqFP
77r7VvCE/JpXv82AN2JTJ/HAn3X7lvMyCsKZLoWrEcEcBH5anvAQKByVt7RerToZ4vSgodskv7nyXX
XXXXXXX

ssh-rsa XXXXXXXXXX1yc2EAAAABIwAAAQEAwvAZK18jKTCHIHQfRV4r7UOYChX0oeKjBbuuLSDhSH
WmhpG3xxJO0pDIedSF3Knb7LX2SfymQYJ7XYIqMjmU0oziv/zi+De/z3M7wJHQUwfMZEDAdR6Mx39w
6Q04/ehQcaszjXi+0Al2wG/kk56lAU23CW/i21o//5GZTzkFKyEJUtWauHWEW9glF5Yy7F64PesqoH
6h5oDNK7LhlT7s4QXRnUJphIlINrW278Dnvyry3liR+tgTJAq3cGHfYsaQCdankDilIQhUazUY0vJO
/gjYCjMuWH6Ek/cst+PCtgnt0XV5Bl079uRUmcACs2pDX5EWrwbPXXXXXXXXX==
```

公開鍵の鍵指紋を表示する。

```
SWP2#show ssh-server host key fingerprint
ssh-dss
1024 MD5:XX:XX:a8:b9:51:93:9d:d2:ec:40:1a:43:66:3a:XX:XX
+---[DSA 1024]----+
|    .* .         |
|=*=+. o          |
|E+X+   o         |
| o . + = + .     |
|.. ..O X .       |
|oo=.B.*.o        |
|  o +   S o      |
|   . o           |
|    E            |
+------[MD5]------+
1024 SHA256:XXXXearwsCXvYTfIKrS6yYSrjMh0fW6W0Bw7aAOXXXX
+---[DSA 1024]----+
|   . +E.         |
|    o o          |
|     o X S       |
|    + = * .      |
|  o . B * .      |
|       + o .     |
|      * * +      |
|X+.@ +o=         |
|@*o.= o.         |
+----[SHA256]-----+

ssh-rsa
2048 MD5:XX:XX:b8:07:e3:5e:57:b8:80:e3:fc:b3:24:17:XX:XX
+---[RSA 2048]----+
|                 |
|...*             |
|*+.              |
|    .            |
|   .   +         |
|                 |
|        E        |
|     . B..       |
|      . oo       |
+------[MD5]------+
2048 SHA256:XXXXMkUuEbkJggPD68UoR+gobWPhgu7qqXzE8iUXXXX
+---[RSA 2048]----+
|*.==+            |
|*o+= . .         |
|*=o.  . S        |
|      * S . .    |
|     + B * o     |
| = = . . .       |
|    o            |
|     .           |
|. * *            |
+----[SHA256]-----+
```

4.19.8 SSH クライアントの生存確認の設定

[書式]

ssh-server client alive enable [*interval* [*count*]]
ssh-server client alive disable
no ssh-server client alive

[パラメーター]

interval : <1-2147483647>
クライアントの生存確認間隔（秒 省略した場合：100）

count : <1-2147483647>
クライアントの生存確認最大カウント数（省略した場合：3）

[初期設定]

ssh-server client alive disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

クライアントの生存確認を行うか否かを設定する。

クライアントに interval で設定した秒間隔で応答を要求するメッセージを送る。count で指定した回数だけ連続して応答がなかったら、このクライアントとの接続を切り、セッションを終了する。

no 形式で実行した場合は初期設定に戻る。

4.20 SSH クライアント

4.20.1 SSH クライアントの起動

[書式]

ssh [*user@*] *host* [*port*]

[パラメーター]

user	:	リモートホストにログインする際に使用するユーザー名
host	:	リモートホスト名、または、IPv4 アドレス(A.B.C.D)、または、IPv6 アドレス(X:X::X:X) IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)
port	:	<1-65535> 使用するポート番号（省略した場合：22）

[初期設定]

なし

[入力モード]

特権 EXEC モード

[説明]

指定したホストへ SSH で接続する。

user を省略した場合、ログイン中のユーザー名を使用して SSH サーバーへのアクセスをする。

無名ユーザーでログイン中に *user* を省略した場合は"root"を使用する。

[ノート]

エスケープ文字はチルダ（~）とする。エスケープ文字は行頭に入力されたときだけ認識される。

行頭からエスケープ文字を 2 回続けて入力した場合には、エスケープ文字がサーバの入力として使用される。

エスケープ文字に続けてピリオド(.)が入力された場合、強制的に接続を閉じる。

エスケープ文字に続けてクエスチョン(?)が入力された場合、エスケープ入力の一覧が表示される。

[設定例]

IPv4 アドレス 192.168.100.1 のホストに、ユーザー名 uname、ポート番号 12345 で SSH 接続する。

```
SWP2#ssh uname@192.168.100.1 12345
```

IPv6 アドレス fe80::2a0:deff:fe11:2233 のホストに、ユーザー名 uname、ポート番号 12345 で SSH 接続する。

```
SWP2#ssh uname@fe80::2a0:deff:fe11:2233%vlan1 12345
```

4.20.2 SSH クライアントの有効化

[書式]

ssh-client *switch*
no ssh-client

[パラメーター]

switch : SSH クライアントを有効にするか否か

設定値	説明
enable	有効にする
disable	無効にする

[初期設定]

ssh-client disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

SSH クライアントとして **ssh** コマンドを使用できるようにする。

no 形式で実行した場合は SSH クライアントを無効にする。

[設定例]

SSH クライアントを有効にする。

```
SWP2(config)#ssh-client enable
```

4.20.3 SSH ホスト情報のクリア

[書式]

clear ssh host *host*

[パラメーター]

host : リモートホスト名、または、IPv4 アドレス(A.B.C.D)、または、IPv6 アドレス(X:X::X:X)

[入力モード]

特権 EXEC モード

[説明]

SSH クライアントとして接続した SSH サーバーの公開鍵を削除する。

[設定例]

SSH ホスト情報をクリアする。

```
SWP2#clear ssh host 192.168.100.1
```

4.21 メール通知

4.21.1 SMTP メールサーバーの設定

[書式]

mail server smtp *id* **host** *host* [**port** *port*] [**encrypt** *method*] [**auth** *username password*]
no mail server smtp *id*

[キーワード]

port : メールサーバーのポート番号を指定する

encrypt : 暗号化の方式を指定する

auth : SMTP 認証で使うアカウント情報を指定する

[パラメーター]

id : <1-10>
メールサーバー ID

host : メールサーバーアドレス、または、ホスト名

IPv4 アドレス(A.B.C.D)、IPv6 アドレス(X:X::X:X)

IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)

ホスト名(64 文字以内、半角英数字と-.:)

port : <1-65535>

メールサーバーのポート番号(省略時は 25, *method* として over-ssl が指定されていた場合は 465)

method : 暗号化の方式

設定値	説明
over-ssl	通信を暗号化する (over SSL)
starttls	通信を暗号化する (STARTTLS)

username : SMTP 認証で使用するユーザー名

(64 文字以内、? " | > と半角スペースを除く半角英数字・半角記号)

password : SMTP 認証で使用するパスワード

(64 文字以内、? " | > と半角スペースを除く半角英数字・半角記号)

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

メール送信に使用するサーバー情報を設定する。

[ノート]

SMTP 認証を行う際、AUTH LOGIN コマンドを使って認証を行う。

SSL/TLS のバージョンは TLSv1, TLSv1.1, TLSv1.2 に対応している。

メールサーバーのアドレスとして IPv6 アドレスを設定する場合、SSL/TLS による暗号化は利用できない。

[設定例]

メール送信サーバーに、smtp-server-test.com を設定する。

```
SWP2(config)#mail server smtp 1 host smtp-server-test.com
```

メール送信サーバーとして smtp-server-test2.com を指定し、暗号化と SMTP 認証を利用する設定を行う。

```
SWP2(config)#mail server smtp 1 host smtp-server-test2.com encrypt over-ssl auth
test_user test_password
```

4.21.2 SMTP メールサーバー名の設定

[書式]

mail server smtp *id* **name** *server_name*
no mail server smtp *id*

[パラメーター]

id : <1-10>

メールサーバー ID

server_name : メールサーバー名

(64 文字以内、?を除く半角英数字・半角記号)

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

メール送信に使用するサーバーの名前を設定する。

[設定例]

メール送信サーバーの名前として test_mail_server を設定する。

```
SWP2(config)#mail server smtp 1 name test_mail_server
```

4.21.3 メール通知のトリガー設定

[書式]

mail notify *temp-id* **trigger** terminal
no mail notify *temp-id* **trigger** terminal

[キーワード]

terminal : 端末監視機能に関するイベントを通知する

[パラメーター]

temp-id : <1-10>
メールテンプレート ID
イベント通知時に使用するテンプレートを指定する

[初期設定]

no mail notify

[入力モード]

グローバルコンフィグレーションモード

[説明]

指定した機能のイベント情報をメール通知するための設定を行う。

[設定例]

メールテンプレート #1 に端末監視機能のイベントトリガーを設定する。

```
SWP2(config)#mail notify 1 trigger terminal
```

4.21.4 メール送信のテンプレート設定モード

[書式]

mail template *temp-id*
no template

[パラメーター]

temp-id : <1-10>
メールテンプレート ID

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

メール送信時に使用するテンプレートを設定するモードに移行する。

テンプレートモードに移行することで下記の項目を設定することができる。テンプレートは最大 10 件作成可能。

- メール送信の宛先アドレス
- メール送信の送信元アドレス
- メール送信の件名
- メール送信待ち時間の設定(イベント通知のみ使用)

[設定例]

メールテンプレート #1 の設定モードに移行する。

```
SWP2(config)#mail template 1
SWP2(config-mail)#
```

4.21.5 メール送信のサーバー ID の設定

[書式]

send server *server-id*
no send server

[パラメーター]

server-id : <1-10>
メールテンプレート ID

[初期設定]

no send server

[入力モード]

メールテンプレートモード

[説明]

使用するメールサーバーの ID を指定する。

[設定例]

メールテンプレート #1 で使用するメールサーバーにサーバー ID #1 を指定する。

```
SWP2(config)#mail template 1
SWP2(config-mail)#send server 1
```

4.21.6 メール送信の送信元メールアドレスの設定

[書式]

send from *address*
no send from *address*

[パラメーター]

address : 送信元メールアドレス
(256 文字以内、半角英数字と_-.@)

[初期設定]

no send from

[入力モード]

メールテンプレートモード

[説明]

送信元メールアドレスを設定する。

[設定例]

メールテンプレート #1 の送信元メールアドレスに sample@test.com を指定する。

```
SWP2(config)#mail template 1
SWP2(config-mail)#send from sample@test.com
```

4.21.7 メール送信の宛先メールアドレスの設定

[書式]

send to *address*
no send to

[パラメーター]

address : 宛先メールアドレス

(256 文字以内、半角英数字と_-.@)

[初期設定]

no send to

[入力モード]

メールテンプレートモード

[説明]

宛先メールアドレスを設定する。(最大 4 件)

[ノート]

本設定はイベント通知の宛先として使用され、証明書の配布先や通知先としては使用されない。

[設定例]

メールテンプレート #1 の宛先メールアドレスに user@test.com を指定する。

```
SWP2(config)#mail template 1
SWP2(config-mail)#send to user@test.com
```

4.21.8 メール送信の件名の設定

[書式]

send subject *subject*
no send subject

[パラメーター]

temp-id : メール送信時の件名
(128 文字以内、?|>を除く半角英数字・半角記号)

[初期設定]

no send subject

[入力モード]

メールテンプレートモード

[説明]

メール送信の件名を指定する。

[ノート]

未設定の場合は以下の件名となる。

- イベント通知 : Notification from SWP2
- 証明書配布 : Certification publishment
- 証明書通知 : Certification expiration

[設定例]

メールテンプレート #1 のメール送信時の件名に "TestMail" を設定する。

```
SWP2(config)#mail template 1
SWP2(config-mail)#send subject TestMail
```

4.21.9 メール送信待ち時間の設定

[書式]

send notify wait-time *time*
no send notify wait-time

[パラメーター]

time : <1-86400>
送信待ち時間(秒)

[初期設定]

send notify wait-time 30

[入力モード]

メールテンプレートモード

[説明]

イベント通知系のメールが実際に送信されるまでの待機時間を設定する。

[ノート]

本設定はイベント通知のメール送信待機時間として使用される。

[設定例]

メールテンプレート #1 のメール送信待ち時間に 60 秒を設定する。

```
SWP2(config)#mail template 1
SWP2(config-mail)#send notify wait-time 60
```

4.21.10 証明書送付時のメール設定

[書式]

mail send certificate *temp-id*
no mail send certificate

[パラメーター]

temp-id : <1-10>
メールテンプレート ID

[初期設定]

no mail send certificate

[入力モード]

RADIUS コンフィグレーションモード

[説明]

RADIUS サーバーのクライアント証明書を送付するときに使用するテンプレート ID を指定する。

RADIUS サーバーのクライアント証明書は、RADIUS サーバー機能の user コマンドで指定したメールアドレスへ送付する。

[ノート]

RADIUS サーバーのクライアント証明書送付のメール本文例

Certification is published.
Name : [名前] ※ user コマンドの NAME オプションの設定値
Account : [ユーザー名] ※ user コマンドの USERID 値
MAC address : XX:XX:XX:XX:XX:XX
Expire : YYYY/MM/DD

[設定例]

RADIUS サーバーのクライアント証明書をメール送付するときに使用するテンプレート ID に #1 を指定する。

```
SWP2(config-radius)#mail send certificate 1
```

4.21.11 証明書通知時のメール設定

[書式]

mail send certificate-notify *temp-id*
no mail send certificate-notify

[パラメーター]

temp-id : <1-10>
メールテンプレート ID

[初期設定]

no mail send certificate-notify

[入力モード]

RADIUS コンフィグレーションモード

[説明]

RADIUS サーバーのクライアント証明書をメール通知するときに使用するテンプレートを指定する。

[ノート]

RADIUS サーバーのクライアント証明書の有効期間切れ事前通知のメール本文例

Your certificate will expire in [X] days.
Name : [名前] ※ user コマンドの NAME オプションの設定値
Account : [ユーザー名] ※ user コマンドの USERID 値
MAC address : XX:XX:XX:XX:XX:XX
Expire : YYYY/MM/DD

[設定例]

RADIUS サーバーのクライアント証明書をメール通知するときに使用するテンプレートに#2 を指定する。

```
SWP2(config-radius)#mail send certificate-notify 2
```

4.21.12 証明書の有効期限切れ通知タイミングの設定

[書式]

mail certificate expire-notify *day* [*day*] [*day*]
no mail certificate expire-notify

[パラメーター]

day : <1-90>
有効期限切れを通知する残存日数

[初期設定]

mail certificate expire-notify 30

[入力モード]

RADIUS コンフィグレーションモード

[説明]

RADIUS サーバーのクライアント証明書の有効期限切れを事前に通知する日数を指定する。
通知日数は 3 件まで指定できる。

[ノート]

day は入力順序に関わらず、降順で表示される。

[設定例]

RADIUS サーバーのクライアント証明書の有効期限切れの事前通知を 50 日前と 10 日前に設定する。

```
SWP2(config-radius)#mail certificate expire-notify 50 10
```

4.21.13 メール送信情報の表示

[書式]

show mail information [*temp-id*]

[パラメーター]

temp-id : <1-10>
メールテンプレート ID

[入力モード]

特権 EXEC モード

[説明]

指定したテンプレート ID のメール送信情報を表示する。

テンプレート ID を省略した場合は、全てのメール情報を表示する。

[設定例]

メールテンプレート #1 のメール情報を表示する。

```
SWP2#show mail information 1
 Template ID          : 1
 Notify trigger       : lan-map, terminal, stack
 LAN map notices      : hardware/loop/sfp-power/queue-usage/poe/snapshot/l2ms
 Server host          : smtp-server.com
 Server port          : 25
 Encryption           : STARTTLS
 Wait time            : 30 sec
 Mail address (from)  : sample@test.com
 Mail address (to)    : user1@test.com
                        user2@test.com
                        user3@test.com
                        user4@test.com
```

4.22 Yamaha Unified Network Operation Service (Y-UNOS)

4.22.1 Y-UNOS 機能の設定

[書式]

y-unos enable
y-unos disable
no y-unos

[キーワード]

enable	:	Y-UNOS 機能を有効にする
disable	:	Y-UNOS 機能を無効にする

[初期設定]

y-unos enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

Y-UNOS (Yamaha Unified Network Operation Service: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) 機能を有効または無効にする。

no 形式で実行した場合は初期設定に戻る。

[ノート]

Y-UNOS 機能は保守 VLAN のみで動作する。保守 VLAN に IPv4 アドレスが設定されていない場合や、保守 VLAN がリンクダウンしている状態では Y-UNOS 機能を停止する。

保守 VLAN を変更した場合は、Y-UNOS の相互自動認識機能用のマルチキャストフレーム転送設定(**l2-mcast flood 239.192.128.250**)を保守 VLAN に適用すること。

Y-UNOS 機能の有効化/無効化には最大 1 秒かかる場合がある。

スタック機能が有効な場合、本コマンドは使用できない。

[設定例]

Y-UNOS 機能を有効にする。

```
SWP2(config)#y-unos enable
```

Y-UNOS 機能を無効にする。

```
SWP2(config)#y-unos disable
```

4.22.2 Y-UNOS 情報の表示

[書式]

show y-unos

[入力モード]

特権 EXEC モード

[説明]

Y-UNOS に関する設定やステータスの情報を表示する。

表示内容は以下のとおり。

- Y-UNOS 機能の設定(Y-UNOS)
- Y-UNOS 機能の状態(Status)
- Y-UNOS 機能の IPv4 アドレス(IPv4-Address)
  - 保守 VLAN の IPv4 アドレスと ID を表示する
- 検出機器の一覧
  - モデル名(Model)
  - シリアル番号(Serial)
  - ファームウェアバージョン(Version)
  - MAC アドレス(MAC-Address)
  - IPv4 アドレス(IPv4-Address)
  - ホスト名(HostName)

Y-UNOS 機能の状態(Status)では以下のいずれかを表示する。

Status	説明
Active	Y-UNOS 機能が動作している状態
Inactive(stack enable)	Y-UNOS 機能が動作していない状態(スタック機能が有効になっている) ※スタック対応機種のみ
Inactive(no ipv4 address)	Y-UNOS 機能が動作していない状態(保守 VLAN に IPv4 アドレスが設定されていない、または保守 VLAN がリンクダウンしている)
Disable	Y-UNOS 機能が無効な状態

[設定例]

Y-UNOS 情報を表示する。

```
SWP2#show y-unos
Y-UNOS       : Enable
Status       : Active
IPv4 address : 192.168.10.6 (vlan1)

Model          Serial     Version     MAC-Address    IPv4-Address    HostName
-------------------------------------------------------------------------------
RM-CR          RMCR00001  V2.0.0      0000.0000.0000 192.168.10.5    RMCR-hostname
SWX3220-16MT   Z740000000 Rev.4.02.11 0000.0000.0000 192.168.10.4    SWX3220
SWX2310-28GT   Z610000000 Rev.2.04.15 0000.0000.0000 192.168.10.28   SW-Hostname002
```

4.23 LLDP

4.23.1 LLDP 機能の有効化

[書式]

lldp run
no lldp run

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体で LLDP 機能を有効にする。

no 形式で実行した場合は、システム全体で LLDP 機能を無効にする。

[ノート]

ポートに対して LLDP 機能を有効にするには以下のコマンドを設定する必要がある。

set lldp enable コマンドの *type* (LLDP エージェントモード)は必要に応じて txrx, txonly, rxonly を設定する。

- **lldp run** (グローバルコンフィグレーションモード)
- **lldp-agent** (インターフェースモード)
- **set lldp enable** *type* (LLDP エージェントモード)

[設定例]

LAN ポート #1 の LLDP 機能の送受信を有効にする。

```
SWP2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set lldp enable txrx
```

4.23.2 システムの説明文の設定

[書式]

lldp system-description *line*
no lldp system-description

[パラメーター]

line : システムの説明文の文字列(255 文字以内)

[初期設定]

no lldp system-description

[入力モード]

グローバルコンフィグレーションモード

[説明]

LLDP 機能で使用する、システムの説明文を設定する。

no 形式で実行した場合は初期設定に戻る。

初期設定の値は、「機種名＋ファームウェアリビジョン」である。

[設定例]

システムの説明文を SWITCH1_POINT_A にする。

```
SWP2(config)#lldp system-description SWITCH1_POINT_A
```

4.23.3 システムの名称の設定

[書式]

lldp system-name *name*
no lldp system-name

[パラメーター]

name : システムの名称の文字列(255 文字以内)

[初期設定]

no lldp system-name

[入力モード]

グローバルコンフィグレーションモード

[説明]

LLDP 機能で使用する、システムの名称を設定する。

no 形式で実行した場合は初期設定に戻る。

初期設定の値は「機種名」である。

設定値は LLDP System Name TLV に設定される。

[設定例]

システムの名称を SWITCH1 にする。

```
SWP2(config)#lldp system-name SWITCH1
```

4.23.4 LLDP エージェントの作成

[書式]

lldp-agent
no lldp-agent

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

LLDP エージェントを作成し、LLDP エージェントモードに遷移する。

no 形式で実行した場合は、LLDP エージェントを削除する。

[ノート]

LLDP エージェントを削除すると LLDP エージェントモードで設定したコマンドも削除される。

[設定例]

port1.1 で LLDP エージェントを作成し、LLDP エージェントモードに移行する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#
```

4.23.5 LLDP による自動設定機能の設定

[書式]

lldp auto-setting *switch*
no lldp auto-setting

[パラメーター]

switch : LLDP による自動設定機能の設定

設定値	説明
enable	LLDP による自動設定機能を有効にする
disable	LLDP による自動設定機能を無効にする

[初期設定]

lldp auto-setting disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

特定のヤマハ機器が送信する LLDP フレームにより、スイッチの設定を自動的に変更する機能を有効にする。

また、**power-inline disable delay** コマンドによる給電停止タイミングの通知機能を有効にする。

LLDP フレームでは以下の機能が設定される。

- フロー制御
- QoS
- IGMP スヌーピング
- EEE
- RADIUS サーバーホスト
- 端末監視

no 形式で実行した場合は初期設定に戻る。

物理インターフェースのみに設定できる。

[ノート]

本機能を使用するためには、**set lldp enable** コマンドで、LLDP フレームを受信できる設定にする必要がある。

[設定例]

LLDP による自動設定機能を有効にする。

```
SWP2(config)#lldp auto-setting enable
```

4.23.6 LLDP 送受信モードの設定

[書式]

set lldp enable *type*
set lldp disable
no set lldp enable

[パラメーター]

type : 送受信モード

設定値	説明
rxonly	受信専用に設定する
txonly	送信専用に設定する
txrx	送信および受信に設定する

[初期設定]

set lldp disable

[入力モード]

LLDP エージェントモード

[説明]

対象インターフェースでの LLDP フレームの送受信モードを設定する。

set lldp disable の場合は、LLDP フレームを送受信しない。

no 形式で実行した場合は、初期設定に戻る。

[設定例]

LAN ポート #1 の LLDP 送受信モードを受信専用に設定する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set lldp enable rxonly
```

4.23.7 管理アドレスの種類の設定

[書式]

set management-address-tlv *type*
no set management-address-tlv

[パラメーター]

type : 管理アドレスの種類

設定値	説明
ip-address	管理アドレスを IP アドレスとする
mac-address	管理アドレスを MAC アドレスとする

[初期設定]

set management-address-tlv ip-address

[入力モード]

LLDP エージェントモード

[説明]

LLDP で使用する、ポートの管理アドレスの種類を設定する。

no 形式で実行した場合は初期設定に戻る。

設定値は LLDP Management Address TLV に設定される。

[設定例]

LAN ポート #1 の管理アドレスの種類を MAC アドレスに設定する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set management-address mac-address
```

4.23.8 基本管理 TLV の設定

[書式]

tlv-select basic-mgmt
no tlv-select basic-mgmt

[初期設定]

なし

[入力モード]

LLDP エージェントモード

[説明]

送信フレームに基本管理 TLV を追加する。

no 形式で実行した場合は、送信フレームから基本管理 TLV を除く。

このコマンドで以下の TLV が LLDP フレームに追加される。

<基本管理 TLV>

(1) Port Description TLV : ポートの説明文

(2) System Name TLV : システムの名称

(3) System Description TLV : システムの説明文

(4) Syatem Capabilities TLV : システムの能力

(5) Management Address TLV : ポートの管理用アドレス (MAC アドレスまたは IP アドレス)

[設定例]

LAN ポート #1 で送信する LLDP フレームに基本管理 TLV を追加する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#tlv-select basic-mgmt
```

4.23.9 IEEE-802.1 TLV の設定

[書式]

tlv-select ieee-8021-org-specific
no tlv-select ieee-8021-org-specific

[初期設定]

なし

[入力モード]

LLDP エージェントモード

[説明]

送信フレームに IEEE-802.1 TLV を追加する。

no 形式で実行した場合は、送信フレームから IEEE-802.1 TLV を除く。

このコマンドで以下の TLV が LLDP フレームに追加される。

<IEEE-802.1 TLV>

(1) Port VLAN ID : ポート VLAN ID

(2) Port and Protocol VLAN ID : プロトコル VLAN ID

(3) Protocol Identity : サポートするプロトコルのリスト

(4) Link Aggregation : リンクアグリゲーション情報

(5) VLAN Name : ポート VLAN の名称

[設定例]

LAN ポート #1 で送信する LLDP フレームに IEEE-802.1 TLV を追加する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#tlv-select ieee-8021-org-specific
```

4.23.10 IEEE-802.3 TLV の設定

[書式]

tlv-select ieee-8023-org-specific
no tlv-select ieee-8023-org-specific

[初期設定]

なし

[入力モード]

LLDP エージェントモード

[説明]

送信フレームに IEEE-802.3 TLV を追加する。

no 形式で実行した場合は、送信フレームから IEEE-802.3 TLV を除く。

このコマンドで以下の TLV が LLDP フレームに追加される。

<IEEE-802.3 TLV>

(1) MAC/PHY Configuration/Status : オートネゴシエーションのサポート情報

(2) Power Via MDI : PoE 情報 (PoE 機能のある機種のみ)

(3) Link Aggregation : リンクアグリゲーション情報

(4) Maximum Frame Size : 最大フレームサイズ

[設定例]

LAN ポート #1 で送信する LLDP フレームに IEEE-802.3 TLV を追加する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#tlv-select ieee-8023-org-specific
```

4.23.11 LLDP-MED TLV の設定

[書式]

tlv-select med
no tlv-select med

[初期設定]

なし

[入力モード]

LLDP エージェントモード

[説明]

送信フレームに LLDP-MED TLV を追加する。

no 形式で実行した場合は、送信フレームから LLDP-MED TLV を除く。

このコマンドで以下の TLV が LLDP フレームに追加される。

<LLDP-MED TLV>

(1) Media Capabilities : 送信する LLDP-MED TLV の種類

(2) Network Policy : Voice VLAN 情報(Voice VLAN が設定されているポートのみ)

(3) Extended Power-via-MDI : 拡張 PoE 情報(PoE 機能のある機種のみ)

[ノート]

Location Identification TLV の値は "Location" が設定されている。

[設定例]

LAN ポート #1 で送信する LLDP フレームに LLDP-MED TLV を追加する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#tlv-select med
```

4.23.12 LLDP フレームの送信間隔の設定

[書式]

set timer msg-tx-interval *tx_interval*
no set timer msg-tx-interval

[パラメーター]

tx_interval : <5-3600>
LLDP フレーム送信間隔(秒)

[初期設定]

set timer msg-tx-interval 30

[入力モード]

LLDP エージェントモード

[説明]

LLDP フレームの送信間隔を設定する。

no 形式で実行した場合は初期設定に戻る。

[設定例]

LAN ポート #1 で送信する LLDP フレームの送信間隔を 60 秒に設定する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set timer msg-tx-interval 60
```

4.23.13 高速送信期間の LLDP フレーム送信間隔の設定

[書式]

set timer msg-fast-tx *fast_tx*
no set timer msg-fast-tx

[パラメーター]

fast_tx : <1-3600>
高速送信期間の LLDP フレーム送信間隔(秒)

[初期設定]

set timer msg-fast-tx 1

[入力モード]

LLDP エージェントモード

[説明]

高速送信期間の LLDP フレーム送信間隔を設定する。

no 形式で実行した場合は初期設定に戻る。

高速送信期間とはポートの接続機器が新しく見つかった直後の期間で、高速送信期間設定用の以下のコマンドに従い LLDP フレームが送信される。

- **set timerx msg-fast-tx** *fast_tx* : 高速送信期間の送信間隔(秒)を設定する。
- **set tx-fast-init** *value* : 高速送信期間に送信する LLDP フレームの個数を設定する。

[設定例]

LAN ポート #1 で高速送信期間の LLDP フレーム送信間隔を 2 秒に設定する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set timer msg-fast-tx 2
```

4.23.14 LLDP フレーム送信停止から再初期化までの時間の設定

[書式]

set timer reinit-delay *reinit_delay*
no set timer reinit-delay

[パラメーター]

reinit_delay : <1-10>
LLDP フレーム送信停止から再初期化までの時間(秒)

[初期設定]

set timer reinit-delay 2

[入力モード]

LLDP エージェントモード

[説明]

LLDP フレーム送信停止から再初期化までの時間を設定する。

no 形式で実行した場合は初期設定に戻る。

[設定例]

LAN ポート #1 で LLDP フレーム送信停止から再初期化までの時間を 10 秒に設定する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set timer reinit-delay 10
```

4.23.15 機器情報の保持時間(TTL)を算出するための乗数の設定

[書式]

set msg-tx-hold *value*
no set msg-tx-hold

[パラメーター]

value : <1-100>
機器情報の保持時間 (TTL) の値を算出するための乗数

[初期設定]

set msg-tx-hold 4

[入力モード]

LLDP エージェントモード

[説明]

機器情報の保持時間 (TTL) を算出するための乗数を設定する。
no 形式で実行した場合は初期設定に戻る。
この設定値は LLDP フレーム送信間隔(msg-tx-interval)に乗算され、さらに＋ 1 して TTL 値(秒)となる。
TTL 値は、Time To Live TLV に設定される。

TTL = msg-tx-interval × msg-tx-hold ＋ 1 (秒)

[設定例]

LAN ポート #1 で機器情報の保持時間 (TTL) を算出するための乗数を 2 に設定する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set msg-tx-hold 2
```

4.23.16 高速送信期間の LLDP フレーム送信個数の設定

[書式]

set tx-fast-init *value*
no set tx-fast-init

[パラメーター]

value : <1-8>
高速送信期間の LLDP フレーム送信個数

[初期設定]

set tx-fast-init 4

[入力モード]

LLDP エージェントモード

[説明]

高速送信期間の LLDP フレーム送信個数を設定する。
no 形式で実行した場合は初期設定に戻る。

[設定例]

LAN ポート #1 で高速送信期間の LLDP フレーム送信個数を 2 に設定する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set tx-fast-init 2
```

4.23.17 ポート単位で管理できる機器の最大接続台数の設定

[書式]

set too-many-neighbors limit *max_value*
no set too-many-neighbors limit

[パラメーター]

max_value : <1-1000>
ポート単位で管理できる機器の最大接続台数

[初期設定]

set too-many-neighbors limit 5

[入力モード]

LLDP エージェントモード

[説明]

ポート単位で管理できる機器の最大台数を設定する。

no 形式で実行した場合は初期設定にも戻る。

ポートの最大接続台数を超えた場合、新しい機器から送信された LLDP フレームは無視する。

[ノート]

コマンドを設定すると、対象ポートで最初の LLDP フレームを受信したときに一度、リモート機器管理テーブルがクリアされる。

[設定例]

LAN ポート #1 でポート単位で管理できる機器の最大台数を 10 に設定する。

```
SWP2(config)#lldp run
SWP2(config)#interface port1.1
SWP2(config-if)#lldp-agent
SWP2(lldp-agent)#set too-many-neighbors limit 10
```

4.23.18 LLDP 機能のインターフェース一括設定

[書式]

lldp interface enable *type*
lldp interface disable

[キーワード]

enable : LLDP 機能を有効にする

disable : LLDP 機能を無効にする

[パラメーター]

type : 送受信モード

設定値	説明
rxonly	受信専用に設定する
txonly	送信専用に設定する
txrx	送信および受信に設定する

[入力モード]

グローバルコンフィグレーションモード

[説明]

LLDP 機能の有効/無効を全ての LAN/SFP+ポートに一括設定する。

有効設定の場合は、指定した LLDP フレームの送受信モードを設定する。

[ノート]

本コマンドはグローバルコンフィグレーションモードのみ実行可能。

なお、本コマンドは各インターフェースの LLDP 設定をするためのものであり、running-config には表示されない。

[設定例]

全ての LAN/SFP+ポートの LLDP 機能を有効にし、LLDP フレームを送受信可能なモードに設定する。

```
SWP2(config)#lldp interface enable txrx
```

4.23.19 インターフェースの状態表示

[書式]

show lldp interface *ifname* [neighbor]

[キーワード]

neighbor : 接続している機器の情報を表示する。

[パラメーター]

ifname : LAN/SFP+ポートのインターフェース名
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

ifname で指定したインターフェースの LLDP 情報を表示する。

neighbor を指定した場合はインターフェースに接続している機器の情報を表示する。

以下の項目が表示される。

show lldp interface *ifname* の場合

- インターフェース及びその統計情報

Agent Mode	ブリッジモード(Nearest bridge 固定)
Enable (tx/rx)	送信モード/受信モード (Y：可能、N：不可)
Message fast transmit time	高速送信期間の LLDP フレーム送信間隔(秒)
Message transmission interval	LLDP フレーム送信間隔(秒)
Reinitialisation delay	送信停止後から再初期化までの時間(秒)
MED Enabled	LLDP-MED TLV 送信の有効/無効
Device Type	デバイスタイプ(NETWORK_CONNECTIVITY 固定)
Total frames transmitted	LLDP フレームの送信数
Total entries aged	TTL 秒以上受信がなく、管理テーブルから削除された機器の数
Total frames received	LLDP フレームの受信数
Total frames received in error	LLDP フレームの受信エラー数
Total frames discarded	破棄された LLDP フレームの数
Total discarded TLVs	破棄された TLV の数
Total unrecognised TLVs	認識できなかった TLV の数

show lldp interface *ifname* neighbor の場合

- 基本管理情報

Interface Name	受信したインターフェース名
System Name	システム名称
System Description	システムの説明
Port Description	ポートの説明

System Capabilities	システムの能力
Interface Numbering	インターフェース番号のタイプ
Interface Number	インターフェース番号
OID Number	OID 番号
Management Address	MAC アドレスまたは IP アドレス

- Mandatory TLV の情報

CHASSIS ID TYPE	CHASSIS ID TLV のタイプと値
PORT ID TYPE	PORT ID TLV のタイプと値
TTL (Time To Live)	機器情報の保持時間(秒)

- 8021 ORIGIN SPECIFIC TLV の情報

Port Vlan id	ポート VLAN の ID
PP Vlan id	プロトコル VLAN の ID
VLAN ID	ポート VLAN の ID
VLAN Name	ポート VLAN の名称
Remote Protocols Advertised	サポートするプロトコルのリスト
Remote VID Usage Digestt	VID Usage Digestt 値
Remote Management Vlan	管理用 VLAN の名称
Link Aggregation Status	リンクアグリゲーションの有効/無効
Link Aggregation Port ID	リンクアグリゲーションポートの ID

- 8023 ORIGIN SPECIFIC TLV の情報

AutoNego Support	オートネゴシエーション機能の有効/無効
AutoNego Capability	オートネゴシエーション可能な通信方式
Operational MAU Type	通信速度とデュプレックスモード
MDI power support	PoE 機能サポートの有無
PSE power pair	PSE パワーペアー
Power class	PoE 給電クラス
Type/source/priority	PoE 給電タイプ、ソース、優先度
PD requested power value	PD 機器が要求する電力 (0.1mW 単位)
PSE allocated power value	PSE 機器が給電できる電力 (0.1mW 単位)
Link Aggregation Status	リンクアグリゲーションの有効/無効
Link Aggregation Port ID	リンクアグリゲーションポートの ID
Max Frame Size	最大フレームサイズ

- LLDP-MED TLV の情報 (LLDP-MED TLV を受信した場合に表示される)

MED Capabilities	LLDP-MED TLV の種類のリスト
MED Capabilities Dev Type	LLDP-MED メディアデバイスタイプ
MED Application Type	アプリケーションタイプ
MED Vlan id	VLAN の ID
MED Tag/Untag	VLAN タグの有無
MED L2 Priority	L2 の優先度

MED DSCP Val	DSCP 値の優先度
MED Location Data Format	位置情報のフォーマット
Latitude Res	緯度の分解能(有効な上位ビット数)
Latitude	緯度(34 ビット)
Longitude Res	経度の分解能(有効な上位ビット数)
Longitude	経度(34 ビット)
AT	高度タイプ
	1:メーター
	2:ビルのフロア
Altitude Res	高度の分解能(有効な上位ビット数)
Altitude	高度(30 ビット)
Datum	測地基準
	0:米国の世界測地系(WGS 84)
	1:北アメリカ測地系(NAD 83)
	2:北アメリカ測地系(NAD 83)の平均既往最低潮位
LCI length	位置情報データの長さ
What	場所の参照位置
	0:DHCP サーバーの場所
	1:クライアントに最も近いと考えられるネットワーク要素の位置
	2:クライアントの位置
Country Code	国コード
CA type	CA (Civic Address) タイプ
MED Inventory	Inventory 情報リスト

位置情報に関しては RFC 3825 を参照

[設定例]

LAN ポート #1 の LLDP 情報を表示する。

```
SWP2#show lldp interface port1.1
Agent Mode                    : Nearest bridge
Enable (tx/rx)                : Y/Y
Message fast transmit time    : 1
Message transmission interval : 30
Reinitialisation 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
SWP2#
```

4.23.20 全てのインターフェースにおける接続機器の情報表示

[書式]

show lldp neighbors

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

全てのインターフェースにおける接続機器の情報を表示する。

(表示形式は **show lldp interface** *ifname* neighbor コマンドを参照)

[設定例]

接続している機器の情報を表示する。

```
SWP2#show lldp neighbors
Interface Name           : port1.1
System Name              : SWP2-10MMF
System Description       : SWP2 Rev.2.03.01 (Fri Sep  7 00:00:00 2018)
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

SWP2#
```

4.23.21 LLDP フレームカウンターのクリア

[書式]

clear lldp counters

[入力モード]

特権 EXEC モード

[説明]

全てのポートの LLDP フレームカウンターをクリアする。

[設定例]

LLDP フレームカウンターをクリアする。

```
SWP2>clear lldp counters
```

4.24 L2MS (Layer 2 management service)の設定

4.24.1 L2MS 制御フレームの送受信設定

[書式]

l2ms filter enable
l2ms filter disable
no l2ms filter

[キーワード]

enable	:	L2MS の制御フレームを送受信できない
disable	:	L2MS の制御フレームを送受信できる

[初期設定]

l2ms filter disable

[入力モード]

インターフェースモード

[説明]

L2MS の制御フレームを送受信するか否かを設定する。

no 形式で実行した場合は、L2MS の制御フレームを送受信できるようになる。

[ノート]

本コマンドは、以下のインターフェースには設定できない。

- VLAN インターフェース
- 論理インターフェースに収容されている物理インターフェース

論理インターフェースに収容されている物理インターフェースは、収容先の本コマンドの設定に従って動作する。なお、物理インターフェースを論理インターフェースに収容する場合に、物理インターフェースの設定は初期値に戻る。

本コマンドの設定に関わらず、以下のいずれかの条件を満たしている場合は、L2MS の制御フレームが送受信されないことがある。

- STP またはループ検出機能によってインターフェースが Blocking 状態になっている
- **switchport trunk native vlan none** コマンドが設定されている
- 論理インターフェースに収容されている

[設定例]

port1.5 で L2MS の制御フレームを送受信しないようにする。

```
SWP2(config)#interface port1.5
SWP2(config-if)#l2ms filter enable
```

4.24.2 L2MS の情報の表示

[書式]

show l2ms [detail]

[キーワード]

detail	:	詳細情報も表示する

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

以下の情報を表示する。

- L2MS マネージャーに管理されているか否か
- L2MS マネージャーの MAC アドレス(管理されている場合)

[ノート]

L2MS が動作していない場合、情報は表示されない。

detail の指定は、L2MS がマネージャーとして動作してる場合のみ有効である。

[設定例]

エージェントとして動作している場合の L2MS 情報を表示する。

```
SWP2>show l2ms
Role : Agent

Status : Managed by Manager (ac44.f23d.0bb9)
```

4.25 スナップショット

4.25.1 スナップショット機能の設定

[書式]

snapshot enable
snapshot disable
no snapshot

[キーワード]

enable	:	スナップショット機能を有効にする
disable	:	スナップショット機能を有効にしない

[初期設定]

snapshot disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

スナップショット機能を有効にする。

no 形式で実行した場合は、スナップショット機能が無効となる。

[ノート]

本コマンドは、L2MS がマネージャーとして動作している場合のみ有効である。

[設定例]

スナップショット機能を有効にする。

```
SWP2(config)#snapshot enable
```

4.25.2 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

[書式]

snapshot trap terminal [except-wireless]
no snapshot trap terminal

[キーワード]

except-wireless　：　無線接続された端末情報をスナップショットの比較対象から除外する。

[初期設定]

no snapshot trap terminal

[入力モード]

グローバルコンフィグレーションモード

[説明]

端末情報をスナップショットの比較対象に含める。

except-wireless オプションを指定した場合は、無線アクセスポイント配下に無線接続された端末情報は、スナップショットの比較対象から除外される。

no 形式で実行した場合は、端末情報はスナップショットの比較対象外となる。

[ノート]

本コマンドは、マネージャーとして動作し、かつ **terminal-watch enable** コマンドと **snapshot enable** コマンドが設定されている場合のみ有効である。

[設定例]

端末情報をスナップショットの比較対象に含める。

```
SWP2(config)#snapshot trap terminal
```

4.25.3 スナップショットの作成

[書式]

snapshot save [after-update]

[キーワード]

after-update　：　ネットワークの接続状態を更新した後、スナップショットとして保存する

[入力モード]

特権 EXEC モード

[説明]

LAN マップのスナップショット機能でベースとなるスナップショットファイルを保存する。

after-update オプションが含まれない場合、現在マネージャーが保持しているネットワークの接続状態をスナップショットファイルとして保存する。

after-update オプションが含まれる場合、ネットワークの接続状態の情報を最新に更新した後、スナップショットファイルとして保存する。

[ノート]

after-update オプションが含まれる場合、ネットワークの接続状態の情報を最新に更新するがネットワークの構成によっては更新が完了するまでに時間がかかる場合がある。

[設定例]

ネットワークの接続状態を更新した後、スナップショットファイルを保存する。

```
SWP2#snapshot save after-update
```

4.25.4 スナップショットの削除

[書式]

snapshot delete

[入力モード]

特権 EXEC モード

[説明]

スナップショットファイルを削除する。

[設定例]

スナップショットファイルを削除する。

```
SWP2#snapshot delete
```

4.26 ファームウェア更新

4.26.1 ファームウェア更新サイトの設定

[書式]

firmware-update url *url*
no firmware-update url

[パラメーター]

url	:	半角英数字および半角記号(255 文字以内)
		ファームウェアが置かれている URL

[初期設定]

firmware-update url http://www.rtpro.yamaha.co.jp/firmware/revision-up/swp2.bin

[入力モード]

グローバルコンフィグレーションモード

[説明]

WEB サーバーに置かれているファームウェアファイルを使ってファームウェア 更新するときのダウンロード先の URL を設定する。

入力形式は“http://サーバーの IP アドレスあるいはホスト名/パス名” という形式となる。

IPv6 アドレスの場合は"[IPv6 アドレス]"のように"[]"で囲う必要がある。

IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)。

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る。

[設定例]

ファームウェアのダウンロード先 URL を http://192.168.100.1/swp2.bin に設定する。

```
SWP2(config)#firmware-update url http://192.168.100.1/swp2.bin
```

4.26.2 ファームウェア更新で使用する HTTP プロキシーサーバーの設定

[書式]

firmware-update http-proxy *server port*
no firmware-update http-proxy

[パラメーター]

server	:	A.B.C.D
		HTTP プロキシーサーバーの IPv4 アドレス
server	:	[X:X::X:X]
		HTTP プロキシーサーバーの IPv6 アドレス
		[X:X::X:X]のように[]で囲う必要がある
		IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)
	:	半角英数字および半角記号(255 文字以内)
		HTTP プロキシーサーバーの FQDN
port	:	<1-65535>

HTTP プロキシーサーバーのリスニングポート番号

[初期設定]

no firmware-update http-proxy

[入力モード]

グローバルコンフィグレーションモード

[説明]

WEB サーバーに置かれているファームウェアファイルを使ってファームウェア 更新するときの HTTP プロキシーサーバーを設定する。

HTTP プロキシーサーバーが設定されていない場合、HTTP プロキシーサーバーを経由せずにファームウェア更新が行われる。

ポート番号も明示的に設定する必要がある。

no 形式で実行した場合は、HTTP プロキシーサーバーの設定を削除する。

[設定例]

HTTP プロキシーサーバーを 192.168.100.1(ポート番号 8080)に設定する。

```
SWP2(config)#firmware-update http-proxy 192.168.100.1 8080
SWP2(config)#
```

4.26.3 ファームウェア更新の実行

[書式]

firmware-update execute [no-confirm] [no-reboot]

[キーワード]

no-confirm	:	ファームウェア更新の確認をしない
no-reboot	:	ファームウェア更新後に再起動しない

[入力モード]

特権 EXEC モード

[説明]

WEB サーバーに置かれているファームウェアファイルと現在実行中のファームウェアのリビジョンをチェックし、書き換え可能であればファームウェアのリビジョンアップを実行する。

書き換え可能なリビジョンのファームウェアが存在すると、確認を求められるので、 更新する場合は "y" を、更新しない場合は "n" を入力する必要がある。

no-confirm を指定すると、確認をせずにリビジョンアップを実行する。

no-reboot を指定すると、リビジョンアップ実行後に再起動しない。次回起動時に更新後のファームウェアで起動する。

[ノート]

firmware-update url コマンドでダウンロード先 URL を変更できる。

firmware-update revision-down enable コマンドを設定すると古いリビジョンへのリビジョンダウンが行えるようになる。

no-reboot 指定時は、**firmware-update revision-time** コマンドが設定されていた場合でも、指定時刻に再起動しない。

[設定例]

WEB サーバーに置かれているファームウェアファイルでファームウェア更新する。

```
SWP2#firmware-update execute
Found the new revision firmware
Current Revision: Rev.2.03.01
New Revision:     Rev.2.03.03
Downloading...
Update to this firmware? (y/n)y
Updating...
Finish
SWP2#
```

4.26.4 ファームウェアダウンロードタイムアウト時間の設定

[書式]

firmware-update timeout *time*
no firmware-update timeout

[パラメーター]

time : <100-86400>
タイムアウト時間(秒)

[初期設定]

firmware-update timeout 300

[入力モード]

グローバルコンフィグレーションモード

[説明]

WEB サーバーからファームウェアをダウンロードするときのタイムアウト時間を設定する。

no 形式で実行した場合は初期設定に戻る。

[設定例]

ファームウェアダウンロードのタイムアウト時間を 120 秒に設定する。

```
SWP2(config)#firmware-update timeout 120
SWP2(config)#
```

4.26.5 リビジョンダウンの許可

[書式]

firmware-update revision-down enable
no firmware-update revision-down

[初期設定]

no firmware-update revision-down

[入力モード]

グローバルコンフィグレーションモード

[説明]

WEB サーバーに置かれているファームウェアファイルを使ってファームウェア更新するとき、現在のリビジョンよりも古いリビジョンへのファームウェアのリビジョンダウンを許可する。

no 形式で実行した場合はリビジョンダウンを許可しない。

[設定例]

リビジョンダウンを許可する。

```
SWP2(config)#firmware-update revision-down enable
SWP2(config)#
```

4.26.6 ファームウェア更新機能設定の表示

[書式]

show firmware-update

[入力モード]

特権 EXEC モード

[説明]

ファームウェア更新機能に関する現在の設定状況を表示する。

以下の項目が表示される。

- ダウンロード先の URL
- プロキシーサーバーの URL
- ダウンロードのタイムアウト時間

- リビジョンダウンの許可
- 次回起動時のファームウェアリビジョン
- 更新後の再起動時刻

[設定例]

ファームウェア更新機能の設定状況を表示する。

```
SWP2#show firmware-update
url: http://www.rtpro.yamaha.co.jp/firmware/revision-up/swp2.bin
http-proxy: -
timeout: 300 (seconds)
revision-down: Disable
firmware revision for next boot: -
reload-time: -
SWP2#
```

4.26.7 ファームウェア更新の再起動時刻の設定

[書式]

firmware-update reload-time *hour* [*min*]
no firmware-update reload-time

[パラメーター]

hour	:	<0-23>
		ファームウェア更新の再起動時刻(時)
min	:	<0-59>
		ファームウェア更新の再起動時刻(分)

[入力モード]

グローバルコンフィグレーションモード

[説明]

ファームウェア更新後の再起動による新ファームウェア適用時刻を設定する。
no 形式で実行した場合はファームウェア更新直後に再起動して新ファームウェアを適用する。

[設定例]

ファームウェア更新の再起動時刻を AM 1:30 に設定する。

```
SWP2(config)#firmware-update reload-time 1 30
SWP2(config)#
```

4.27 スケジュール

4.27.1 スケジュールの設定

[書式]

schedule *id* **time** *date time template_id*
schedule *id* **event** *event template_id*
no schedule *id*

[パラメーター]

id	:	<1-10>
		スケジュール番号
date	:	<1-12> または * / <1-12> または sun, mon, ... , sat または *

月/日

月の設定例	設定内容
1	1 月
1,2	1 月と 2 月
2-	2 月から 12 月まで
2-7	2 月から 7 月まで
-7	1 月から 7 月まで
*	毎月

日の設定例	設定内容
1	1 日
1,2	1 日と 2 日
2-	2 日から 12 日まで
2-7	2 日から 7 日まで
-7	1 日から 7 日まで
mon	月曜日
sat,sun	土曜日と日曜日
mon-fri	月曜日から金曜日まで
-fri	日曜日から金曜日まで
*	毎月

time : <0-23> または * : <0-59> または * : <0-59>

時:分:秒 (秒の指定は省略可能)

時の設定例	設定内容
12	12 時
12,13	12 時と 13 時
12-	12 時から 23 時まで
10-20	10 時から 20 時まで
-20	0 時から 20 時まで
*	毎時

分の設定例	設定内容
30	30 分
15,45	15 分と 45 分
30-	30 分から 59 分まで
15-45	15 分から 45 分まで
-45	0 分から 45 分まで
*	毎分

event : イベント

設定値	説明
startup	起動したとき

template_id : <1-10>
スケジュールテンプレート番号

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

time を使用してスケジュールを設定した場合、指定した時刻になったときに指定されたスケジュールテンプレートに記述されているアクションを実行する。

event を使用してスケジュールを設定した場合、指定したイベントが発生ときに指定されたスケジュールテンプレートに記述されているアクションを実行する。

no 形式で実行した場合は、指定した ID のスケジュールを削除する。

[ノート]

複数のスケジュールが同時刻に実行される場合、ID の小さい方から順に実行される。

日の指定で数字と曜日を混在させて指定することはできない。

秒の指定を省略した場合、00 秒を指定した場合と同じ設定になる。

月日と時間の設定では"-"や","を用いた範囲指定や"*"による全指定をすることができる。ただし秒数に"-"や","を用いた範囲指定や"*"による全指定をすることはできない。

[設定例]

毎週月曜日の 0,1,2,12,21,22,23 時ちょうどにスケジュールテンプレート #1 を実行するスケジュール #1 を設定する。

```
SWP2(config)#schedule time */mon -2,12-14,21-:0 1
```

4.27.2 スケジュールテンプレートの説明文の設定

[書式]

description *line*
no description

[パラメーター]

line : 半角英数字および半角記号(64 文字以内)
スケジュールテンプレートの説明文

[初期設定]

no description

[入力モード]

スケジュールテンプレートモード

[説明]

スケジュールテンプレートの説明文を設定する。

no 形式で実行した場合は、スケジュールテンプレートの説明文を削除する。

[設定例]

スケジュールテンプレート #1 に説明文を設定する。

```
SWP2(config)#schedule template 1
SWP2(config-schedule)#description Get tech-support
```

4.27.3 スケジュールテンプレートの有効/無効の設定

[書式]

action *switch*
no action

[パラメーター]

switch : スケジュールテンプレートの設定

設定値	説明
enable	スケジュールテンプレートを有効にする
disable	スケジュールテンプレートを無効にする

[初期設定]

action enable

[入力モード]

スケジュールテンプレートモード

[説明]

スケジュールテンプレートを有効または無効にする。

本コマンドで disable を指定することで、トリガーの起動によるアクションの実行を止めることができる。

no 形式で実行した場合は、スケジュールテンプレートを有効にする。

[設定例]

スケジュールテンプレート #1 を無効にする。

```
SWP2(config)#schedule template 1
SWP2(config-schedule)#action disable
```

4.27.4 スケジュールテンプレートの設定

[書式]

schedule template *template_id*
no schedule template

[パラメーター]

template_id : <1-10>
スケジュールテンプレート番号

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

スケジュールテンプレートを設定するモードに移行する。

no 形式で実行した場合は、指定したスケジュールテンプレートを削除する。

[設定例]

スケジュールテンプレート #1 を設定するモードに移行する。

```
SWP2(config)#schedule template 1
SWP2(config-schedule)#
```

4.27.5 スケジュールテンプレートのコマンド実行の設定

[書式]

cli-command *id command*
no cli-command *id*

[パラメーター]

id : <1-20>

コマンド番号

command : コマンド

[初期設定]

なし

[入力モード]

スケジュールテンプレートモード

[説明]

スケジュール機能のトリガーが起動したときに実行されるコマンドを設定する。

no 形式で実行した場合、指定した番号のコマンドを削除する。

[ノート]

同じスケジュールテンプレートに cli-command コマンドと 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 コマンドは動作しない。

複数のコマンドを指定した場合、コマンド番号が小さい方から順に実行される。

複数のコマンドを指定した場合、コマンドが途中で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る。

トリガーが起動した時点で、特権 EXEC モードでコマンドが実行されるため、コマンドによっては適切なモードに遷移するためのコマンドもあわせて設定する必要がある。

設定を保存する場合は最後の write コマンドを実行する必要がある。

省略形でコマンドを指定することはできない。例えばインターフェースとして Port1.1 の入力モードに入る場合、int port1.1 ではなく、interface port1.1 と記述する必要がある。

以下のコマンドは実行できない。

backup system, 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 で始まるコマンド, no ntpdate で始まるコマンド, password-encryption, no password-encryption, ping, ping6, quit, reload, 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, startup-config select, no startup-config select, system-diagnostics on-demand execute(*1), telnet, traceroute, traceroute6, unregister yno, yno enable, yno disable

(*1):system-diagnostics on-demand execute no-confirm は実行可能

[設定例]

スケジュールテンプレート #1 のコマンド番号 #1 に copy tech-support sd コマンドを登録する。

```
SWP2(config)#schedule template 1
SWP2(config-schedule)#cli-command 1 copy tech-support sd
```

4.28 保守運用一般

4.28.1 ホスト名の設定

[書式]

hostname *hostname*
no hostname [*hostname*]

[パラメーター]

hostname : 半角英数字および半角記号(63 文字以内)
ホスト名

[初期設定]

hostname SWP2

[入力モード]

グローバルコンフィグレーションモード

[説明]

ホスト名を設定する。

本コマンドで設定したホスト名はコマンドプロンプトとして使用する。 SNMP アクセス可能な場合は、MIB 変数 sysName の値として使用する。

no 形式で実行した場合は設定を初期値に戻す。

[設定例]

ホスト名を"yamaha"に設定する。

```
SWP2(config)#hostname yamaha
yamaha(config)#
```

4.28.2 システムの再起動

[書式]

reload
restart

[入力モード]

特権 EXEC モード

[説明]

システムを再起動する。

[ノート]

実行中の設定(ランニングコンフィグ)が起動時の設定(スタートアップコンフィグ) から変更されている場合、再起動により変更が無効になるため、必要に応じて、 **reload** コマンドや **restart** コマンド実行前に、 **copy running-config startup-config** コマンドや **write** コマンド、または **save** コマンドを実行すること。

[設定例]

システムを再起動する。

```
SWP2#reload
reboot system? (y/n): y
```

4.28.3 設定の初期化

[書式]

cold start

[入力モード]

特権 EXEC モード

[説明]

工場出荷時の設定で再起動する。SYSLOG も初期化する。

[ノート]

コマンド実行時に特権パスワードを入力する必要がある。

特権パスワードが初期設定の状態では、本コマンドを実行することができません。前もって特権パスワードを変更する必要があります。

[設定例]

設定を初期化する。

```
SWP2#cold start
Password:
```

4.28.4 初期 LED モードの設定

[書式]

led-mode default *mode*
no led-mode default

[パラメーター]

mode : 初期 LED モード

設定値	説明
link-act	LINK/ACT モード
vlan	VLAN モード
off	OFF モード

[初期設定]

led-mode default link-act

[入力モード]

グローバルコンフィグレーションモード

[説明]

初期 LED モードを設定する。

本コマンドを実行すると、設定したモードで LED が点灯する。 また、エラーが発生し STATUS モードに移行した場合でも、エラー解消後は設定した LED モードに戻る。

no 形式で実行すると、初期設定に戻る。

[設定例]

初期 LED モードを OFF モードに設定する。

```
SWP2(config)#led-mode default off
```

4.28.5 LED モードの表示

[書式]

show led-mode

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

LED モードの設定や状態を表示する。

以下の項目を表示する。

- 初期 LED モードの設定
- 現在の LED モードの状態

[設定例]

LED モードの設定や状態を表示する。

```
SWP2>show led-mode
default mode : off
current mode : link-act
```

4.28.6 ポートエラー LED 状態の表示

[書式]

show error port-led

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

エラーが発生しているポートの ID と以下のエラー要因を表示する。

項目	説明
loop-detected (blocking)	ループ検出してブロッキング中
loop-detected (shutdown)	ループ検出して shutdown 中

項目	説明
sfp rx-power error (low)	SFP 受光レベルが正常範囲より低下
sfp rx-power error (high)	SFP 受光レベルが正常範囲より上昇

[設定例]

ポートのエラー状態を表示する。

```
SWP2>show error port-led
 ID              error
-----------------------------------------
 port1.1         loop-detected (blocking)
```

4.28.7 ディップスイッチの状態表示

[書式]

show dipsw

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

ディップスイッチの起動時の状態と現在の状態を表示する。

[設定例]

ディップスイッチの状態を表示する。

```
SWP2>show dipsw
 DIPSW              SW1   SW2   SW3   SW4
-------------------------------------
 Startup status :   ON    OFF   OFF   ON
 Current status :   ON    OFF   OFF   ON
```

4.28.8 「このスイッチを探す」機能開始

[書式]

find switch start *sec method*

[パラメーター]

sec : <5-3600>

「このスイッチを探す」時間(秒)

method : 方法

パラメーター	説明
led	橙色でポート LED を点滅させます。

[入力モード]

特権 EXEC モード

[説明]

指定した秒数と方法で「このスイッチを探す」機能を実行する。

[ノート]

現在の LED モードが OFF モードになっている場合、LED を点滅できません。

[設定例]

LED により 10 秒間だけ「このスイッチを探す」機能を開始する。

```
SWP2#find switch start 10 led
```

4.28.9 「このスイッチを探す」機能停止

[書式]

find switch stop

[入力モード]

特権 EXEC モード

[説明]

「このスイッチを探す」機能を停止する。

[設定例]

「このスイッチを探す」機能を停止する。

```
SWP2#find switch stop
```

4.28.10 ProAV プロファイル種別の設定

[書式]

proav profile-type *type* [**name** *name*]
no proav profile-type

[パラメーター]

type : ProAV プロファイル種別

設定値	説明
dante-primary	Dante プライマリー
dante-secondary	Dante セカンダリー
extron-nav	Extron NAV
ndi	NDI

name : プロファイル識別名

? スペースを除く半角英数字および半角記号(32 文字以内)

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

ProAV プロファイル種別を設定する。

本コマンドは、Web GUI の ProAV 設定ページで VLAN と ProAV プロファイルの対応識別のために用いられる。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

本コマンドを CLI で実行しても、ProAV プロファイルの設定は適用されない。

第 5 章

インターフェース制御

5.1 インターフェース基本設定

5.1.1 説明文の設定

[書式]

description *line*
no description

[パラメーター]

line : 半角英数字および半角記号(80 文字以内)
対象インターフェースに対する説明文

[初期設定]

no description

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して説明文を設定する。no 形式で実行した場合は、説明文を削除する。

[設定例]

LAN ポート #1 に説明文を設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#description Connected to rtx1210-router
```

5.1.2 シャットダウン

[書式]

shutdown
no shutdown

[初期設定]

no shutdown

[入力モード]

インターフェースモード

[説明]

対象インターフェースをシャットダウンして使用しないようにする。
本コマンドが設定されたインターフェースは、接続されてもリンクアップしなくなる。
no 形式で実行した場合は、対象インターフェースを使用できるようになる。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。
論理インターフェースを対象として本コマンドを設定した場合は、そのインターフェースに所属する全ての LAN/SFP+ポートの設定が変更される。

[設定例]

LAN ポート #1 をシャットダウンして使用しないようにする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#shutdown
```

5.1.3 通信速度・通信モードの設定

[書式]

speed-duplex *type*
no speed-duplex

[パラメーター]

type : 通信速度・通信モードタイプ

通信速度・通信モードタイプ	説明
auto	オートネゴシエーション
10000-full	10Gbps/Full
1000-full	1000Mbps/Full
100-full	100Mbps/Full
100-half	100Mbps/Half
10-full	10Mbps/Full
10-half	10Mbps/Half

[初期設定]

speed-duplex auto

[入力モード]

インターフェースモード

[説明]

通信速度と通信モードを設定する。
no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドによる設定変更を行うと、当該インターフェースが一時的にリンクダウンする。
本コマンドは LAN/SFP+ポートにのみ設定可能。
LAN ポートに *type*10000-full は設定できない。
SFP+ポートに設定できる *type* は auto と 10000-full のみである。

[設定例]

LAN ポート #1 の通信速度/通信モードを 100Mbps/Full に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#speed-duplex 100-full
```

5.1.4 MRU 設定

[書式]

mru *mru*
no mru

[パラメーター]

mru : <64-10240>
受信可能な最大フレームサイズ(設定する値は偶数であること)

[初期設定]

mru 1522

[入力モード]

インターフェースモード

[説明]

受信可能な最大フレームサイズを設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートにのみ設定可能。

[設定例]

LAN ポート #1 の mru を 9000 バイトに設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#mru 9000
```

5.1.5 クロス／ストレート自動判別設定

[書式]

mdix auto *action*

no mdix auto

[パラメーター]

type : クロス／ストレート自動判別の動作

設定値	説明
enable	クロス/ストレート自動判別を有効にする
disable	クロス/ストレート自動判別を無効にする

[初期設定]

mdix auto enable

[入力モード]

インターフェースモード

[説明]

クロス/ストレート自動判別を有効にする。有効にすると自動的に必要なケーブル接続タイプ(ストレートまたはクロス)を検出し、接続を適切に設定する。

no 形式で実行した場合は、自動判別が無効になり MDI となる。

[ノート]

本コマンドは LAN ポートにのみ設定可能。

本コマンドによる設定変更を行うと、当該インターフェースが一時的にリンクダウンする。

[設定例]

LAN ポート #1 のクロスストレートの自動判別設定を無効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#mdix auto disable
```

5.1.6 EEE 設定

[書式]

eee *action*

no eee

[パラメーター]

type : EEE の動作

設定値	説明
enable	EEE を有効にする
disable	EEE を無効にする

[初期設定]

eee disable

[入力モード]

インターフェースモード

[説明]

省電力機能 Energy Efficient Ethernet(EEE)を有効にする。

no 形式で実行した場合は、EEE が無効になる。

[ノート]

本コマンドは LAN ポートにのみ設定可能。

本コマンドによる設定変更を行うと、当該インターフェースが一時的にリンクダウンする。

[設定例]

LAN ポート #1 の EEE を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#eee enable
```

5.1.7 EEE 対応可否を表示する

[書式]

show eee capabilities interface *ifname*

[パラメーター]

ifname : LAN ポートのインターフェース名
表示するインターフェース

[入力モード]

非特権 EXEC モード、 特権 EXEC モード

[説明]

指定したインターフェースが EEE に対応しているかどうかを表示する。

以下の項目が表示される。

項目	説明
interface	インターフェース名
EEE(efficient-ethernet)	自身が EEE に対応しているか否か
Link Partner	対向機が EEE に対応しているか否か

[ノート]

対向機が接続されていない場合は、EEE に対応していないと表示される。

[設定例]

LAN ポート #1 の EEE 対応可否を表示する。

[対向機が EEE に対応している場合]

```
SWP2#show eee capabilities interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  yes (1000-T, 100-TX)
  Link Partner            :  yes (1000-T, 100-TX)
```

[対向機が EEE に対応していない場合]

```
SWP2#show eee capabilities interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  yes (1000-T, 100-TX)
  Link Partner            :  not enabled
```

5.1.8 EEE ステータス情報を表示する

[書式]

show eee status interface *ifname*

[パラメーター]

ifname : LAN ポートのインターフェース名

表示するインターフェース

[入力モード]

非特権 EXEC モード、 特権 EXEC モード

[説明]

指定したインターフェースの EEE ステータスを表示する。

以下の項目が表示される。

項目	説明
interface	インターフェース名
EEE(efficient-ethernet)	EEE が有効か否か
Rx LPI Status	受信側の省電力モードの状態
Tx LPI Status	送信側の省電力モードの状態
Wake Error Count	エラーカウント

[設定例]

LAN ポート #1 の EEE ステータスを表示する。

[EEE が無効の場合]

```
SWP2#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Disabled
  Rx LPI Status           :  None
  Tx LPI Status           :  None
  Wake Error Count        :  0
```

[EEE が有効の場合]

```
SWP2#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Operational
  Rx LPI Status           :  Received
  Tx LPI Status           :  Received
  Wake Error Count        :  0
```

[EEE が有効かつ省電力モードへ移行中の場合]

```
SWP2#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Operational
  Rx LPI Status           :  Interrupted
  Tx LPI Status           :  Interrupted
  Wake Error Count        :  0
```

[EEE が有効かつ省電力モードへ移行している場合]

```
SWP2#show eee status interface port1.1
interface:port1.1
  EEE(efficient-ethernet):  Operational
  Rx LPI Status           :  Low Power
  Tx LPI Status           :  Low Power
  Wake Error Count        :  0
```

5.1.9 ポートミラーリングの設定

[書式]

mirror interface *ifname* direction *direct*

no mirror interface *ifname* [direction *direct*]

[キーワード]

direction : トラフィックの監視方向を設定する

[パラメーター]

ifname : LAN/SFP+ポートのインターフェース名

トラフィックをミラーリングするインターフェース

direct : トラフィックの監視方向

トラフィックの監視方向	説明
both	受信側と送信側の両方
receive	受信側
transmit	送信側

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースをスニファーポート、*ifname* をモニターポートとして、*direct* で設定されたトラフィックをミラーリングする。

no 形式で実行した場合は、ミラーリングの設定を削除する。

[ノート]

本コマンドは LAN/SFP+ポートのみ設定可能。

スニファーポートに設定できるインターフェースは 1 つのみ。

[設定例]

LAN ポート #1 をスニファーポートとして、LAN ポート #4 の送受信フレームと LAN ポート #5 の送信フレームをミラーリングする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#mirror interface port1.4 direction both
SWP2(config-if)#mirror interface port1.5 direction transmit
```

5.1.10 ポートミラーリングの状態表示

[書式]

show mirror [interface *ifname*]

[キーワード]

interface : 表示する監視ポートを指定する

[パラメーター]

ifname : LAN/SFP ポートのインターフェース名

表示する監視ポート

[入力モード]

非特権 EXEC モード、 特権 EXEC モード

[説明]

ポートミラーリングの設定を表示する。interface を省略した場合は、全ての監視ポートに対する設定が表示される。

1 つの監視ポートごとに、以下の項目が表示される。

項目	説明
Monitored Port	監視ポートのインターフェース名
Sniffer Port	スニファーポートのインターフェース名
Direction	トラフィックの監視方向

[設定例]

ミラーリングポートの設定を表示する。

```
SWP2#show mirror
Sniffer Port   Monitored Port  Direction
=============  ==============  ==========
```

```
port1.1         port1.4         both
port1.1         port1.5         transmit
```

5.1.11 インターフェースの状態表示

[書式]

show interface [*type* [*index*]]

[パラメーター]

type : インターフェースタイプ

インターフェースタイプ	説明
port	物理インターフェース
vlan	VLAN インターフェース
sa	スタティック論理インターフェース
po	LACP 論理インターフェース

index : インデックス番号

インターフェース ID	説明
1.X	筐体に印字された物理インターフェースの番号(X)を指定する。
<1－4094>	VLAN ID を指定する。
<1－96>	スタティック論理インターフェース番号を指定する。
<1－127>	LACP 論理インターフェース番号を指定する。

[入力モード]

非特権 EXEC モード、 特権 EXEC モード

[説明]

ifname で指定したインターフェースの状態を表示する。*ifname* を省略した場合は、全てのインターフェースの状態を表示する。

以下の項目が表示される。

項目	説明
Interface	インターフェース名
Link is	リンクステータス ※2 (shutdown 時は要因を表示する) • shutdown 設定時 : (by shutdown) • ポートエラー検出時 : (by err-disable)
Hardware is	インターフェース種別(Ethernet、VLAN など)
HW addr	物理(MAC)アドレス ※1
Description	インターフェースの説明文
ifIndex	インターフェースインデックス番号
MRU	Maximum Receive Unit ※4
ARP ageing timeout	ARP タイムアウト時間(ARP エントリー保持時間) ※3
Speed-Duplex	通信速度、通信モードの設定値と動作状態 ※1

項目		説明
Auto MDI/MDIX		Auto MDI/MDIX 有効/無効 ※1
IPv4 address		IP アドレス/マスク長 ※3 (IP アドレス設定時のみ表示される)
broadcast		IP ブロードキャストアドレス ※3 (IP アドレス設定時のみ表示される)
Switchport mode		スイッチポートのモード • access : タグなし • trunk : タグ付き
Ingress filter		入力フィルタリングの状態 • enable : 有効 • disable : 無効
Acceptable frame types		受信可能なフレームタイプ • all : 全てのフレームを受信(タグ有無関係なし) • vlan-tagged only : VLAN タグの付いたフレームのみ受信
Default Vlan		タグなしフレームを扱う VLAN ID • タグなしポートの場合 : **switchport access vlan** コマンドで指定した VLAN • タグ付きポートの場合 : ネイティブ VLAN • タグ付きポートでタグ付きパケットのみ受信設定の場合 : None • 未指定時 : vlan1
Configured Vlans		該当インターフェースが所属している VLAN ID の一覧
input	packets	受信パケット数 ※2
	bytes	受信バイト数 ※2
	multicast packets	受信マルチキャストパケット数 ※2
	drop packets	受信バッファ溢れしたパケット数 ※2,※5
output	packets	送信パケット数 ※2
	bytes	送信バイト数 ※2
	multicast packets	送信マルチキャストパケット数 ※2
	broadcast packets	送信ブロードキャストパケット数 ※2
	drop packets	テールドロップした送信パケット数 ※2,※5

※1 物理インターフェースのみ表示
※2 物理インターフェース、論理インターフェースのみ表示
※3 VLAN インターフェースのみ表示
※4 論理インターフェースおよび VLAN インターフェースの場合は、そのインターフェースに属している物理インターフェースの最小値を表示
※5 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。

[設定例]

LAN ポート #1 の状態を表示する。

```
SWP2# show interface port 1.1
Interface port1.1
  Link is UP
  Hardware is Ethernet
  HW addr: 00a0.de00.0000
  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          : 320
           bytes            : 25875
           multicast packets: 301
    output packets          : 628
           bytes            : 129895
           multicast packets: 628
           broadcast packets: 0
           drop packets     : 0
```

VLAN #1 の状態を表示する。

```
SWP2#show interface vlan 1
Interface vlan1
  Hardware is VLAN
  Description: Connected to router(VLAN)
  ifIndex 301, ARP ageing timeout 1200
  IPv4 address 192.168.100.240/24 broadcast 192.168.100.255
                                                  (u)-Untagged, (t)-Tagged
VLAN ID  Name                             State   Member ports
======= ================================ ======= ======================
1       default                          ACTIVE  port1.1(u) port1.2(u)
                                                 port1.3(u) port1.4(u)
                                                 port1.5(u) port1.6(u)
                                                 port1.7(u) port1.8(u)
```

5.1.12 インターフェースの状態の簡易表示

[書式]

show interface brief

[入力モード]

非特権 EXEC モード、 特権 EXEC モード、個別コンフィグレーションモード

[説明]

インターフェースの状態を簡易表示する。

以下の項目が表示される。

項目	説明
Interface	インターフェース名
Type	インターフェース種別 ※2
PVID	タグなしフレームを扱う VLAN ID ※2
Mode	スイッチポートのモード ※2 • access : タグなし • trunk : タグ付き
Status	リンクステータス

項目	説明
Reason	リンクダウンの要因 • AD: shutdown 設定 • ED: ポートエラー検出 • PD: 上記以外
Speed	通信速度の動作状態 ※2
Port Ch	所属する論理インターフェースの種別 ※1 • (S) : スタティック論理インターフェース • (P) : LACP 論理インターフェース 所属する論理インターフェースの ID
Description	インターフェースの説明文

※1 物理インターフェースのみ表示
※2 物理インターフェース、論理インターフェースのみ表示

[設定例]

インターフェースの状態を簡易表示する。

```
SWP2#show interface brief

Codes: ETH - Ethernet, AGG - Aggregate , PVID - Port Vlan-id
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down


--------------------------------------------------------------------------------
Ethernet   Type  PVID  Mode       Status  Reason  Speed Port    Description
Interface                                           Ch #
--------------------------------------------------------------------------------
port1.1    ETH   1     access     up      --      1g    (S)1    --
port1.2    ETH   1     access     up      --      1g    --      --
port1.3    ETH   1     access     down    PD      auto  --      --
port1.4    ETH   1     access     down    AD      auto  --      --
port1.5    ETH   1     access     up      --      1g    --      --
port1.6    ETH   1     access     up      --      1g    --      --
port1.7    ETH   1     access     up      --      1g    --      --
port1.8    ETH   1     access     up      --      1g    --      --


--------------------------------------------------------------------------------
Interface    Status   Reason  Description
--------------------------------------------------------------------------------
vlan1        up       --      --
vlan2        down     PD      --


--------------------------------------------------------------------------------
Port-channel  Type  PVID  Mode       Status   Reason  Speed  Description
Interface
--------------------------------------------------------------------------------
sa1           AGG   1     access     up       --      1g     --
```

5.1.13 インターフェースのリセット

[書式]

interface reset *ifname*

[パラメーター]

ifname : LAN/SFP+ポートまたは論理インターフェース
リセットするインターフェース

[入力モード]

特権 EXEC モード

[説明]

指定したインターフェースをリセットする。

[ノート]

対象インターフェースのリンク状態をリセットし、リンクを再確立する。

なお、リセットに伴い一時的にリンクダウンが発生する。

論理インターフェースに所属している LAN/SFP+ポートには実行できない。

[設定例]

LAN ポート #1 をリセットする

```
SWP2#interface reset port1.1
```

5.1.14 フレームカウンター表示

[書式]

show frame-counter [*ifname*]

[パラメーター]

ifname : LAN/SFP ポートのインターフェース名
表示するインターフェース

[入力モード]

非特権 EXEC モード、 特権 EXEC モード

[説明]

ifname で指定したインターフェースのフレームカウンター情報を表示する。*ifname* を省略した場合は、全てのインターフェースの情報を表示する。

以下の項目が表示される。

項目	説明
Packets	送信／受信パケット数
Octets	送信／受信オクテット数
Broadcast packets	ブロードキャストパケット送信数／受信数
Multicast packets	マルチキャストパケット送信数／受信数
Unicast packets	ユニキャストパケット送信数／受信数
Undersize packets	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)
Oversize packets	オーバーサイズパケット受信数(1523 オクテット以上のパケット※1)
Fragments	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)
Jabbers	ジャバーパケット受信数(1523 オクテット以上で CRC が異常であるパケット※1)
FCS errors	FCS エラーパケット受信数
RX errors	受信エラー数
TX errors	送信エラー数
Collisions	コリジョン発生回数
Drop packets	テールドロップした送信パケット数、バッファ溢れにより受信できなかったパケット数 ※2
64octet packets	64 オクテット長のパケット送受信数
65-127octet packets	65～127 オクテット長のパケット送受信数
128-255octet packets	128～255 オクテット長のパケット送受信数

項目	説明
256-511octet packets	256～511 オクテット長のパケット送受信数
512-1023octet packets	512～1023 オクテット長のパケット送受信数
1024-MAXoctet packets	1024～最大オクテット長(※1)のパケット送受信数

※1 各インターフェースの MRU に依存して変動する。
※2 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。

[設定例]

LAN ポート #1 のフレームカウンターを表示する。

```
SWP2#show frame-counter port1.1
Interface port1.1 Ethernet MAC counters:
  Received:
    Packets               : 84
    Octets                : 6721
    Broadcast packets     : 8
    Multicast packets     : 76
    Unicast   packets     : 0
    Undersize packets     : 0
    Oversize  packets     : 0
    Fragments             : 0
    Jabbers               : 0
    FCS errors            : 0
    RX errors             : 0

  Transmitted:
    Packets               : 91
    Octets                : 11193
    Broadcast packets     : 0
    Multicast packets     : 91
    Unicast   packets     : 0
    TX errors             : 0
    Collisions            : 0
    Drop packets          : 0

  Received and Transmitted:
    64octet       packets : 1
    65-127octet   packets : 166
    128-255octet  packets : 7
    256-511octet  packets : 1
    512-1023octet packets : 0
    1024-MAXoctet packets : 0
```

5.1.15 フレームカウンターのクリア

[書式]

clear counters *ifname*
clear counters all

[キーワード]

all : すべてのインターフェースのフレームカウンターをクリアする

[パラメーター]

ifname : LAN/SFP+ポートまたは論理インターフェースのインターフェース名
対象のインターフェース

[入力モード]

特権 EXEC モード

[説明]

インターフェースのフレームカウンターをクリアする。
ifname を指定した場合は、そのインターフェースのフレームカウンターをクリアする。

ifname に論理インターフェースを指定した場合は、そのインターフェースに所属する全ての LAN/SFP+ポートのフレームカウンターをクリアする。

[設定例]

LAN ポート #1 のフレームカウンターをクリアする。

```
SWP2#clear counters port1.1
```

5.1.16 SFP+モジュールの状態表示

[書式]

show ddm status [interface *ifname*]

[キーワード]

interface : 表示する SFP+ポートを指定する

[パラメーター]

ifname : SFP+ポートのインターフェース名

表示する SFP+ポート

[入力モード]

非特権 EXEC モード、 特権 EXEC モード

[説明]

SFP+モジュールの状態を表示する。

1 つの項目に対して SFP+ポートごとに現在値、上限閾値、下限閾値が表示される。

項目	説明
Temperature	モジュール内部温度(℃)
Voltage	電圧値(V)
Current	電流値(mA)
TX-Power	発光の強度(dBm)
RX-Power	受光の強度(dBm)

[設定例]

SFP+モジュールの状態を表示する。

```
SWP2#show ddm status
             Temperature  High Alarm   High Warning Low Warning  Low Alarm
Interface    (Celsius)    Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.11     42.7         100.0         85.0        -40.0        -55.0
 port1.12     40.7          95.0         90.0        -20.0        -25.0

             Voltage      High Alarm   High Warning Low Warning  Low Alarm
Interface    (V)          Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.11    3.37         3.62         3.46         3.13         2.97
 port1.12    3.34         3.89         3.70         2.89         2.70

             Current      High Alarm   High Warning Low Warning  Low Alarm
Interface    (mA)         Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.11      4.0          16.0         15.0          2.0          2.0
 port1.12      6.2          17.0         14.0          2.0          1.0

             TX-Power     High Alarm   High Warning Low Warning  Low Alarm
Interface    (dBm)        Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
 port1.11     -5.4806       0.4139       0.0000     -10.7058     -12.2184
 port1.12     -5.4714      -1.9997      -1.9997     -11.0237     -11.7392

             RX-Power     High Alarm   High Warning Low Warning  Low Alarm
Interface    (dBm)        Threshold    Threshold    Threshold    Threshold
------------ ------------ ------------ ------------ ------------ ------------
```

```
port1.11      -7.5696       2.5527        0.0000      -16.9897      -40.0000
port1.12      -8.7614       1.0002       -1.0017      -18.0134      -20.0000
```

5.1.17 SFP+モジュールの受光レベル監視の設定

[書式]

sfp-monitor rx-power *action*
no sfp-monitor rx-power

[パラメーター]

action : SFP+モジュールの受光レベル監視の動作

設定値	説明
enable	SFP+モジュールの受光レベル監視を有効にする
disable	SFP+モジュールの受光レベル監視を無効にする

[初期設定]

sfp-monitor rx-power enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

SFP+モジュールの受光レベル監視を設定する。

[設定例]

SFP+モジュールの受光レベル監視を無効にする。

```
SWP2(config)#sfp-monitor rx-power disable
```

5.1.18 送信キューの使用率監視の設定(システム)

[書式]

tx-queue-monitor usage-rate *action*
no tx-queue-monitor usage-rate

[パラメーター]

action : システム全体の送信キューの使用率監視の設定

設定値	説明
enable	システム全体の送信キューの使用率監視を有効にする
disable	システム全体の送信キューの使用率監視を無効にする

[初期設定]

tx-queue-monitor usage-rate enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体の送信キューの使用率監視を有効または無効にする。

no 形式で実行した場合は初期設定に戻す。

[ノート]

送信キューの使用率監視を有効にするためには、本コマンドに加えて、インターフェースでも送信キューの使用率監視を有効にする必要がある。

[設定例]

システム全体で送信キューの使用率監視を無効にする。

```
SWP2(config)#tx-queue-monitor usage-rate disable
```

5.1.19 送信キューの使用率監視の設定(インターフェース)

[書式]

tx-queue-monitor usage-rate *action*
no tx-queue-monitor usage-rate

[パラメーター]

action : 対象インターフェースの送信キューの使用率監視の設定

設定値	説明
enable	対象インターフェースの送信キューの使用率監視を有効にする
disable	対象インターフェースの送信キューの使用率監視を無効にする

[初期設定]

tx-queue-monitor usage-rate enable

[入力モード]

インターフェースモード

[説明]

対象インターフェースの送信キューの使用率監視を有効または無効にする。

no 形式で実行した場合は初期設定に戻す。

[ノート]

本コマンドは LAN/SFP+ポートにのみ設定可能。

送信キューの使用率監視を有効にするためには、本コマンドに加えて、システム全体でも送信キューの使用率監視を有効にする必要がある。

[設定例]

LAN ポート #1 の送信キューの使用率監視を無効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#tx-queue-monitor usage-rate disable
```

5.1.20 送信キューの使用率監視の設定表示

[書式]

show tx-queue-monitor

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

送信キューの使用率監視の設定を表示する。

表示内容は以下のとおり。

- システム全体の送信キューの使用率監視の設定
- LAN/SFP+ポートごとの設定
  - インターフェース名(port)
  - LAN/SFP+ポートの送信キューの使用率監視の設定(usage-rate)。

[設定例]

送信キューの使用率監視の設定を表示する。

```
SWP2>show tx-queue-monitor
usage-rate: Enable
```

```
port      usage-rate
--------------------
port1.1       enable
port1.2       enable
port1.3       enable
port1.4       enable
port1.5       enable
port1.6       enable
port1.7      disable
   :            :
port2.1       enable
   :            :
```

5.2 リンクアグリゲーション

5.2.1 スタティック論理インターフェースの設定

[書式]

static-channel-group *link-id*
no static-channel-group

[パラメーター]

link-id : <1-96>
スタティック論理インターフェース番号

[入力モード]

インターフェースモード

[説明]

対象インターフェースを *link-id* で指定したスタティック論理インターフェースに所属させる。

no 形式で実行した場合は、対象インターフェースをスタティック論理インターフェースから脱退させる。

[ノート]

本コマンドは LAN/SFP+ポートにのみ設定可能。

スタティック論理インターフェースが存在しない *link-id* に対して、LAN/SFP+ポートを所属させる場合は、新たにスタティック論理インターフェースが生成される。

スタティック論理インターフェースから脱退させた結果、所属する LAN/SFP+ポートが無くなった場合は、スタティック論理インターフェースが削除される。

1 つのスタティック論理インターフェースに最大 8 つの LAN/SFP+ポートを所属させることができる。

既に存在しているスタティック論理インターフェースに対して所属させる場合は、LAN/SFP+ポートとスタティック論理インターフェースで、以下の設定を全て一致させること。設定が異なる場合はエラーとなる。

- VLAN の設定
- QoS のトラストモード設定(デフォルト CoS 値、ポート優先度を含む)
- ループ検出の設定(ループ検出の有効/無効、ポートブロッキングの有効/無効

新たにスタティック論理インターフェースが生成される場合は、LAN/SFP+ポートの上記設定がスタティック論理インターフェースの初期設定となる。

LAN/SFP+ポートをスタティック論理インターフェースに所属させると、MSTP の設定が初期設定値に戻る。また、スタティック論理インターフェースから脱退した場合も MSTP の設定が初期設定値に戻る。

1 つの LAN/SFP+ポートを複数の論理インターフェースに所属させることは出来ない。no 形式で脱退させてから異なる論理インターフェースに所属させること。

[設定例]

LAN ポート #1 をスタティック論理インターフェース #5 に所属させる。

```
SWP2(config)#interface port1.1
SWP2(config-if)#static-channel-group 5
```

5.2.2 スタティック論理インターフェースの状態表示

[書式]

show static-channel-group

[入力モード]

非特権 EXEC モード, 特権 EXEC モード

[説明]

スタティック論理インターフェースの状態を表示する。

存在するスタティック論理インターフェースごとに以下の項目が表示される。

- スタティック論理インターフェース名
- ロードバランス機能のルール
- 所属している LAN/SFP+ポートのインターフェース名

ロードバランス機能のルールについては、**port-channel load-balance** コマンドの *type* パラメーター参照のこと。

[設定例]

スタティック論理インターフェースの状態を表示する。

```
SWP2#show static-channel-group
% Static Aggregator: sa5
% Load balancing: src-dst-mac
% Member:
   port1.1
   port1.2
   port1.3
   port1.4
```

5.2.3 LACP 論理インターフェースの設定

[書式]

channel-group *link-id* **mode** *mode*

no channel-group

[パラメーター]

link-id : <1-127>

LACP 論理インターフェース番号

mode : 動作モード

mode	**説明**
active	LACP を ACTIVE モードで機能させる。 ACTIVE モードでは、対向機器に対して自発的に LACP フレームを送信する。
passive	LACP を PASSIVE モードで機能させる。 PASSIVE モードでは、対向機器から LACP フレームを受信した場合にのみ LACP フレームを送信する。

[入力モード]

インターフェースモード

[説明]

対象インターフェースを *link-id* で指定した LACP 論理インターフェースに所属させる。

no 形式で実行した場合は、対象インターフェースを LACP 論理インターフェースから脱退させる。

[ノート]

本コマンドは LAN/SFP+ポートにのみ設定可能。

LACP 論理インターフェースに LAN/SFP+ポートを所属させた場合は、当該 LAN/SFP+ポートに **lacp timeout long** が設定される。

また、LACP 論理インターフェースから脱退させた場合は、当該 LAN/SFP+ポートの **lacp timeout** コマンドの設定が削除される。

LACP 論理インターフェースが存在しない *link-id* に対して、LAN/SFP+ポートを所属させる場合は、新たに LACP 論理インターフェースが生成される。

LACP 論理インターフェースから脱退させた結果、所属する LAN/SFP+ポートが無くなった場合は、LACP 論理インターフェースが削除される。

1 つの LACP 論理インターフェースに最大 12 の LAN/SFP+ポートを所属させることができる。

所属する LAN/SFP+ポート数が、8 つまでは LACP 論理インターフェースに即時に束ねられ、8 つを越えた分については障害発生に備えての待機ポートとなる。

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ない。(所属は可能だが LACP リンクアグリゲーションとして動作はしない。)

通信速度が異なる LAN/SFP+ポートが同一 LACP 論理インターフェースに所属している場合の動作は異速度リンクアグリゲーションの設定に依存する。 詳細は **lacp multi-speed** コマンドを参照のこと。

既に存在している LACP 論理インターフェースに対して LAN/SFP+ポートを所属させる場合は、LAN/SFP+ポートと LACP 論理インターフェースで、以下の設定を全て一致させること。設定が異なる場合はエラーとなる。

- VLAN の設定
- QoS のトラストモード設定(デフォルト CoS 値、ポート優先度を含む)
- ループ検出の設定(ループ検出の有効/無効、ポートブロッキングの有効/無効)

新たに LACP 論理インターフェースが生成される場合は、LAN/SFP+ポートの上記設定が LACP 論理インターフェースの初期設定となる。

LAN/SFP+ポートを LACP 論理インターフェースに所属させると、MSTP の設定が初期設定値に戻る。

また、LACP 論理インターフェースから脱退した場合も MSTP の設定が初期設定値に戻る。

1 つの LAN/SFP+ポートを複数の論理インターフェースに所属させることは出来ない。

no 形式で脱退させてから異なる論理インターフェースに所属させること。

[設定例]

LAN ポート #1 を ACTIVE モードで LACP 論理インターフェース #10 に所属させる。

```
SWP2(config)#interface port1.1
SWP2(config-if)#channel-group 10 mode active
```

5.2.4 LACP 論理インターフェースの状態表示

[書式]

show etherchannel [*ifname*]

[パラメーター]

ifname : LAN/SFP+ポートのインターフェース名
LACP 論理インターフェースを構成しているインターフェース

[入力モード]

非特権 EXEC モード, 特権 EXEC モード

[説明]

ifname を省略した場合、LACP 論理インターフェースの状態を表示する。

存在する LACP 論理インターフェースごとに以下の項目が表示される。

- LACP 論理インターフェース名
- ロードバランス機能のルール
- 所属している LAN/SFP+ポートのインターフェース名

ロードバランス機能のルールについては、**port-channel load-balance** コマンドの *type* パラメーター参照のこと。

ifname を指定した場合、LACP 論理インターフェースを構成している、LAN/SFP+ポートの状態を表示する。

以下の項目が表示される。

項目	説明
Etherchannel portN.N	LAN/SFP+ポート名
Physical admin key	物理的な特性を識別する鍵(bandwidth,duplex,mru,VLAN 構成から作成)

項目	説明
Receive machine state	LACP プロトコル Receive machine 遷移変数の状態 • "Invalid" • "Initialize" • "Port disabled" • "LACP disabled" • "Expired" • "Defaulted" • "Current"
Periodic Transmission machine state	LACP プロトコル Periodic Transmission 遷移変数の状態 • "Invalid" • "No periodic" • "Fast periodic" (1 秒間隔で送信) • "Slow periodic" (30 秒間隔で送信) • "Periodic"
Mux machine state	LACP プロトコル Receive machine 遷移変数の状態 • "Detached" • "Waiting" • "Attached" • "Collecting/Distributing"
Selection	使用状態 • "Selected" • "Unselectedic" • "Standby"
Information	以下の表を参照(Actor 自分自身、Partner 対向相手)
Aggregator ID	LACP 上の識別 ID

Information では以下の項目が表示される。

項目	説明
LAG	LACP システム ID(プライオリティ、MAC アドレス)
Admin Key	LACP 鍵の元となる ID(論理ポート番号)
Port priority	LACP ポート優先度
Ifindex	インターフェース番号
Timeout	Timeout 値("Long"=90 秒、"Short"=3 秒)
Active	LACP 動作モード("Active", "Passive")
Synchronized	Synchronization フラグ
Collecting	Collecting フラグ
Distributing	Distributing フラグ
Defaulted	Defaulted フラグ
Expired	Expired フラグ

[設定例]

LACP 論理インターフェースの状態を表示する。

```
SWP2#show etherchannel
% Lacp Aggregator: po10
% Load balancing: src-dst-mac
% Member:
   port1.1
   port1.2
```

```
  port1.3
  port1.4
```

LACP 論理インターフェースを構成している、LAN/SFP+ポートの状態を表示する。

```
SWP2#show etherchannel port1.1
Etherchannel port1.1
 Physical admin key                          3
 Receive machine state                    Current
 Periodic Transmission machine state      Slow periodic
 Mux machine state                        Collecting/Distributing
 Selection                                Selected
 Information    Actor                          Partner
  LAG           0x8000, 00-a0-de-e0-e0-e0      0x8000, 00-a0-de-11-11-11
  Admin Key       0001                           0001
  Port Priority  32768                          32768
  Ifindex         5001                           5001
  Timeout       Long                           Long
  Active             1                              1
  Synchronized       1                              1
  Collecting         1                              1
  Distributing       1                              1
  Defaulted          0                              0
  Expired            0                              0
```

5.2.5 LACP システム優先度の設定

[書式]

lacp system-priority *priority*
no lacp system-priority

[パラメーター]

priority : <1-65535>

LACP システム優先度
小さいほど優先度が高い

[初期設定]

lacp system-priority 32768

[入力モード]

グローバルコンフィグレーションモード

[説明]

LACP システム優先度を設定する。

no 形式で実行した場合は設定を初期値に戻す。

[ノート]

LACP 論理インターフェースが対向機器と接続された場合、システム優先度を比較して、優先度が高い方に制御権が与えられる。

[設定例]

LACP システム優先度を 100 に設定する。

```
SWP2(config)#lacp system-priority 100
```

5.2.6 LACP システム優先度の表示

[書式]

show lacp sys-id

[入力モード]

非特権 EXEC モード, 特権 EXEC モード

[説明]

LACP システム優先度と LACP システム ID を表示する。

以下の項目が表示される。

- LACP システム優先度(0x で始まる 16 進数)
- LACP システム ID

[ノート]

LACP システム優先度は、**lacp system-priority** コマンドで設定できる。

LACP システム ID は、MAC アドレスから生成される。

[設定例]

LACP のシステム優先度を表示する。

```
SWP2>show lacp sys-id
% System 0x8000, 00-a0-de-e0-e0-e0
```

5.2.7 LACP 異速度リンクアグリゲーションの設定

[書式]

lacp multi-speed *switch*
no lacp multi-speed

[パラメーター]

switch : 異速度リンクアグリゲーション機能の有効・無効設定

設定値	説明
enable	異速度リンクアグリゲーションを有効にする
disable	異速度リンクアグリゲーションを無効にする

[初期設定]

lacp multi-speed disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

LACP における異速度リンクアグリゲーション機能の有効・無効を設定する。

no 形式で実行した場合は設定を初期値に戻す。

[ノート]

異速度リンクアグリゲーションが有効の場合の動作

- 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する。
- ロードバランスはすべての所属ポートを同等に扱う。
- 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する。

異速度リンクアグリゲーションが無効の場合の動作

- 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する。
  - 通信速度が異なる他のポートはスタンバイのままとする。
  - 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する。
- 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する。

[設定例]

異速度リンクアグリゲーションを有効に設定する。

```
SWP2(config)#lacp multi-speed enable
```

5.2.8 LACP タイムアウトの設定

[書式]

lacp timeout *duration*

[パラメーター]

duration : タイムアウトを指定する

duration	説明
short	タイムアウトを 3 秒とする
long	タイムアウトを 90 秒とする

[入力モード]

インターフェースモード

[説明]

LACP タイムアウトを設定する。

[ノート]

本コマンドは LACP 論理インターフェースに所属している LAN/SFP+ポートにのみ設定可能。

LACP 論理インターフェースに LAN/SFP+ポートを所属させた場合は、当該 LAN/SFP+ポートに **lacp timeout long** が設定される。

また、LACP 論理インターフェースから脱退させた場合は、当該 LAN/SFP+ポートの **lacp timeout** コマンドの設定が削除される。

LACP タイムアウトとは、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見なすまでの時間を表す。

また、LACP タイムアウトの設定は LACP フレームに格納されて対向機器に送られ、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る。

自身の LACP フレームの送信間隔は、対向機器から送られてくる LACP フレーム内に格納されている LACP タイムアウトに依存する。

[設定例]

LAN ポート #1 の LACP タイムアウトを short に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#lacp timeout short
```

5.2.9 LACP フレームカウンターのクリア

[書式]

clear lacp [*link-id*] **counters**

[パラメーター]

link-id : <1-127>

LACP 論理インターフェース番号

[入力モード]

特権 EXEC モード

[説明]

LACP のフレームカウンターをクリアする。

link-id を省略した場合は、存在する全ての LACP 論理インターフェースのフレームカウンターをクリアする。

[設定例]

全ての LACP 論理インターフェースのフレームカウンターをクリアする。

```
SWP2#clear lacp counters
```

5.2.10 LACP フレームカウンターの表示

[書式]

show lacp-counter [*link-id*]

[パラメーター]

link-id : <1-127>

LACP 論理インターフェース番号

[入力モード]

非特権 EXEC モード, 特権 EXEC モード

[説明]

LACP のフレームカウンターを表示する。

link-id を省略した場合は、存在する全ての LACP 論理インターフェースのフレームカウンターを表示する。

所属している LAN/SFP+ポートごとに、以下の項目が表示される。

- 送受信された LACP フレーム
- 送受信された Marker プロトコルフレーム
- 送受信されたエラーフレーム

[設定例]

全ての LACP 論理インターフェースのフレームカウンターを表示する。

```
SWP2#show lacp-counter
% Traffic statistics
Port       LACPDUs          Marker          Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
% Aggregator po1 , ID 4601
port1.1  297     298     0       0       0       0
port1.2  306     299     0       0       0       0
port1.3  305     298     0       0       0       0
port1.4  309     1350    0       0       0       0
port1.5  186     186     0       0       0       0
```

5.2.11 ロードバランス機能のルールの設定

[書式]

port-channel load-balance *type*

no port-channel load-balance

[パラメーター]

type : 転送先インターフェースを決めるためのルール

type	説明
dst-ip	宛先 IPv4/IPv6 アドレス
dst-mac	宛先 MAC アドレス
dst-port	宛先 TCP/UDP ポート番号
src-dst-ip	送信元および宛先 IPv4/IPv6 アドレス
src-dst-mac	送信元および宛先 MAC アドレス
src-dst-port	送信元および宛先 TCP/UDP ポート番号
src-ip	送信元 IPv4/IPv6 アドレス
src-mac	送信元 MAC アドレス
src-port	送信元 TCP/UDP ポート番号

[初期設定]

port-channel load-balance dst-ip

[入力モード]

グローバルコンフィグレーションモード

[説明]

ロードバランス機能の転送先インターフェースを決めるためのルールを設定する。

受信したフレーム内の L2/L3/L4 情報を使用し、転送先が決定される。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドはシステム全体の設定となる。

IPv4/IPv6 パケットではないフレームの場合は、設定されているルールに関わらず、送信元および宛先 MAC アドレスを元に転送先インターフェースが決定する。

[設定例]

ロードバランス機能で、送信元および宛先 IPv4/IPv6 アドレスを元に転送先インターフェースを決定するように設定する。

```
SWP2(config)#port-channel load-balance src-dst-ip
```

5.2.12 LACP 論理インターフェースのプロトコル状態表示

[書式]

show etherchannel status [*link-id*] [summary | detail]

[キーワード]

summary	:	概略表示
detail	:	詳細表示

[パラメーター]

link-id	:	<1-127> LACP 論理インターフェース番号

[入力モード]

非特権 EXEC モード, 特権 EXEC モード

[説明]

link-id で指定した LACP 論理インターフェースの状態を表示する。

link-id を省略したときは、全ての LACP 論理インターフェース状態を表示する。

summary を指定した場合は概略表示し、detail を指定した場合は詳細表示する。

summary も、detail も省略したときは、summary が指定されたものとする。

以下の項目が表示される。

項目	説明
Aggregator	LACP 論理インターフェース
ID	LACP 論理インターフェース上の識別 ID
Actor LAG	自分自身の LACP システム ID(プライオリティ、MAC アドレス)
Admin Key	自分自身の LACP 鍵の元となる ID(論理ポート番号)
Status	リンクアグリゲーションのステータス("Not ready"/"Ready")
Partner LAG	対向相手の LACP システム ID(プライオリティ、MAC アドレス)
Partner Key	対向相手の LACP 鍵の元となる ID
Link count	データ通信中ポート数/通信可能なポート数
Link	構成する LAN/SFP+ポート一覧(詳細は以下の表)

Link には以下の項目が表示される。

使用状態	説明
"Unselected"	LACP 制御プロトコル通信中。
"Selected"	LACP が有効な、LAN/SFP+ポートとして選択した。

使用状態	説明
"Standby"	LACP が有効な、LAN/SFP+ポートとし、待機ポートとした。

Synchronization フラグ	説明
"no"	Synchronization フラグが立っていない。
"yes"	Synchronization フラグが立っている。

使用状態と、Synchronization フラグから、リンクアップした LAN/SFP+ポートの状態がわかる。

使用状態	Synchronization	リンクアップした LAN/SFP+ポートの状態
Unselected	no	LACP 制御プロトコル通信中。
Selected	no	LACP が有効な、LAN/SFP+ポートとして選択した。リンクアグリゲーションとして束ねるための、ネゴシエーション中。
Standby	no	LACP が有効な、LAN/SFP+ポートとして選択し、待機ポートと決定した。
Selected	yes	LACP が有効な、LAN/SFP+ポートとして選択した。リンクアグリゲーションとして束ねられてデータ通信可能となった。

[設定例]

LACP 論理インターフェースの状態を表示する。

```
SWP2#show etherchannel status summary
Aggregator po1
 ID          4601
 Status       Ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    1/  1
Aggregator po2
 ID          4602
 Status       Not ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
Aggregator po127
 ID          4727
 Status       Not ready
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1


SWP2#show etherchannel status detail
Aggregator po1
 ID          4601
 Status       Ready
 Actor   LAG  0x8000, 00-a0-de-e0-e0-e0
 Admin Key      0001
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    1/  1
 Link
  port1.1     Selected     Synchronized  yes
Aggregator po2
 ID          4602
 Status       Ready
 Actor   LAG  0x8000, 00-a0-de-e0-e0-e0
 Admin Key      0002
```

```
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
 Link
  port1.2     Selected     Synchronized  no
  port1.3     Unselected   Synchronized  no
Aggregator po127
 ID          4727
 Status       Ready
 Actor   LAG  0x8000, 00-a0-de-e0-e0-e0
 Admin Key      0127
 Partner LAG  0x8000, 00-a0-de-11-11-11
 Partner Key    0001
 Link count    0/  1
 Link
  port1.4     Selected     Synchronized  no
```

5.2.13 LACP ポート優先度の設定

[書式]

lacp port-priority *priority*
no lacp port-priority

[パラメーター]

priority : <1-65535>
LACP ポート優先度
小さいほど優先度が高い

[初期設定]

lacp port-priority 32768

[入力モード]

インターフェースモード

[説明]

LACP ポート優先度を設定する。

no 形式で実行した場合は設定を初期値に戻す。

[ノート]

LACP 論理インターフェースに束ねるときの LAN/SFP+ポート数が 8 つまでは LACP 論理インターフェースに即時に束ねられ、8 つを越えた分については障害発生に備えて待機ポートとなる。

このような時、LAN/SFP+ポート間で優先順位が評価されて、優先順位の高いものから束ねられる。

優先順位の評価方法は、以下の通りである。

1) LACP ポート優先度が小さい程優先される。

2) LACP ポート優先度が同じであれば、インターフェース番号が小さい程優先される。

SFP+ポートを優先させる場合は、LACP ポート優先度を他のポートより小さく設定する必要がある。

[設定例]

LACP ポート優先度を 1024 に設定する。

```
SWP2(config-if)#channel-group 1 mode active
SWP2(config-if)#lacp port-priority 1024
```

5.3 ポート認証

5.3.1 システム全体での IEEE 802.1X 認証機能の設定

[書式]

aaa authentication dot1x
no aaa authentication dot1x

[初期設定]

no aaa authentication dot1x

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体で IEEE 802.1X 認証を有効にする。

no 形式で実行した場合は、システム全体で IEEE 802.1X 認証を無効にする。

認証は、**radius-server host** コマンドで設定した RADIUS サーバーを使用する。

[ノート]

実際に IEEE 802.1X 認証を使用するためには、対象インターフェースでも IEEE 802.1X 認証を 有効にする必要がある。(**dot1x port-control** コマンド)

[設定例]

システム全体で IEEE 802.1X 認証を有効化する。

```
SWP2(config)#aaa authentication dot1x
```

5.3.2 システム全体での MAC 認証機能の設定

[書式]

aaa authentication auth-mac
no aaa authentication auth-mac

[初期設定]

no aaa authentication auth-mac

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体で MAC 認証を有効にする。

no 形式で実行した場合は、システム全体で MAC 認証を無効にする。

認証は、**radius-server host** コマンドで設定した RADIUS サーバーを使用する。

[ノート]

実際に MAC 認証を使用するためには、対象インターフェースでも MAC 認証を有効にする必要がある。 (**auth-mac enable** コマンド)

[設定例]

システム全体で MAC 認証を有効化する。

```
SWP2(config)#aaa authentication auth-mac
```

5.3.3 システム全体での Web 認証機能の設定

[書式]

aaa authentication auth-web
no aaa authentication auth-web

[初期設定]

no aaa authentication auth-web

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体で Web 認証を有効にする。

no 形式で実行した場合は、システム全体で Web 認証を無効にする。

認証は、**radius-server host** コマンドで設定した RADIUS サーバーを使用する。

[ノート]

実際に Web 認証を使用するためには、対象インターフェースでも Web 認証を有効にする必要がある。 (**auth-web enable** コマンド)

[設定例]

システム全体で Web 認証を有効化する。

```
SWP2(config)#aaa authentication auth-web
```

5.3.4 IEEE 802.1X 認証機能の動作モード設定

[書式]

dot1x port-control *mode*

no dot1x port-control

[パラメーター]

mode : IEEE 802.1X 認証の動作モード

動作モード	説明
auto	IEEE 802.1X 認証の Authenticator として動作する
force-authorized	IEEE 802.1X 認証の認証済みポートに固定設定する
force-unauthorized	IEEE 802.1X 認証の未認証ポートに固定設定する

[初期設定]

no dot1x port-control

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、IEEE 802.1X 認証機能の動作モードを設定する。

no 形式でコマンドを実行した場合は、対象インターフェースの IEEE 802.1X 認証機能は無効となる。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

[設定例]

LAN ポート #1 で、IEEE 802.1X 認証機能の動作モードを auto に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#dot1x port-control auto
```

5.3.5 IEEE 802.1X 認証の未認証ポートでの転送制御の設定

[書式]

dot1x control-direction *direction*

no dot1x control-direction

[パラメーター]

direction : 未認証ポートでのパケット転送動作を設定

転送動作	説明
both	送受信とも破棄する。
in	受信のみ破棄する。

[初期設定]

dot1x control-direction both

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、IEEE 802.1X 認証の未認証時のパケット転送動作を変更する。

no 形式で実行した場合は、初期設定に戻る。

both を指定している場合、サプリカントから受信したパケットを破棄し、他のポートから サプリカントの接続されているインターフェースへのブロードキャスト/マルチキャストパケットも破棄する。

in を指定している場合、サプリカントから受信したパケットのみを破棄し、他のポートから サプリカントの接続されているインターフェースへのブロードキャスト/マルチキャストパケットは転送する。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

対象インターフェースで、ホストモードをマルチサプリカントモードに設定した場合や MAC 認証と併用した場合は、自動的に in となる。

対象インターフェースでゲスト VLAN の設定をしている場合は、本コマンドの設定自体が無効となる。

本コマンドの設定を変更すると、認証状態は初期状態に戻る。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド)

[設定例]

LAN ポート #1 の未認証ポートでのパケット転送動作を受信のみ破棄にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#dot1x control-direction in
```

5.3.6 EAPOL パケットの送信回数の設定

[書式]

dot1x max-auth-req *count*
no dot1x max-auth-req

[パラメーター]

count : <1-10>
EAPOL パケットの最大送信回数

[初期設定]

dot1x max-auth-req 2

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、EAPOL パケットの送信回数の最大値を設定する。

no 形式でコマンドを実行した場合は、初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド)

[設定例]

LAN ポート #1 で、EAPOL パケットの送信回数を 3 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#dot1x max-auth-req 3
```

5.3.7 MAC 認証機能の設定

[書式]

auth-mac enable
auth-mac disable

no auth-mac

[キーワード]

enable	:	MAC 認証機能を有効にする
disable	:	MAC 認証機能を無効にする

[初期設定]

auth-mac disable

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、MAC 認証を有効にする。

no 形式で実行した場合、または、disable を指定した場合は、MAC 認証を無効にする。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

実際に MAC 認証を使用するためには、システム全体でも MAC 認証を有効にする必要がある。 (**aaa authentication auth-mac** コマンド)

[設定例]

LAN ポート #1 の MAC 認証機能を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth-mac enable
```

5.3.8 MAC 認証時の MAC アドレス形式の設定

[書式]

auth-mac auth-user *type case*

no auth-mac auth-user

[パラメーター]

type : 形式を指定

設定値	形式
hyphen	xx-xx-xx-xx-xx-xx
colon	xx:xx:xx:xx:xx:xx
unformatted	xxxxxxxxxxxx

case : 大文字・小文字を指定

設定値	説明
lower-case	小文字(a～f)
upper-case	大文字(A～F)

[初期設定]

auth-mac auth-user hyphen lower-case

[入力モード]

グローバルコンフィグレーションモード

[説明]

MAC 認証において、認証時に使用するユーザー名・パスワードの形式を変更する。

MAC 認証では、サプリカントの MAC アドレスをユーザー名・パスワードとして使用し RADIUS サーバーへ認証を要求する。

no 形式で実行した場合は、初期設定に戻る。

[ノート]

本コマンドを使用するためには、対象インターフェースで MAC 認証機能を有効にする必要がある。 (**auth-mac enable** コマンド)

[設定例]

MAC 認証に使用する MAC アドレス形式をハイフンなし、大文字に変更する。

```
SWP2(config)#auth-mac auth-user unformatted upper-case
```

5.3.9 MAC 認証のスタティック登録の設定

[書式]

auth-mac static enable
auth-mac static disable
no auth-mac static

[キーワード]

enable	:	スタティック登録を有効にする
disable	:	スタティック登録を無効にする

[初期設定]

auth-mac static disable

[入力モード]

インターフェースモード

[説明]

MAC 認証機能で、認証をパスしたサプリカントの MAC アドレスを FDB にスタティックエントリーとして登録する。

no 形式で実行した場合、または、disable を指定した場合は、スタティック登録を無効にする。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

本コマンドの設定を変更すると、認証状態は初期状態に戻る。

通常、MAC 認証は FDB にダイナミックエントリーとして登録するためエージングタイムアウトの対象となるが、本コマンド有効時はスタティックエントリーとして登録するため対象外となる。

clear auth state コマンド、または、**auth clear-state time** コマンドで、スタティック登録(認証情報)をクリアすることができる。

本コマンドを使用するためには、対象インターフェースで MAC 認証機能を有効にする必要がある。 (**auth-mac enable** コマンド)

[設定例]

LAN ポート #1 の MAC 認証のスタティック登録を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth-mac static enable
```

5.3.10 Web 認証機能の設定

[書式]

auth-web enable
auth-web disable
no auth-web

[キーワード]

enable	:	Web 認証機能を有効にする
disable	:	Web 認証機能を無効にする

[初期設定]

auth-web disable

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、Web 認証を有効にする。

no 形式で実行した場合、または、disable を指定した場合は、Web 認証を無効にする。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

実際に Web 認証を使用するためには、システム全体でも Web 認証を有効にする必要がある。 (**aaa authentication auth-web** コマンド)

マルチサプリカントモード以外では Web 認証機能を有効にすることはできません。

ゲスト VLAN との併用はできません。

[設定例]

LAN ポート #1 の Web 認証機能を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth-web enable
```

5.3.11 ホストモードの設定

[書式]

auth host-mode *mode*

no auth host-mode

[パラメーター]

mode : ポート認証の動作モード

動作モード	説明
single-host	1 ポートあたり 1 サプリカントのみ通信を許可するモードで、 最初に認証をパスしたサプリカントのみを許可する
multi-host	1 ポートあたり複数サプリカントの通信を許可するモードで、 最初のサプリカントが認証をパスすると、同じポート配下の サプリカントは認証を行わなくても通信が可能となる
multi-supplicant	1 ポートあたり複数サプリカントの通信を許可するモードで サプリカント毎に通信の許可・拒否を決定する

[初期設定]

auth host-mode single-host

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、ポート認証の動作モードを変更する。

no 形式で実行した場合は、初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

本コマンドの設定を変更すると、認証状態は初期状態に戻る。

マルチサプリカントモードでダイナミック VLAN を利用する場合、サプリカント単位で VLAN を指定することが可能。

マルチホストモードでダイナミック VLAN を利用する場合、2 番目以降のサプリカントは最初のサプリカントが適用した VLAN ID が適用される。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド、**auth-mac enable** コマンド、**auth-web enable** コマンド)

[設定例]

LAN ポート #1 をマルチサプリカントモードに変更する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth host-mode multi-supplicant
```

5.3.12 認証順序の設定

[書式]

auth order dot1x auth-mac
auth order auth-mac dot1x
no auth order

[キーワード]

dot1x	:	IEEE 802.1X 認証方式
auth-mac	:	MAC 認証方式

[初期設定]

auth order dot1x auth-mac

[入力モード]

インターフェースモード

[説明]

ポート認証機能で、認証方式を併用した場合、認証を行う順番を設定する。

no 形式で実行した場合は、初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

Web 認証は、本設定に関係なく Web 認証画面で ID/Password を入力したときに認証を行う。

IEEE 802.1X 認証、MAC 認証、Web 認証の設定が無効な場合、その認証方式は実施されない。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド、**auth-mac enable** コマンド、**auth-web enable** コマンド)

[設定例]

LAN ポート #1 の認証方式の順番を、MAC 認証 -> IEEE 802.1X 認証の順番で行うように設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth order auth-mac dot1x
```

5.3.13 再認証の設定

[書式]

auth reauthentication
no auth reauthentication

[初期設定]

no auth reauthentication

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、サプリカントの再認証を有効にする。

no 形式で実行した場合は、再認証を無効にする。

本設定を有効にした場合は、認証に成功したサプリカントを定期的に再認証する。

再認証の間隔は、**auth timeout reauth-period** コマンドで変更できる。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

IEEE 802.1X 認証時は、再認証のタイミングになると、サプリカントに EAPOL パケットを送信して ユーザー情報を再取得し、RADIUS サーバーに認証要求を行う。

MAC 認証時は、再認証のタイミングになると、サプリカントの MAC アドレスをユーザー名、および、パスワードと見なして RADIUS サーバーに認証要求を行う。

Web 認証時は、再認証のタイミングになると、サプリカントの認証状態を未認証に遷移させる。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド、**auth-mac enable** コマンド、**auth-web enable** コマンド)

[設定例]

LAN ポート #1 の再認証を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth reauthentication
```

5.3.14 ダイナミック VLAN の設定

[書式]

auth dynamic-vlan-creation
no auth dynamic-vlan-creation

[初期設定]

no auth dynamic-vlan-creation

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、ダイナミック VLAN を有効にする。

no 形式で実行した場合は、ダイナミック VLAN を無効にする。

ダイナミック VLAN が有効なインターフェースでは、RADIUS サーバーから指定された属性値 (Tunnel-Private-Group-ID)をもとに、所属 VLAN を動的に変更する。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

本コマンドの設定を変更すると、認証状態は初期状態に戻る。

マルチサプリカントモードでダイナミック VLAN を利用する場合、サプリカント単位で VLAN を指定することが可能。

マルチホストモードでダイナミック VLAN を利用する場合、2 番目以降のサプリカントは最初のサプリカントが適用した VLAN ID が適用される。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド、**auth-mac enable** コマンド、**auth-web enable** コマンド)

[設定例]

LAN ポート #1 でダイナミック VLAN を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth dynamic-vlan-creation
```

5.3.15 ゲスト VLAN の設定

[書式]

auth guest-vlan *vlan-id*
no auth guest-vlan

[パラメーター]

vlan-id : <1-4094>
ゲスト VLAN 用の VLAN ID

[初期設定]

no auth guest-vlan

[入力モード]

インターフェースモード

[説明]

対象インターフェースに接続されているサプリカントが未認証、あるいは、認証失敗のときに所属するゲスト VLAN を指定する。

no 形式で実行した場合は、ゲスト VLAN の設定を削除する。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

本コマンドの設定を変更すると、認証状態は初期状態に戻る。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド、**auth-mac enable** コマンド)

本コマンドは、Web 認証が有効なとき設定できません。

[設定例]

LAN ポート #1 でゲスト VLAN #10 を指定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth guest-vlan 10
```

5.3.16 認証失敗後の抑止期間の設定

[書式]

auth timeout quiet-period *time*
no auth timeout quiet-period

[パラメーター]

time : <1-65535>

認証失敗後、サプリカントとの通信を拒否する期間(秒)

[初期設定]

auth timeout quiet-period 60

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、認証失敗後の認証抑止期間を設定する。

no 形式で実行した場合は、初期設定に戻る。

認証抑止期間中に受信したパケットはすべて破棄する。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド、**auth-mac enable** コマンド、**auth-web enable** コマンド)

[設定例]

LAN ポート #1 の抑止期間の設定を 300 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth timeout quiet-period 300
```

5.3.17 再認証間隔の設定

[書式]

auth timeout reauth-period *time*
no auth timeout reauth-period

[パラメーター]

time : <300-86400>

サプリカントの再認証間隔(秒)

[初期設定]

auth timeout reauth-period 3600

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、サプリカントの再認証間隔を設定する。

no 形式で実行した場合は、初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

本コマンドを使用するためには、対象インターフェースでポート認証機能、かつ、再認証機能を有効にする必要がある。 (**dot1x port-control** コマンド、**auth-mac enable** コマンド、**auth-web enable** コマンド、**auth reauthentication** コマンド)

[設定例]

LAN ポート #1 の再認証間隔の設定を 1200 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth timeout reauth-period 1200
```

5.3.18 RADIUS サーバー全体の応答待ち時間の設定

[書式]

auth timeout server-timeout *time*

no auth timeout server-timeout

[パラメーター]

time : <1-65535>

認証要求に対する認証サーバーからの応答待ち時間(秒)

[初期設定]

auth timeout server-timeout 30

[入力モード]

インターフェースモード

[説明]

対象インターフェースでポート認証を行うときの、RADIUS サーバー全体からの応答待ち時間を設定する。

no 形式で実行した場合は、初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

本設定値は、
(**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) 以上にする必要がある。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド、**auth-mac enable** コマンド、**auth-web enable** コマンド)

[設定例]

LAN ポート #1 の認証要求に対する RADIUS サーバー全体の応答待ち時間を 180 秒に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth timeout server-timeout 180
```

5.3.19 サプリカント応答待ち時間の設定

[書式]

auth timeout supp-timeout *time*

no auth timeout supp-timeout

[パラメーター]

time : <1-65535>

サプリカントからの応答待ち時間(秒)

[初期設定]

auth timeout supp-timeout 30

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、ポート認証を行うときのサプリカントからの応答待ち時間を設定する。

no 形式で実行した場合は、初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

本コマンドを使用するためには、対象インターフェースでポート認証機能を有効にする必要がある。 (**dot1x port-control** コマンド、**auth-mac enable** コマンド、**auth-web enable** コマンド)

[設定例]

LAN ポート #1 のサプリカントからの応答待ち時間を 180 秒に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth timeout supp-timeout 180
```

5.3.20 RADIUS サーバーホストの設定

[書式]

radius-server host *host* [auth-port *port*] [timeout *time*] [retransmit *count*] [key *secret*]

no radius-server host

[キーワード]

auth-port	:	RADIUS サーバーの認証用 UDP ポート番号を設定する
timeout	:	RADIUS サーバーへの要求に対する応答待機時間を設定する
retransmit	:	RADIUS サーバーへの要求再送回数を設定する
key	:	RADIUS サーバーとの通信時に使用するパスワードを設定する

[パラメーター]

host	:	IPv4 アドレス(A.B.C.D) または IPv6 アドレス(X:X::X:X) IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)
port	:	<0-65535> 認証用 UDP ポート番号(省略時は初期値の 1812 を使用する)
time	:	<1-1000> 応答待機時間(秒)(省略時は radius-server timeout コマンド設定(初期値 5 秒)に従う)
count	:	<0-100> 要求再送回数(省略時は radius-server retransmit コマンド設定(初期値 3 回)に従う)
secret	:	半角英数字および、'?'、スペースを除く半角記号(128 文字以内) 共有パスワード(省略時は radius-server key コマンド設定に従う)

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

認証サーバーリストにサーバーを追加する。

最大エントリー数は 8 である。

no 形式でコマンドを実行した場合は、指定したサーバーを認証サーバーリストから削除する。

[ノート]

設定値は、(**radius-server timeout** コマンドの設定値) x (**radius-server retransmit** コマンドの設定値 + 1) x (RADIUS サーバー数) の値が、**auth timeout server-timeout** コマンドの設定値内になるように調整する必要がある。

LLDP 自動設定機能で設定された **radius-server host** コマンドの末尾には、一時的な設定であることを表す"dynamic"オプションが付与される。 "dynamic"オプションが付与されている場合、**write** コマンドを実行してもスタートアップコンフィグに保存されない。

[設定例]

IP アドレス 192.168.100.100、応答待機時間 10 秒、要求再送回数 5 回として認証サーバーリストに追加する。

```
SWP2(config)#radius-server host 192.168.100.100 timeout 10 retransmit 5
```

IP アドレス 192.168.100.101、認証用 UDP ポート 1645、共有パスワード"abcde"を認証サーバーリストに追加する。

```
SWP2(config)#radius-server host 192.168.100.101 auth-port 1645 key abcde
```

ローカル RADIUS サーバーを認証サーバーリストに追加する。

```
SWP2(config)#radius-server host 127.0.0.1 key secret_local
```

5.3.21 RADIUS サーバー 1 台あたりの応答待ち時間の設定

[書式]

radius-server timeout *time*
no radius-server timeout

[パラメーター]

time : <1-1000>
要求応答待機時間(秒)

[初期設定]

radius-server timeout 5

[入力モード]

グローバルコンフィグレーションモード

[説明]

RADIUS サーバー 1 台あたりの応答待ち時間を設定する。

no 形式でコマンドを実行した場合は、初期設定に戻る。

[ノート]

radius-server host コマンドでサーバー固有の要求応答待機時間が設定されている場合、 **radius-server host** コマンドの設定に従う。

設定値は、
(**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) の値が、**auth timeout server-timeout** コマンドの設定値内になるように調整する必要がある。

[設定例]

RADIUS サーバー 1 台あたりの応答待ち時間を 10 秒に設定する。

```
SWP2(config)#radius-server timeout 10
```

5.3.22 RADIUS サーバーへの要求再送回数の設定

[書式]

radius-server retransmit *count*
no radius-server retransmit

[パラメーター]

count : <0-100>

要求再送回数

[初期設定]

radius-server retransmit 3

[入力モード]

グローバルコンフィグレーションモード

[説明]

RADIUS サーバーへの要求再送回数を設定する。

no 形式でコマンドを実行した場合は、初期設定に戻る。

[ノート]

radius-server host コマンドでサーバー固有の要求再送回数が設定されている場合、 **radius-server host** コマンドの設定に従う。

[設定例]

RADIUS サーバーへの要求再送回数を 5 回に設定する。

```
SWP2(config)#radius-server retransmit 5
```

5.3.23 RADIUS サーバー共有パスワードの設定

[書式]

radius-server key *secret*
no radius-server key

[パラメーター]

secret : 共有パスワード

半角英数字および、'?'、スペースを除く半角記号(128 文字以内)

[初期設定]

no radius-server key

[入力モード]

グローバルコンフィグレーションモード

[説明]

RADIUS サーバーとの通信時に使用する共有パスワードを設定する。

no 形式でコマンドを実行した場合は、初期設定に戻る。

[ノート]

radius-server host コマンドでサーバー固有の共有パスワードが設定されている場合、 **radius-server host** コマンドの設定に従う。

[設定例]

RADIUS サーバーとの共有パスワードとして"abcde"を設定する。

```
SWP2(config)#radius-server key abcde
```

5.3.24 RADIUS サーバー使用抑制時間の設定

[書式]

radius-server deadtime *time*
no radius-server deadtime

[パラメーター]

time : <0-1440>

RADIUS サーバーの使用抑制時間(分)

[初期設定]

radius-server deadtime 0

[入力モード]

グローバルコンフィグレーションモード

[説明]

RADIUS サーバーへの要求がタイムアウトしたとき、該当サーバーの使用を抑制する時間を設定する。

no 形式でコマンドを実行した場合は、初期設定に戻る。

[設定例]

RADIUS サーバー使用抑制時間を 1 分に設定する。

```
SWP2(config)#radius-server deadtime 1
```

5.3.25 RADIUS サーバーに通知する NAS-Identifier 属性の設定

[書式]

auth radius attribute nas-identifier *line*
no auth radius attribute nas-identifier

[パラメーター]

line : 識別文字(253 文字以内)
NAS-Identifier 属性として設定する任意の文字列

[初期設定]

no auth radius attribute nas-identifier

[入力モード]

グローバルコンフィグレーションモード

[説明]

ポート認証機能において、RADIUS サーバーに NAS-Identifier 属性として通知する任意の文字列を設定する。

本設定をした場合は、RADIUS サーバーに NAS-Identifier 属性として通知し、設定を削除した場合は通知を停止する。

no 形式でコマンドを実行した場合は、初期設定に戻る。

[設定例]

RADIUS サーバーに通知する NAS-Identifier 属性に「Nas-ID-001」をセットする。

```
SWP2(config)#auth radius attribute nas-identifier Nas-ID-001
```

5.3.26 RADIUS サーバー無応答時の認証の設定

[書式]

auth no-response-authorized
no auth no-response-authorized

[初期設定]

no auth no-response-authorized

[入力モード]

グローバルコンフィグレーションモード

[説明]

RADIUS サーバー無応答時に、認証成功したものとして動作する。

IEEE802.1X 認証、MAC 認証、WEB 認証の各認証において、RADIUS サーバーからの応答がなくタイムアウトした場合、それぞれの認証方式で認証成功したものとして動作する。

なお、本コマンドを使用する場合は、**auth reauthentication** コマンドと **auth timeout reauth-period** コマンドで再認証の設定を行うこと。

再認証の間隔を適切に設定することで、一時的に認証許可された状態を限定的にすることができる。

[ノート]

セキュリティ上の問題となる恐れがあるため、本コマンドを使用する際はセキュリティーポリシーを十分に検討すること。

本コマンドが有効かつ RADIUS サーバーが無応答と判定したときは、以下の動作となる。

- RADIUS サーバーからの応答がタイムアウトしたときの認証方式にしたがって認証を許可する
- IEEE802.1X 認証では、サプリカントの仕様などによって正常に動作しない場合がある
- RADIUS サーバーが複数設定されている場合、すべての RADIUS サーバーからの応答が無かった場合にのみ、認証成功とする
- ダイナミック VLAN を使用している場合であっても、ポートに設定されている VLAN で動作する
- すべてのサプリカントを認証許可にするため、ゲスト VLAN は動作しない
- RADIUS サーバーホストの設定がない場合は、本コマンドが設定されていても認証成功にはならない

[設定例]

RADIUS サーバー無応答時に認証を成功にする。

```
SWP2(config)#auth no-response-authorized
```

5.3.27 ポート認証情報の表示

[書式]

show auth status [interface *ifname*]

[キーワード]

interface	:	特定のインターフェースの情報のみを表示する

[パラメーター]

ifname	:	インターフェース名 表示するインターフェース

[入力モード]

非特権 EXEC モード、 特権 EXEC モード

[説明]

ポート認証機能の設定状態、および現在の認証状態を表示する。

[設定例]

ポート認証情報を表示する。

```
SWP2#show auth status
[System information]
  802.1X Port-Based Authentication : Enabled
  MAC-Based Authentication         : Disabled
  WEB-Based Authentication         : Enabled

  Clear-state time : Not configured

  Redirect URL :
    Not configured

  Auth-web custom-file :
    There is no custom-file

  RADIUS server address :
    192.168.100.101 (port:1812)

[Interface information]
  Interface port1.1 (up)
    802.1X Authentication   : Auto (configured:auto)
    MAC Authentication      : Disabled (configured:disable)
    WEB Authentication      : Disabled (configured:disable)
    Host mode               : Single-host
    Dynamic VLAN creation   : Disabled
    Guest VLAN              : Disabled
    Reauthentication        : Disabled
    Reauthentication period : 60 sec
    MAX request             : 2 times
    Supplicant timeout      : 30 sec
    Quiet period            : 60 sec
    Controlled directions   : Both (configured:both)
    Protocol version        : 2
    Clear-state time        : Not configured
```

```
    Authentication status    : Authorized

  Interface port1.4 (down)
    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
```

5.3.28 サプリカント情報の表示

[書式]

show auth supplicant [interface *ifname*]

[キーワード]

interface : 特定のインターフェースの情報のみを表示する

[パラメーター]

ifname : インターフェース名
表示するインターフェース

[入力モード]

特権 EXEC モード

[説明]

ポート認証におけるサプリカント情報を表示する。

[設定例]

LAN ポート #1 のサプリカント情報を表示する。

```
SWP2#show auth supplicant interface port1.1
Port     MAC address       User name         Status          VLAN Method
-------- ----------------- ----------------- --------------- ---- ------
port1.1  0011.2233.4455    user              Authorized         1 802.1X
```

5.3.29 統計情報の表示

[書式]

show auth statistics [interface *ifname*]

[キーワード]

interface : 特定のインターフェースの統計情報のみを表示する

[パラメーター]

ifname : インターフェース名
表示するインターフェース

[入力モード]

非特権 EXEC モード、 特権 EXEC モード

[説明]

ポート認証におけるパケットの統計情報を表示する。

[設定例]

LAN ポート #1 の統計情報を表示する。

```
SWP2#show auth statistics interface port1.1
Interface port1.1
  EAPOL frames:
    Received frames      : 11
      EAPOL Start        : 1
      EAPOL Logoff       : 0
      EAP Response ID    : 1
      EAP Response       : 9
      Invalid EAPOL      : 0
      EAP Length error   : 0
      Last EAPOL version : 1
      Last EAPOL source  : 0011.2233.4455
    Transmitted frames   : 11
      EAP Request ID     : 1
      EAP Request        : 9
      EAP Success        : 1
      EAP Fail           : 0

  RADIUS packets:
    Received packets     : 10
      Access Request     : 0
      Access Challenge   : 9
      Access Accept      : 1
      Access Reject      : 0
    Transmitted packets  : 10
      Access Request     : 10
```

5.3.30 統計情報のクリア

[書式]

clear auth statistics [interface *ifname*]

[キーワード]

interface : 特定のインターフェースの統計情報のみをクリアする

[パラメーター]

ifname : インターフェース名
表示するインターフェース

[入力モード]

特権 EXEC モード

[説明]

ポート認証におけるパケットの統計情報をクリアする。

[設定例]

LAN ポート #1 の統計情報をクリアする。

```
SWP2#clear auth statistics interface port1.1
```

5.3.31 RADIUS サーバー設定情報の表示

[書式]

show radius-server

[入力モード]

特権 EXEC モード

[説明]

RADIUS サーバーに関する設定情報を表示する。

認証サーバーリストに登録してある RADIUS サーバーの設定情報(サーバーホスト、認証用 UDP ポート番号、 共有パスワード、要求応答待機時間、要求再送回数、サーバー使用抑制時間)を表示する。

[設定例]

RADIUS サーバーに関する設定情報を表示する。

```
SWP2#show radius-server
Server Host : 192.168.100.101
```

```
  Authentication Port : 1812
  Secret Key          : abcde
  Timeout             : 10 sec
  Retransmit Count    : 5
  Deadtime            : 0 min

Server Host : 192.168.100.102
  Authentication Port : 1645
  Secret Key          : fghij
  Timeout             : 5 sec
  Retransmit Count    : 3
  Deadtime            : 0 min
```

5.3.32 Web 認証成功後のリダイレクト先 URL の設定

[書式]

auth-web redirect-url *url*
no auth-web redirect-url

[パラメーター]

url	:	半角英数字および半角記号（最大 256 文字） リダイレクト先の URL

[初期設定]

no auth-web redirect-url

[入力モード]

グローバルコンフィグレーションモード

[説明]

Web 認証成功後にリダイレクトする URL を指定する。

no 形式で実行した場合は認証後のリダイレクト機能を無効にする。

[ノート]

"?"を含んだ URL を指定することはできません。

[設定例]

Web 認証成功後のリダイレクト先に http://192.168.100.200 を指定する。

```
SWP2(config)#auth-web redirect-url http://192.168.100.200
```

5.3.33 認証状態のクリア

[書式]

clear auth state [all] [interface *ifname*] [supplicant *mac-addr*]

[キーワード]

all	:	全てのサプリカントの認証状態をクリアする
interface	:	特定のインターフェースに接続されているサプリカントの認証状態をクリアする
supplicant	:	特定のサプリカントの認証状態をクリアする

[パラメーター]

ifname	:	インターフェース名 クリアするインターフェース
mac-addr	:	hhhh.hhhh.hhhh (h は 16 進数) 対象の MAC アドレス

[入力モード]

特権 EXEC モード

[説明]

サプリカントの認証状態をクリアする。

[設定例]

LAN ポート #1 に接続されているサプリカントの認証状態をクリアする。

```
SWP2#clear auth state interface port1.1
```

5.3.34 認証状態のクリアする時刻の設定(システム)

[書式]

auth clear-state time *time*
no auth clear-state time

[パラメーター]

time : <0-23>
認証状態をクリアする時刻

[初期設定]

no auth clear-state time

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体にサプリカントの認証状態をクリアする時刻を設定する。

no 形式で実行した場合は、認証状態をクリアする時刻の設定を削除する。

[ノート]

インターフェースに認証状態をクリアする時刻が設定されている場合、 インターフェースに設定された時刻で認証状態のクリアを行う。

[設定例]

システム全体でサプリカントの認証状態をクリアする時刻を 12 時に設定する。

```
SWP2(config)#auth clear-state time 12
```

5.3.35 認証状態のクリアする時刻の設定(インターフェース)

[書式]

auth clear-state time *time*
no auth clear-state time

[パラメーター]

time : <0-23>
認証状態をクリアする時刻

[初期設定]

no auth clear-state time

[入力モード]

インターフェースモード

[説明]

対象インターフェイスにサプリカントの認証状態をクリアする時刻を設定する。

no 形式で実行した場合は、認証状態をクリアする時刻の設定を削除する。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

対象インターフェイスではシステム全体に認証状態をクリアする時刻が設定されていても、 本コマンドで設定された時刻で認証状態のクリアを行う。

[設定例]

LAN ポート #1 に接続されたサプリカントの認証状態をクリアする時刻を 12 時に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#auth clear-state time 12
```

5.3.36 EAP パススルーの設定

[書式]

pass-through eap *switch*
no pass-through eap

[パラメーター]

switch : EAP パススルーの動作

設定値	説明
enable	EAP パススルーを有効にする
disable	EAP パススルーを無効にする

[初期設定]

pass-through eap enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

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。

disable を指定した場合は、EAP フレームを破棄する。

no 形式で実行した場合、または、enable を指定した場合は、EAPOL フレームを転送する。

[ノート]

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ない。

[設定例]

EAP パススルーを無効にする。

```
SWP2(config)#pass-through eap disable
```

5.4 ポートセキュリティー

5.4.1 ポートセキュリティー機能の設定

[書式]

port-security enable
port-security disable
no port-security

[キーワード]

enable : ポートセキュリティー機能を有効にする

disable : ポートセキュリティー機能を無効にする

[初期設定]

port-security disable

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、ポートセキュリティー機能を有効にする。

no 形式で実行した場合、または、disable を指定した場合は、対象インターフェースでポートセキュリティー機能を無効にする。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

ポートセキュリティー機能を有効にした時点で、登録されていない端末は破棄される。

[設定例]

LAN ポート #1 のポートセキュリティー機能を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#port-security enable
```

5.4.2 許可 MAC アドレス登録

[書式]

port-security mac-address *mac-addr action ifname* vlan *vlan-id*
no port-security mac-address *mac-addr action ifname* vlan *vlan-id*

[キーワード]

vlan : VLAN ID を指定

[パラメーター]

mac-addr : hhhh.hhhh.hhhh (h は 16 進数)
対象の MAC アドレス

action : mac-addr 宛のフレームに対する動作

設定値	説明
forward	転送する

ifname : LAN/SFP+ポートまたは論理インターフェース
対象のインターフェース名

vlan-id : <1-4094>
対象の VLAN ID

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

ポートセキュリティーを有効にしたポートで通信を許可する MAC アドレスを登録する。

no 形式で実行した場合は、登録を削除する。

[設定例]

MAC アドレス 00:A0:DE:00:00:01 を、LAN ポート #1 の許可アドレスとして登録する。

```
SWP2(config)#port-security mac-address 00a0.de00.0001 forward port1.1 vlan 1
```

5.4.3 セキュリティー違反時の動作の設定

[書式]

port-security violation *action*
no port-security violation

[パラメーター]

action : ポートセキュリティー違反時の動作

動作モード	説明
discard	パケット破棄
shutdown	ポートをシャットダウン

[初期設定]

port-security violation discard

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して、ポートセキュリティー違反時の動作アクションを設定する。

no 形式で実行した場合は、初期設定に戻る。

[ノート]

shutdown モードでシャットダウンされたポートを復旧させる場合は、no shutdown コマンドを用いる。

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

[設定例]

LAN ポート #1 の違反時の動作をポートダウンに変更する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#port-security violation shutdown
```

5.4.4 ポートセキュリティー情報の表示

[書式]

show port-security status

[入力モード]

特権 EXEC モード

[説明]

ポートセキュリティー情報を表示する。

[設定例]

ポートセキュリティー情報を表示する。

```
SWP2#show port-security status
 Port     Security  Action    Status    Last violation
 -------- --------- --------- --------- -----------------
 port1.1  Enabled   Discard   Blocking  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
```

5.5 エラー検出機能

5.5.1 errdisable 状態からの自動復旧機能の設定

[書式]

errdisable auto-recovery *function* [interval *interval*]

no errdisable auto-recovery *function*

[キーワード]

interval : 自動復旧時間の設定

[パラメーター]

function : errdisable の原因となる機能

設定値	説明
bpduguard	BPDU ガード機能
loop-detect	ループ検出機能

interval : <10-1000000>

自動復旧するまでの時間(秒)

[初期設定]

no errdisable auto-recovery bpduguard (BPDU ガード機能)

errdisable auto-recovery loop-detect interval 300 (ループ検出機能)

[入力モード]

グローバルコンフィグレーションモード

[説明]

エラー検出機能によって errdisable 状態になったときに自動的に復旧する機能を有効にして、自動復旧するまでの時間を設定する。

interval を省略した場合は、300 秒が設定される。

no 形式で実行した場合は、自動復旧機能が無効となる。

[ノート]

本コマンドを実行する前に BPDU ガード機能によって errdisable 状態になった LAN/SFP+ポートでは、次回 BPDU を検出したときに設定の変更が反映される。

[設定例]

BPDU ガードで errdisable 状態になったときの自動復旧を有効にし、復旧時間を 600 秒にする。

```
SWP2(config)#errdisable auto-recovery bpduguard interval 600
```

ループ検出で errdisable 状態になったときの自動復旧を無効にする。

```
SWP2(config)#no errdisable auto-recovery loop-detect
```

5.5.2 エラー検出機能の情報表示

[書式]

show errdisable

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

エラー検出機能の情報を表示する。

以下の項目が表示される。

- errdisable 状態からの自動復旧が有効か否か
- errdisable 状態のインターフェースおよびエラーを検出した機能

[設定例]

エラー検出機能の情報を表示する。

```
SWP2>show errdisable

function         auto recovery          interval
-----------------------------------------------
BPDU guard       disable
Loop detect      enable                      300
Port-security    disable

port             reason
---------------------------
port1.1          BPDU guard
port1.7          Loop detect
sa1              Loop detect
```

第 6 章

Layer 2 機能

6.1 FDB(フォワーディングデータベース)

6.1.1 MAC アドレス学習機能の設定

[書式]

mac-address-table learning enable
mac-address-table learning disable
no mac-address-table learning

[キーワード]

enable	:	MAC アドレス学習機能を有効にする
disable	:	MAC アドレス学習機能を無効にする

[初期設定]

mac-address-table learning enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

MAC アドレス学習機能の有効/無効を設定する。

no 形式で実行すると、MAC アドレス学習機能機能が有効となる。

[ノート]

MAC アドレス学習機能が無効な場合は、フレームを受信しても MAC アドレステーブルにダイナミックエントリーが登録されない。

[設定例]

MAC アドレス学習機能を有効にする。

```
SWP2(config)#mac-address-table learning enable
```

6.1.2 ダイナミックエントリーのエージングタイム設定

[書式]

mac-address-table ageing-time *time*
no mac-address-table ageing-time

[パラメーター]

time	:	<10-400>
		エージングタイム(秒)

[初期設定]

mac-address-table ageing-time 300

[入力モード]

グローバルコンフィグレーションモード

[説明]

ダイナミックエントリーのエージングタイムを設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドで設定した時間と、実際にダイナミックエントリーが MAC アドレステーブルから削除されるまでの時間との間で、誤差が生じる場合がある。

[設定例]

ダイナミックエントリーのエージングタイムを 400 秒にする。

```
SWP2(config)#mac-address-table ageing-time 400
```

6.1.3 ダイナミックエントリーの削除

[書式]

clear mac-address-table dynamic
clear mac-address-table dynamic address *mac-addr*
clear mac-address-table dynamic vlan *vlan-id*
clear mac-address-table dynamic interface *ifname* [instance *inst*]

[キーワード]

address	:	MAC アドレスを指定する
vlan	:	VLAN ID を指定する
interface	:	インターフェースを指定する
instance	:	MST インスタンスを指定する

[パラメーター]

mac-addr	:	hhhh.hhhh.hhhh (h は 16 進数)
		対象の MAC アドレス
ifname	:	LAN/SFP+ポートまたは論理インターフェースの名前
		対象のインターフェース
vlan-id	:	<1-4094>
		対象の VLAN ID
inst	:	<1-63>
		対象の MST インスタンス ID

[入力モード]

特権 EXEC モード

[説明]

MAC アドレステーブルからダイナミックエントリーを削除する。
キーワードを指定した場合は、対象条件に一致したエントリーのみを削除する。
キーワードを指定しない場合は、全てのダイナミックエントリーを削除する。

[設定例]

MAC アドレスが 00a0.de11.2233 のダイナミックエントリーを削除する。

```
SWP2#clear mac-address-table dynamic address 00a0.de11.2233
```

6.1.4 スタティックエントリーの設定

[書式]

mac-address-table static *mac-addr action ifname* [vlan *vlan-id*]
no mac-address-table static *mac-addr action ifname* [vlan *vlan-id*]

[キーワード]

vlan	:	VLAN ID を指定する

[パラメーター]

mac-addr	:	hhhh.hhhh.hhhh (h は 16 進数)
		対象の MAC アドレス
action	:	mac-addr 宛のフレームに対する動作

設定値	説明
forward	転送する
discard	破棄する

ifname : LAN/SFP+ポートまたは論理インターフェースの名前
対象のインターフェース

vlan-id : <1-4094>
対象の VLAN ID

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

MAC アドレステーブルにスタティックエントリーを登録する。

action に forward を設定した場合は、設定した MAC アドレスおよび VLAN ID に一致した受信フレームを、設定したインターフェースに転送する。
action に discard を設定した場合は、設定した MAC アドレスおよび VLAN ID に一致した受信フレームを、破棄する。

no 形式で実行した場合は、MAC アドレステーブルからスタティックエントリーを削除する。

vlan を省略した場合は、VLAN #1 が設定される。

[ノート]

action に discard を設定した場合は、*mac-addr* にマルチキャスト MAC アドレスを指定することはできない。

mac-addr に以下の MAC アドレスを指定することはできない。

- 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

[設定例]

00a0.de11.2233 宛のフレームを LAN ポート #2 に転送するよう登録する。

```
SWP2(config)#mac-address-table static 00a0.de11.2233 forward port1.2
```

6.1.5 MAC アドレステーブルの表示

[書式]

show mac-address-table

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

MAC アドレステーブルを表示する。

以下の項目が表示される。

- VLAN ID
- インターフェース名
- MAC アドレス
- フレームに対する動作
- エントリーの種類
- エージングタイム

[設定例]

MAC アドレステーブルを表示する。

```
SWP2>show mac-address-table
VLAN  port      mac             fwd      type     timeout
   1  port1.1   00a0.de11.2233  forward  static         0
   1  sa1       1803.731e.8c2b  forward  dynamic      300
   1  sa2       782b.cbcb.218d  forward  dynamic      300
```

6.1.6 MAC アドレス数の表示

[書式]

show mac-address-table count
show mac-address-table count interface *ifname*
show mac-address-table count vlan *vlan-id*

[キーワード]

interface	:	特定のインターフェースの MAC アドレス数のみ表示する
vlan	:	特定の VLAN の MAC アドレス数のみ表示する

[パラメーター]

ifname	:	表示するインターフェースの名前 LAN/SFP+ポートまたは論理インターフェースのみ指定可能
vlan-id	:	<1-4094> 表示する VLAN ID

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

FDB エントリに登録されている MAC アドレス数を表示する。

自動学習により登録されたダイナミックアドレス、および、手動登録されたスタティックアドレスの登録数が表示される。

[設定例]

FDB エントリに登録されている MAC アドレス数を表示する。

```
SWP2>show mac-address-table count
 MAC Entries for all vlans
  Dynamic Address   : 20
  Static Address    : 10
  Total MAC Address : 30
```

6.2 VLAN

6.2.1 VLAN モードへの移行

[書式]

vlan database

[入力モード]

グローバルコンフィグレーションモード

[説明]

VLAN インターフェースの設定を行うための VLAN モードに移行する。

[ノート]

VLAN モードからグローバルコンフィグレーションモードに戻るには **exit** コマンドを使用し、特権 EXEC モードに戻るには **end** コマンドを使用する。

[設定例]

VLAN モードに移行する。

```
SWP2(config)#vlan database
SWP2(config-vlan)#
```

6.2.2 VLAN インターフェースの設定

[書式]

vlan *vlan-id* [name *name*] [state *state*]
no vlan *vlan-id*

[キーワード]

name	:	VLAN の名前を指定する
state	:	VLAN の状態を指定する

[パラメーター]

vlan-id	:	<2-4094> VLAN ID
name	:	半角英数字および半角記号(32 文字以内) VLAN の名前
state	:	フレームの転送を行うか否かの状態

設定値	説明
enable	フレームを転送する
disable	フレームを転送しない

[初期設定]

なし

[入力モード]

VLAN モード

[説明]

VLAN インターフェースを設定する。

no 形式で実行した場合は、VLAN インターフェースを削除する。

name を省略した場合は、VLAN の名前に"VLANxxxx"(xxxx は 4 桁の VLAN ID)が自動的に設定される。

state を省略した場合は、enable が設定される。

disable を指定した場合は、当該 VLAN インターフェースへの設定は全て削除される。

[ノート]

既に *name* が設定されている VLAN ID に対して、name を省略して本コマンドを設定した場合は、既に設定されている *name* のまま変更されない。

vlan-id には複数の VLAN ID を指定することができ、以下のように、"-" や ","を使用する。

- VLAN #2 から VLAN #4 までを選択する場合 : 2-4
- VLAN #2 と VLAN #4 を選択する場合 : 2,4

ただし、複数の VLAN ID を指定した場合は、name を指定することができない。

[設定例]

VLAN #1000 を Sales という名前で設定する。

```
SWP2(config-vlan)#vlan 1000 name Sales
```

6.2.3 プライベート VLAN の設定

[書式]

private-vlan *vlan-id type*
no private-vlan *vlan-id type*

[パラメーター]

vlan-id : <2-4094>

vlan コマンドで設定されている VLAN ID

type : プライベート VLAN の種別

設定値	説明
primary	プライマリー VLAN
community	セカンダリー VLAN(コミュニティー VLAN)
isolated	セカンダリー VLAN(アイソレート VLAN)

[初期設定]

なし

[入力モード]

VLAN モード

[説明]

vlan-id をプライベート VLAN として使用する。

no 形式で実行した場合は、プライベート VLAN の設定が削除されて、通常の VLAN として使用する。

[ノート]

コミュニティー VLAN として設定すると、プライマリー VLAN のプロミスカスポートおよび同じコミュニティー VLAN に所属する他のインターフェースとは通信できるが、他のコミュニティー VLAN およびアイソレート VLAN に所属するインターフェースとは通信できなくなる。

アイソレート VLAN として設定すると、プライマリー VLAN のプロミスカスポートとのみ通信することができるが、コミュニティー VLAN およびアイソレート VLAN に所属する他のインターフェースとは通信できなくなる。

[設定例]

以下のプライベート VLAN を設定する。

- VLAN #100 : プライマリー VLAN
- VLAN #101 : セカンダリー VLAN(コミュニティー VLAN)
- VLAN #102 : セカンダリー VLAN(コミュニティー VLAN)
- VLAN #103 : セカンダリー VLAN(アイソレート VLAN)

```
SWP2(config-vlan)#vlan 100
SWP2(config-vlan)#vlan 101
SWP2(config-vlan)#vlan 102
SWP2(config-vlan)#vlan 103
SWP2(config-vlan)#private-vlan 100 primary
SWP2(config-vlan)#private-vlan 101 community
SWP2(config-vlan)#private-vlan 102 community
SWP2(config-vlan)#private-vlan 103 isolated
```

6.2.4 プライマリー VLAN に対するセカンダリー VLAN の設定

[書式]

private-vlan *vlan-id* **association** add *2nd-vlan-ids*
private-vlan *vlan-id* **association** remove *2nd-vlan-ids*
no private-vlan *vlan-id* **association**

[キーワード]

add : 指定した VLAN を関連付ける

remove : 指定した VLAN の関連付けを削除する

[パラメーター]

vlan-id : <2-4094>

プライマリー VLAN に設定されている VLAN ID

2nd-vlan-ids : <2-4094>

セカンダリー VLAN に設定されている VLAN ID

複数指定する場合、以下のように、"-" や ","を使用すること

- VLAN #2 から VLAN #4 までを選択する場合: 2-4
- VLAN #2 と VLAN #4 を選択する場合: 2,4

[初期設定]

なし

[入力モード]

VLAN モード

[説明]

プライベート VLAN のプライマリー VLAN に対して、セカンダリー VLAN(アイソレート VLAN、コミュニティー VLAN)の関連付けを設定する。

add を指定することで *vlan-id* と *2nd-vlan-ids* の関連付けを設定する。

remove を指定することで *vlan-id* と *2nd-vlan-ids* の関連付けを削除する。

no 形式で実行した場合は、プライマリー VLAN への関連付けをすべて削除する。

[設定例]

以下のプライベート VLAN を設定したのち、プライマリー VLAN に対してセカンダリー VLAN を関連付ける。

- VLAN #100 : プライマリー VLAN
- VLAN #101 : セカンダリー VLAN(コミュニティー VLAN)
- VLAN #102 : セカンダリー VLAN(コミュニティー VLAN)
- VLAN #103 : セカンダリー VLAN(アイソレート VLAN)

```
SWP2(config-vlan)#vlan 100
SWP2(config-vlan)#vlan 101
SWP2(config-vlan)#vlan 102
SWP2(config-vlan)#vlan 103
SWP2(config-vlan)#private-vlan 100 primary
SWP2(config-vlan)#private-vlan 101 community
SWP2(config-vlan)#private-vlan 102 community
SWP2(config-vlan)#private-vlan 103 isolated
SWP2(config-vlan)#private-vlan 100 association add 101
SWP2(config-vlan)#private-vlan 100 association add 102
SWP2(config-vlan)#private-vlan 100 association add 103
```

6.2.5 アクセスポート(タグなしポート)の設定

[書式]

switchport mode access

[初期設定]

switchport mode access

[入力モード]

インターフェースモード

[説明]

対象インターフェースのポート種別をアクセスポートに設定する。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースを対象として本コマンドを設定した場合は、そのインターフェースに所属する全ての LAN/SFP+ポートの設定が変更される。

ポート種別をトランクポートからアクセスポートに変更した場合は、**switchport trunk allowed vlan** コマンドの設定および **switchport trunk native vlan** コマンドの設定が初期設定に戻る。

アクセスポートとして所属する VLAN ID は、**switchport access vlan** コマンドで設定する。

[設定例]

LAN ポート #1 をアクセスポートに設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode access
```

6.2.6 アクセスポート(タグなしポート)の所属 VLAN の設定

[書式]

switchport access vlan *vlan-id*

no switchport access vlan

[パラメーター]

vlan-id : <1-4094>

所属する VLAN ID

[初期設定]

switchport access vlan 1

[入力モード]

インターフェースモード

[説明]

対象インターフェースがアクセスポートとして所属する VLAN ID を設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは **switchport mode access** コマンドが設定されている LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースを対象として本コマンドを設定した場合は、そのインターフェースに所属する全ての LAN/SFP+ポートの設定が変更される。

ポート種別をトランクポートに変更した場合は、本コマンドの設定が初期設定に戻る。

[設定例]

LAN ポート #1 がアクセスポートとして所属する VLAN を VLAN #10 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport access vlan 10
```

6.2.7 トランクポート(タグ付きポート)の設定

[書式]

switchport mode trunk [ingress-filter *action*]

[キーワード]

ingress-filter : 入力フィルターの動作を指定する

[パラメーター]

action : 入力フィルターの動作

設定値	説明
enable	入力フィルターを有効にする
disable	入力フィルターを無効にする

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースのポート種別をトランクポートに設定する。

ingress-filter を省略した場合は、enable が設定される。

入力フィルターが有効な場合は、受信フレームの VLAN ID がインターフェースの所属している VLAN ID と一致したときのみ、フレームを転送する。

入力フィルターが無効な場合は、すべてのフレームを転送する。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースを対象として本コマンドを設定した場合は、そのインターフェースに所属する全ての LAN/SFP+ポートの設定が変更される。

ポート種別をアクセスポートからトランクポートに変更した場合は、**switchport access vlan** コマンドの設定が初期設定に戻る。

トランクポートとして所属する VLAN ID は、**switchport trunk allowed vlan** コマンドで設定する。また、ネイティブ VLAN の設定は **switchport trunk native vlan** コマンドで設定する。

[設定例]

LAN ポート #1 をトランクポートに設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode trunk
```

6.2.8 トランクポート(タグ付きポート)の所属 VLAN の設定

[書式]

switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add *vlan-ids*
switchport trunk allowed vlan except *vlan-ids*
switchport trunk allowed vlan remove *vlan-ids*
no switchport trunk

[キーワード]

all	:	vlan コマンドで設定されているすべての VLAN に所属させる
none	:	全ての VLAN から脱退させる
add	:	指定した VLAN に所属させる
except	:	指定した VLAN 以外の、vlan コマンドで設定されているすべての VLAN に所属させる
remove	:	指定した VLAN から脱退させる

[パラメーター]

vlan-ids : <1-4094>

vlan コマンドで設定されている VLAN ID

複数指定する場合、以下のように、"-" や ","を使用すること

- VLAN #2 から VLAN #4 までを選択する場合: 2-4
- VLAN #2 と VLAN #4 を選択する場合: 2,4

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースがトランクポートとして所属する VLAN ID を設定する。

no 形式で実行した場合、所属する VLAN ID がすべて削除されてポート種別がアクセスポートに変更される。

[ノート]

本コマンドは **switchport mode trunk** コマンドが設定されている LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースを対象として本コマンドを設定した場合は、そのインターフェースに所属する全ての LAN/SFP+ポートの設定が変更される。

ポート種別をアクセスポートに変更した場合は、本コマンドの設定が初期設定に戻る。

all または except を指定して設定した場合は、その後に変更した **vlan** コマンドの内容が常に反映される。

all または except を指定して設定した場合は、以下の設定を行うと、残りの所属している VLAN ID を add で指定した設定に変更される。

- remove を指定して所属している VLAN ID を削除した場合
- **switchport trunk native vlan** コマンドで所属している VLAN ID を指定した場合

except を指定して設定を行った後、add を指定して除外していた VLAN ID に所属させた場合は、所属している VLAN ID を add で指定した設定に変更される。

remove を指定した後に所属していない VLAN ID を指定するとエラーになる。

本コマンドと **switchport trunk native vlan** コマンドの設定は、後着優先となる。

- 本コマンドで所属させた VLAN ID を指定して **switchport trunk native vlan** コマンドを設定した場合、指定した VLAN ID から脱退させられる。
- **switchport trunk native vlan** コマンドで設定されている VLAN ID を指定して所属させた場合、**switchport trunk native vlan none** が設定される。

switchport trunk allowed vlan add コマンドで、*vlan-ids* に"-"や","を組み合わせて指定した場合、古いバージョン(Rev.2.00.08 以前)に戻すとコマンド設定に失敗する。結果として、正常に通信できなくなる可能性がある。(設定例: switchport trunk allowed vlan add 101,103-105)

[設定例]

LAN ポート #1 をトランクポートに設定して VLAN #2 に所属させる。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode trunk
SWP2(config-if)#switchport trunk allowed vlan add 2
```

6.2.9 トランクポート(タグ付きポート)のネイティブ VLAN の設定

[書式]

switchport trunk native vlan *vlan-id*
switchport trunk native vlan none
no switchport trunk native vlan

[キーワード]

none	:	ネイティブ VLAN を無効にする

[パラメーター]

vlan-id	:	<1-4094>
		vlan コマンドで設定されている VLAN ID

[初期設定]

switchport trunk native vlan 1

[入力モード]

インターフェースモード

[説明]

対象インターフェースのネイティブ VLAN を設定する。

none を指定した場合は、ネイティブ VLAN が無効になる。これにより対象インターフェースでは、受信したタグなしフレームを破棄する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは **switchport mode trunk** コマンドが設定されている LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースを対象として本コマンドを設定した場合は、そのインターフェースに所属する全ての LAN/SFP+ポートの設定が変更される。

ポート種別をアクセスポートに変更した場合は、本コマンドの設定が初期設定に戻る。

本コマンドと **switchport trunk allowed vlan** コマンドの設定は、後着優先となる。

- **switchport trunk allowed vlan** コマンドで所属させた VLAN ID を指定して本コマンドを設定した場合、指定した VLAN ID から脱退させられる。
- 本コマンドで設定した VLAN ID を **switchport trunk allowed vlan** コマンドで所属させた場合、**switchport trunk native vlan none** が設定される。

[設定例]

LAN ポート #1 をトランクポートに設定してネイティブ VLAN に VLAN #2 を設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode trunk
SWP2(config-if)#switchport trunk native vlan 2
```

6.2.10 プライベート VLAN のポート種別の設定

[書式]

switchport mode private-vlan *port-type*
no switchport mode private-vlan *port-type*

[パラメーター]

port-type : ポートの動作

設定値	説明
promiscuous	プロミスカスポート
host	ホストポート

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースのプライベート VLAN のポート種別を設定する。

no 形式で実行した場合、対象インターフェースに設定されているプライベート VLAN の設定を削除する。

[ノート]

本コマンドは **switchport mode access** コマンドが設定されている LAN/SFP+ポートにのみ設定可能。

加えて、以下のインターフェースで promiscuous を設定できる。

- トランクポートとして動作しているインターフェース
- 論理インターフェース

[設定例]

LAN ポート #1 をプロミスカスポート、LAN ポート #2 をホストポートに設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport mode private-vlan promiscuous
SWP2(config-if)#exit
SWP2(config)#interface port1.2
SWP2(config-if)#switchport mode private-vlan host
```

6.2.11 プライベート VLAN のホストポートの設定

[書式]

switchport private-vlan host-association *pri-vlan-id* add *2nd-vlan-id*

no switchport private-vlan host-association

[キーワード]

add	:	プライマリー VLAN に対するセカンダリー VLAN を設定する

[パラメーター]

pri-vlan-id	:	<2-4094> プライマリー VLAN として設定されている VLAN ID
2nd-vlan-id	:	<2-4094> セカンダリー VLAN として設定されている VLAN ID

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースがプライベート VLAN のホストポートとして所属するプライマリー VLAN を設定して、セカンダリー VLAN を関連付ける。

no 形式で実行した場合、対象インターフェースがホストポートとして所属するプライマリー VLAN の設定およびセカンダリー VLAN の関連付けを削除する。

[ノート]

本コマンドは **switchport mode private-vlan** コマンドでホストポートとして設定されている LAN/SFP+ポートにのみ設定可能。

pri-vlan-id と *2nd-vlan-id* は、**private-vlan association** コマンドで関連付けられている必要がある。

switchport mode private-vlan コマンドでポートの種別がホストポート以外に設定された場合、本コマンドの設定は削除される。

[設定例]

各インターフェースに以下のプライベート VLAN を設定する。

- LAN ポート #1 : プライマリー VLAN #100、セカンダリー VLAN #101
- LAN ポート #2 : プライマリー VLAN #100、セカンダリー VLAN #102
- LAN ポート #3 : プライマリー VLAN #100、セカンダリー VLAN #103

```
SWP2(config)# interface port1.1
SWP2(config-if)# switchport mode private-vlan host
SWP2(config-if)# switchport private-vlan host-association 100 add 101
SWP2(config-if)# interface port1.2
SWP2(config-if)# switchport mode private-vlan host
SWP2(config-if)# switchport private-vlan host-association 100 add 102
SWP2(config-if)# interface port1.3
SWP2(config-if)# switchport mode private-vlan host
SWP2(config-if)# switchport private-vlan host-association 100 add 103
```

6.2.12 プライベート VLAN のプロミスカスポートの設定

[書式]

switchport private-vlan mapping *pri-vlan-id* add *2nd-vlan-ids*
switchport private-vlan mapping *pri-vlan-id* remove *2nd-vlan-ids*
no switchport private-vlan mapping

[キーワード]

add	:	プライマリー VLAN に対するセカンダリー VLAN を設定する
remove	:	プライマリー VLAN に対するセカンダリー VLAN を削除する

[パラメーター]

pri-vlan-id	:	<2-4094> プライマリー VLAN として設定されている VLAN ID

2nd-vlan-ids : <2-4094>

セカンダリー VLAN に設定されている VLAN ID

複数指定する場合、以下のように、"-" や ","を使用すること

- VLAN #2 から VLAN #4 までを選択する場合: 2-4
- VLAN #2 と VLAN #4 を選択する場合: 2,4

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースがプロミスカスポートとして所属するプライマリー VLAN を設定して、セカンダリー VLAN を関連付ける。

no 形式で実行した場合、対象インターフェースがプロミスカスポートとして所属するプライマリー VLAN の設定およびセカンダリー VLAN の関連付けを削除する。

[ノート]

本コマンドは **switchport mode private-vlan** コマンドでプロミスカスポートとして設定されている LAN/SFP+ポートにのみ設定可能。

加えて、プロミスカスポートとして設定されている以下のインターフェースでも設定できる。

- トランクポートとして動作しているインターフェース
- 論理インターフェース

pri-vlan-id と *2nd-vlan-ids* は、**private-vlan association** コマンドで関連付けられている必要がある。

論理インターフェースを対象として本コマンドを設定した場合は、そのインターフェースに所属する全ての LAN/SFP+ポートの設定が変更される。

switchport mode private-vlan コマンドでポートの種別がプロミスカスポート以外に設定された場合、本コマンドの設定は削除される。

コミュニティー VLAN は、複数のプロミスカスポートに対して関連付けることができる。

1 つのプライマリー VLAN に対して、複数のプロミスカスポートを設定できる。

アイソレート VLAN 内のインターフェースは、1 つのプロミスカスポートとのみ通信が可能なため、1 つのアイソレート VLAN に関連付けられるプロミスカスポートは 1 つのみ。

[設定例]

LAN ポート #1 をプロミスカスポートとして動作させて、プライマリー VLAN #100 を設定し、セカンダリー VLAN #101, #102, #103 を関連付ける。

```
SWP2(config)# interface port1.1
SWP2(config-if)# switchport mode private-vlan promiscuous
SWP2(config-if)# switchport private-vlan mapping 100 add 101
SWP2(config-if)# switchport private-vlan mapping 100 add 102
SWP2(config-if)# switchport private-vlan mapping 100 add 103
```

6.2.13 ボイス VLAN の設定

[書式]

switchport voice vlan *type*

no switchport voice vlan

[パラメーター]

type : タイプ

設定値	説明
<1-4094>	VLAN ID
dot1p	プライオリティタグフレームを使用する
untagged	タグなしフレームを使用する

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

ボイス VLAN の設定をする。 アクセスポートに設定した物理インターフェースのみ設定できる。

VLAN ID を指定した場合、指定した VLAN ID の 802.1p タグつきフレームを音声トラフィックとして利用する。

dot1p を指定した場合、プライオリティタグフレーム(VLAN ID は 0 で、CoS 値が指定された 802.1p タグ)を 音声トラフィックとして利用する。

untagged を指定した場合、タグなしフレームを音声トラフィックとして利用する。

[設定例]

LAN ポート #1 をボイス VLAN として VLAN #100 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport voice vlan 100
```

6.2.14 ボイス VLAN の CoS 値の設定

[書式]

switchport voice cos *value*
no switchport voice cos

[パラメーター]

value : <0-7>

接続機器に設定する CoS 値

[初期設定]

switchport voice cos 5

[入力モード]

インターフェースモード

[説明]

接続機器で音声トラフィックに使用すべき CoS 値を設定する。

以下のときに LLDP-MED で接続機器に設定を通知する。

- 該当ポートでボイス VLAN が設定されている。
- 該当ポートで LLDP-MED 送受信が可能。

[設定例]

LAN ポート #1 でボイス VLAN として使用すべき CoS 値を 6 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport voice cos 6
```

6.2.15 ボイス VLAN の DSCP 値の設定

[書式]

switchport voice dscp *value*
no switchport voice dscp

[パラメーター]

value : <0-63>

接続機器に設定する DSCP 値

[初期設定]

switchport voice dscp 0

[入力モード]

インターフェースモード

[説明]

接続機器で音声トラフィックに使用すべき DSCP 値を設定する。

以下のときに LLDP-MED で接続機器に設定を通知する。

- 該当ポートでボイス VLAN が設定されている。
- 該当ポートで LLDP-MED 送受信が可能。

[設定例]

LAN ポート #1 でボイス VLAN として使用すべき DSCP 値を 63 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport voice dscp 63
```

6.2.16 マルチプル VLAN グループの設定

[書式]

switchport multiple-vlan group *group-ids*
no switchport multiple-vlan group

[パラメーター]

group-ids : <1-256>

マルチプル VLAN グループ ID

複数指定する場合、以下のように、"-" や ","を使用すること

- グループ #2 からグループ #4 までを選択する場合: 2-4
- グループ #2 とグループ #4 を選択する場合: 2,4

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

マルチプル VLAN のグループを指定する。

インターフェースに対してグループを指定した場合、該当インターフェースでは、マルチプル VLAN グループが同じインターフェース間のみで通信できる。同じ VLAN でも、マルチプル VLAN グループが違う場合、通信できない。

物理インターフェース、リンクアグリゲーション論理インターフェースのみ指定できる。

初期状態では各インターフェースはマルチプル VLAN グループに所属しない。

no 形式で実行した場合、初期設定に戻る。

[ノート]

プライベート VLAN との併用はできない。

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る。

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。自発のパケットはマルチプル VLAN グループ設定の影響を受けない。

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る。

- 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

[設定例]

LAN ポート #1 をマルチプル VLAN グループ #10 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#switchport multiple-vlan group 10
SWP2(config-if)#exit
```

6.2.17 マルチプル VLAN グループの名前の設定

[書式]

multiple-vlan group *group-id* **name** *name*
no multiple-vlan group *group-id*

[パラメーター]

group-id : <1-256>
マルチプル VLAN グループ ID

name : 半角英数字および半角記号(32 文字以内)
マルチプル VLAN グループの名前

[初期設定]

multiple-vlan group *group-id* name GROUPxxxx ※xxxx は 4 桁のグループ ID

[入力モード]

グローバルコンフィグレーションモード

[説明]

マルチプル VLAN グループに名前を設定する。

no 形式で実行した場合は、初期値に戻る。

設定した名前は、**show vlan multiple-vlan** コマンドで表示される。

[設定例]

マルチプル VLAN グループ#10 を Network1 という名前に設定する。

```
SWP2(config)#multiple-vlan group 10 name Network1
```

6.2.18 マルチプル VLAN 設定時の YMPI フレーム透過機能の設定

[書式]

multiple-vlan transfer ympi *switch*
no multiple-vlan transfer ympi

[パラメーター]

switch : マルチプル VLAN 設定時の YMPI フレーム透過機能の動作

設定値	説明
enable	透過機能を有効にする
disable	透過機能を無効にする

[初期設定]

multiple-vlan transfer ympi enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

マルチプル VLAN 設定時に、ヤマハ無線アクセスポイントの管理フレームである YMPI フレームを透過させるかどうかを設定する。

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、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したい場合、有効にする必要がある。

no 形式で実行した場合は初期設定に戻る。

[設定例]

マルチプル VLAN 設定時の YMPI フレーム透過機能を無効にする。

```
SWP2(config)#multiple-vlan transfer ympi disable
```

6.2.19 VLAN 情報の表示

[書式]

show vlan *vlan-id*
show vlan brief

[キーワード]

brief	:	全ての VLAN 情報を表示する

[パラメーター]

vlan-id	:	<1-4094> 表示する VLAN ID

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

指定した VLAN ID の情報を表示する。

以下の項目が表示される。

項目	説明
VLAN ID	VLAN ID
Name	VLAN の名前
State	VLAN の状態 (フレームを転送するか否か) • ACTIVE : 転送する • SUSPEND : 転送しない
Member ports	VLAN ID に所属しているインターフェース • (u) : アクセスポート(タグなしポート) • (t) : トランクポート(タグ付きポート)

[設定例]

全 VLAN 情報を表示する。

```
SWP2>show vlan brief
(u)-Untagged, (t)-Tagged

VLAN ID  Name                             State   Member ports
======= ================================ ======= ======================
1       default                          ACTIVE  port1.1(u) port1.2(u)
                                                 port1.3(u) port1.4(u)
                                                 port1.5(u) port1.6(u)
                                                 port1.7(u) port1.8(u)
```

6.2.20 プライベート VLAN 情報の表示

[書式]

show vlan private-vlan

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

プライベート VLAN の情報を表示する。

以下の項目が表示される。

項目	説明
PRIMARY	プライマリー VLAN の VLAN ID
SECONDARY	セカンダリー VLAN の VLAN ID

項目	説明
TYPE	セカンダリー VLAN の種類 • isolated : アイソレート VLAN • community : コミュニティー VLAN
INTERFACES	ホストポートとして所属しているインターフェース

[設定例]

プライベート VLAN の情報を表示する。

```
SWP2>show vlan private-vlan
PRIMARY       SECONDARY          TYPE         INTERFACES
-------        ---------       ----------      ----------
      2              21         isolated
      2              22         community
```

6.2.21 マルチプル VLAN グループ設定情報の表示

[書式]

show vlan multiple-vlan [**group** *group-id*]

[キーワード]

group : 特定のマルチプル VLAN グループの情報を表示する

[パラメーター]

group-id : <1-256>

マルチプル VLAN グループ ID

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

マルチプル VLAN グループの設定状態を表示する。

group 指定を省略した場合は、実際にインターフェースに割り当てられているグループすべてを表示する

YMPI フレーム透過機能の設定状態も表示する。

[設定例]

マルチプル VLAN グループの設定状態を表示する。

```
SWP2>show vlan multiple-vlan
GROUP ID  Name                             Member ports
========= ================================ ======================
1         GROUP0001                        port1.1 port1.2
                                           port1.5

YMPI transfer: Enable
```

6.3 STP(スパニングツリープロトコル)

6.3.1 システムのスパニングツリーの設定

[書式]

spanning-tree shutdown
no spanning-tree shutdown

[初期設定]

no spanning-tree shutdown

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体のスパニングツリーを無効にする。

no 形式で実行した場合は、システム全体のスパニングツリーを有効にする。

[ノート]

スパニングツリーを有効にするためには、本コマンドに加えてインターフェースでもスパニングツリーを有効にする必要がある。

[設定例]

システム全体でスパニングツリーを無効にする。

```
SWP2(config)#spanning-tree shutdown
```

6.3.2 転送遅延時間の設定

[書式]

spanning-tree forward-time *time*
no spanning-tree forward-time

[パラメーター]

time : <4-30>
転送遅延時間(秒)

[初期設定]

spanning-tree forward-time 15

[入力モード]

グローバルコンフィグレーションモード

[説明]

転送遅延時間を設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドの設定は以下の条件を満たす必要がある。

2 × (ハロータイム + 1) ≦ 最大エージング時間 ≦ 2 × (転送遅延時間 - 1)

最大エージング時間は、**spanning-tree max-age** コマンドで設定できる。

ハロータイムは常に 2 秒で、変更することはできない。

[設定例]

転送遅延時間を 10 秒に設定する。

```
SWP2(config)#spanning-tree forward-time 10
```

6.3.3 最大エージング時間の設定

[書式]

spanning-tree max-age *time*
no spanning-tree max-age

[パラメーター]

time : <6-40>
最大エージング時間(秒)

[初期設定]

spanning-tree max-age 20

[入力モード]

グローバルコンフィグレーションモード

[説明]

最大エージング時間を設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

最大エージング時間とは、再構成を試行するまでに L2 スイッチがスパニングツリーコンフィギュレーションメッセージを受信せずに待機する時間である。

本コマンドの設定は以下の条件を満たす必要がある。

2 × (ハロータイム + 1) ≦ 最大エージング時間 ≦ 2 × (転送遅延時間 - 1)

転送遅延時間は、**spanning-tree forward-time** コマンドで設定できる。

ハロータイムは常に 2 秒で、変更することはできない。

[設定例]

最大エージング時間を 25 秒に設定する。

```
SWP2(config)#spanning-tree max-age 25
```

6.3.4 ブリッジプライオリティの設定

[書式]

spanning-tree priority *priority*
no spanning-tree priority

[パラメーター]

priority : <0-61440> (4096 の倍数)
プライオリティ値

[初期設定]

spanning-tree priority 32768

[入力モード]

グローバルコンフィグレーションモード

[説明]

ブリッジプライオリティを設定する。数値が小さいほど優先度が高い。

no 形式で実行した場合は初期設定に戻る。

[ノート]

MSTP の場合は CIST(インスタンス #0)に対する設定となる。

[設定例]

ブリッジプライオリティを 4096 に設定する

```
SWP2(config)#spanning-tree priority 4096
```

6.3.5 インターフェースのスパニングツリーの設定

[書式]

spanning-tree *switch*

[パラメーター]

switch : スパニングツリーの動作

設定値	説明
enable	スパニングツリーを有効にする
disable	スパニングツリーを無効にする

[初期設定]

spanning-tree enable

[入力モード]

インターフェースモード

[説明]

対象インターフェースのスパニングツリーの動作を設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

[設定例]

LAN ポート #1 でスパニングツリーを無効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree disable
```

6.3.6 インターフェースのリンクタイプの設定

[書式]

spanning-tree link-type *type*
no spanning-tree link-type

[パラメーター]

type : リンクタイプ

設定値	説明
point-to-point	ポイントツーポイントリンク
shared	共有リンク

[初期設定]

spanning-tree link-type point-to-point

[入力モード]

インターフェースモード

[説明]

対象インターフェースのリンクタイプを設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

LAN/SFP+ポートを論理インターフェースに所属させた場合は、当該 LAN/SFP+ポートに対する本コマンドの設定が、初期設定に戻る。

[設定例]

LAN ポート #1 のリンクタイプを shared に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree link-type shared
```

6.3.7 インターフェースの BPDU フィルタリングの設定

[書式]

spanning-tree bpdu-filter *filter*
no spanning-tree bpdu-filter

[パラメーター]

filter : BPDU フィルタリングの動作

設定値	説明
enable	BPDU フィルタリングを有効にする
disable	BPDU フィルタリングを無効にする

[初期設定]

spanning-tree bpdu-filter disable

[入力モード]

インターフェースモード

[説明]

対象インターフェースの BPDU フィルタリングを設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

LAN/SFP+ポートを論理インターフェースに所属させた場合は、当該 LAN/SFP+ポートに対する本コマンドの設定が、初期設定に戻る。

[設定例]

LAN ポート #1 の BPDU フィルタリングを有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree bpdu-filter enable
```

6.3.8 インターフェースの BPDU ガードの設定

[書式]

spanning-tree bpdu-guard *guard*
no spanning-tree bpdu-guard

[パラメーター]

guard : BPDU ガードの動作

設定値	説明
enable	BPDU ガードを有効にする
disable	BPDU ガードを無効にする

[初期設定]

spanning-tree bpdu-guard disable

[入力モード]

インターフェースモード

[説明]

対象インターフェースの BPDU ガードを設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

LAN/SFP+ポートを論理インターフェースに所属させた場合は、当該 LAN/SFP+ポートに対する本コマンドの設定が、初期設定に戻る。

LAN/SFP+ポートが BPDU ガードによって **shutdown** された場合は、当該インターフェースに対して **no shutdown** コマンドを実行することで復旧できる。

論理インターフェースが BPDU ガードによって **shutdown** された場合は、当該インターフェースに対して **shutdown** コマンドを実行した後に **no shutdown** コマンドを実行することで復旧できる。

[設定例]

LAN ポート #1 の BPDU ガードを有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree bpdu-guard enable
```

6.3.9 インターフェースのパスコストの設定

[書式]

spanning-tree path-cost *path-cost*
no spanning-tree path-cost

[パラメーター]

path-cost : <1-200000000>
パスコスト値

[初期設定]

インターフェースのリンク速度に応じて、以下の値を使用する。

リンク速度	パスコスト値
1000Mbps	20000
100Mbps	200000
10Mbps	2000000

論理インターフェースは、所属している LAN/SFP+ポートのリンク速度を合計した値を元に、パスコスト値が決まる。

[入力モード]

インターフェースモード

[説明]

対象インターフェースのパスコストを設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

MSTP の場合は CIST(インスタンス #0)に対する設定となる。

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

LAN/SFP+ポートを論理インターフェースに所属させた場合は、当該 LAN/SFP+ポートに対する本コマンドの設定が、初期設定に戻る。

[設定例]

LAN ポート #1 のパスコストを 100000 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree path-cost 100000
```

6.3.10 インターフェースのプライオリティの設定

[書式]

spanning-tree priority *priority*
no spanning-tree priority

[パラメーター]

priority : <0-240> (16 の倍数)
プライオリティ値

[初期設定]

spanning-tree priority 128

[入力モード]

インターフェースモード

[説明]

対象インターフェースのプライオリティを設定する。

no 形式で実行した場合は初期設定に戻る。

数値が小さいほど優先度が高く、対向インターフェースがルートポートになる可能性が高くなる。

[ノート]

MSTP の場合は CIST(インスタンス #0)に対する設定となる。

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

LAN/SFP+ポートを論理インターフェースに所属させた場合は、当該 LAN/SFP+ポートに対する本コマンドの設定が、初期設定に戻る。

[設定例]

LAN ポート #1 のプライオリティを 64 に設定する

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree priority 64
```

6.3.11 インターフェースのエッジポートの設定

[書式]

spanning-tree edgeport
no spanning-tree edgeport

[初期設定]

no spanning-tree edgeport

[入力モード]

インターフェースモード

[説明]

対象インターフェースのエッジポートを設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

LAN/SFP+ポートを論理インターフェースに所属させた場合は、当該 LAN/SFP+ポートに対する本コマンドの設定が、初期設定に戻る。

[設定例]

LAN ポート #1 をエッジポートにする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree edgeport
```

6.3.12 スパニングツリーの状態表示

[書式]

show spanning-tree [interface *ifname*]

[キーワード]

interface	:	表示するインターフェースを指定する

[パラメーター]

ifname	:	LAN/SFP+ポートまたは論理インターフェースの名前 表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

スパニングツリーの状態を表示する。

interface を省略した場合は、全てのインターフェースの状態が表示される。

MSTP の場合は CIST(インスタンス #0)の情報を表示する。

以下の項目が表示される。

項目	説明
Bridge up	スパニングツリープロトコルの有効/無効
Root Path Cost	ルートブリッジのパスコスト
Root Port	ルートポートのインターフェースインデックス番号。ルートブリッジのときは 0 と表示される。論理インターフェースの場合は論理インターフェースのインターフェースインデックス番号で表示される。
Bridge Priority	ブリッジプライオリティ
Forward Delay	ルートブリッジの転送遅延時間設定値
Hello Time	ルートブリッジのハロータイム設定値
Max Age	ルートブリッジの最大エージング時間設定値
Root Id	ルートのブリッジ識別子。ルートのブリッジプライオリティ(16 進数先頭 4 桁)と MAC アドレスで構成される
Bridge Id	ブリッジ識別子。ブリッジプライオリティ(16 進数先頭 4 桁)と MAC アドレスで構成される
topology change(s)	トポロジーチェンジが発生した回数(厳密には TC フラグの付いた BPDU の数を示す)
last topology change	最後にトポロジーチェンジが発生した日時
Ifindex	インターフェースインデックス番号
Port Id	インターフェースのポート ID
Role	インターフェースの役割。Disabled、Designated、Rootport、Alternate のいずれか
State	インターフェースの状態。Listening、Learning、Forwarding、Discarding のいずれか
Designated Path Cost	パスコスト
Configured Path Cost	インターフェースのパスコスト設定値
Add type Explicit ref count	インターフェースが所属する STP ドメインの数
Designated Port Id	Designated ポートの ID
Priority	インターフェースのプライオリティ
Root	ルートのブリッジ識別子。ルートのブリッジプライオリティ(16 進数先頭 4 桁)と MAC アドレスで構成される
Designated Bridge	ブリッジ識別子。ブリッジプライオリティ(16 進数先頭 4 桁)と MAC アドレスで構成される
Message Age	メッセージ経過時間
Hello Time	ハロータイム設定値
Forward Delay	転送遅延時間設定値
Forward Timer	実際の転送遅延タイマー
Msg Age Timer	インターフェースが BPDU の情報を破棄するタイマー。初期設定の場合、STP は 20 秒から、RSTP/MSTP は Hello Time×3 の時間をカウントダウンする

項目	説明
Hello Timer	ハローの送信に使用するタイマー。0 になった時点でハローパケットを送信する
topo change timer	トポロジーチェンジタイマー
forward-transitions	インターフェースが Forward State になった回数
Version	スパニングツリープロトコルの動作モード(バージョン)
Received	受信した BPDU のタイプ
Send	送信する BPDU のタイプ
portfast configured	エッジポートの設定値と現在の状態。portfast off、portfast on、edgeport on のいずれか
bpdu-guard	インターフェースの BPDU ガード機能の設定値と現在の状態
bpdu-filter	インターフェースの BPDU フィルタリング機能の設定値と現在の状態
root guard configured	ルートガード機能の設定値と現在の状態
Configured Link Type	インターフェースのリンクタイプの設定値と現在の状態。point-to-point または shared
auto-edge configured	オートエッジの設定値と現在の状態

[設定例]

LAN ポート #1 のスパニングツリーの状態を表示する。

```
SWP2>show spanning-tree interface port1.1
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% Default: CIST Root Id 8000ac44f2300110
% Default: CIST Reg Root Id 8000ac44f2300110
% Default: CIST Bridge Id 8000ac44f2300110
% Default: 6 topology change(s)  - last topology change Tue Feb 27 19:52:52 2018

%   port1.1: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Designated -
State Forwarding
%   port1.1: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.1: Configured Path Cost 20000  - Add type Explicit ref count 1
%   port1.1: Designated Port Id 0x8389 - CIST Priority 128  -
%   port1.1: CIST Root 8000ac44f2300110
%   port1.1: Regional Root 8000ac44f2300110
%   port1.1: Designated Bridge 8000ac44f2300110
%   port1.1: Message Age 0 - Max Age 20
%   port1.1: CIST Hello Time 2 - Forward Delay 15
%   port1.1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   port1.1: forward-transitions 1
%   port1.1: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   port1.1: No portfast configured - Current  portfast off
%   port1.1: bpdu-guard  disabled  - Current bpdu-guard off
%   port1.1: bpdu-filter disabled  - Current bpdu-filter off
%   port1.1: no root guard configured     - Current root guard off
%   port1.1: Configured Link Type point-to-point - Current point-to-point
%   port1.1: No auto-edge configured - Current port Auto Edge off
```

6.3.13 スパニングツリーの BPDU の統計情報の表示

[書式]

show spanning-tree statistics [interface *ifname*]

[キーワード]

interface　　：　表示するインターフェースを指定する

[パラメーター]

ifname : LAN/SFP+ポートまたは論理インターフェースの名前
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

スパニングツリーの BPDU の統計情報の表示する。

interface を省略した場合は、全てのインターフェースの状態が表示される。

[設定例]

LAN ポート #1 の BPDU の統計情報を表示する。

```
SWP2>show spanning-tree statistics interface port1.1
                 Port number = 905 Interface = port1.1
                 ================================
% BPDU Related Parameters
% ------------------------
% Port Spanning Tree                 : Enable
% Spanning Tree Type                 : Multiple Spanning Tree Protocol
% Current Port State                 : Forwarding
% Port ID                            : 8389
% Port Number                        : 389
% Path Cost                          : 20000
% Message Age                        : 0
% Designated Root                    : ac:44:f2:30:01:10
% Designated Cost                    : 0
% Designated Bridge                  : ac:44:f2:30:01:10
% Designated Port Id                 : 0x8389
% Top Change Ack                     : FALSE
% Config Pending                     : FALSE

% PORT Based Information & Statistics
% -----------------------------------
% Config Bpdu's xmitted              : 3
% Config Bpdu's received             : 0
% TCN Bpdu's xmitted                 : 2
% TCN Bpdu's received                : 3
% Forward Trans Count                : 1

% STATUS of Port Timers
% ---------------------
% Hello Time Configured              : 2
% Hello timer                        : ACTIVE
% Hello Time Value                   : 0
% Forward Delay Timer                : INACTIVE
% Forward Delay Timer Value          : 0
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 3
% Next State                         : Discard/Blocking
% Topology Change Time               : 0

% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : ac:44:f2:30:01:10
% Bridge Hello Time                  : 2
```

```
% Bridge Forward Delay                : 15
% Topology Change Initiator           : 5001
% Last Topology Change Occured        : Tue Feb 27 19:52:52 2018
% Topology Change                     : FALSE
% Topology Change Detected            : TRUE
% Topology Change Count               : 6
% Topology Change Last Recvd from     : 00:a0:de:ae:b8:79
```

6.3.14 プロトコル互換モードのクリア

[書式]

clear spanning-tree detected protocols [interface *ifname*]

[キーワード]

interface : クリアするインターフェースを指定する

[パラメーター]

ifname : LAN/SFP+ポートまたは論理インターフェースの名前
クリアするインターフェース

[入力モード]

特権 EXEC モード

[説明]

STP 互換モードで動作していたインターフェースを通常モードへ戻す。

interface を省略した場合は、全てのインターフェースの状態がクリアされる。

[ノート]

STP の BPDU を受信した場合、受信したインターフェースは STP 互換モードで動作するようになる。しかし、その後 STP の BPDU を受信しなくなっても、当該インターフェースは STP 互換モードで動作し続ける。このような場合に本コマンドを実行することで、STP 互換モードから通常モードへ戻すことができる。

[設定例]

LAN ポート #1 を STP 互換から通常モードへ戻す。

```
SWP2#clear spanning-tree detected protocols interface port1.1
```

6.3.15 MST モードへの移行

[書式]

spanning-tree mst configuration

[入力モード]

グローバルコンフィグレーションモード

[説明]

MST インスタンスや MST リージョンの設定を行うための MST モードに移行する。

[ノート]

MST モードからグローバルコンフィグレーションモードに戻るには **exit** コマンドを使用し、特権 EXEC モードに戻るには **end** コマンドを使用する。

[設定例]

MST モードに移行する。

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#
```

6.3.16 MST インスタンスの生成

[書式]

instance *instance-id*
no instance

[パラメーター]

instance-id : <1-15>
インスタンス ID

[初期設定]

なし

[入力モード]

MST モード

[説明]

MST インスタンスを生成する。

no 形式で実行した場合は、MST インスタンスを削除する。

[ノート]

MST インスタンスの生成と VLAN との関連付けは、**instance vlan** コマンドで設定する。

[設定例]

MST インスタンス #1 を生成する。

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#instance 1
```

6.3.17 MST インスタンスに対する VLAN の設定

[書式]

instance *instance-id* **vlan** *vlan-id*
no instance *instance-id* **vlan** *vlan-id*

[パラメーター]

instance-id : <1-15>
インスタンス ID

vlan-id : <2-4094>
vlan コマンドで設定されている VLAN ID

[初期設定]

なし

[入力モード]

MST モード

[説明]

MST インスタンスに対して VLAN を関連付ける。

no 形式で実行した場合は、MST インスタンスに対する VLAN の関連付けを削除する。削除した結果、MST インスタンスに対して 1 つも VLAN が関連付けられていない場合は、MST インスタンスを削除する。

生成されていない MST インスタンスを指定した場合は、MST インスタンスの生成も行われる。

[ノート]

他の MST インスタンスに関連付けられている VLAN ID を指定することはできない。

MST インスタンスに関連付けられる VLAN の数はシステム全体で最大 256 個までとする。

[設定例]

MST インスタンス #1 に VLAN #2 を関連付ける。

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#instance 1 vlan 2
```

6.3.18 MST インスタンスのプライオリティの設定

[書式]

instance *instance-id* **priority** *priority*
no instance *instance-id* **priority**

[パラメーター]

instance-id : <1-15>
インスタンス ID

priority : <0-61440> (4096 の倍数)
プライオリティ値

[初期設定]

instance *instance-id* priority 32768

[入力モード]

MST モード

[説明]

MST インスタンスのプライオリティを設定する。
数値が小さいほど優先度が高く、MST インスタンス内のルートブリッジになる可能性が高くなる。
no 形式で実行した場合は初期設定に戻る。

[設定例]

MST インスタンス #2 のプライオリティを 4096 に設定する。

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#instance 2
SWP2(config-mst)#instance 2 priority 4096
```

6.3.19 MST リージョン名の設定

[書式]

region *region-name*
no region

[パラメーター]

region-name : 半角英数字および半角記号(32 文字以内)
リージョン名

[初期設定]

region Default

[入力モード]

MST モード

[説明]

MST リージョン名を設定する。
no 形式で実行した場合は初期設定に戻る。

[設定例]

MST リージョン名を Test1 に設定する。

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#region Test1
```

6.3.20 MST リージョンのリビジョン番号の設定

[書式]

revision *revision*

[パラメーター]

revision : <0-65535>

リビジョン番号

[初期設定]

revision 0

[入力モード]

MST モード

[説明]

MST リージョンのリビジョン番号を設定する。

no 形式で実行した場合は初期設定に戻る。

[設定例]

MST リージョンのリビジョン番号を 2 に設定する。

```
SWP2(config)#spanning-tree mst configuration
SWP2(config-mst)#revision 2
```

6.3.21 インターフェースに対する MST インスタンスの設定

[書式]

spanning-tree instance *instance-id*

no spanning-tree instance

[パラメーター]

instance-id : <1-15>

生成されている MST インスタンスの ID

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースに対して MST インスタンスを設定する。

no 形式で実行した場合は、MST インスタンスの設定を削除する。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

LAN/SFP+ポートを論理インターフェースに所属させた場合は、当該 LAN/SFP+ポートに対する本コマンドの設定が、初期設定に戻る。

[設定例]

LAN ポート #1 に MST インスタンス #2 を設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree instance 2
```

6.3.22 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

[書式]

spanning-tree instance *instance-id* **priority** *priority*

no spanning-tree instance *instance-id* **priority**

[パラメーター]

instance-id : <1-15>

対象インターフェースに設定されている MST インスタンスの ID

priority : <0-240> (16 の倍数)
プライオリティ値

[初期設定]

spanning-tree instance *instance-id* priority 128

[入力モード]

インターフェースモード

[説明]

MST インスタンスにおける対象インターフェースのプライオリティを設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

LAN/SFP+ポートを論理インターフェースに所属させた場合は、当該 LAN/SFP+ポートに対する本コマンドの設定が、初期設定に戻る。

[設定例]

LAN ポート #1 の MST インスタンス #2 のプライオリティを 16 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree instance 2
SWP2(config-if)#spanning-tree instance 2 priority 16
```

6.3.23 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

[書式]

spanning-tree instance *instance-id* **path-cost** *path-cost*
no spanning-tree instance *instance-id* **path-cost**

[パラメーター]

instance-id : <1-15>
対象インターフェースに設定されている MST インスタンスの ID

path-cost : <1-200000000>
パスコスト値

[初期設定]

インターフェースのリンク速度に応じて、以下の値を使用する。

リンク速度	パスコスト値
1000Mbps	20000
100Mbps	200000
10Mbps	2000000

論理インターフェースは、所属している LAN/SFP+ポートのリンク速度を合計した値を元に、パスコスト値が決まる。

[入力モード]

インターフェースモード

[説明]

MST インスタンスにおける対象インターフェースのパスコストを設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは LAN/SFP+ポートおよび論理インターフェースにのみ設定可能。

論理インターフェースに所属している LAN/SFP+ポートに対して本コマンドを設定することはできない。

LAN/SFP+ポートを論理インターフェースに所属させた場合は、当該 LAN/SFP+ポートに対する本コマンドの設定が、初期設定に戻る。

[設定例]

LAN ポート #1 の MST インスタンス #2 のパスコストを 100000 に設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#spanning-tree instance 2
SWP2(config-if)#spanning-tree instance 2 path-cost 100000
```

6.3.24 MST リージョン情報の表示

[書式]

show spanning-tree mst config

[入力モード]

非特権 EXEC モード、特権 EXEC モード、インターフェースモード

[説明]

MST リージョンの識別情報を表示する。

[設定例]

MST リージョンの識別情報を表示する。

```
SWP2>show spanning-tree mst config
%
%  MSTP Configuration Information for bridge Default :
%----------------------------------------------------------
%  Format Id      : 0
%  Name           : Default
%  Revision Level : 0
%  Digest         : 0xAC36177F50283CD4B83821D8AB26DE62
%----------------------------------------------------------
```

6.3.25 MSTP 情報の表示

[書式]

show spanning-tree mst [detail] [interface *ifname*]

[キーワード]

detail	:	詳細情報を表示する
interface	:	表示するインターフェースを指定する

[パラメーター]

ifname	:	LAN/SFP+ポートまたは論理インターフェースの名前 表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード、インターフェースモード

[説明]

MSTP の情報を表示する。

通常は MST インスタンスと VLAN およびインターフェースの関連付け情報を表示する。

detail を指定した場合は、インターフェースおよび MST インスタンスの詳細情報を表示する。

interface を省略した場合は、すべてのインターフェースの情報が表示される。

[ノート]

ifname に、論理インターフェースに所属している LAN/SFP+ポートを指定することはできない。

[設定例]

MSTP の情報を表示する。

```
SWP2>show spanning-tree mst
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
```

```
Max-hops 20
% Default: CIST Root Id 8000ac44f2300110
% Default: CIST Reg Root Id 8000ac44f2300110
% Default: CIST Bridge Id 8000ac44f2300110
% Default: 9 topology change(s)  - last topology change Tue Feb 27 20:14:35 2018

%
%   Instance        VLAN
%   0:              1
%   1:              100 (port1.8)
```

LAN ポート #8 の MSTP の詳細情報を表示する

```
SWP2>show spanning-tree mst detail interface port1.8
% Default: Bridge up - Spanning Tree Enabled  - topology change detected
% Default: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% Default: CIST Root Id 8000ac44f2300110
% Default: CIST Reg Root Id 8000ac44f2300110
% Default: CIST Bridge Id 8000ac44f2300110
% Default: 9 topology change(s)  - last topology change Tue Feb 27 20:14:35 2018

%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Designated -
State Forwarding
%   port1.8: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.8: Configured Path Cost 20000  - Add type Explicit ref count 2
%   port1.8: Designated Port Id 0x8390 - CIST Priority 128  -
%   port1.8: CIST Root 8000ac44f2300110
%   port1.8: Regional Root 8000ac44f2300110
%   port1.8: Designated Bridge 8000ac44f2300110
%   port1.8: Message Age 0 - Max Age 20
%   port1.8: CIST Hello Time 2 - Forward Delay 15
%   port1.8: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   port1.8: forward-transitions 1
%   port1.8: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   port1.8: No portfast configured - Current  portfast off
%   port1.8: bpdu-guard  disabled  - Current bpdu-guard off
%   port1.8: bpdu-filter disabled  - Current bpdu-filter off
%   port1.8: no root guard configured     - Current root guard off
%   port1.8: Configured Link Type point-to-point - Current point-to-point
%   port1.8: No auto-edge configured - Current port Auto Edge off
%

% Instance  1:  Vlans: 100
% Default: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% Default: MSTI Root Id 8001ac44f2300110
% Default: MSTI Bridge Id 8001ac44f2300110
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Designated -
State Forwarding
%   port1.8: Designated Internal Path Cost 0  - Designated Port Id 0x8390
%   port1.8: Configured Internal Path Cost 20000
%   port1.8: Configured CST External Path cost 20000
%   port1.8: CST Priority 128  - MSTI Priority 128
%   port1.8: Designated Root 8001ac44f2300110
%   port1.8: Designated Bridge 8001ac44f2300110
%   port1.8: Message Age 0
%   port1.8: Hello Time 2 - Forward Delay 15
%   port1.8: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

6.3.26 MST インスタンス情報の表示

[書式]

show spanning-tree mst instance *instance-id* [interface *ifname*]

[キーワード]

interface : 表示するインターフェースを指定する

[パラメーター]

instance-id : <1-15>

生成されている MST インスタンスの ID

ifname : LAN/SFP+ポートまたは論理インターフェースの名前

表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード、インターフェースモード

[説明]

指定した MST インスタンスの情報を表示する。

interface を省略した場合は、指定した MST インスタンスが設定されているすべてのインターフェースの情報が表示される。

[ノート]

ifname に、論理インターフェースに所属している LAN/SFP+ポートを指定することはできない。

[設定例]

MST インスタンス #1 の情報を表示する。

```
SWP2>show spanning-tree mst instance 1
% Default: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% Default: MSTI Root Id 8001ac44f2300110
% Default: MSTI Bridge Id 8001ac44f2300110
%   port1.8: Port Number 912 - Ifindex 5008 - Port Id 0x8390 - Role Designated -
State Forwarding
%   port1.8: Designated Internal Path Cost 0  - Designated Port Id 0x8390
%   port1.8: Configured Internal Path Cost 20000
%   port1.8: Configured CST External Path cost 20000
%   port1.8: CST Priority 128  - MSTI Priority 128
%   port1.8: Designated Root 8001ac44f2300110
%   port1.8: Designated Bridge 8001ac44f2300110
%   port1.8: Message Age 0
%   port1.8: Hello Time 2 - Forward Delay 15
%   port1.8: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

6.4 ループ検出

6.4.1 ループ検出機能の設定(システム)

[書式]

loop-detect *switch*

no loop-detect

[パラメーター]

switch : システム全体のループ検出機能の設定

設定値	説明
enable	システム全体のループ検出機能を有効にする
disable	システム全体のループ検出機能を無効にする

[初期設定]

loop-detect disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体のループ検出機能を有効または無効にする。

no 形式で実行した場合は初期設定に戻す。

[ノート]

システム全体でスパニングツリー機能とループ検出機能を併用できる。

ループ検出機能を有効にするためには、本コマンドに加えて、インターフェースでもループ検出機能を有効にする必要がある。

ループ検出機能が有効な場合でも、以下のインターフェースではループ検出機能は動作しない。

- スパニングツリー機能が動作している LAN/SFP+ポートおよび論理インターフェース。ただし、Forwarding ポートでは LDF の送受信を行うため、誤接続等によりループが発生した場合は、ループ検出機能が動作する。
- ミラーリング機能のミラーポートとして動作している LAN/SFP+ポート

[設定例]

システム全体でループ検出機能を有効にする。

```
SWP2(config)#loop-detect enable
```

システム全体でループ検出機能を無効にする。

```
SWP2(config)#loop-detect disable
```

6.4.2 ループ検出機能の設定(インターフェース)

[書式]

loop-detect *switch*
no loop-detect

[パラメーター]

switch : 対象インターフェースのループ検出機能の設定

設定値	説明
enable	対象インターフェースのループ検出機能を有効にする
disable	対象インターフェースのループ検出機能を無効にする

[初期設定]

loop-detect enable

[入力モード]

インターフェースモード

[説明]

対象インターフェースのループ検出機能を有効または無効にする。

no 形式で実行した場合は初期設定に戻す。

[ノート]

ループ検出機能を有効にするためには、本コマンドに加えて、システム全体でもループ検出機能を有効にする必要がある。

本コマンドの設定が異なる 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ない。ただし、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る。

論理インターフェースに所属している LAN/SFP+ポートは本コマンドの実行はできない。

ループ検出機能が有効な場合でも、以下のインターフェースではループ検出機能は動作しない。

- スパニングツリー機能が動作している LAN/SFP+ポートおよび論理インターフェース。ただし、Forwarding ポートでは LDF の送受信を行うため、誤接続等によりループが発生した場合は、ループ検出機能が動作する。
- ミラーリング機能のミラーポートとして動作している LAN/SFP+ポート

スパニングツリー機能(STP)およびループ検出機能(LPD)の設定状態に対して、どちらの機能が有効になるかを以下の表に示す。

	インターフェース			
	LPD 無効		LPD 有効	
	STP 無効	STP 有効	STP 無効	STP 有効

システム	LPD 無効	STP 無効	-	-	-	-
		STP 有効	-	STP	-	STP
	LPD 有効	STP 無効	-	-	LPD	LPD
		STP 有効	-	STP	LPD	STP

[設定例]

LAN ポート #1 のループ検出機能を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#loop-detect enable
```

スタティック論理インターフェース #1 のループ検出機能を有効にする。

```
SWP2(config)#interface sa1
SWP2(config-if)#loop-detect enable
```

LACP 論理インターフェース #1 のループ検出機能を有効にする。

```
SWP2(config)#interface po1
SWP2(config-if)#loop-detect enable
```

LAN ポート #1 のループ検出機能を無効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#loop-detect disable
```

6.4.3 ループ検出時の Port Blocking の設定

[書式]

loop-detect blocking *switch*
no loop-detect blocking

[パラメーター]

switch : 対象インターフェースの Port Blocking の設定

設定値	説明
enable	対象インターフェースの Port Blocking を有効にする
disable	対象インターフェースの Port Blocking を無効にする

[初期設定]

loop-detect blocking enable

[入力モード]

インターフェースモード

[説明]

対象インターフェースで、ループを検出した場合の Blocking を有効または無効にする。

no 形式で実行した場合は初期設定に戻す。

[ノート]

本コマンドの設定が異なる 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ない。ただし、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る。

論理インターフェースに所属している LAN/SFP+ポートは本コマンドの実行はできない。

[設定例]

LAN ポート #1 でループを検出した場合に Blocking するようにする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#loop-detect blocking enable
```

スタティック論理インターフェース #1 でループを検出した場合に Blocking するようにする。

```
SWP2(config)#interface sa1
SWP2(config-if)#loop-detect blocking enable
```

LACP 論理インターフェース #1 でループを検出した場合に Blocking するようにする。

```
SWP2(config)#interface po1
SWP2(config-if)#loop-detect blocking enable
```

LAN ポート #1 でループを検出した場合に Blocking しないようにする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#loop-detect blocking disable
```

6.4.4 Port Blocking のループ解消を一定間隔で確認する

[書式]

loop-detect blocking interval *interval*
no loop-detect blocking interval

[パラメーター]

interval : <10-3600>
ループ解消確認の間隔時間（秒）

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

通常、ループが解消されると、即座に Blocking は解除される。

このコマンドを設定すると、一定間隔でループが解消されているか確認するようになる。

ループが解消されていれば Blocking を解除するが、ループが解消されていなければ、再度その時間が経過するまで Blocking を継続する。

no 形式で実行した場合は、初期設定に戻す。

[ノート]

Port Blocking 状態のポートがリンクダウンした場合、Port Blocking は即時に解除される。

[設定例]

Port Blocking のループ解消確認の間隔時間を 300 秒に設定する。

```
SWP2(config)#loop-detect blocking interval 300
```

6.4.5 ループ検出状態のリセット

[書式]

loop-detect reset

[入力モード]

特権 EXEC モード

[説明]

全てのインターフェースのループ検出状態をリセットする。

[ノート]

本コマンドは、システム全体のループ検出機能が有効な場合にのみ実行することができる。

[設定例]

ループ検出状態をリセットする。

```
SWP2#loop-detect reset
```

6.4.6 ループ検出機能の状態表示

[書式]

show loop-detect

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

ループ検出機能の設定や状態を表示する。

表示内容は以下のとおり。

- システム全体のループ検出機能の設定
- Port Blocking のループ解消確認の間隔時間("auto" または "N seconds")
- LAN/SFP+ポートおよび論理インターフェースごとのループ検出の状態
  - インターフェース名(port, sa, po)
  - LAN/SFP+ポートおよび論理インターフェースのループ検出機能の設定(loop-detect)。ループ検出機能が動作している場合は、(*)が付与される
  - Port Blocking の設定状態(port-blocking)
  - ループの検出状態(status)

[ノート]

論理インターフェースに所属している LAN/SFP+ポートは表示しない。

[設定例]

ループ検出状態の状態を表示する。

```
SWP2>show loop-detect
loop-detect: Enable
port-blocking interval: 300 seconds

port      loop-detect    port-blocking           status
-------------------------------------------------------
port1.1        enable(*)        enable         Detected
port1.2        enable(*)        enable         Blocking
port1.3        enable(*)        enable           Normal
port1.4        enable(*)       disable           Normal
port1.5        enable(*)        enable           Normal
port1.6        enable(*)        enable         Shutdown
port1.7       disable           enable           ------
   :             :                :                :
sa1            enable(*)        enable         Blocking
   :             :                :                :
po1            enable(*)        enable           Normal
   :             :                :                :
-------------------------------------------------------
(*): Indicates that the feature is enabled.
```

6.5 DHCP スヌーピング

6.5.1 DHCP スヌーピングの有効/無効設定 (システム)

[書式]

ip dhcp snooping *switch*
no ip dhcp snooping

[パラメーター]

switch : システム全体の DHCP スヌーピング機能の設定

設定値	説明
enable	システム全体の DHCP スヌーピング機能の設定を有効にする
disable	システム全体の DHCP スヌーピング機能の設定を無効にする

[初期設定]

ip dhcp snooping disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体の DHCP スヌーピング機能の設定を有効または無効にする。

no 形式で実行した場合は初期設定に戻す。

[ノート]

DHCP スヌーピング機能を有効にするためには、本コマンドに加えて、VLAN インターフェースでも DHCP スヌーピング機能を有効にする必要がある。

さらに、**ip dhcp snooping trust** コマンドで DHCP サーバーが接続されているポートを設定する必要がある。

[設定例]

システム全体で DHCP スヌーピング機能を有効にする。

```
SWP2(config)#ip dhcp snooping enable
```

システム全体で DHCP スヌーピング機能を無効にする。

```
SWP2(config)#ip dhcp snooping disable
```

6.5.2 DHCP スヌーピングの有効/無効設定 (VLAN)

[書式]

ip dhcp snooping *switch*
no ip dhcp snooping

[パラメーター]

switch : 対象インターフェースの DHCP スヌーピング機能の設定

設定値	説明
enable	対象インターフェースの DHCP スヌーピング機能の設定を有効にする
disable	対象インターフェースの DHCP スヌーピング機能の設定を無効にする

[初期設定]

ip dhcp snooping disable

[入力モード]

インターフェースモード

[説明]

対象インターフェースの DHCP スヌーピング機能の設定を有効または無効にする。

no 形式で実行した場合は初期設定に戻す。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

DHCP スヌーピング機能を有効にするためには、本コマンドに加えて、システム全体でも DHCP スヌーピング機能を有効にする必要がある。

さらに、**ip dhcp snooping trust** コマンドで DHCP サーバーが接続されているポートを設定する必要がある。

[設定例]

VLAN1 で DHCP スヌーピング機能を有効にする。

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip dhcp snooping enable
```

VLAN1 で DHCP スヌーピング機能を無効にする。

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip dhcp snooping disable
```

6.5.3 DHCP スヌーピングのポート種別設定

[書式]

ip dhcp snooping trust
no ip dhcp snooping trust

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースを DHCP スヌーピングの Trusted ポートに設定する。

no 形式で実行した場合は初期設定に戻す。

初期状態ではすべてのポートが Untrusted ポートに設定されている。

[ノート]

本コマンドは LAN/SFP ポートおよび論理インターフェースにのみ設定できる。

論理インターフェースに所属している LAN/SFP ポートは設定できない。

Trusted ポートでは DHCP パケットのフィルタリングが行われず、信頼された DHCP サーバーが接続されているポートに設定する。

Untrusted ポートでは、以下の DHCP パケットのフィルタリング処理が実行される。

- DHCP サーバーから送信される DHCP パケットを破棄する。
- 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受信した IP アドレス解放要求（DHCP RELEASE）および IP アドレス重複検出通知（DHCP DECLINE）を破棄する。
- 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 パケットを破棄する。
- 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 パケットを破棄する。

[設定例]

port1.5 を Trusted ポートに指定する。

```
SWP2(config)#interface port1.5
SWP2(config-if)#ip dhcp snooping trust
```

6.5.4 MAC アドレス検証の有効/無効設定

[書式]

ip dhcp snooping verify mac-address *switch*
no ip dhcp snooping verify mac-address

[パラメーター]

switch : MAC アドレス検証の設定

設定値	説明
enable	MAC アドレス検証の設定を有効にする
disable	MAC アドレス検証の設定を無効にする

[初期設定]

ip dhcp snooping verify mac-address enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

Untrusted ポートで受信した 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 パケットを破棄する。

no 形式で実行した場合は初期設定に戻す。

[設定例]

MAC アドレス検証の設定を無効にする。

```
SWP2(config)#ip dhcp snooping verify mac-address disable
```

6.5.5 Option 82 の有効/無効設定

[書式]

ip dhcp snooping information option *switch*
no ip dhcp snooping information option

[パラメーター]

switch : Option 82 の設定

設定値	説明
enable	Option 82 の設定を有効にする
disable	Option 82 の設定を無効にする

[初期設定]

ip dhcp snooping information option enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

DHCP パケットの Option 82 情報の付加、検査、削除の有効/無効の設定を行う。

no 形式で実行した場合は初期設定に戻す。

Option 82 が有効の場合、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、

DHCP サーバーから DHCP クライアント宛ての戻りパケットの Option 82 情報を削除して転送する。

Option 82 情報は以下のとおり。

- Remote-ID
  - デフォルトでは、本機の MAC アドレスが付与される。
  - **ip dhcp snooping information option format remote-id** コマンドで、Remote-ID に任意の文字列（半角英数字および半角記号）を付与することができる。
- 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 とインターフェース番号が付与される。
  - **ip dhcp snooping vlan vlan-id 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る。
- Subscriber-ID
  - デフォルトでは付与されない。
  - **ip dhcp snooping subscriber-id** コマンドで、対象ポートの Subscriber-ID に任意の文字列を設定することで付与される。

また、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、その DHCP パケットを破棄する。

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ことができる。

[設定例]

Option 82 の設定を無効にする。

```
SWP2(config)#ip dhcp snooping information option disable
```

6.5.6 Option 82 付きパケットの Untrusted ポート受信許可設定

[書式]

ip dhcp snooping information option allow-untrusted
no ip dhcp snooping information option allow-untrusted

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

Untrusted ポートで Option 82 情報が付与された DHCP パケットの転送を有効にする。

no 形式で実行した場合は初期設定に戻す。

[設定例]

Untrusted ポートで Option 82 情報が付与された DHCP パケットの転送を有効にする。

```
SWP2(config)#ip dhcp snooping information option allow-untrusted
```

6.5.7 Option 82 の Remote-ID の設定

[書式]

ip dhcp snooping information option format remote-id string *remoteid*
ip dhcp snooping information option format remote-id hostname
no ip dhcp snooping information option format remote-id

[キーワード]

string	:	REMOTEID 文字列を指定する
hostname	:	REMOTEID にホスト名を設定する

[パラメーター]

remoteid	:	任意の文字列 (半角英数字および半角記号 63 文字以内)

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

Option 82 の Remote-ID に任意の文字列を付与することができる。

ただし、任意の文字列に"?"を含めることはできない。

no 形式で実行した場合は、Remote-ID に本機の MAC アドレスが付与される。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

Remote-ID に任意の文字列を付与する。

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip dhcp snooping information option format remote-id pc1
```

6.5.8 Option 82 の Circuit-ID の設定

[書式]

ip dhcp snooping information option format-type circuit-id vlan-port
ip dhcp snooping information option format-type circuit-id string *string*
ip dhcp snooping information option format-type circuit-id vlan-ifindex

no ip dhcp snooping information option format-type circuit-id

[キーワード]

vlan-port	:	Circuit-ID type 0 VLAN ID, Module(スタック ID), ポート番号を使用する
string	:	Circuit-ID type 1 任意の文字列を使用する
vlan-ifindex	:	Circuit-ID type 2 VLAN ID, ifindex を使用する

[パラメーター]

string	:	任意の文字列 (半角英数字および半角記号 63 文字以内)

[初期設定]

ip dhcp snooping information option format-type circuit-id vlan-ifindex

[入力モード]

インターフェースモード

[説明]

Option 82 の Circuit-ID で使用する情報を指定する。

vlan-port を指定した場合は、DHCP クライアントから DHCP パケットを受信した VLAN ID と、スタック番号、ポート番号を付与する。

string を指定した場合は、任意の文字列を付与する。ただし、任意の文字列に"?"を含めることはできない。

vlan-ifindex を指定した場合は、DHCP クライアントから DHCP パケットを受信した VLAN ID と、インターフェース番号を付与する。

no 形式で実行した場合は、初期設定に戻る。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

Circuit ID に DHCP クライアントから DHCP パケットを受信した VLAN ID とポート番号を付与する。

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip dhcp snooping information option format-type circuit-id vlan-port
```

6.5.9 Option 82 の Subscriber-ID の設定

[書式]

ip dhcp snooping subscriber-id *subid*
no ip dhcp snooping subscriber-id

[パラメーター]

subid	:	任意の文字列 (半角英数字および半角記号 50 文字以内)

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象ポートの Subscriber-ID に任意の文字列(1～50 文字)を設定する。ただし、文字列に"?"を含めることはできない。

no 形式で実行した場合は、Option 82 情報に Subscriber-ID が付与されない。

[ノート]

本コマンドは LAN/SFP ポートおよび論理インターフェースにのみ設定できる。

論理インターフェースに所属している LAN/SFP ポートは設定できない。

[設定例]

port1.1 の Suscriber-ID を設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#ip dhcp snooping subscriber-id a_room
```

6.5.10 DHCP パケット受信レート制限の設定

[書式]

ip dhcp snooping limit rate *limit*
no ip dhcp snooping limit rate

[パラメーター]

limit : 10 - 125
1 秒あたりに受信可能な DHCP パケット数 (pps)

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

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。
受信レートの上限を超過した場合、受信レートを超えた受信 DHCP パケットは破棄する。
no 形式で実行した場合は、DHCP パケットの受信レート制限を行わない。

[設定例]

システム全体の DHCP パケット受信レートを 100pps に設定する。

```
SWP2(config)#ip dhcp snooping limit rate 100
```

6.5.11 DHCP パケット破棄時 SYSLOG 出力の有効/無効設定

[書式]

ip dhcp snooping logging *switch*
no ip dhcp snooping logging

[パラメーター]

switch : DHCP パケット破棄時 SYSLOG 出力の設定

設定値	説明
enable	DHCP パケット破棄時に SYSLOG に出力する
disable	DHCP パケット破棄時に SYSLOG に出力しない

[初期設定]

ip dhcp snooping logging enable

[入力モード]

グローバルコンフィグレーションモード

[説明]

DHCP パケット破棄時に破棄理由を SYSLOG に出力する。
no 形式で実行した場合は初期設定に戻す。

[設定例]

DHCP パケット破棄時に SYSLOG に出力する。

```
SWP2(config)#ip dhcp snooping logging enable
```

6.5.12 DHCP スヌーピングのシステム設定情報の表示

[書式]

show ip dhcp snooping

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

DHCP スヌーピングのシステム設定情報を表示する。

[設定例]

DHCP スヌーピングのシステム設定情報を表示する。

```
SWP2>show ip dhcp snooping
DHCP Snooping Information for system:
  DHCP Snooping service ..... Enabled
  Option 82 insertion ..... Enabled
  Option 82 on untrusted ports ..... Disabled
  Verify MAC address ..... Enabled
  Rate limit ..... 100 pps
  Logging ..... Enabled
```

6.5.13 DHCP スヌーピングのインターフェース設定情報の表示

[書式]

show ip dhcp snooping interface

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

DHCP スヌーピングのインターフェース設定情報を表示する。

[設定例]

DHCP スヌーピングのインターフェース設定情報を表示する。

```
SWP2>show ip dhcp snooping interface
DHCP Snooping information for vlan1:
  DHCP snooping ... Enabled
  Remote-ID ..... 00a0.de00.0001
  Circuit-ID ..... vlan-ifindex
  Interface   Type        Subscriber-ID
  ----------  ----------  ----------------
  port1.1     Trusted
  port1.2     Untrusted   a_room
  port1.10    Untrusted   b_room

DHCP Snooping information for vlan2:
  DHCP snooping ... Enabled
  Remote-ID ..... yamaha
  Circuit-ID ..... vlan-port
  Interface   Type        Subscriber-ID
  ----------  ----------  ----------------
  port1.3     Trusted
  port1.4     Untrusted   c_room
  port1.5     Untrusted   d_room

DHCP Snooping information for vlan3:
  DHCP snooping ... Disabled

DHCP Snooping information for vlan4:
  DHCP snooping ... Enabled
  Remote-ID ..... yamaha
  Circuit-ID ..... torakusu
  Interface   Type        Subscriber-ID
  ----------  ----------  ----------------
  port1.8     Untrusted   e_room
  port1.9     Trusted
```

6.5.14 バインディングデータベースの表示

[書式]

show ip dhcp snooping binding

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

バインディングデータベースに登録されているエントリー情報を表示する。

エントリー情報は以下のとおりです。

- 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

[設定例]

バインディングデータベースの内容を表示する。

```
SWP2>show ip dhcp snooping binding
DHCP Snooping Bindings:
Total number of bindings in database: 4

VLAN  Interface  MAC address     IP address       Expires(sec)
----  ---------  --------------  ---------------  ------------
   1  port1.1    0000.1111.2222  192.168.100.2          259170
   1  port1.2    0000.3333.4444  192.168.100.3          112000
   2  sa1        0000.5555.6666  192.168.200.2          100000
   2  port1.10   0000.7777.8888  192.168.200.3        infinite
```

6.5.15 DHCP スヌーピングの統計情報表示

[書式]

show ip dhcp snooping statistics

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

DHCP スヌーピングの統計情報を表示する。

インターフェースごとに、受信した DHCP パケットと破棄された DHCP パケットの数を表示する。

[ノート]

DHCP パケット受信レート制限の設定によって破棄されたパケットはカウントされない。

[設定例]

DHCP スヌーピングの統計情報を表示する。

```
SWP2>show ip dhcp snooping statistics
DHCP Snooping Statistics:

VLAN  Interface  IN-Packets  IN-Discards
----  ---------  ----------  -----------
   1  port1.1           200          100
   1  port1.2           300            0
   1  port1.5             0            0
   2  port1.3             0            0
   2  port1.4             0            0
   2  sa1                50            2
```

6.5.16 バインディングデータベースのクリア

[書式]

clear ip dhcp snooping binding

[入力モード]

特権 EXEC モード

[説明]

バインディングデータベースをクリアする。

[設定例]

バインディングデータベースをクリアする。

```
SWP2#clear ip dhcp snooping binding
```

6.5.17 DHCP スヌーピングの統計情報のクリア

[書式]

clear ip dhcp snooping statistics

[入力モード]

特権 EXEC モード

[説明]

DHCP スヌーピングの統計情報をクリアする。

[設定例]

DHCP スヌーピングの統計情報をクリアする。

```
SWP2#clear ip dhcp snooping statistics
```

第 7 章

Layer 3 機能

7.1 IPv4 アドレス管理

7.1.1 IPv4 アドレスの設定

[書式]

ip address *ip_address*/*mask* [secondary] [label *textline*]
ip address *ip_address netmask* [secondary] [label *textline*]
no ip address *ip_address*/*mask* [secondary]
no ip address *ip_address netmask* [secondary]
no ip address

[キーワード]

label	:	IPv4 アドレスにラベルを設定する
secondary	:	セカンダリーアドレスとして設定する

[パラメーター]

ip_address	:	A.B.C.D
		IPv4 アドレス
mask	:	<1-31>
		マスクビット数
netmask	:	A.B.C.D
		IPv4 アドレス形式のネットマスク
textline	:	ラベル（64 文字以内）

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

VLAN インターフェースに対して IPv4 アドレスとネットマスクを設定する。

IPv4 アドレスは 1 つの VLAN インターフェースに、プライマリーアドレスを 1 個と、セカンダリーアドレスを 4 個まで設定できる。

システム全体で設定できる IPv4 アドレスは最大 8 個までである。

セカンダリーアドレスを設定するためには、あらかじめプライマリーアドレスを設定する必要がある。

no 形式で実行した場合は、指定した IPv4 アドレスを削除する。IPv4 アドレスを指定しなかった場合は、全ての IPv4 アドレスを削除する。

セカンダリーアドレスを設定している状態で、プライマリーアドレスを削除することはできない。

ラベルを指定した場合は、**show interface** コマンドで「IPv4 address」欄に表示される。

[ノート]

複数のインターフェースに同一サブネットの IPv4 アドレスを割り当てることはできない。

[設定例]

VLAN #1 に IPv4 アドレスとして 192.168.1.100 を設定する。

```
SWP2(config)#interface vlan1
SWP2(config-if)#ip address 192.168.1.100/24
```

7.1.2 IPv4 アドレスの表示

[書式]

show ip interface [*interface*] **brief**

[パラメーター]

interface : VLAN インターフェース名

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

インターフェース毎の IPv4 アドレスを表示する。

表示内容は以下のとおり。

- IPv4 アドレス
  - セカンダリーアドレスの場合、IPv4 アドレスの後に "(secondary)" を付加して表示する。
  - **ip address dhcp** コマンドによって動的に IPv4 アドレスが設定されている場合は、IPv4 アドレスの前に "*" を付加して表示する。
  - **ip address dhcp** コマンドを設定後に IPv4 アドレスが設定されていない場合(サーバ検索中等)は、"searching" と表示する。
  - **ip address** コマンドが設定されていない場合は "unassigned" と表示する。
- 物理層の状態
- データリンク層の状態

インターフェースを指定した場合はそのインターフェースの情報を、省略した場合は IPv4 アドレスを設定できる全てのインターフェースの情報を表示する。

[ノート]

指定したインターフェースが IPv4 アドレスを割り当てられないものである場合はエラーになる。

[設定例]

全ての VLAN インターフェースの IPv4 アドレスを表示する。

```
SWP2>show ip interface brief
Interface      IP-Address                      Admin-Status          Link-Status
vlan1          192.168.1.100/24
               192.168.101.100/24 (secondary)  up                    up
vlan2          192.168.2.100/24                up                    down
vlan3          unassigned                      up                    down
```

7.1.3 DHCP クライアントによる動的 IPv4 アドレスの設定

[書式]

ip address dhcp [hostname *hostname*]

no ip address

[キーワード]

hostname : DHCP サーバーのホスト名を設定する

[パラメーター]

hostname : ホスト名または IPv4 アドレス(A.B.C.D)

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

DHCP クライアントを使用して、DHCP サーバーから付与された IPv4 アドレスを VLAN インターフェースに対して設定する。

DHCP サーバーを指定すると、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る。

IPv4 アドレスを取得した状態で **no ip address** コマンドを実行すると、取得していた IP アドレスの開放メッセージを DHCP サーバーに送る。

DHCP クライアントが設定されているインターフェースに、セカンダリーアドレスは設定できない。

no 形式で実行した場合は、DHCP クライアントの設定を削除する。

[ノート]

DHCP サーバーに対して要求するリース期間は 72 時間で固定とする。ただし、実際にリースされる期間は DHCP サーバーの設定に依存する。

本コマンドにより DHCP サーバーからデフォルトゲートウェイ、DNS サーバー、デフォルトドメイン名を取得した場合でも、**ip route, dns-client name-server, dns-client domain-name** コマンドの設定のほうが優先される。

本コマンドを設定しても DHCP サーバーから IPv4 アドレスが取得できない場合、Auto IP 機能が有効な VLAN インターフェースに限り、IPv4 リンクローカルアドレス(169.254.xxx.xxx/16)が自動的に割り当てられる。

[設定例]

VLAN #100 に DHCP クライアントによって IPv4 アドレスを付与する。

```
SWP2(config)#interface vlan100
SWP2(config-if)#ip address dhcp
```

7.1.4 DHCP クライアントの状態の表示

[書式]

show dhcp lease

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

DHCP クライアントの状態を表示する。以下の項目が表示される。

- DHCP クライアントとして動作しているインターフェース
- 割り当てられた IPv4 アドレス
- リース期限
- リース延長要求期限
- リース再取得期限
- DHCP サーバー名
- DHCP オプションとして取得した情報
  - ネットマスク
  - デフォルトゲートウェイ
  - リース時間
  - DNS サーバー
  - DHCP サーバー ID
  - ドメイン名

[ノート]

[設定例]

DHCP クライアントの状態を表示する。

```
SWP2>show dhcp lease
Interface vlan1
-------------------------------------------------------------------------------
IP Address:                   192.168.100.2
Expires:                      2018/01/01 00:00:00
Renew:                        2018/01/01 00:00:00
Rebind:                       2018/01/01 00:00:00
Server:
Options:
  subnet-mask                 255.255.255.0
  default-gateway             192.168.100.1
  dhcp-lease-time             259200
  domain-name-servers         192.168.100.1
```

```
dhcp-server-identifier      192.168.100.1
domain-name                 example.com
```

7.1.5 Auto IP 機能の設定

[書式]

auto-ip *switch*
no auto-ip

[パラメーター]

switch : Auto IP 機能の動作

設定値	説明
enable	Auto IP 機能を有効にする
disable	Auto IP 機能を無効にする

[初期設定]

auto-ip disable

[入力モード]

インターフェースモード

[説明]

VLAN インターフェースに対して、IPv4 リンクローカルアドレス(169.254.xxx.xxx/16)を自動生成する Auto IP 機能を有効にする。

Auto IP 機能は、**ip address dhcp** コマンドを設定後に、DHCP サーバーから IPv4 アドレスが取得できない場合にのみ機能する。

Auto IP 機能は、1 つの VLAN インターフェースにのみ有効にすることができる。

no 形式で実行した場合は初期設定に戻す。

[ノート]

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 アドレスが取得できた場合、IPv4 リンクローカルアドレスを破棄して、DHCP サーバーから取得した IPv4 アドレスを使用する。

[設定例]

VLAN #2 の Auto IP 機能を有効にする。

```
SWP2(config)#interface vlan2
SWP2(config-if)#auto-ip enable
```

7.2 IPv4 経路制御

7.2.1 IPv4 静的経路設定

[書式]

ip route *ip_address*/*mask gateway* [*number*]
ip route *ip_address*/*mask* null [*number*]
ip route *ip_address netmask gateway* [*number*]
ip route *ip_address netmask* null [*number*]
no ip route *ip_address*/*mask* [*gateway* [*number*]]
no ip route *ip_address*/*mask* [null [*number*]]
no ip route *ip_address netmask* [*gateway* [*number*]]
no ip route *ip_address netmask* [null [*number*]]

[キーワード]

null : パケットを転送せずに破棄する

[パラメーター]

ip_address : A.B.C.D

IPv4 アドレス
デフォルトゲートウェイを指定するときは 0.0.0.0 とする

mask : <1-31>
マスクビット数
デフォルトゲートウェイを指定するときは 0 とする

netmask : A.B.C.D
アドレス形式のネットマスク
デフォルトゲートウェイを指定するときは 0.0.0.0 とする

gateway : A.B.C.D
ゲートウェイの IPv4 アドレス

number : <1-255>
管理距離（経路選択時の優先度）（省略した場合：1）
値が小さいほど優先度が高い。

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

IPv4 の静的経路を追加する。

no 形式で実行した場合は、指定した経路を削除する。

[設定例]

デフォルトゲートウェイを 192.168.1.1 とする。

```
SWP2(config)#ip route 0.0.0.0/0 192.168.1.1
```

送り先が 172.16.0.0/16 の場合のゲートウェイを 192.168.2.1 とする。

```
SWP2(config)#ip route 172.16.0.0 255.255.0.0 192.168.2.1
```

7.2.2 IPv4 転送表の表示

[書式]

show ip route [*ip_address*[/*mask*]]

[パラメーター]

ip_address : A.B.C.D
IPv4 アドレス

mask : <0-32>
マスクビット数（省略した場合：32）

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

IPv4 転送表（FIB: Forwarding Information Base）を表示する。

IPv4 アドレスを省略した場合は、FIB の内容をすべて表示する。

IPv4 アドレスまたはネットワークアドレスを指定した場合、宛先がそれらと一致する経路エントリーの詳細情報を表示する。

[設定例]

IPv4 転送表をすべて表示する。

```
SWP2>show ip route
Codes: C - connected, S - static
       * - candidate default
```

```
Gateway of last resort is 192.168.100.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 192.168.100.1, vlan1
S       172.16.0.0/16 [1/0] via 192.168.200.240, vlan100
S       192.168.1.1/32 [1/0] is directly connected, vlan100
C       192.168.100.0/24 is directly connected, vlan1
C       192.168.200.0/24 is directly connected, vlan100
```

192.168.100.10 宛てのパケットを送るときに使用される経路を表示する。

```
SWP2>show ip route 192.168.100.10
Routing entry for 192.168.100.0/24
  Known via "connected", distance 0, metric 0, best
  * is directly connected, vlan1
```

7.2.3 IPv4 経路表の表示

[書式]

show ip route database

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

IPv4 経路表（RIB: Routing Information Base）を表示する。

[設定例]

IPv4 経路表を表示する。

```
SWP2>show ip route database
Codes: C - connected, S - static
       > - selected route, * - FIB route

S    *> 0.0.0.0/0 [1/0] via 192.168.100.1, vlan1
S    *> 172.16.0.0/16 [1/0] via 192.168.200.240, vlan100
S    *> 192.168.1.1/32 [1/0] is directly connected, vlan100
C    *> 192.168.100.0/24 is directly connected, vlan1
C    *> 192.168.200.0/24 is directly connected, vlan100

Gateway of last resort is not set
```

7.2.4 IPv4 経路表に登録されている経路エントリーのサマリーの表示

[書式]

show ip route summary

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

IPv4 経路表（RIB: Routing Information Base）に登録されている経路エントリーのサマリーを表示する。

[設定例]

IPv4 経路表に登録されている経路エントリーのサマリーを表示する。

```
SWP2>show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 1
Route Source    Networks
connected       2
static          3
Total           5
```

7.3 ARP

7.3.1 ARP テーブルの表示

[書式]

show arp

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

ARP キャッシュを表示する。

[設定例]

ARP キャッシュを表示する。

```
SWP2>show arp
 IP Address       MAC Address   Interface  Type
192.168.100.10  00a0.de00.0000 vlan1    dynamic
192.168.100.100 00a0.de00.0001 vlan1    static
```

7.3.2 ARP テーブルの消去

[書式]

clear arp-cache

[入力モード]

特権 EXEC モード

[説明]

ARP キャッシュをクリアする。

[設定例]

ARP キャッシュをクリアする。

```
SWP2#clear arp-cache
```

7.3.3 静的 ARP エントリーの設定

[書式]

arp *ip_address mac_address interface*
no arp *ip_address*

[パラメーター]

ip_address	:	A.B.C.D
		IP アドレス
mac_address	:	HHHH.HHHH.HHHH
		MAC アドレス
interface	:	portN.M
		物理インターフェイス名

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

静的グループ ARP エントリーを作成する。

no 形式で実行した場合は、指定したエントリーを削除する。

[設定例]

port1.1 に接続された IP アドレス 192.168.100.100、MAC アドレス 00a0.de00.0000 の静的 ARP エントリーを作成する。

```
SWP2(config)#arp 192.168.100.100 00a0.de00.0000 port1.1
```

7.3.4 ARP タイムアウトの設定

[書式]

arp-ageing-timeout *time*

no arp-ageing-timeout [*time*]

[パラメーター]

time : <1-3000>

ARP エントリー保持時間（秒）

[初期設定]

arp-ageing-timeout 300

[入力モード]

インターフェースモード

[説明]

対象 VLAN インターフェースにおける ARP エントリー保持時間を変更する。この時間内に受信されなかった ARP エントリーは削除される。

no 形式で実行した場合は、ARP エントリー時間を 300 秒にする。

[設定例]

VLAN #1 の ARP エントリー保持時間を 10 分に変更する。

```
SWP2(config)#interface vlan1
SWP2(config)#arp-aging-timeout 600
```

7.3.5 ARP タイムアウト時の ARP リクエスト送信方式の設定

[書式]

arp-ageing-timeout request *mode*

no arp-ageing-timeout request

[パラメーター]

mode : ARP リクエスト送信方式

設定値	説明
unicast	ARP タイムアウト時に送信する ARP リクエストをユニキャストで送信する
broadcast	ARP タイムアウト時に送信する ARP リクエストをブロードキャストで送信する

[初期設定]

arp-ageing-timeout request unicast

[入力モード]

インターフェースモード

[説明]

対象 VLAN インターフェースにおいて ARP エントリーの保持時間が満了したときに送信する ARP リクエストの方式を設定する。

no 形式で実行した場合は初期設定に戻す。

[設定例]

VLAN #1 の ARP エントリーの保持時間が満了したときに送信する ARP リクエストをブロードキャストで送信する。

```
SWP2(config)#interface vlan1
SWP2(config)#arp-aging-timeout request broadcast
```

7.4 IPv4 転送制御

7.4.1 IPv4 転送設定

[書式]

ip forwarding *switch*

no ip forwarding [*switch*]

[パラメーター]

switch : IPv4 パケットの転送設定

設定値	説明
enable	IPv4 パケットの転送を有効にする
disable	IPv4 パケットの転送を無効にする

[初期設定]

ip forwarding disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

IPv4 パケットの転送を有効または無効にする。

no 形式で実行した場合は初期設定に戻す。

7.4.2 IPv4 転送設定の表示

[書式]

show ip forwarding

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

IPv4 パケットの転送設定を表示する。

[設定例]

IPv4 パケットの転送設定を表示する。

```
SWP2>show ip forwarding
IP forwarding is on
```

7.4.3 MTU の設定

[書式]

mtu *mtu*

no mtu

[パラメーター]

mtu : <68-9216>

送信可能な最大パケットサイズ

[初期設定]

mtu 1500

[入力モード]

インターフェースモード

[説明]

VLAN インターフェースから送信可能なパケットサイズの最大値(MTU 値)を設定する。

本製品が送信するパケット、および本製品が L3 転送(ルーティング)するパケットが対象となり、本製品が L2 転送(スイッチング)するイーサフレームは対象外となる。

IPv4 ヘッダーの Total Length が MTU 値を超えるパケットを L3 転送する場合、IP フラグメントされて送信される。

IPv6 ヘッダーの Payload Length が MTU 値を超えるパケットを L3 転送する場合、ICMPv6 エラーが返送されてパケットは破棄される。

mru コマンドで設定されたイーサフレーム長に収まるサイズのパケットがルーティングの対象となるため、ジャンボフレームをルーティングする場合には mru コマンドで受信可能なイーサフレーム長を調整する必要がある。

no 形式で実行した場合は初期設定に戻す。

[ノート]

本コマンドは VLAN インターフェースにのみ設定可能。

MTU 値は、初期値を除いて最大で 7 つまで異なる値を設定することができる。

ipv6 enable が設定された VLAN インターフェースでは、MTU の設定可能範囲は <1280-9216> となる。

MTU 値が 1280 よりも小さく設定されている VLAN インターフェースに対して ipv6 enable コマンドを設定することはできない。

[設定例]

VLAN インターフェース #1 に所属する LAN ポート #1 と、VLAN インターフェース #2 に所属する LAN ポート #2 間で、10240 バイトまでのジャンボフレームを許容し、MTU を 2000 バイトにする。

```
SWP2(config)#interface port1.1-2
SWP2(config-if)#mru 10240
SWP2(config-if)#interface vlan1-2
SWP2(config-if)#mtu 2000
```

7.5 IPv4 疎通確認

7.5.1 IPv4 疎通確認

[書式]

ping *host* [repeat *count*] [size *datalen*] [timeout *timeout*] [source *ip_address*]

[キーワード]

repeat	:	実行回数を設定する
size	:	ICMP データ部分の長さ(バイト単位)を設定する
timeout	:	実行回数分の Echo リクエストを送信した後の応答待ち時間を設定する
source	:	ICMP パケットの送信元アドレスを設定する

[パラメーター]

host : ICMP Echo を送信する宛先

ホスト名、または、宛先の IP アドレス(A.B.C.D)

count : 実行回数（省略した場合：5）

設定値	説明
<1-2147483647>	指定した回数実行する
continuous	Ctrl+C が入力されるまで実行を繰り返す

datalen : <36-18024>

ICMP データ部分の長さ(バイト)（省略した場合：56）

timeout : <1-65535>

応答待ち時間（省略した場合：2）

実行回数を continuous にした場合は無視される

ip_address : A.B.C.D

IPv4 アドレス

[入力モード]

特権 EXEC モード

[説明]

ICMP Echo を指定したホストに送出し、ICMP Echo Reply の応答を待つ。

応答があれば、その旨を表示する。コマンドの終了後に統計情報を表示する。

[設定例]

IP アドレス 192.168.100.254 宛てにデータサイズ 120 バイト、実行回数は 3 回で疎通確認を行う。

```
SWP2#ping 192.168.100.254 repeat 3 size 120
PING 192.168.100.254 (192.168.100.254): 120 data bytes
128 bytes from 192.168.100.254: seq=0 ttl=255 time=8.368 ms
128 bytes from 192.168.100.254: seq=1 ttl=255 time=9.946 ms
128 bytes from 192.168.100.254: seq=2 ttl=255 time=10.069 ms

--- 192.168.100.254 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 8.368/9.461/10.069 ms
```

7.5.2 IPv4 経路確認

[書式]

traceroute *host*

[パラメーター]

host : 経路を確認する宛先

ホスト名、または、宛先の IPv4 アドレス(A.B.C.D)

[入力モード]

特権 EXEC モード

[説明]

指定したホストまでの経路情報を表示する。

[設定例]

192.168.100.1 までの経路確認を行う。

```
SWP2#traceroute 192.168.100.1
traceroute to 192.168.100.1 (192.168.100.1), 30 hops max
 1  192.168.10.1 (192.168.10.1)  0.563 ms  0.412 ms  0.428 ms
 2  192.168.20.1 (192.168.20.1)  0.561 ms  0.485 ms  0.476 ms
 3  192.168.30.1 (192.168.30.1)  0.864 ms  0.693 ms  21.104 ms
 4  192.168.40.1 (192.168.40.1)  0.751 ms  0.783 ms  0.673 ms
 5  192.168.50.1 (192.168.50.1)  7.689 ms  7.527 ms  7.168 ms
 6  192.168.100.1 (192.168.100.1)  33.948 ms  10.413 ms  7.681 ms
```

7.6 IPv6 アドレス管理

7.6.1 IPv6 の設定

[書式]

ipv6 *switch*

no ipv6

[パラメーター]

switch : IPv6 の動作

設定値	説明
enable	IPv6 を有効にする
disable	IPv6 を無効にする

[初期設定]

ipv6 disable

[入力モード]

インターフェースモード

[説明]

VLAN インターフェースに対して IPv6 を有効にしリンクローカルアドレスを自動設定する。

IPv6 は最大 8 個までの VLAN インターフェースで有効にすることができる。

IPv6 を無効にした場合、関連する設定も同時に削除される。

no 形式で実行した場合は初期設定に戻る。

[ノート]

自動設定されたリンクローカルアドレスは、**show ipv6 interface brief** コマンドで確認できる。

[設定例]

VLAN #1 の IPv6 を有効にする。

```
SWP2(config)#interface vlan1
SWP2(config-if)#ipv6 enable
```

7.6.2 IPv6 アドレスの設定

[書式]

ipv6 address *ipv6_address*/*prefix_len*
no ipv6 address *ipv6_address*/*prefix_len*
no ipv6 address

[パラメーター]

ipv6_address	:	X:X::X:X IPv6 アドレス
prefix_len	:	<0-127> IPv6 プレフィックス長

[入力モード]

インターフェースモード

[説明]

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。

IPv6 アドレスは **ipv6 enable** コマンドが設定されている VLAN インターフェースに設定することができる。

本コマンドは、**ipv6 address autoconfig**、**ipv6 address dhcp**、**ipv6 address pd** コマンドと併用できる。

IPv6 アドレスは 1 つの VLAN インターフェースに、グローバルアドレス(RA 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 個設定できる。

システム全体で設定できる IPv6 アドレスは最大 8 個までである(自動的に割り当てられるリンクローカルアドレスを除く)。

no 形式で実行した場合は、指定した IPv6 アドレスを削除する。IPv6 アドレスを指定しなかった場合は、全ての IPv6 アドレス(RA 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)を削除する。

[ノート]

複数のインターフェースに同一サブネットの IPv6 アドレスを割り当てることはできない。

[設定例]

VLAN #1 に IPv6 アドレスとして 2001:db8:1::2 を設定する。

```
SWP2(config)#interface vlan1
SWP2(config-if)#ipv6 address 2001:db8:1::2/64
```

7.6.3 IPv6 アドレスの RA 設定

[書式]

ipv6 address autoconfig [stateless]
no ipv6 address autoconfig

[キーワード]

stateless	:	ステートレス DHCPv6 を動作させる

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

RA を使用して、VLAN インターフェースに IPv6 アドレスを設定する。

RA は **ipv6 enable** コマンドが設定されている VLAN インターフェースに設定することができる。

本コマンドは、**ipv6 address**、**ipv6 address pd** コマンドと併用できる。

ipv6 address dhcp、**dhcpv6-server** (DHCPv6 サーバー対応モデルのみ) コマンドがすでに設定されている VLAN インターフェースには設定できない。

本コマンドを有効にした後、Router Lifetime が有効な RA を受信した場合、RA を送信した機器のアドレスが、デフォルトゲートウェイに追加される。

また、Router Lifetime が 0 の RA を受信した場合は、デフォルトゲートウェイから RA を送信した機器のアドレスが削除される。

ただし、**ipv6 nd accept-ra-default-routes disable** コマンドが設定されている場合は、RA に基づくデフォルトゲートウェイの追加は行われない。

stateless を指定した場合、DHCPv6 の Inoformation-request を送信して、DHCPv6 ステートレスモードで動作する。

stateless を指定した場合は、**ipv6 dhcp client pd** コマンドがすでに設定されている VLAN インターフェースには設定できない。

1 つの VLAN インターフェースに、DHCPv6 ステートレスは 1 つだけ設定できる。

stateless を指定した本コマンドは最大で 8 の VLAN インターフェースに設定できる。

ipv6 address autoconfig stateless コマンドを設定した後、**ipv6 address autoconfig** コマンドで上書きした場合、DHCPv6 ステートレスモードは停止する。

no 形式で実行した場合は、RA の設定を削除する。

[ノート]

受信した RA の O フラグがオンであるかオフであるかに関係なく、stateless を指定すると、DHCPv6 のステートレス動作が有効になる。

ステートレス動作時、DHCPv6 サーバーに対して、「OPTION_DNS_SERVERS」(オプションコード 23)と、「OPTION_DOMAIN_LIST」(オプションコード 24) を要求する。

DHCPv6 サーバーから複数のオプションが返ってきたとき、DNS サーバーは 3 件、ドメインリストは 6 件まで取得できる。

ステートレス動作時の要求によって取得した DNS サーバー、ドメインリストは、**show ipv6 dhcp interface** コマンドで確認できる。

取得したドメインリストのドメイン名の末尾に「.」がない場合は、「.」が付与される。

本コマンドにより DHCPv6 サーバーから DNS サーバー、検索ドメインリストを取得した場合でも、**dns-client name-server**、**dns-client domain-list** コマンドの設定のほうが優先される。

システムに設定された DNS サーバー、ドメインリストは、**show dns-client** コマンドで確認できる。

[設定例]

VLAN #1 に、RA を使用して IPv6 アドレスを設定する。

```
SWP2(config)#interface vlan1
SWP2(config-if)#ipv6 address autoconfig
```

7.6.4 DHCPv6 クライアントによる動的 IPv6 アドレスの設定

[書式]

ipv6 address dhcp
no ipv6 address dhcp

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

DHCPv6 クライアントを使用して、DHCPv6 サーバーから付与された IPv6 アドレスを VLAN インターフェースに対して設定する。

本コマンドは、**ipv6 enable** コマンドが設定されている VLAN インターフェースに設定できる。

1 つの VLAN インターフェースに、本コマンドは 1 つだけ設定できる。

本コマンドは、**ipv6 address**、**ipv6 address pd** コマンドと併用できる。

本コマンドは、最大で 8 の VLAN インターフェースに設定できる。

ipv6 dhcp client pd、**ipv6 address autoconfig**、**dhcpv6-server**(DHCPv6 サーバー対応モデルのみ) コマンドがすでに設定されている VLAN インターフェースには設定できない。

IPv6 アドレスを取得した状態で **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 サーバーに送る。

no 形式で実行した場合は DHCPv6 クライアントの設定を削除する。

ipv6 コマンドが disable に設定された場合、本コマンドも削除される。

[ノート]

本コマンドで IPv6 アドレスを自動設定する場合、プレフィックス長は「/128」となる。

受信した RA の M フラグがオンであるかオフであるかに関係なく、本コマンドを設定すると、DHCPv6 のステートフル動作(IA_NA)が有効になる。

DHCPv6 クライアントは、DHCPv6 サーバーに対して、「OPTION_DNS_SERVERS」(オプションコード 23)と、「OPTION_DOMAIN_LIST」(オプションコード 24) を要求する。

DHCPv6 サーバーから複数のオプションが返ってきたとき、DNS サーバーは 3 件、ドメインリストは 6 件まで取得できる。

DHCPv6 クライアントの要求によって取得した DNS サーバー、ドメインリストは、**show ipv6 dhcp interface** コマンドで確認できる。

取得したドメインリストのドメイン名の末尾に「.」がない場合は、「.」が付与される。

本コマンドにより DHCPv6 サーバーから DNS サーバー、検索ドメインリストを取得した場合でも、**dns-client name-server**、**dns-client domain-list** コマンドの設定のほうが優先される。

システムに設定された DNS サーバー、ドメインリストは、**show dns-client** コマンドで確認できる。

本コマンドを有効にした後、Router Lifetime が有効な RA を受信した場合、RA を送信した機器のアドレスが、デフォルトゲートウェイに追加される。

また、Router Lifetime が 0 の RA を受信した場合は、デフォルトゲートウェイから RA を送信した機器のアドレスが削除される。

ただし、**ipv6 nd accept-ra-default-routes disable** コマンドが設定されている場合は、RA に基づくデフォルトゲートウェイの追加は行われない。

[設定例]

VLAN #100 に DHCPv6 クライアントによって IPv6 アドレスを付与する。

```
SWP2(config)#interface vlan100
SWP2(config-if)#ipv6 address dhcp
```

7.6.5 DHCPv6-PD を使用した IPv6 アドレスの設定

[書式]

ipv6 address pd *pd_prefixname pd_ipv6_address*/*prefix_len*
no ipv6 address pd *pd_prefixname pd_ipv6_address*/*prefix_len*

[パラメーター]

pd_prefixname	:	DHCPv6-PD クライアント (ipv6 dhcp client pd コマンド) で設定したプレフィックス名 半角英数字、ドット(.)、ハイフン(-)、アンダーバー(_) (32 文字以内)
pd_ipv6_address	:	X:X::X:X

DHCPv6-PD クライアントで取得したプレフィックスにもとづく IPv6 アドレス

DHCPv6-PD クライアントで取得したプレフィックスに対して、下位 (残り) の部分を設定する

DHCPv6-PD クライアントで取得したプレフィックス部分に対しては、「0」を指定する必要がある

prefix_len : <0-127>

IPv6 プレフィックス長

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

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。

IPv6 アドレスは **ipv6 enable** コマンドが設定されている VLAN インターフェースに設定することができる。

DHCPv6-PD クライアント機能によって取得したプレフィックスに基づき IPv6 アドレスを生成する。

生成された IPv6 アドレスは、**show ipv6 interface** コマンドで確認できる。

本コマンドは、**ipv6 address**、**ipv6 address autoconfig**、**ipv6 address dhcp** コマンドと併用できる。

IPv6 アドレスは 1 つの VLAN インターフェースに、グローバルアドレス(RA 設定、 DHCPv6 クライアントを含む)を 5 個までと、リンクローカルアドレスを 1 個設定できる。

システム全体で設定できる IPv6 アドレスは最大 8 個までである(自動的に割り当てられるリンクローカルアドレスを除く)。

no 形式で実行した場合は、指定した IPv6 アドレスを削除する。

[ノート]

DHCPv6-PD クライアント機能で、プレフィックス情報を取得できていない場合は、IPv6 アドレスは生成されない。

プレフィックス情報と下位アドレスの組み合わせが正しくない場合や、インターフェース間でサブネットが重複した場合も、IPv6 アドレスは生成されない。

[設定例]

VLAN #100 で DHCPv6-PD クライアントによって IPv6 プレフィックスを取得する。

取得したプレフィックス名「PD_VLAN100」を用いて、VLAN #200 に、IPv6 アドレスを設定する。

ここでは、「PD_VLAN100」にて、「2001:db8:1:aaf0::/60」を取得したと仮定する。

以下の設定で VLAN #200 に、「2001:db8:1:aaf2::1/64」が設定される。

```
SWP2(config)#interface vlan100
SWP2(config-if)#ipv6 dhcp client pd PD_VLAN100
SWP2(config)#interface vlan200
SWP2(config-if)#ipv6 address pd PD_VLAN100 ::2:0:0:0:1/64
```

7.6.6 DHCPv6-PD クライアントの設定

[書式]

ipv6 dhcp client pd *prefixname*
no ipv6 dhcp client pd

[パラメーター]

prefixname : 割り当てられたプレフィックスに付ける内部的な名前

半角英数字、ドット(.)、ハイフン(-)、アンダーバー(_) (32 文字以内)

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

対象インターフェースで DHCPv6-PD クライアント機能を有効化し、プレフィックスの割り当てを要求するように設定する。

本コマンドは、**ipv6 enable** コマンドが設定されている VLAN インターフェースに設定できる。

本コマンドの *prefixname* で取得したプレフィックスは、以下で使用できる。

- **ipv6 address pd** コマンドにて、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** コマンドにて、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** コマンドにて、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)

1 つの VLAN インターフェースに、本コマンドは 1 つだけ設定できる。

本コマンドは最大で 8 の VLAN インターフェースに設定できる。

ipv6 address dhcp、**ipv6 address autoconfig stateless**、**dhcpv6-server**(DHCPv6 サーバー対応モデルのみ) コマンドがすでに設定されている VLAN インターフェースには設定できない。

IPv6 プレフィックスを取得した状態で **no ipv6 dhcp client pd** コマンドを実行すると、取得していたプレフィックスの解放メッセージを DHCPv6 サーバーに送る。

no 形式で実行した場合は DHCPv6-PD クライアントの設定を削除する。

ipv6 コマンドが disable に設定された場合、本コマンドも削除される。

[ノート]

受信した RA の M フラグがオンであるかオフであるかに関係なく、本コマンドを設定すると、DHCPv6-PD のステートフル動作(IA_PD)が有効になる。

DHCPv6-PD クライアントは、DHCPv6 サーバーに対して、「OPTION_DNS_SERVERS」(オプションコード 23)と、「OPTION_DOMAIN_LIST」(オプションコード 24) を要求する。

DHCPv6 サーバーから複数のオプションが返ってきたとき、DNS サーバーは 3 件、ドメインリストは 6 件まで取得できる。

DHCPv6-PD クライアントで取得した DNS サーバー、ドメインリストは、DHCPv6 モードの **dns-server**、**domain-name** コマンドで利用することができる。(DHCPv6 サーバー対応モデルのみ)

DHCPv6-PD クライアントの要求によって取得した DNS サーバー、ドメインリストは、**show ipv6 dhcp interface** コマンドで確認できる。

取得したドメインリストのドメイン名の末尾に「.」がない場合は、「.」が付与される。

本コマンドにより DHCPv6-PD サーバーから DNS サーバー、検索ドメインリストを取得した場合でも、**dns-client name-server**、**dns-client domain-list** コマンドの設定のほうが優先される。

システムに設定された DNS サーバー、ドメインリストは、**show dns-client** コマンドで確認できる。

本コマンドを有効にした後、Router Lifetime が有効な RA を受信した場合、RA を送信した機器のアドレスが、デフォルトゲートウェイに追加される。

また、Router Lifetime が 0 の RA を受信した場合は、デフォルトゲートウェイから RA を送信した機器のアドレスが削除される。

ただし、**ipv6 nd accept-ra-default-routes disable** コマンドが設定されている場合は、RA に基づくデフォルトゲートウェイの追加は行われない。

[設定例]

VLAN #100 で DHCPv6-PD クライアントによって IPv6 プレフィックスを取得する。

取得したプレフィックス名「PD_VLAN100」を用いて、VLAN #200 に、IPv6 アドレスを設定する。

ここでは、「PD_VLAN100」にて、「2001:db8:1:aaf0::/60」を取得したと仮定する。

以下の設定で VLAN #200 に、「2001:db8:1:aaf2::1/64」が設定される。

```
SWP2(config)#interface vlan100
SWP2(config-if)#ipv6 dhcp client pd PD_VLAN100
SWP2(config)#interface vlan200
SWP2(config-if)#ipv6 address pd PD_VLAN100 ::2:0:0:0:1/64
```

7.6.7 RA によるデフォルトゲートウェイの自動登録設定

[書式]

ipv6 nd accept-ra-default-routes *switch*

no ipv6 nd accept-ra-default-routes

[パラメーター]

switch : RA によるデフォルトゲートウェイ自動登録設定

設定値	説明
enable	RA によるデフォルトゲートウェイ自動登録設定を有効にする
disable	RA によるデフォルトゲートウェイ自動登録設定を無効にする

[初期設定]

ipv6 nd accept-ra-default-routes enable

[入力モード]

インターフェースモード

[説明]

対象のインターフェースで受信したルーター広告(RA)の始点アドレスにもとづく、IPv6 のデフォルトゲートウェイの自動登録の有効/無効を設定する。

本コマンドは、**ipv6 enable** コマンドが設定されている VLAN インターフェースに設定できる。

no 形式で実行した場合は設定を初期値に戻す。

ipv6 コマンドが disable に設定された場合、本コマンドも削除される。

[ノート]

ipv6 address dhcp、**ipv6 dhcp client pd**、**ipv6 address autoconfig** コマンド設定時 RA を受信したときに、本コマンドの設定が適用される。

これらのコマンドが設定されていない場合は、本コマンドが有効に設定されていても、デフォルトゲートウェイの自動登録は行われない。

[設定例]

VLAN #100 で RA によるデフォルトゲートウェイ自動登録設定を無効にする。

```
SWP2(config)#interface vlan100
SWP2(config-if)#ipv6 nd accept-ra-default-routes disable
```

7.6.8 IPv6 アドレスの表示

[書式]

show ipv6 interface [*interface*] **brief**

[パラメーター]

interface : VLAN インターフェース名

表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

インターフェース毎の IPv6 アドレスを表示する。

- IPv6 アドレス
  - **ipv6 address dhcp** コマンドによって動的に IPv6 アドレスが設定されている場合は、IPv6 アドレスの前に "*" を付加して表示する。
  - **ipv6 address dhcp** コマンドを設定後に IPv6 アドレスが設定されていない場合(サーバ検索中等)は、"searching" と表示する。
  - **ipv6 address pd** コマンドで *pd_prefixname* を用いて設定したアドレスの場合は、IPv6 アドレスの前に "*" を付加して表示する。
  - IPv6 アドレスが設定されていない場合は "unassigned" となる。
- 物理層の状態

- データリンク層の状態

インターフェースを指定した場合はそのインターフェースの情報を、省略した場合は IPv6 アドレスが設定された全てのインターフェースの情報を表示する。

[ノート]

指定したインターフェースが IPv6 アドレスを割り当てられないものである場合はエラーになる。

[設定例]

全ての VLAN インターフェースの IPv6 アドレスを表示する。

```
SWP2>show ipv6 interface brief
Interface        IPv6-Address                                  Admin-Status
Link-Status
vlan1            2001:db8:1::2/64
                 2001:db8:2::2/64
                 fe80::2a0:deff:fe:2/64                        up                      up
vlan2            2001:db8:2::2/64
                 fe80::2a0:deff:fe:2/64                        up
down
vlan3            unassigned                                    up
down
```

7.6.9 DHCPv6 クライアントの状態の表示

[書式]

show ipv6 dhcp interface [*ifname*]

[パラメーター]

ifname : VLAN インターフェース名

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

DHCPv6 クライアントの状態を表示する。

ifname を指定しなかった場合、すべての VLAN インターフェースの情報を表示する。

[ノート]

[設定例]

すべての VLAN インターフェースの DHCPv6 クライアントの状態を表示する。

```
SWP2#show ipv6 dhcp interface
Interface vlan1
  Client Type        : IA_NA
  Address            : 2001:db8:1:aa10::dd2d
  IAID               : 0f28924a
  DUID               : 0001000100000000000a0de000000
  preferred lifetime : 604800
  valid lifetime     : 2592000
  expires            : 2023/4/19 07:25:48

Interface vlan2
  Client Type        : Stateless
  DUID               : 000100012ce737dbac44f284efdd
  DNS Server         : 2001:db8:1:bb10::100
  DNS Server         : 2001:db8:1:bb10::200
  Domain Name        : example.com.

Interface vlan100
  Client Type        : IA_PD
  Prefix name        : PD_VLAN100
  prefix             : 2001:db8:1:aaf0::/60
  IAID               : 0f28924a
  DUID               : 0001000100000000000a0de000000
  preferred lifetime : 604800
  valid lifetime     : 2592000
  expires            : 2023/4/19 08:08:04
  DNS Server         : 2001:db8:2::100
```

```
DNS Server          : 2001:db8:2::200
Domain Name         : example.com.
```

7.6.10 DHCPv6 クライアントのリセット

[書式]

clear ipv6 dhcp client *ifname*

[パラメーター]

ifname : VLAN インターフェース名

[入力モード]

特権 EXEC モード

[説明]

対象のインターフェースで動作している DHCPv6 クライアントをクリアする。

本コマンドを実行すると、対象のインターフェースで取得した DHCPv6 の情報が一度消去される。

そのときに、取得していた IPv6 アドレスの解放メッセージを DHCPv6 サーバーへ送る。

その後、DHCPv6 サーバーへの要求が再度送信され、DHCPv6 クライアントの再設定を行う。

DHCPv6-PD クライアントを使用していた場合、**ipv6 address pd** コマンドで、取得したプレフィックスを使用していたとき、設定していたインターフェースのアドレスも再設定される。

DHCPv6 サーバー機能にて、DHCPv6 モードの **range** コマンド、**prefix-delegation** コマンド、**dns-server** コマンド、**domain-name** コマンドで、取得した情報を使用していたとき、DHCPv6 サーバー機能も再設定される。(DHCPv6 サーバー対応モデルのみ)

[ノート]

[設定例]

VLAN #100 の DHCPv6 クライアントをクリアする。

```
SWP2#clear ipv6 dhcp client vlan100
```

7.6.11 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

[書式]

ipv6 dhcp client nd-prefix *prefix_len*
no ipv6 dhcp client nd-prefix

[パラメーター]

prefix_len : <1-127>
受信する ND のプレフィックス長

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

ipv6 address dhcp コマンドによって IPv6 アドレス(プレフィックス /128)が自動設定された VLAN インターフェースでは、送信元 IPv6 アドレスにかかわらずすべての ND(Neighbor Discovery)パケットを受信する。

本コマンドを設定すると、ND パケット受信時に以下の両者を、設定したプレフィックスの範囲で比較し、同一セグメントの場合にはその ND パケットを受信する。同一セグメントではない場合には、その ND パケットを破棄する。

- **ipv6 address dhcp** コマンドによって自動設定された IPv6 アドレス
- 受信した ND パケットの送信元 IPv6 アドレス

本コマンドは、**ipv6 enable** コマンドが設定されている VLAN インターフェースに設定することができる。

本コマンドの対象となる ND パケットは、NS(Neighbor Solicitation)、NA(Neighbor Advertisement)のみである。

no 形式で実行した場合は、DHCPv6 クライアント設定時に受信する ND のプレフィックスを削除する。

[ノート]

ipv6 address dhcp コマンドによって IPv6 アドレス(プレフィックス /128)が自動設定された VLAN インターフェースでのみ動作する。

[設定例]

ipv6 address dhcp コマンドによって IPv6 アドレスが自動設定された VLAN #1 で、サブネット /64 からの ND パケットのみ受信できるようにする。

```
SWP2(config)#interface vlan1
SWP2(config-if)#ipv6 dhcp client nd-prefix 64
```

7.7 IPv6 経路制御

7.7.1 IPv6 静的経路設定

[書式]

ipv6 route *ipv6_address*/*prefix_len gateway* [*number*]
ipv6 route *ipv6_address*/*prefix_len* null [*number*]
no ipv6 route *ipv6_address*/*prefix_len* [*gateway* [*number*]]
no ipv6 route *ipv6_address*/*prefix_len* [null [*number*]]

[キーワード]

null	:	パケットを転送せずに破棄する

[パラメーター]

ipv6_address	:	X:X::X:X IPv6 アドレス デフォルトゲートウェイを指定するときは :: (0:0:0:0:0:0:0:0 の省略形) とする
prefix_len	:	<1-127> IPv6 プレフィックス デフォルトゲートウェイを指定するときは 0 とする
gateway	:	X:X::X:X ゲートウェイの IPv6 アドレス IPv6 リンクローカルアドレスを指定するときは、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)
number	:	<1-255> 管理距離（経路選択時の優先度）（省略した場合：1） 値が小さいほど優先度が高い。

[入力モード]

グローバルコンフィグレーションモード

[説明]

IPv6 の静的経路を追加する。

no 形式で実行した場合は、指定した経路を削除する。

[ノート]

デフォルトゲートウェイの設定は、RA による設定よりも、静的経路による設定が最優先される。

[設定例]

送り先が 2001:db8:2::/64 の場合のゲートウェイを 2001:db8:1::1 とする。

```
SWP2(config)#ipv6 route 2001:db8:2::/64 2001:db8:1::1
```

デフォルトゲートウェイを経路 VLAN #1 上の fe80::2a0:deff:fe:1 とする。

```
SWP2(config)#ipv6 route ::/0 fe80::2a0:deff:fe:1%vlan1
```

7.7.2 IPv6 転送表の表示

[書式]

show ipv6 route [*ipv6_address*[/*prefix_len*]]

[パラメーター]

ipv6_address	:	X:X::X:X
		IPv6 アドレス
mask	:	<0-128>
		IPv6 プレフィックス長（省略した場合：128）

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

IPv6 転送表（FIB: Forwarding Information Base）を表示する。

IPv6 アドレスを省略した場合は、FIB の内容をすべて表示する。

IPv6 アドレスまたはネットワークアドレスを指定した場合、宛先がそれらと一致する経路エントリーの詳細情報を表示する。

[ノート]

[設定例]

IPv6 転送表をすべて表示する。

```
SWP2>show ipv6 route
Codes: C - connected, S - static
Timers: Uptime

S      ::/0 [1/0] via fe80::2a0:deff:fe:1, vlan1, 00:03:08
C      2001:db8:1::/64 via ::, vlan1, 00:01:10
S      2001:db8:2::/64 [1/0] via 2001:db8:1::1, vlan1, 00:01:52
C      fe80::/64 via ::, vlan1, 00:03:08
```

2001:db8:1::2 宛てのパケットを送るときに使用される経路を表示する。

```
SWP2>show ipv6 route 2001:db8:1::2
Routing entry for 2001:db8:1::/64
  Known via "connected", distance 0, metric 0, best
  Last update 00:18:27 ago
  * directly connected, vlan1
```

7.7.3 IPv6 経路表の表示

[書式]

show ipv6 route database

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

IPv6 経路表（RIB: Routing Information Base）を表示する。

[ノート]

[設定例]

IPv6 経路表を表示する。

```
SWP2>show ipv6 route database
Codes: C - connected, S - static
       > - selected route, * - FIB route
Timers: Uptime

S   *> ::/0 [1/0] via fe80::2a0:deff:fe:1, vlan1, 00:21:39
C   *> 2001:db8:1::/64 via ::, vlan1, 00:19:41
S   *> 2001:db8:2::/64 [1/0] via 2001:db8:1::1, vlan1, 00:20:23
C   *> fe80::/64 via ::, vlan1, 00:21:39
```

7.7.4 IPv6 経路表に登録されている経路エントリーのサマリーの表示

[書式]

show ipv6 route summary

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

IPv6 経路表（RIB: Routing Information Base）に登録されている経路エントリーのサマリーを表示する。

[ノート]

[設定例]

IPv6 経路表のサマリーを表示する。

```
SWP2>show ipv6 route summary
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 1
Route Source    Networks
connected       2
static          2
Total           4
```

7.8 Neighbor キャッシュ

7.8.1 静的 Neighbor キャッシュエントリーの設定

[書式]

ipv6 neighbor *ipv6_address interface mac_address interface*
no ipv6 neighbor *ipv6_address interface*

[パラメーター]

ipv6_address	:	X:X::X:X
		IPv6 アドレス
interface	:	vlanN
		VLAN インターフェイス名
mac_address	:	HHHH.HHHH.HHHH
		MAC アドレス
interface	:	portN.M
		物理インターフェイス名

[入力モード]

グローバルコンフィグレーションモード

[説明]

Neighbor キャッシュに静的エントリーを追加する。
no 形式で実行した場合は、指定した静的エントリーを削除する。

[ノート]

[設定例]

VLAN #1 上の port1.1 にある、IPv6 アドレス 2001:db8:cafe::1 の MAC アドレスを Neighbor キャッシュに設定する。

```
SWP2(config)#ipv6 neighbor 2001:db8:cafe::1 vlan1 00a0.de80.cafe port1.1
```

7.8.2 Neighbor キャッシュテーブルの表示

[書式]

show ipv6 neighbors

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

Neighbor キャッシュテーブルを表示する。

[ノート]

[設定例]

Neighbor キャッシュテーブルを表示する。

```
SWP2>show ipv neighbors
 IPv6 Address                              MAC Address     Interface  Type
2001:db8:1:0:3538:5dc7:6bc4:1a23          0011.2233.4455   vlan1      dynamic
2001:db8:cafe::1                          00a0.de80.cafe   vlan1      static
fe80::0211:22ff:fe33:4455                 0011.2233.4455   vlan1      dynamic
fe80::6477:88ff:fe99:aabb                 6677.8899.aabb   vlan1      dynamic
```

7.8.3 Neighbor キャッシュテーブルの消去

[書式]

clear ipv6 neighbors

[入力モード]

特権 EXEC モード

[説明]

Neighbor キャッシュをクリアする。

[ノート]

[設定例]

Neighbor キャッシュをクリアする。

```
SWP2#clear ipv6 neighbors
```

7.9 IPv6 転送制御

7.9.1 IPv6 転送設定

[書式]

ipv6 forwarding *switch*
no ipv6 forwarding [*switch*]

[パラメーター]

switch : IPv6 パケットの転送設定

設定値	説明
enable	IPv6 パケットの転送を有効にする
disable	IPv6 パケットの転送を無効にする

[初期設定]

ipv6 forwarding disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

IPv6 パケットの転送を有効または無効にする。
no 形式で実行した場合は初期設定に戻す。

7.9.2 IPv6 転送設定の表示

[書式]

show ipv6 forwarding

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

IPv6 パケットの転送設定を表示する。

[設定例]

IPv6 パケットの転送設定を表示する。

```
SWP2>show ipv6 forwarding
IPv6 forwarding is on
```

7.10 IPv6 疎通確認

7.10.1 IPv6 疎通確認

[書式]

ping6 *host* [repeat *count*] [size *datalen*] [timeout *timeout*] [source *ipv6_address*]

[キーワード]

repeat	:	実行回数を設定する
size	:	ICMPv6 データ部分の長さ(バイト単位)を設定する
timeout	:	実行回数分の Echo リクエストを送信した後の応答待ち時間を設定する
source	:	ICMPv6 パケットの送信元アドレスを設定する

[パラメーター]

host : ホスト名、または、IPv6 アドレス(X:X::X:X)

ICMPv6 Echo を送信する宛先

IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)

count : 実行回数（省略した場合：5）

設定値	説明
<1-2147483647>	指定した回数実行する
continuous	Ctrl+C が入力されるまで実行を繰り返す

datalen : <36-18024>

ICMP データ部分の長さ(バイト)（省略した場合：56）

timeout : <1-65535>

応答待ち時間（省略した場合：2）

実行回数を continuous にした場合は無視される

ipv6_address : X:X::X:X

IPv6 アドレス

[入力モード]

特権 EXEC モード

[説明]

ICMPv6 Echo を指定したホストに送出し、ICMPv6 Echo Reply が送られてくるのを待つ。

送られてきたら、その旨を表示する。コマンドが終了すると簡単な統計情報を表示する。

[ノート]

[設定例]

fe80::2a0:deff:fe11:2233 宛てに疎通確認を行う。

```
SWP2#ping6 fe80::2a0:deff:fe11:2233%vlan1
PING fe80::2a0:deff:fe11:2233%vlan1 (fe80::2a0:deff:fe11:2233%vlan1): 56 data bytes
64 bytes from fe80::2a0:deff:fe11:2233: seq=0 ttl=64 time=2.681 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=1 ttl=64 time=4.760 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=2 ttl=64 time=10.045 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=3 ttl=64 time=10.078 ms
64 bytes from fe80::2a0:deff:fe11:2233: seq=4 ttl=64 time=10.210 ms

--- fe80::2a0:deff:fe11:2233%vlan1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.681/7.554/10.210 ms
```

7.10.2 IPv6 経路確認

[書式]

traceroute6 *host*

[パラメーター]

host : 経路を確認する宛先

ホスト名、または、宛先の IPv6 アドレス(X:X::X:X)

[入力モード]

特権 EXEC モード

[説明]

指定したホストまでの経路情報を表示する。

[ノート]

[設定例]

2001:db8:1::2 までの経路確認を行う。

```
SWP2#traceroute6 2001:db8:1::2
traceroute to 2001:db8:1::2 (2001:db8:1::2), 30 hops max
 1  2001:db8:10::1 (2001:db8:10::1)  0.563 ms  0.412 ms  0.428 ms
 2  2001:db8:20::1 (2001:db8:20::1)  0.561 ms  0.485 ms  0.476 ms
 3  2001:db8:30::1 (2001:db8:30::1)  0.864 ms  0.693 ms  21.104 ms
 4  2001:db8:40::1 (2001:db8:40::1)  0.751 ms  0.783 ms  0.673 ms
 5  2001:db8:50::1 (2001:db8:50::1)  7.689 ms  7.527 ms  7.168 ms
 6  2001:db8:1::2 (2001:db8:1::2)  33.948 ms  10.413 ms  7.681 ms
```

7.11 DNS クライアント

7.11.1 DNS への問い合わせ機能の設定

[書式]

dns-client *switch*

no dns-client

[パラメーター]

switch : DNS クライアントの動作

設定値	説明
enable	DNS クライアントを有効にする
disable	DNS クライアントを無効にする

[初期設定]

dns-client disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

DNS への問い合わせ機能を有効または無効にする。

no 形式で実行した場合は無効にする。

[設定例]

DNS への問い合わせ機能を有効にする。

```
SWP2(config)#dns-client enable
```

7.11.2 DNS サーバーリストの設定

[書式]

dns-client name-server *server*
no dns-client name-server *server*

[パラメーター]

server : A.B.C.D

DNS サーバーの IPv4 アドレス

: X:X::X:X

DNS サーバーの IPv6 アドレス

IPv6 リンクローカルアドレスを指定する場合は、送出インターフェースも指定する必要がある(fe80::X%vlanN の形式)

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

DNS サーバーリストにサーバーを追加する。

サーバーは最大 3 件まで設定できる。

no 形式で実行した場合は、指定したサーバーを DNS サーバーリストから削除する。

[ノート]

ip address dhcp、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 address autoconfig stateless** コマンドによって DHCP サーバーから DNS サーバーリストを取得した場合、本コマンドの設定が優先される。

ただし、本コマンドによる DNS サーバーリストの登録数が 3 件未満の場合は、合計 3 件までリストの末尾に DHCP サーバーから取得した DNS サーバーリストを追加する。

[設定例]

DNS サーバーリストに IP アドレス 192.168.100.1、2001:db8::1234、fe80::2a0:deff:fe11:2233 を追加する。

```
SWP2(config)#dns-client name-server 192.168.100.1
SWP2(config)#dns-client name-server 2001:db8::1234
SWP2(config)#dns-client name-server fe80::2a0:deff:fe11:2233%vlan1
```

7.11.3 デフォルトドメイン名の設定

[書式]

dns-client domain-name *name*
no dns-client domain-name *name*

[パラメーター]

name : ドメイン名（最大 256 文字）

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

DNS 問い合わせ時に使用するデフォルトドメイン名を設定する。

no 形式で実行した場合はデフォルトドメイン名を削除する。

[ノート]

ip address dhcp コマンドによって DHCP サーバーからデフォルトドメイン名(オプションコード 15)を取得した場合、本コマンドの設定が優先される。

dns-client domain-list コマンドで検索ドメインリストが設定されている場合は、本コマンドで設定したデフォルトドメイン名、および、**ip address dhcp** コマンドによって自動設定されたデフォルトドメイン名は使用されない。

[設定例]

デフォルトドメイン名を example.com に設定する。

```
SWP2(config)#dns-client domain-name example.com
```

7.11.4 検索ドメインリストの設定

[書式]

dns-client domain-list *name*
no dns-client domain-list *name*

[パラメーター]

name : ドメイン名（最大 256 文字）

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

DNS 問い合わせ時に使用する検索ドメインリストにドメイン名を追加する。

検索ドメインリストは最大 6 件までドメインを登録できる。

no 形式で実行した場合は、指定したドメイン名を検索ドメインリストから削除する。

[ノート]

本コマンドで検索ドメインリストが設定されている場合、**dns-client domain-name** コマンドで設定したデフォルトドメイン名、および、**ip address dhcp** コマンドによって自動設定されたデフォルトドメイン名は使用されない。

ipv6 address dhcp、**ipv6 dhcp client pd**、**ipv6 address autoconfig stateless** コマンドによって DHCP サーバーから検索ドメインリストを取得した場合、本コマンドの設定が優先される。

ただし、本コマンドによる検索ドメインリストの登録数が 6 件未満の場合は、合計 6 件までリストの末尾に DHCP サーバーから取得した検索ドメインリストを追加する。

[設定例]

ドメイン名 example1.com, example2.com を検索ドメインリストに追加する。

```
SWP2(config)#dns-client domain-list example1.com
SWP2(config)#dns-client domain-list example2.com
```

7.11.5 DNS クライアント情報の表示

[書式]

show dns-client

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

DNS クライアント情報を表示する。

表示内容は以下のとおり。

項目	説明
DNS Client is enabled	DNS クライアントが有効
DNS Client is disabled	DNS クライアントが無効
Default domain	デフォルトドメイン名
Domain list	検索ドメインリスト
Name Servers	DNS サーバーリスト(IP アドレス)

[設定例]

DNS クライアント情報を表示する。

```
SWP2>show dns-client

DNS client is enabled
 Default domain  : example.com
 Domain list     : example1.com example2.com
 Name Servers    : 192.168.100.1 2001:db8::1234 fe80::2a0:deff:fe11:2233%vlan1

 * - Values assigned by DHCP or DHCPv6 Client.
```

第 8 章

IP マルチキャスト制御

8.1 IP マルチキャスト基本設定

8.1.1 未知のマルチキャストフレームの処理方法の設定

[書式]

l2-unknown-mcast *mode*

[パラメーター]

mode : マルチキャストフレームの処理方法

設定値	説明
discard	破棄する
flood	フラッディングする

[初期設定]

l2-unknown-mcast flood

[入力モード]

グローバルコンフィグレーションモード

[説明]

MAC アドレステーブルに登録されていないマルチキャストフレームの処理方法を設定する。

[設定例]

未知のマルチキャストを破棄する。

```
SWP2(config)#l2-unknown-mcast discard
```

8.1.2 未知のマルチキャストフレームの処理方法の設定(インターフェース)

[書式]

l2-unknown-mcast *mode*

no l2-unknown-mcast

[パラメーター]

mode : マルチキャストフレームの処理方法

設定値	説明
discard	破棄する
flood	フラッディングする

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

VLAN インターフェースで受信した MAC アドレステーブルに登録されていないマルチキャストフレームの処理方法を設定する。

no 形式で実行した場合は初期設定に戻り、システム全体の未知のマルチキャストフレーム処理方法の設定に従う。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

本コマンドはシステム全体の未知のマルチキャストフレーム処理方法の設定より優先される。

[設定例]

VLAN #1 で受信した MAC アドレステーブルに登録されていないマルチキャストフレームを破棄する。

```
SWP2(config)#interface vlan1
SWP2(config-if)#l2-unknown-mcast discard
```

8.1.3 リンクローカルマルチキャストフレームの転送設定

[書式]

l2-unknown-mcast forward link-local
no l2-unknown-mcast forward link-local

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

l2-unknown-mcast discard を設定しているとき、リンクローカルマルチキャストアドレスのフレームを破棄せずに転送する。

no 形式で実行した場合は、指定した設定を削除する。

[ノート]

本コマンドにおける、リンクローカルマルチキャストアドレスは以下の範囲とする。

- IPv4: 224.0.0.0/24
- IPv6: ff02::/112

IPv4 マルチキャストアドレスを指定する形式は廃止された。この形式が含まれるコンフィグを読み込んだ場合は自動的に **l2-mcast flood** コマンドに置き換えられる。

[設定例]

リンクローカルマルチキャストアドレスのフレームを未知のマルチキャストとして破棄せずに転送する。

```
SWP2(config)#l2-unknown-mcast discard
SWP2(config)#l2-unknown-mcast forward link-local
```

8.1.4 マルチキャストフレームの転送設定

[書式]

l2-mcast flood *ipv4_addr*
no l2-mcast flood *ipv4_addr*

[パラメーター]

ipv4_addr : A.B.C.D
IPv4 マルチキャストアドレス

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

VLAN インターフェースで受信したマルチキャスト通信の中で宛先が指定した IPv4 マルチキャストアドレスのフレームをフラッディングする。

本コマンドはシステム全体で 100 個まで設定ができる。

no 形式で実行した場合は、指定した IPv4 マルチキャストアドレスの設定を削除する。

また、IPv4 マルチキャストアドレスを省略した場合は、すべての設定を削除する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

本コマンドで指定された IPv4 マルチキャストアドレスは IGMP スヌーピングの対象外となる。

[設定例]

VLAN #1 で受信した宛先 IPv4 アドレスが 239.0.0.251 のフレームをフラッディングする。

```
SWP2(config)#interface vlan1
SWP2(config-if)#l2-mcast flood 239.0.0.251
```

8.1.5 トポロジー変更時の IGMP/MLD クエリー送信機能の有効／無効設定

[書式]

l2-mcast snooping tcn-query enable *time*
l2-mcast snooping tcn-query disable
no l2-mcast snooping tcn-query

[パラメーター]

time : <1-30>

IGMP/MLD クエリー送信待ち時間(秒)

[初期設定]

l2-mcast snooping tcn-query disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

スパニングツリーによるトポロジー変更時に、クエリアーが IGMP/MLD クエリーを送信する機能の動作を設定する。

no 形式で実行した場合は初期設定に戻る。

IGMP/MLD スヌーピングとスパニングツリーを併用した際に、トポロジー変更によってマルチキャスト通信が一時的に途絶えることがあるが、本機能を使用すればこの期間を短縮することができる。

有効にした場合は、トポロジー変更を検出すると、指定された時間待ったあとに IGMP/MLD クエリーを送信する。

無効にした場合は、トポロジー変更があっても IGMP/MLD クエリーを送信しない。

[設定例]

トポロジー変更時の IGMP/MLD クエリー送信を有効にし、待ち時間を 5 秒に設定する。

```
SWP2(config)#l2-mcast snooping tcn-query enable 5
```

トポロジー変更時の IGMP/MLD クエリー送信を無効にする。

```
SWP2(config)#l2-mcast snooping tcn-query disable
```

8.2 IGMP スヌーピング

8.2.1 IGMP スヌーピングの有効／無効設定

[書式]

ip igmp snooping *switch*
no ip igmp snooping

[パラメーター]

switch : IGMP スヌーピングの動作

設定値	説明
enable	IGMP スヌーピングを有効にする
disable	IGMP スヌーピングを無効にする

[初期設定]

ip igmp snooping enable

[入力モード]

インターフェースモード

[説明]

インターフェースの IGMP スヌーピングの動作を設定する。

no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

VLAN #2 の IGMP スヌーピングを有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping enable
```

VLAN #2 の IGMP スヌーピングを無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping disable
```

8.2.2 IGMP スヌーピング高速脱退の設定

[書式]

ip igmp snooping fast-leave [auto-assignment]
no ip igmp snooping fast-leave

[キーワード]

auto-assignment : LAN/SFP ポート配下にスイッチが接続されている場合に高速脱退機能を無効にする。

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

インターフェースの IGMP スヌーピング高速脱退を有効にする。

no 形式で実行すると、IGMP スヌーピング高速脱退を無効にする。

auto-assignment オプションが指定された場合は、LAN/SFP ポート配下にスイッチが接続されている場合、そのポートでのみ自動的に高速脱退機能を無効にする。

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「Enabled Capabilities」に「Bridge」が含まれているか否かで判定する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

本コマンドは、LAN/SFP+ポートに複数のホストが接続されている VLAN インターフェースでは、auto-assignment オプションを有効にするか、高速脱退機能自体を無効にすること。

[設定例]

VLAN #2 の IGMP スヌーピング高速脱退を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping fast-leave
```

VLAN #2 の IGMP スヌーピング高速脱退を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping fast-leave
```

8.2.3 マルチキャストルーターの接続先の設定

[書式]

ip igmp snooping mrouter interface *ifname*
no ip igmp snooping mrouter interface *ifname*

[パラメーター]

ifname : LAN/SFP+ポートのインターフェース名
設定するインターフェース

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

マルチキャストルーターが接続されている LAN/SFP+ポートを静的に設定する。

no 形式で実行すると、設定を破棄する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

設定した LAN/SFP+ポートには、マルチキャストルーターが接続されていること。レシーバーから IGMP レポートを受信すると、設定した LAN/SFP+ポートに転送する。

[設定例]

マルチキャストルーターの接続先として LAN ポート #8 を設定する。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping mrouter interface port1.8
```

マルチキャストルーターの接続先から LAN ポート #8 を外す。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping mrouter interface port1.8
```

8.2.4 クエリー送信機能の設定

[書式]

ip igmp snooping querier
no ip igmp snooping querier

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

IGMP クエリー送信機能を有効にする。

no 形式で実行すると、IGMP クエリー送信機能を無効にする。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

本機能を有効にしたまま IP アドレスを変更すると、変更後に正しい IP アドレスでクエリーを送信しなくなるので注意すること。

[設定例]

VLAN #2 の送信機能を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping querier
```

VLAN #2 の送信機能を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping querier
```

8.2.5 IGMP クエリー送信間隔の設定

[書式]

ip igmp snooping query-interval *interval*
no ip igmp snooping query-interval

[パラメーター]

interval : <20-18000>
クエリー送信間隔(秒)

[初期設定]

ip igmp snooping query-interval 125

[入力モード]

インターフェースモード

[説明]

IGMP クエリーの送信間隔を設定する。

no 形式で実行すると、IGMP クエリーの送信間隔を初期設定に戻す。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

VLAN #2 のクエリー送信間隔を 30 秒に設定する。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping query-interval 30
```

VLAN #2 のクエリー送信間隔を初期値に戻す。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping query-interval
```

8.2.6 IGMP パケットの TTL 値検証機能の設定

[書式]

ip igmp snooping check ttl *switch*
no ip igmp snooping check ttl

[パラメーター]

switch : IGMP パケットの TTL 値検証機能

設定値	説明
enable	有効にする
disable	無効にする

[初期設定]

ip igmp snooping check ttl enable

[入力モード]

インターフェースモード

[説明]

IGMP パケットの TTL 値検証機能を設定する。

no 形式で実行した場合は初期設定に戻る。

有効にした場合は、IP ヘッダーの TTL 値が不正(1 以外)な IGMP パケットを破棄する。

無効にした場合は、当該パケットを破棄せず、TTL 値を 1 に補正して転送する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

VLAN #2 で IGMP パケットの TTL 値検証機能を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check ttl enable
```

VLAN #2 で IGMP パケットの TTL 値検証機能を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check ttl disable
```

8.2.7 IGMP パケットの RA 検証機能の設定

[書式]

ip igmp snooping check ra *switch*

no ip igmp snooping check ra

[パラメーター]

switch : IGMP パケットの RA 検証機能

設定値	説明
enable	有効にする
disable	無効にする

[初期設定]

ip igmp snooping check ra disable

[入力モード]

インターフェースモード

[説明]

IGMPv2/IGMPv3 パケットの RA 検証機能を設定する。

no 形式で実行した場合は初期設定に戻る。

有効にした場合は、IP ヘッダーに RA（Router Alert）オプションが含まれていない IGMPv2/IGMPv3 パケットを破棄する。

無効にした場合は、当該パケットを破棄せず、IP ヘッダーに RA オプションを付与して転送する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

VLAN #2 で IGMP パケットの RA 検証機能を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check ra enable
```

VLAN #2 で IGMP パケットの RA 検証機能を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check ra disable
```

8.2.8 IGMP パケットの ToS 検証機能の設定

[書式]

ip igmp snooping check tos *switch*

no ip igmp snooping check tos

[パラメーター]

switch : IGMP パケットの ToS 検証機能

設定値	説明
enable	有効にする
disable	無効にする

[初期設定]

ip igmp snooping check tos disable

[入力モード]

インターフェースモード

[説明]

IGMP パケットの ToS 検証機能を設定する。

no 形式で実行した場合は初期設定に戻る。

有効にした場合は、IP ヘッダーの ToS の IP Precidence 値(3 ビット)が不正(B'110 以外)な IGMPv3 パケットを破棄し、それ以外は ToS を 0xc0 に上書きして転送する。

無効にした場合は、IGMP パケットを破棄せずに、ToS を 0xc0 に上書きして転送する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

VLAN #2 で IGMP パケットの ToS 検証機能を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check tos enable
```

VLAN #2 で IGMP パケットの ToS 検証機能を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping check tos disable
```

8.2.9 IGMP バージョンの設定

[書式]

ip igmp snooping version *version*
no ip igmp snooping version

[パラメーター]

version : <2-3>

IGMP バージョン

[初期設定]

ip igmp snooping version 3

[入力モード]

インターフェースモード

[説明]

IGMP のバージョンを設定する。

no 形式で実行すると、IGMP バージョンを初期設定(V3)に戻す。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

設定と異なるバージョンの IGMP パケットを受信した場合、以下の動作となる。

- V2 設定時
  - V3 クエリーを受信した場合、V2 クエリーとして転送

  - V3 レポートを受信した場合、破棄
- V3 設定時
  - V2 クエリーを受信した場合、V2 クエリーとして転送
  - V2 レポートを受信した場合、V3 レポートとして転送

[設定例]

VLAN #2 で IGMP バージョンを 2 に設定する。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping version 2
```

VLAN #2 で IGMP バージョンを初期値に戻す。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ip igmp snooping version
```

8.2.10 IGMP レポート抑制機能の設定

[書式]

ip igmp snooping report-suppression *switch*
no ip igmp snooping report-suppression

[パラメーター]

switch : IGMP レポート抑制機能

設定値	説明
enable	有効にする
disable	無効にする

[初期設定]

ip igmp snooping report-suppression enable

[入力モード]

インターフェースモード

[説明]

IGMP レポート抑制機能を設定する。

no 形式で実行した場合は初期設定に戻る。

有効にした場合は、受信した Report メッセージや Leave メッセージから得た情報をもとに、最小限のメッセージをマルチキャストルーターポートへ送信する。

無効にした場合は、受信した Report メッセージや Leave メッセージを逐次マルチキャストルーターポートへ転送する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

VLAN #2 で IGMP レポート抑制機能を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping report-suppression enable
```

VLAN #2 で IGMP レポート抑制機能を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping report-suppression disable
```

8.2.11 IGMP レポート転送機能の設定

[書式]

ip igmp snooping report-forward *switch*
no ip igmp snooping report-forward

[パラメーター]

switch : IGMP レポート転送機能

設定値	説明
enable	有効にする
disable	無効にする

[初期設定]

ip igmp snooping report-forward disable

[入力モード]

インターフェースモード

[説明]

IGMP レポート転送機能を設定する。

no 形式で実行した場合は初期設定に戻る。

有効にした場合は、マルチキャストルーターポートに加えて、LAN/SFP+ポート配下にスイッチが接続されている場合に、そのポートに対して IGMP Report メッセージや Leave メッセージを転送する。

無効にした場合は、マルチキャストルーターポートにのみ、IGMP Report メッセージや Leave メッセージを転送する。

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「Enabled Capabilities」に「Bridge」が含まれているか否かで判定する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

本機能を有効にする場合は、IGMP レポート抑制機能を無効にすること。

[設定例]

VLAN #2 で IGMP レポート転送機能を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping report-forward enable
```

VLAN #2 で IGMP レポート転送機能を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping report-forward disable
```

8.2.12 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の設定

[書式]

ip igmp snooping mrouter-port data-suppression *switch*
no ip igmp snooping mrouter-port data-suppression

[パラメーター]

switch : 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

設定値	説明
enable	有効にする
disable	無効にする

[初期設定]

ip igmp snooping mrouter-port data-suppression disable

[入力モード]

インターフェースモード

[説明]

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設定する。

no 形式で実行した場合は初期設定に戻る。

有効にした場合は、マルチキャストルーターポートで Report メッセージを受信した場合のみ該当データをマルチキャストルーターポートへ転送する。

無効にした場合は、いずれかのポートで Report メッセージを受信していれば、該当データはマルチキャストルーターポートにも転送される。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

VLAN #2 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有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping mrouter-port data-suppression enable
```

VLAN #2 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無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ip igmp snooping mrouter-port data-suppression disable
```

8.2.13 マルチキャストルーター接続ポート情報の表示

[書式]

show ip igmp snooping mrouter *ifname*

[パラメーター]

ifname : VLAN インターフェース名
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

動的に学習された、または静的に設定したマルチキャストルーター接続ポート情報を表示する。

[設定例]

VLAN #2 のマルチキャストルーター接続ポートの情報を表示する。

```
SWP2#show ip igmp snooping mrouter vlan2
VLAN    Interface             IP-address    Expires
2       port1.8(dynamic)         192.168.100.216        00:00:49
```

8.2.14 IGMP グループメンバーシップ情報の表示

[書式]

show ip igmp snooping groups [detail]
show ip igmp snooping groups *A.B.C.D* [detail]
show ip igmp snooping groups *ifname* [detail]

[キーワード]

detail : 詳細情報

[パラメーター]

A.B.C.D : マルチキャストグループアドレス

ifname : VLAN インターフェース名
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

IGMP グループメンバーシップ情報を表示する。

[設定例]

IGMP グループメンバーシップの情報を表示する。

```
SWP2#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
1      239.255.255.250          port1.5        R      01:06:02   00:03:45
192.168.100.11    V3
```

IGMP グループメンバーシップの詳細情報を表示する。

```
SWP2#show ip igmp snooping groups detail
IGMP Snooping Group Membership Details
Flags: (R - Remote, S - Static)

Interface:      port1.5
Group:          239.255.255.250
Flags:          R
Uptime:         01:07:10
Group mode:     Exclude (Expires: 00:04:13)
Last reporter:  192.168.100.11
Source list is empty
```

8.2.15 インターフェースの IGMP 関連情報を表示

[書式]

show ip igmp snooping interface *ifname*

[パラメーター]

ifname : VLAN インターフェース名
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

VLAN インターフェースの IGMP 関連情報を表示する。

[設定例]

VLAN #1 の IGMP 関連情報を表示する。

```
SWP2#show ip igmp snooping interface vlan1

IGMP Snooping information for vlan1
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2/v3 fast-leave is enabled
 IGMPv2/v3 fast-leave auto-assignment is enabled
 IGMPv1/v2 Report suppression enabled
 IGMPv3 Report suppression enabled
 IGMPv1/v2/v3 Report forwarding enabled
 IGMP Snooping check TTL is enabled
 IGMP Snooping check RA is enabled
 IGMP Snooping check ToS is enabled
 IGMP Snooping Mrouter-port Data suppression disabled
 Router port detection using IGMP Queries
 Number of router-ports: 1
 Number of Groups: 1
 Number of v1-reports: 0
 Number of v2-reports: 6
 Number of v2-leaves: 0
 Number of v3-reports: 127
 Active Ports:
  port1.1 (F,R)
  port1.2

  F - Fast-leave auto-assignment is enabled
```

```
R - Report forwarding is enabled
```

8.2.16 IGMP グループメンバーシップのエントリー削除

[書式]

clear ip igmp snooping
clear ip igmp snooping group *A.B.C.D*
clear ip igmp snooping interface *ifname*

[キーワード]

group	:	削除するマルチキャストグループアドレスを指定する
interface	:	削除する VLAN インターフェースを指定する

[パラメーター]

A.B.C.D	:	マルチキャストグループアドレス "*"は全エントリー
ifname	:	VLAN インターフェース名 削除するインターフェース

[入力モード]

特権 EXEC モード

[説明]

IGMP グループメンバーシップのエントリーを削除する。

[設定例]

VLAN #1 の IGMP グループメンバーシップのエントリーを削除する。

```
SWP2#clear ip igmp snooping interface vlan1
```

8.3 MLD スヌーピング

8.3.1 MLD スヌーピングの有効／無効設定

[書式]

ipv6 mld snooping *switch*
no ipv6 mld snooping

[パラメーター]

switch : MLD スヌーピングの動作

設定値	説明
enable	MLD スヌーピングを有効にする
disable	MLD スヌーピングを無効にする

[初期設定]

ipv6 mld snooping enable

[入力モード]

インターフェースモード

[説明]

インターフェースの MLD スヌーピングの動作を設定する。
no 形式で実行した場合は初期設定に戻る。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

VLAN #2 の MLD スヌーピングを有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping enable
```

VLAN #2 の MLD スヌーピングを無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping disable
```

8.3.2 MLD スヌーピング高速脱退の設定

[書式]

ipv6 mld snooping fast-leave
no ipv6 mld snooping fast-leave

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

インターフェースの MLD スヌーピング高速脱退を有効にする。

no 形式で実行すると、MLD スヌーピング高速脱退を無効にする。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。また、MLD スヌーピングが有効な場合のみ設定できる。

本コマンドは、LAN/SFP+ポートに複数のホストが接続されている VLAN インターフェースでは有効化しないこと。

[設定例]

VLAN #2 の MLD スヌーピング高速脱退を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping fast-leave
```

VLAN #2 の MLD スヌーピング高速脱退を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping fast-leave
```

8.3.3 マルチキャストルーターの接続先の設定

[書式]

ipv6 mld snooping mrouter interface *ifname*
no ipv6 mld snooping mrouter interface *ifname*

[パラメーター]

ifname : LAN/SFP+ポートのインターフェース名
設定するインターフェース

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

マルチキャストルーターが接続されている LAN/SFP+ポートを静的に設定する。

no 形式で実行すると、設定を破棄する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。また、MLD スヌーピングが有効な場合のみ設定できる。

設定した LAN/SFP+ポートには、マルチキャストルーターが接続されていること。レシーバーから MLD レポートを受信すると、設定した LAN/SFP+ポートに転送する。

[設定例]

マルチキャストルーターの接続先として LAN ポート #8 を設定する。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping mrouter interface port1.8
```

マルチキャストルーターの接続先から LAN ポート #8 を外す。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping mrouter interface port1.8
```

8.3.4 クエリー送信機能の設定

[書式]

ipv6 mld snooping querier
no ipv6 mld snooping querier

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

MLD クエリー送信機能を有効にする。

no 形式で実行すると、MLD クエリー送信機能を無効にする。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。また、MLD スヌーピングが有効な場合のみ設定できる。

本機能を使用する場合は必ず **ipv6 enable** コマンドをいずれかの VLAN インターフェースに設定すること。 **ipv6 enable** コマンドが設定されていない場合、MLD クエリーは送信されないので注意すること。

[設定例]

VLAN #2 の MLD クエリー送信機能を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping querier
```

VLAN #2 の MLD クエリー送信機能を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping querier
```

8.3.5 MLD クエリー送信間隔の設定

[書式]

ipv6 mld snooping query-interval *interval*
no ipv6 mld snooping query-interval

[パラメーター]

interval : <20-18000>
クエリー送信間隔(秒)

[初期設定]

ipv6 mld snooping query-interval 125

[入力モード]

インターフェースモード

[説明]

MLD クエリーの送信間隔を設定する。

no 形式で実行すると、MLD クエリーの送信間隔を初期設定に戻す。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。また、MLD スヌーピングが有効な場合のみ設定できる。

[設定例]

VLAN #2 のクエリー送信間隔を 30 秒に設定する。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping query-interval 30
```

VLAN #2 のクエリー送信間隔を初期値に戻す。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping query-interval
```

8.3.6 MLD バージョンの設定

[書式]

ipv6 mld snooping version *version*
no ipv6 mld snooping version

[パラメーター]

version : <1-2>
MLD バージョン

[初期設定]

ipv6 mld snooping version 2

[入力モード]

インターフェースモード

[説明]

MLD のバージョンを設定する。

no 形式で実行すると、MLD バージョンを初期設定(V2)に戻す。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。また、MLD スヌーピングが有効な場合のみ設定できる。

設定と異なるバージョンの MLD パケットを受信した場合、以下の動作となる。

- V1 設定時
  - V2 クエリーを受信した場合、V1 クエリーとして転送
  - V2 レポートを受信した場合、破棄
- V2 設定時
  - V1 クエリーを受信した場合、V1 クエリーとして転送
  - V1 レポートを受信した場合、V2 レポートとして転送

[設定例]

VLAN #2 で MLD バージョンを 1 に設定する。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping version 1
```

VLAN #2 で MLD バージョンを初期値に戻す。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#no ipv6 mld snooping version
```

8.3.7 MLD レポート抑制機能の設定

[書式]

ipv6 mld snooping report-suppression *switch*
no ipv6 mld snooping report-suppression

[パラメーター]

switch : MLD レポート抑制機能

設定値	説明
enable	有効にする
disable	無効にする

[初期設定]

ipv6 mld snooping report-suppression enable

[入力モード]

インターフェースモード

[説明]

MLD レポート抑制機能を設定する。

no 形式で実行した場合は初期設定に戻る。

有効にした場合は、受信した Report メッセージや Leave メッセージから得た情報をもとに、最小限のメッセージをマルチキャストルーターポートへ送信する。

無効にした場合は、受信した Report メッセージや Leave メッセージを逐次マルチキャストルーターポートへ転送する。

[ノート]

本コマンドは VLAN インターフェースにのみ設定できる。

[設定例]

VLAN #2 で MLD レポート抑制機能を有効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping report-suppression enable
```

VLAN #2 で MLD レポート抑制機能を無効にする。

```
SWP2#configure terminal
SWP2(config)#interface vlan2
SWP2(config-if)#ipv6 mld snooping report-suppression disable
```

8.3.8 マルチキャストルーター接続ポート情報の表示

[書式]

show ipv6 mld snooping mrouter *ifname*

[パラメーター]

ifname : VLAN インターフェース名
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

動的に学習された、または静的に設定したマルチキャストルーター接続ポート情報を表示する。

[設定例]

VLAN #2 のマルチキャストルーター接続ポートの情報を表示する。

```
SWP2#show ipv6 mld snooping mrouter vlan2
VLAN    Interface             IP-address    Expires
2       port1.11(dynamic)         fe80::ae44:f2ff:fe30:291        00:01:04
```

8.3.9 MLD グループメンバーシップ情報の表示

[書式]

show ipv6 mld snooping groups [detail]
show ipv6 mld snooping groups *X*:*X*::*X*:*X* [detail]
show ipv6 mld snooping groups *ifname* [detail]

[キーワード]

detail	:	詳細情報

[パラメーター]

X:X::X:X	:	マルチキャストグループアドレス
ifname	:	VLAN インターフェース名 表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

MLD グループメンバーシップ情報を表示する。

[設定例]

MLD グループメンバーシップの情報を表示する。

```
SWP2#show ipv6 mld snooping groups
MLD Connected Group Membership
Group Address                              Interface            Uptime   Expires  Last
Reporter
ff15::1                                    port1.3              00:00:44 00:01:07
fe80::a00:27ff:fe8b:87e3
```

MLD グループメンバーシップの詳細情報を表示する。

```
SWP2#show ipv6 mld snooping groups detail
MLD Snooping Group Membership Details
Flags: (R - Remote, S - Static)

Interface:      port1.3
Group:          ff15::1
Uptime:         00:00:03
Group mode:     Include ()
Last reporter:  fe80::a00:27ff:fe8b:87e3
Group source list: (R - Remote, M - SSM Mapping, S - Static )
    Source Address                           Uptime    v2 Exp    Fwd  Flags
    fe80::221:70ff:fef9:8a39               00:00:03  00:01:06  Yes  R
```

8.3.10 インターフェースの MLD 関連情報を表示

[書式]

show ipv6 mld snooping interface *ifname*

[パラメーター]

ifname	:	VLAN インターフェース名 表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

VLAN インターフェースの MLD 関連情報を表示する。

[設定例]

VLAN #1 の MLD 関連情報を表示する。

```
SWP2#show ipv6 mld snooping interface vlan1
```

```
MLD Snooping information for vlan1
 MLD Snooping enabled
 Snooping Querier none
 MLD Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 MLDv1 fast-leave is disabled
 MLDv1 Report suppression enabled
 MLDv2 Report suppression enabled
 Router port detection using MLD Queries
 Number of router-ports: 0
 Number of Groups: 0
 Number of v1-reports: 0
 Number of v1-leaves: 0
 Number of v2-reports: 127
 Number of v1-query-warnings: 0
 Number of v2-query-warnings: 0
 Active Ports:
  port1.1
  port1.2
```

8.3.11 MLD グループメンバーシップのエントリー削除

[書式]

clear ipv6 mld snooping
clear ipv6 mld snooping group *X:X::X:X*
clear ipv6 mld snooping interface *ifname*

[キーワード]

group	:	削除するマルチキャストグループアドレスを指定する
interface	:	削除する VLAN インターフェースを指定する

[パラメーター]

X:X::X:X	:	マルチキャストグループアドレス "*"は全エントリー
ifname	:	VLAN インターフェース名 削除するインターフェース

[入力モード]

特権 EXEC モード

[説明]

MLD グループメンバーシップのエントリーを削除する。

[設定例]

VLAN #1 の MLD グループメンバーシップのエントリーを削除する。

```
SWP2#clear ipv6 mld snooping interface vlan1
```

第 9 章

トラフィック制御

9.1 ACL

9.1.1 IPv4 アクセスリストの生成

[書式]

access-list *ipv4-acl-id* [*seq_num*] *action protocol src-info* [*src-port*] *dst-info* [*dst-port*] [**ack**] [**fin**] [**psh**] [**rst**] [**syn**] [**urg**]
no access-list *ipv4-acl-id* [*seq_num*] [*action protocol src-info* [*src-port*] *dst-info* [*dst-port*] [**ack**] [**fin**] [**psh**] [**rst**] [**syn**] [**urg**]]

[キーワード]

ack : protocol に tcp を指定した場合、条件に TCP ヘッダの ACK フラグを指定する。

fin : protocol に tcp を指定した場合、条件に TCP ヘッダの FIN フラグを指定する。

psh : protocol に tcp を指定した場合、条件に TCP ヘッダの PSH フラグを指定する。

rst : protocol に tcp を指定した場合、条件に TCP ヘッダの RST フラグを指定する。

syn : protocol に tcp を指定した場合、条件に TCP ヘッダの SYN フラグを指定する。

urg : protocol に tcp を指定した場合、条件に TCP ヘッダの URG フラグを指定する。

[パラメーター]

ipv4-acl-id : <1-2000>

IPv4 アクセスリストの ID

seq_num : <1-65535>

シーケンス番号。対象アクセスリスト内におけるエントリーの位置を指定する。

シーケンス番号を省略した場合は、リストの最後尾にエントリーが追加される。このとき、既存の最後尾エントリーに 10 を加算した値が新規エントリーの番号として自動採番される。(最初にシーケンス番号なしで追加した場合、エントリーの番号は 10 になる。)

action : アクセス条件に対する動作を指定する

設定値	説明
deny	条件を"拒否"する
permit	条件を"許可"する

protocol : 対象とするプロトコル種別を指定する

設定値	説明
<0-255>	IP ヘッダのプロトコル番号
any	すべての IPv4 パケット
tcp	TCP パケット
udp	UDP パケット

src-info : 条件とする送信元 IPv4 アドレス情報を設定する

設定値	説明
A.B.C.D E.F.G.H	ワイルドカードビット(E.F.G.H)付きの IPv4 アドレス(A.B.C.D)を指定する
A.B.C.D/M	サブネットマスク長(Mbit)付きの IPv4 アドレス(A.B.C.D)を指定する
host A.B.C.D	単一の IPv4 アドレス(A.B.C.D)を指定する
any	すべての IPv4 アドレスを対象とする

src-port : <0-65535>

protocol に tcp, udp を指定した場合、条件とする送信元ポート番号<0-65535>を指定する。省略することも可能

指定方法	説明
eq X	ポート番号(X)を指定する
range X Y	ポート番号(X)から(Y)を指定する

dst-info : 条件とする宛先 IPv4 アドレス情報を設定する

設定値	説明
A.B.C.D E.F.G.H	ワイルドカードビット(E.F.G.H)付きの IPv4 アドレス(A.B.C.D)を指定する
A.B.C.D/M	サブネットマスク長(Mbit)付きの IPv4 アドレス(A.B.C.D)を指定する
host A.B.C.D	単一の IPv4 アドレス(A.B.C.D)を指定する
any	すべての IPv4 アドレスを対象とする

dst-port : <0-65535>

protocol に tcp, udp を指定した場合、条件とする宛先ポート番号<0-65535>を指定する。省略することも可能

指定方法	説明
eq X	ポート番号(X)を指定する
range X Y	ポート番号(X)から(Y)を指定する

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

IPv4 アクセスリストを生成する。

生成したアクセスリストには、複数(MAX:256 件)の条件を設定することができる。

生成した IPv4 アクセスリストを適用させる場合は、インターフェースモードで **access-group** コマンドを使用する。

no 形式で action 以降を指定した場合は、条件全てが一致する IPv4 アクセスリストを削除する。

no 形式で action 以降を指定しなかった場合は、アクセスリストの ID が一致する IPv4 アクセスリストを削除する。

[ノート]

LAN/SFP+ポートおよび論理インターフェースに適用しているアクセスリストは、no 形式で削除することはできない。必ず適用を解除してから削除すること。

src-port, dst-port 共に、range で範囲が指定できるが、このように範囲を指定した IPv4 アクセスリストはシステム全体で一つだけ **access-group** コマンドでインターフェースに適用できる。

[設定例]

送信元 192.168.1.0/24 のセグメントから、172.16.1.1 への通信を拒否する IPv4 アクセスリスト #1 を作成する。

```
SWP2(config)#access-list 1 deny any 192.168.1.0 0.0.0.255 host 172.16.1.1
```

IPv4 アクセスリスト #1 を削除する。

```
SWP2(config)#no access-list 1
```

9.1.2 IPv4 アクセスリストの説明文追加

[書式]

access-list *ipv4-acl-id* **description** *line*
no access-list *ipv4-acl-id* **description**

[パラメーター]

ipv4-acl-id : <1-2000>
説明文を追加する IPv4 アクセスリストの ID

line : 追加する説明文。ASCII で 32 文字まで設定可能

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

生成してある IPv4 アクセスリストに説明文を追加する。
no 形式で実行した場合、IPv4 アクセスリストの説明文を削除する。

[ノート]

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た後も、本コマンドで説明文を追加することは可能。(後着の説明文が上書きする)

[設定例]

送信元 192.168.1.0/24 のセグメントから、172.16.1.1 への通信を拒否する IPv4 アクセスリスト #1 を作成し、説明文「Test」を追加する。

```
SWP2(config)#access-list 1 deny any 192.168.1.0 0.0.0.255 host 172.16.1.1
SWP2(config)#access-list 1 description Test
```

9.1.3 IPv4 アクセスリストの適用

[書式]

access-group *ipv4-acl-id direction*
no access-group *ipv4-acl-id direction*

[パラメーター]

ipv4-acl-id : <1-2000>
適用する IPv4 アクセスリストの ID

direction : 適用フレームの方向を指定する

設定値	説明
in	受信フレームに対して適用させる
out	送信フレームに対して適用させる

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

LAN/SFP+ポートおよび論理インターフェースに IPv4 アクセスリストを適用する。

受信/送信フレームがアクセスリストの条件と一致した場合、アクセスリストのアクションが該当フレームに対するアクション(permit, deny)となる。

no 形式で実行した場合、適用したアクセスリストを LAN/SFP+ポートおよび論理インターフェースから削除する。

[ノート]

アクセスリストは、同一のインターフェースに、受信フレーム(in)と送信フレーム(out)のそれぞれに 1 つずつしか登録できない。

送信フレームに対するアクセスリストは LAN/SFP+ポートに対してのみ適用可能。

制約事項は以下の通り。

ポート番号範囲(range X Y)を指定した IPv4 アクセスリストは、送信フレーム(out)に適用できない。

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ない。

受信フレームに対するアクセスリスト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ない。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る。

[設定例]

LAN ポート #1 の受信フレームに対して、アクセスリスト #1 を適用する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#access-group 1 in
```

9.1.4 IPv6 アクセスリストの生成

[書式]

access-list *ipv6-acl-id* [*seq_num*] *action src-info*
no access-list *ipv6-acl-id* [*seq_num*] [*action src-info*]

[パラメーター]

ipv6-acl-id : <3001-4000>

IPv6 アクセスリストの ID

seq_num : <1-65535>

シーケンス番号。対象アクセスリスト内におけるエントリーの位置を指定する。

シーケンス番号を省略した場合は、リストの最後尾にエントリーが追加される。このとき、既存の最後尾エントリーに 10 を加算した値が新規エントリーの番号として自動採番される。(最初にシーケンス番号なしで追加した場合、エントリーの番号は 10 になる。)

action : アクセス条件に対する動作を指定する

設定値	説明
deny	条件を"拒否"する
permit	条件を"許可"する

src-info : 条件とする送信元 IPv6 アドレス情報を設定する

設定値	説明
X:X::X:X/M	サブネットマスク長(Mbit)付きの IPv6 アドレス(X:X::X:X)を指定する
any	すべての IPv6 アドレスを対象とする

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

IPv6 アクセスリストを生成する。

生成したアクセスリストには、複数(MAX:256 件)の条件を設定することができる。

生成したアクセスリストを適用させる場合は、インターフェースモードで **access-group** コマンドを使用する。

no 形式で action 以降を指定した場合は、条件全てが一致する IPv6 アクセスリストを削除する。

no 形式で action 以降を指定しなかった場合は、アクセスリストの ID が一致する IPv6 アクセスリストを削除する。

[ノート]

LAN/SFP+ポートおよび論理インターフェースに適用しているアクセスリストは、no 形式で削除することはできない。必ず適用を解除してから削除すること。

[設定例]

3ffe:506::/32 からのパケットを拒否する IPv6 アクセスリスト #3002 を作成する。

```
SWP2(config)#access-list 3002 deny 3ffe:506::/32
```

IPv6 アクセスリスト #3002 を削除する。

```
SWP2(config)#no access-list 3002
```

9.1.5 IPv6 アクセスリストの説明文追加

[書式]

access-list *ipv6-acl-id* **description** *line*
no access-list *ipv6-acl-id* **description**

[パラメーター]

ipv6-acl-id	:	<3001-4000> 説明文を追加する IPv6 アクセスリストの ID
line	:	追加する説明文。ASCII で 32 文字まで設定可能

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

生成してある IPv6 アクセスリストに説明文を追加する。

no 形式で実行した場合、IPv6 アクセスリストの説明文を削除する。

[ノート]

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た後も、本コマンドで説明文を追加することは可能。(後着の説明文で上書きする)

[設定例]

3ffe:506::/32 からのパケットを拒否する IPv6 アクセスリスト #3002 を作成し、説明文「Test」を追加する。

```
SWP2(config)#access-list 3002 deny 3ffe:506::/32
SWP2(config)#access-list 3002 description Test
```

9.1.6 IPv6 アクセスリストの適用

[書式]

access-group *ipv6-acl-id direction*
no access-group *ipv6-acl-id direction*

[パラメーター]

ipv6-acl-id : <3001-4000>

適用する IPv6 アクセスリストの ID

direction : 適用フレームの方向を指定する

設定値	説明
in	受信フレームに対して適用させる
out	送信フレームに対して適用させる

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

LAN/SFP+ポートおよび論理インターフェースに IPv6 アクセスリストを適用する。

受信/送信フレームがアクセスリストの条件と一致した場合、アクセスリストのアクションが該当フレームに対するアクション(permit, deny)となる。

no 形式で実行した場合、適用したアクセスリストを LAN/SFP+ポートおよび論理インターフェースから削除する。

[ノート]

アクセスリストは、同一のインターフェースに、受信フレーム(in)と送信フレーム(out)のそれぞれに 1 つずつしか登録できない。

送信フレームに対するアクセスリストは LAN/SFP+ポートに対してのみ適用可能である。

制約事項は以下の通り。

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ない。

受信フレームに対するアクセスリスト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ない。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る。

[設定例]

LAN ポート #1 の受信フレームに対して、IPv6 アクセスリスト #3002 を適用する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#access-group 3002 in
```

9.1.7 MAC アクセスリストの生成

[書式]

access-list *mac-acl-id* [*seq_num*] *action src-info dst-info*

no access-list *mac-acl-id* [*seq_num*] [*action src-info dst-info*]

[パラメーター]

mac-acl-id : <2001-3000>

MAC アクセスリストの ID

seq_num : <1-65535>

シーケンス番号。対象アクセスリスト内におけるエントリーの位置を指定する。

シーケンス番号を省略した場合は、リストの最後尾にエントリーが追加される。このとき、既存の最後尾エントリーに 10 を加算した値が新規エントリーの番号として自動採番される。(最初にシーケンス番号なしで追加した場合、エントリーの番号は 10 になる。)

action : アクセス条件に対する動作を指定する

設定値	説明
deny	条件を"拒否"する
permit	条件を"許可"する

src-info : 条件とする送信元 MAC アドレス情報を設定する

設定値	説明
HHHH.HHHH.HHHH WWWW.WWWW.WWWW	ワイルドカードビット(WWWW.WWWW.WWWW)付きの MAC アドレス(HHHH.HHHH.HHHH)を指定する
host HHHH.HHHH.HHHH	単一の MAC アドレス(HHHH.HHHH.HHHH)を指定する
any	すべての MAC アドレスを対象とする

dst-info : 条件とする宛先 MAC アドレス情報を設定する

設定値	説明
HHHH.HHHH.HHHH WWWW.WWWW.WWWW	ワイルドカードビット(WWWW.WWWW.WWWW)付きの MAC アドレス(HHHH.HHHH.HHHH)を指定する
host HHHH.HHHH.HHHH	単一の MAC アドレス(HHHH.HHHH.HHHH)を指定する
any	すべての MAC アドレスを対象とする

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

MAC アクセスリストを生成する。

生成したアクセスリストには、複数(MAX:256 件)の条件を設定することができる。

生成したアクセスリストを適用させる場合は、インターフェースモードで **access-group** コマンドを実行する。

no 形式で action 以降を指定した場合は、条件全てが一致する MAC アクセスリストを削除する。

no 形式で action 以降を指定しなかった場合は、アクセスリストの ID が一致する MAC アクセスリストを削除する。

[ノート]

LAN/SFP+ポートおよび論理インターフェースに適用しているアクセスリストは、no 形式で削除することはできない。必ず適用を解除してから削除すること。

"W", "H"は 0-9,a-f,A-F からなる 1 文字となる。

[設定例]

MAC アドレス 00-A0-DE-12-34-56 からのフレームを拒否する MAC アクセスリスト #2001 を作成する。

```
SWP2(config)#access-list 2001 deny mac 00A0.DE12.3456 0000.0000.0000 any
```

MAC アクセスリスト #2001 を削除する。

```
SWP2(config)#no access-list 2001
```

9.1.8 MAC アクセスリストの説明文追加

[書式]

access-list *mac-acl-id* **description** *line*

no access-list *mac-acl-id* **description**

[パラメーター]

mac-acl-id : <2001-3000>
説明文を追加する MAC アクセスリストの ID

line : 追加する説明文。ASCII で 32 文字まで設定可能

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

生成してある MAC アクセスリストに説明文を追加する。

no 形式で実行した場合、MAC アクセスリストの説明文を削除する。

[ノート]

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た後も、本コマンドで説明文を追加することは可能。(後着の説明文が上書きする)

[設定例]

MAC アドレス 00-A0-DE-12-34-56 からのフレームを拒否する MAC アクセスリスト #2001 を作成し、説明文「Test」を追加する。

```
SWP2(config)#access-list 2001 deny mac 00A0.DE12.3456 0000.0000.0000 any
SWP2(config)#access-list 2001 description Test
```

9.1.9 MAC アクセスリストの適用

[書式]

access-group *mac-acl-id direction*
no access-group *mac-acl-id direction*

[パラメーター]

mac-acl-id : <2001-3000>
適用する MAC アクセスリストの ID

direction : 適用フレームの方向を指定する

設定値	説明
in	受信フレームに対して適用させる

[初期設定]

なし

[入力モード]

インターフェースモード

[説明]

LAN/SFP+ポートおよび論理インターフェースに対して MAC アクセスリストを適用する。

受信フレームがアクセスリストの条件と一致した場合、アクセスリストのアクションが該当フレームに対するアクション(permit, deny)となる。

no 形式で実行した場合、適用したアクセスリストを LAN/SFP+ポートおよび論理インターフェースから削除する。

[ノート]

同一のインターフェースに複数のアクセスリストを登録することはできない。

制約事項は以下の通り。

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ない。

受信フレームに対するアクセスリスト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ない。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る。

[設定例]

LAN ポート #1 の受信フレームに対して、アクセスリスト #2001 を適用する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#access-group 2001 in
```

9.1.10 生成したアクセスリストの表示

[書式]

show access-list [*acl_id*]

[パラメーター]

acl-id : <1-2000>, <2001-3000>, <3001-4000>
アクセスリストの ID

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

登録されているアクセスリストを表示する。

acl_id を省略した場合は、全てのアクセスリストを表示する。

インターフェースに適用され、かつ、条件にあったフレームを 1 つ以上受信または転送した場合、そのフレームの統計数(match)も表示する。

[ノート]

トラフィック分類(QoS)の条件にあったフレームの統計数(match)もカウントアップする。

[設定例]

一覧を表示する。

```
SWP2>show access-list
IPv4 access list 1
    10 deny any 192.168.1.0/24 host 172.16.1.1 [match= 62]
MAC access list 2001
    10 deny host 00A0.DE12.3456 any [match= 123]
IPv6 access list 3002
    10 deny 3ffe:506::/32
```

9.1.11 統計数のクリア

[書式]

clear access-list counters [*acl_id*]

[パラメーター]

acl-id : <1-2000>, <2001-3000>, <3001-4000>
アクセスリストの ID

[入力モード]

特権 EXEC モード

[説明]

show access-list コマンドで表示される統計数(match)をクリアする。

[設定例]

統計数をクリアする。

```
SWP2>clear access-list counters
```

9.1.12 インターフェースに適用したアクセスリストの表示

[書式]

show access-group

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

インターフェース毎に、適用されている全アクセスリストの ID を表示する。

[設定例]

一覧を表示する。

```
SWP2>show access-group
Interface port1.1 : IPv4 access group 1 in
Interface port1.7 : IPv6 access group 3002 in
Interface port1.8 : MAC access group 2001 in
```

9.1.13 VLAN アクセスマップの設定および VLAN アクセスマップモードへの移行

[書式]

vlan access-map *access-map-name*
no vlan access-map *access-map-name*

[パラメーター]

access-map-name : 半角英数字および半角記号(256 文字以内)
アクセスマップ名

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

access-map-name で指定した名前の VLAN アクセスマップを作成したのち、VLAN アクセスマップを設定するための VLAN アクセスマップモードに移行する。

no 形式で実行した場合は、指定した VLAN アクセスマップを削除する。

[ノート]

VLAN アクセスマップモードからグローバルコンフィグレーションモードに戻るには **exit** コマンドを使用し、特権 EXEC モードに戻るには **end** コマンドを使用する。

[設定例]

VAM001 という名前の VLAN アクセスマップを作成して、VLAN アクセスマップモードへ移行する。

```
SWP2(config)#vlan access-map VAM001
SWP2(config-vlan-access-map)#
```

9.1.14 VLAN アクセスマップに対するアクセスリストの設定

[書式]

match access-list *list-id*
no match access-list *list-id*

[パラメーター]

list-id : <1-2000>, <2001-3000>, <3001-4000>
access-list コマンドで設定されているアクセスリスト番号

[初期設定]

なし

[入力モード]

VLAN アクセスマップモード

[説明]

対象 VLAN アクセスマップに適用するアクセスリストを設定する。

no 形式で実行した場合は、指定したアクセスリストを対象 VLAN アクセスマップから削除する。

[ノート]

1 つの VLAN アクセスマップに対して設定可能なアクセスリストは、1 つのみ。

show vlan access-map コマンドで設定を確認できる。

[設定例]

VAM001 という名前の VLAN アクセスマップを作成して、192.168.0.1 からのパケットを拒否するアクセスリストを設定する。

```
SWP2(config)#access-list 2 deny any 192.168.0.1/32 any
SWP2(config)#vlan access-map VAM001
SWP2(config-vlan-access-map)#match access-list 2
```

9.1.15 VLAN アクセスマップフィルターの設定

[書式]

vlan filter *access-map-name vlan-id* [*direction*]
no vlan filter *access-map-name vlan-id* [*direction*]

[パラメーター]

access-map-name : 半角英数字および半角記号(256 文字以内)
vlan access-map コマンドで設定されているアクセスマップ名

vlan-id : <1-4094>
vlan コマンドで enable 状態に設定されている VLAN ID

direction : 適用フレームの方向を指定する。省略した場合は受信フレームに対して適用される

設定値	説明
in	受信フレームに対して適用させる
out	送信フレームに対して適用させる

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

指定した VLAN に VLAN アクセスマップフィルターを適用する。

no 形式で実行した場合は、指定した VLAN に対する VLAN アクセスマップフィルターを削除する。

[ノート]

disable 状態に設定されている VLAN ID に対して本コマンドを設定することはできない。

VLAN アクセスマップは、同一のインターフェースに、受信フレーム(in)と送信フレーム(out)にそれぞれ 1 つずつ適用できる。

ただし、以下のアクセスリストを設定した VLAN アクセスマップは、送信フレーム(out)に適用できない。

- MAC アクセスリスト
- ポート番号範囲(range X Y)を指定した IPv4 アクセスリスト

[設定例]

VAM001 という名前の VLAN アクセスマップを作成して、192.168.0.1 からのパケットを拒否するアクセスリストを設定したのち、VLAN #1000 の受信フレームに対して VAM001 を適用する。

```
SWP2(config)#vlan database
SWP2(config-vlan)#vlan 1000
```

```
SWP2(config-vlan)#exit
SWP2(config)#access-list 2 deny any 192.168.0.1/32 any
SWP2(config)#vlan access-map VAM001
SWP2(config-vlan-access-map)#match access-list 2
SWP2(config-vlan-access-map)#exit
SWP2(config)#vlan filter VAM001 1000 in
```

9.1.16 VLAN アクセスマップの表示

[書式]

show vlan access-map

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

登録されている VLAN アクセスマップを表示する。

以下の項目が表示される。

- VLAN アクセスマップの名前
- VLAN アクセスマップに適用されているアクセスリスト

[設定例]

VLAN アクセスマップの情報を表示する。

```
SWP2>show vlan access-map
Vlan access-map VAM001
    match ipv4 access-list 2
```

9.1.17 VLAN アクセスマップフィルターの表示

[書式]

show vlan filter

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

VLAN アクセスマップフィルターの適用情報を表示する。

以下の項目が表示される。

- VLAN アクセスマップの名前
- VLAN アクセスマップが適用されている VLAN ID
- VLAN アクセスマップが適用されているフレームの方向(in/out)

[設定例]

VLAN アクセスマップフィルターの情報を表示する。

```
SWP2>show vlan filter
Vlan Filter VAM001 is applied to vlan 1000 in
Vlan Filter VAM001 is applied to vlan 1001 out
Vlan Filter VAM002 is applied to vlan 2000-2001 in
```

9.2 QoS (Quality of Service)

9.2.1 QoS の有効・無効制御

[書式]

qos *action*
qos_disable

[パラメーター]

action : Qos の動作

設定値	説明
enable	Qos を有効にする
disable	Qos を無効にする

[初期設定]

no qos

[入力モード]

グローバルコンフィグレーションモード

[説明]

QoS を有効にする。

no 形式で実行した場合、QoS を無効する。このとき、関連する QoS 設定も同時に削除する。

[ノート]

フロー制御のシステム設定が有効な場合、Qos を有効にすることはできない。

QoS 関連コマンドは、QoS を有効にしておかないと実行できないものが多数ある。

[設定例]

QoS を有効にする。

```
SWP2(config)#qos enable
```

QoS を無効にする。

```
SWP2(config)#qos disable
```

9.2.2 デフォルト CoS の設定

[書式]

qos cos *value*
no qos cos

[パラメーター]

value : <0-7>
デフォルト CoS 値

[初期設定]

qos cos 0

[入力モード]

インターフェースモード

[説明]

LAN/SFP+ポートおよび論理インターフェースのデフォルト CoS を設定する。

no 形式で実行した場合、初期値(CoS=0)を設定する。

デフォルト CoS は、インターフェースのトラストモードが CoS に設定されている状態でタグなしフレームを受信した際に使用される。(フレームに CoS が設定されていないため)

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

実行するインターフェースのトラストモードが CoS ではない場合、本コマンドは実行エラーとなる。

デフォルト CoS 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ない。

実行するインターフェースが論理インターフェースに所属している LAN/SFP+ポートの場合、本コマンドは実行エラーとなる。ただし、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る。

[設定例]

デフォルト CoS 値を 2 に設定する。

```
SWP2(config-if)#qos cos 2
```

デフォルト CoS 値を初期値に戻す。

```
SWP2(config-if)#no qos cos
```

9.2.3 トラストモードの設定

[書式]

qos trust *mode*
no qos trust

[パラメーター]

mode : トラストモード

設定値	説明
cos	送信キューを CoS 値に基づいて決定する
dscp	送信キューを DSCP 値に基づいて決定する
port-priority	受信ポートに設定された優先度を適用する

[初期設定]

qos trust cos

[入力モード]

インターフェースモード

[説明]

LAN/SFP+ポートおよび論理インターフェースのトラストモードを設定する。

no 形式で実行した場合、初期値(CoS トラストモード)を設定する。

トラストモードが cos の場合は、受信フレームの CoS 値を使用して送信キューの決定を行い、dscp の場合は、受信フレームの DSCP 値を使用して送信キューの決定を行う。port-priority の場合は、受信インターフェースに設定された優先度に基づいて、送信キューの決定を行う。

CoS 値や DSCP 値、受信ポートに対応付ける送信キューは、以下のコマンドで変更することができる。

トラストモード	送信キュー決定に使用する設定値	対応コマンド
CoS	CoS-送信キュー ID 変換テーブル	**qos cos-queue**
DSCP	DSCP-送信キュー ID 変換テーブル	**qos dscp-queue**
Port Priority	受信ポートごとに設定された優先度	**qos port-priority-queue**

なお、QoS の一連の処理の中で、送信キューを決定する(変更する)タイミングは 4 種類ある。

1. 送信キュー割り当て時
2. クラスマップによる送信キュー指定
3. クラスマップによるプレマーキング指定
4. クラスマップによるリマーキング指定

2, 3, 4 はトラストモード"CoS"または"DSCP"の場合のみ指定可能であり、いずれの場合も自身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」を参照することにより、送信キューが割り当てられる。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

LAN/SFP+ポートおよび論理インターフェースにポリシーマップが適用されている場合、トラストモードの変更はできない。

トラストモードが異なる 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ない。

論理インターフェースに所属している LAN/SFP+ポートはトラストモードの変更はできない。ただし、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る。

QoS 機能では、トラストモードによって実行制限があるものや、表示結果の異なるものがある。

[設定例]

LAN/SFP+ポートおよび論理インターフェースのトラストモードを DSCP に設定する。

```
SWP2(config-if)#qos trust dscp
```

LAN/SFP+ポートおよび論理インターフェースのトラストモードをデフォルト(CoS)に設定する。

```
SWP2(config-if)#no qos trust
```

9.2.4 QoS 機能の設定状態の表示

[書式]

show qos

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

QoS 機能の有効(Enable)、無効(Disable)状態を表示する。

[設定例]

システムの QoS の設定状態を表示する。

```
SWP2#show qos
  Enable
```

9.2.5 インターフェースの QoS 情報の表示

[書式]

show qos interface [*ifname*]

[パラメーター]

ifname : LAN/SFP+ポートおよび論理インターフェース名。省略時は全ポートを対象とする。
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

指定したインターフェースの QoS 設定情報を表示する。表示内容は以下のとおり。

項目	説明
Port Trust Mode	インターフェースのトラストモード(CoS/DSCP/Port-Priority)
Input Policy-Map Name	インターフェースに適用済みのポリシーマップ名とクラスマップ情報(注 1)
Port Default CoS Priority	デフォルト CoS 値(注 2)
Port-Priority-Queue	ポート優先度(注 3)
Egress Traffic Shaping	トラフィックシェーピング(ポート単位)
Egress Traffic Queue Shaping	トラフィックシェーピング(キュー単位)
Queue Scheduling	送信キューのスケジューリング方式と重み
CoS (Queue)	CoS-送信キュー ID 変換テーブル(注 2)
DSCP (Queue)	DSCP-送信キュー ID 変換テーブル(注 4)
Special Queue Assignment: Sent From CPU	CPU から送信されるフレームの送信キュー指定

注 1) 適用されているポリシーマップがない場合は表示されない。クラスマップ情報の詳細は **show class-map** コマンドを参照のこと。

注 2) トラストモードが"CoS"の場合のみ表示される。

注 3) トラストモードが"ポート優先"の場合のみ表示される。

注 4) トラストモードが"DSCP"の場合のみ表示される。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

LAN ポート #1 の QoS 設定を表示する。(トラストモード CoS)

```
SWP2#show qos interface port1.1

  Port Trust Mode: CoS

  Port Default CoS Priority: 0

  Egress Traffic Shaping: Rate 30016 Kbps, Burst 1876 KByte

  Queue Scheduling:
  Queue0 : Weight  1 ( 5.3%)
  Queue1 : Weight  1 ( 5.3%)
  Queue2 : Weight  2 (10.5%)
  Queue3 : Weight  5 (26.3%)
  Queue4 : Weight  5 (26.3%)
  Queue5 : Weight  5 (26.3%)
  Queue6 : SP
  Queue7 : SP

  Cos (Queue): 0(2), 1(0), 2(1), 3(3), 4(4), 5(5), 6(6), 7(7)

  Special Queue Assignment:
    Sent From CPU: Queue7
```

LAN ポート #1 の QoS 設定を表示する。(トラストモード DSCP)

```
SWP2#show qos interface port1.1

  Port Trust Mode: DSCP

  Egress Traffic Shaping: Not Configured

  Queue Scheduling:
  Queue0 : SP
  Queue1 : SP
  Queue2 : SP
  Queue3 : SP
  Queue4 : SP
  Queue5 : SP
  Queue6 : SP
  Queue7 : SP

  DSCP (Queue):  0(2),  1(2),  2(2),  3(2),  4(2),  5(2),  6(2),  7(2)
                 8(0),  9(0), 10(0), 11(0), 12(0), 13(0), 14(0), 15(0)
                16(1), 17(1), 18(1), 19(1), 20(1), 21(1), 22(1), 23(1)
                24(3), 25(3), 26(3), 27(3), 28(3), 29(3), 30(3), 31(3)
                32(4), 33(4), 34(4), 35(4), 36(4), 37(4), 38(4), 39(4)
                40(5), 41(5), 42(5), 43(5), 44(5), 45(5), 46(5), 47(5)
                48(6), 49(6), 50(6), 51(6), 52(6), 53(6), 54(6), 55(6)
                56(7), 57(7), 58(7), 59(7), 60(7), 61(7), 62(7), 63(7)

  Special Queue Assignment:
    Sent From CPU: Queue7
```

9.2.6 送信キュー使用率の表示

[書式]

show qos queue-counters [*ifname*]

[パラメーター]

ifname : LAN/SFP+ポート名。省略時は全ポートを対象とする。
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

指定した LAN/SFP+ポートの送信キュー毎の使用率を表示する。キューの使用率は以下で計算する。

(キューの使用率) = (キューに格納されているバッファ数) / (キューの最大長)

[ノート]

本コマンドは QoS の状態(有効/無効)にかかわらず使用できる。

[設定例]

LAN ポート #1 のキュー使用率を表示する。

```
SWP2#show qos queue-counters port1.1
QoS: Enable
Interface port1.1 Queue Counters:
  Queue 0          59.4 %
  Queue 1          15.0 %
  Queue 2           0.0 %
  Queue 3           0.0 %
  Queue 4           0.0 %
  Queue 5           3.6 %
  Queue 6           0.0 %
  Queue 7           0.1 %
```

9.2.7 CoS-送信キュー ID 変換テーブルの設定

[書式]

qos cos-queue *cos-value queue-id*
no qos cos-queue *cos-value*

[パラメーター]

cos-value : <0-7>
変換元の CoS 値

queue-id : <0-7>
CoS 値に対応する送信キュー ID

[初期設定]

[ノート] 参照

[入力モード]

グローバルコンフィグレーションモード

[説明]

送信キューを決定するために使用する CoS-送信キュー ID 変換テーブルの値を設定する。

no 形式で実行した場合、指定した CoS 値の送信キュー ID を初期設定に戻す。

CoS-送信キュー ID 変換テーブルは、トラストモードが CoS に設定されている場合に使用される。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

CoS-送信キュー ID 変換テーブルの初期設定は下表のとおり。

CoS 値	送信キュー
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

[設定例]

CoS 値"0"に対して送信キュー #4 を割り当てる。

```
SWP2(config)#qos cos-queue 0 4
```

CoS 値"0"の送信キュー ID を初期値に戻す。

```
SWP2(config)#no qos cos-queue 0
```

9.2.8 DSCP-送信キュー ID 変換テーブルの設定

[書式]

qos dscp-queue *dscp-value queue-id*
no qos dscp-queue *dscp-value*

[パラメーター]

dscp-value : <0-63>
変換元の DSCP 値

queue-id : <0-7>
DSCP 値に対応する送信キュー ID

[初期設定]

[ノート] 参照

[入力モード]

グローバルコンフィグレーションモード

[説明]

送信キューを決定するために使用する DSCP-送信キュー ID 変換テーブルの値を設定する。
no 形式で実行した場合、指定した DSCP 値の送信キュー ID を初期設定に戻す。
DSCP-送信キュー ID 変換テーブルは、トラストモードが DSCP に設定されている場合に使用される。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。
DSCP-送信キュー ID 変換テーブルの初期設定は下表のとおり。

DSCP 値	送信キュー
0-7	2
8-15	0
16-23	1
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

[設定例]

DSCP 値"0"に対して送信キュー #4 を割り当てる。

```
SWP2(config)#qos dscp-queue 0 4
```

DSCP 値"23"の送信キュー ID を初期値に戻す。

```
SWP2(config)#no qos dscp-queue 23
```

9.2.9 ポート優先度の設定

[書式]

qos port-priority-queue *queue-id*
no qos port-priority-queue

[パラメーター]

queue-id : <0-7>

LAN/SFP+ポートに設定する送信キュー ID

[初期設定]

qos port-priority-queue 2

[入力モード]

インターフェースモード

[説明]

LAN/SFP+ポートおよび論理インターフェースに、受信インターフェースに対応する優先度(送信キュー ID)を設定する。

no 形式で実行した場合、指定したインターフェースの送信キュー ID を初期値(2)に戻す。

ポート優先度は、トラストモードが"ポート優先"に設定されている場合の送信キューの決定に使用される。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

実行するインターフェースのトラストモードが"ポート優先"ではない場合、本コマンドは実行エラーとなる。

ポート優先度が異なる 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ない。

実行するインターフェースが論理インターフェースに所属している LAN/SFP+ポートの場合、本コマンドは実行エラーとなる。ただし、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る。

[設定例]

LAN ポート #1 のポート優先度として、送信キュー ID #4 を割り当てる。

```
SWP2#interface port1.1
SWP2(config-if)#qos port-priority-queue 4
```

9.2.10 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

[書式]

qos queue sent-from-cpu *queue-id*
no qos queue sent-from-cpu

[パラメーター]

queue-id : <0-7>
送信キュー ID

[初期設定]

qos queue sent-from-cpu 7

[入力モード]

グローバルコンフィグレーションモード

[説明]

スイッチ本体(CPU)から各 LAN/SFP+ポートへ送信されるフレームの格納先の送信キューを設定する。

no 形式で実行した場合、初期値(7)を設定する。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

CPU から送信されるフレームの優先度を下げると、より優先度の高いキューからの送信が優先されるため、高負荷の状態で L2MS やループ検出などの機能が動作しなくなる可能性がある。このため、本設定値は可能な限り大きな値(高優先度)とすることを推奨する。

[設定例]

CPU から送信されるフレームの格納先送信キューを #5 に設定する。

```
SWP2(config)#qos queue sent-from-cpu 5
```

9.2.11 クラスマップ(トラフィックの分類条件)の生成

[書式]

class-map *name*
no class-map *name*

[パラメーター]

name : クラスマップ名 (20 文字以下、大文字小文字を区別する)

[入力モード]

グローバルコンフィグレーションモード

[説明]

クラスマップを生成する。

クラスマップは、受信フレームをトラフィッククラスに分類するための条件を定義するものであり、**match** コマンドで定義した条件とそれに対するアクション(permit/deny)で構成される。 クラスマップのアクションは、次のようになる。

- アクセスリスト(ACL)を指定した場合(**match access-group** コマンドを実行)

  ACL に対するアクションがクラスマップのアクションとなる。
- アクセスリスト(ACL)以外を指定した場合

  許可(permit)となる。

生成後、その内容を指定するクラスマップモードに移動する。

no 形式で実行した場合は、指定したクラスマップを削除する。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

指定したクラスマップが生成済みの場合、前回の設定に対して変更が行なわれる。 ただし、ポリシーマップが LAN/SFP+ポートおよび論理インターフェースに適用済みの場合、ポリシーマップに関連付けられているクラスマップは編集・削除することはできない。

[設定例]

クラスマップ"class1"を作成する。

```
SWP2(config)#class-map class1
SWP2(config-cmap)#
```

9.2.12 クラスマップの関連付け

[書式]

class *name*
no class *name*

[パラメーター]

name : クラスマップ名

[入力モード]

ポリシーマップモード

[説明]

ポリシーマップにクラスマップを関連付ける。

クラスマップの関連付けに成功すると、ポリシーマップ・クラスモードに移動する。ポリシーマップ・クラスモードでは、トラフィッククラス毎に以下の設定を行うことができる。

- プレマーキングまたは送信キュー指定
- メータリング
- ポリシング
- リマーキング

no 形式で実行した場合は、ポリシーマップからクラスマップの関連付けを解除する。

ポリシーマップの適用された LAN/SFP+ポートおよび論理インターフェースでは、関連付けをしたクラスマップの条件に従って受信フレームをトラフィッククラスに分類する。 クラスマップのアクションが permit の場合、該当トラフィッククラスに対してユーザーの指定した QoS 処理が行われる。

一つのポリシーマップに関連付けられるクラスマップは、8 つまでとする。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

deny アクションのトラフィッククラスに対して、QoS 処理の設定をしても意味がない。

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする。

- 10.1.0.0 のネットワークからのトラフィックを許可
- CIR:48kbps, CBS:12kbyte, EBS:12kbyte で、帯域クラスを分類
- Green:転送、Yellow:DSCP 値を 10 に書き換え、Red:破棄

[トラフィッククラスの定義]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.13 トラフィック分類条件の設定(access-list)

[書式]

match access-list *acl-id*
no match access-list *acl-id*

[パラメーター]

acl-id : <1 - 2000>
IPv4 アクセスリスト ID
: <2001 - 3000>
MAC アクセスリスト ID
: <3001 - 4000>
IPv6 アクセスリスト ID

[入力モード]

クラスマップモード

[説明]

トラフィッククラスの分類条件にアクセスリストを使用する。

受信フレームがアクセスリストの条件に一致した場合、アクセスリストのアクションがトラフィッククラスのアクション(permit, deny)となる。

no 形式で実行した場合、アクセスリストによる条件設定を削除する。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

トラフィック分類でアクセスリストに設定できる条件は最大 39 件までとなる。

[設定例]

クラスマップ"class1"の分類条件にアクセスリスト #1 を設定する。

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
```

9.2.14 トラフィック分類条件の設定(CoS)

[書式]

match cos *cos-list*

no match cos

[パラメーター]

cos-list : <0 - 7>

分類条件として使用する CoS 値。最大 8 個まで登録できる。

[入力モード]

クラスマップモード

[説明]

トラフィッククラスの分類条件に VLAN タグヘッダの CoS 値を使用する。

no 形式で実行した場合、CoS の条件設定を削除する。

登録数の上限(8 個)まで、設定を繰り返すことができる。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

クラスマップ"class1"の分類条件に CoS 値"1"と"2"を設定する。

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match cos 1 2
```

9.2.15 トラフィック分類条件の設定(TOS 優先度)

[書式]

match ip-precedence *tos-list*

no match ip-precedence

[パラメーター]

tos-list : <0 - 7>

分類条件として使用する IP ヘッダの TOS 優先度(precedence)フィールド値。最大 8 個まで登録できる。

[入力モード]

クラスマップモード

[説明]

トラフィッククラスの分類条件に IP ヘッダの TOS 優先度(precedence)フィールド値を使用する。

no 形式で実行した場合、TOS 優先度による条件設定を削除する。

登録数の上限(8 個)まで、設定を繰り返すことができる。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

クラスマップ"class1"の分類条件に TOS 優先度"3"と"4"を設定する。

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match ip-precedence 3 4
```

9.2.16 トラフィック分類条件の設定(DSCP)

[書式]

match ip-dscp *dscp-list*

no match ip-dscp

[パラメーター]

dscp-list : <0 - 63>

分類条件として使用する IP ヘッダの DSCP(DiffServ Code Point)フィールド値。最大 8 個まで登録できる。

[入力モード]

クラスマップモード

[説明]

トラフィッククラスの分類条件に IP ヘッダの DSCP(DiffServ Code Point)フィールド値を使用する。

no 形式で実行した場合、DSCP による条件設定を削除する。

登録数の上限(8 個)まで、設定を繰り返すことができる。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

クラスマップ"class1"の分類条件に DSCP 値"48"と"56"を設定する。

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match ip-dscp 48 56
```

9.2.17 トラフィック分類条件の設定(Ethernet Type)

[書式]

match ethertype *type*
match ethertype *type* tagged
match ethertype *type* untagged
no match ethertype

[キーワード]

tagged : 条件に VLAN タグ付きを指定する

untagged : 条件に VLAN タグなしを指定する

[パラメーター]

type : イーサネットフレームのタイプを指定する。

設定値	説明
0xXXXX	タイプ値の 16 進表記
any	全てのフレーム

[入力モード]

クラスマップモード

[説明]

トラフィッククラスの分類条件にイーサネットフレームのタイプ値と VLAN タグの有無を使用する。

no 形式で実行した場合、イーサネットフレームのタイプ値と VLAN タグの有無による条件設定を削除する。

既に **match ethertype** コマンドで設定を行っている場合は、内容を変更する。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

tagged 指定はアクセスポートに適用した場合無効となる(アクセスポートではタグ付きフレームを扱わないため)。

[設定例]

クラスマップ"class1"の分類条件に、イーサネットフレームのタイプ値"0x0800"を設定する。

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match ethertype 0x0800
```

9.2.18 トラフィック分類条件の設定(VLAN ID)

[書式]

match vlan *id*
no match vlan

[パラメーター]

id : <1 - 4094>
分類条件として使用する VLAN ID

[入力モード]

クラスマップモード

[説明]

トラフィッククラスの分類条件に VLAN ID を使用する。
no 形式で実行した場合、VLAN ID による条件設定を削除する。
登録数の上限(30 個)まで、設定を繰り返すことができる。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

クラスマップ"class1"の分類条件に VLAN #20 を設定する。

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match vlan 20
```

9.2.19 トラフィック分類条件の設定(VLAN ID レンジ指定)

[書式]

match vlan-range *id-start* **to** *id-end*

[パラメーター]

id-start : <1 - 4094>
分類条件として使用する VLAN ID の開始値。

id-end : <1 - 4094>
分類条件として使用する VLAN ID の終了値。開始から終了までの指定範囲は最大で 30。

[入力モード]

クラスマップモード

[説明]

トラフィッククラスの分類条件に VLAN ID を使用する。
分類条件を削除する場合は、**no match vlan** コマンドを使用する。
match vlan コマンドの設定と併用することができる。
登録数の上限(30 個)まで、**match vlan** コマンドや **match vlan-range** コマンドの設定を繰り返すことができる。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

クラスマップ"class1"の分類条件に、VLAN #20 から#30 までを設定する。

```
SWP2(config)#class-map class1
SWP2(config-cmap)#match vlan-range 20 to 30
```

9.2.20 クラスマップ情報の表示

[書式]

show class-map [*name*]

[パラメーター]

name : クラスマップ名。省略時、すべてのクラスマップ情報が表示される。

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

指定したクラスマップの情報(分類条件)を表示する。クラスマップ毎の表示内容は以下のとおり。

セクション	項目	説明
分類条件(match)	Match Access-List	アクセスリスト ID
	Match ethertype	Ethernet Type
	Match vlan	VLAN ID
	Match vlan-range	
	Match CoS	CoS 値
	Match IP precedence	TOS 優先度
	Match IP DSCP	DSCP 値

- 分類条件は、各種別のうち設定されているものが一つだけ表示される。
- 分類条件は、対応するコマンド(match)が設定されていない場合は表示されない。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

クラスマップ"class1"の情報を表示する。

```
SWP2#show class-map class1

    Class-Map Name: class1
      Match vlan 10
```

9.2.21 受信フレームに対するポリシーマップの生成

[書式]

policy-map *name*
no policy-map *name*

[パラメーター]

name : ポリシーマップ名 (32 文字以下、大文字小文字を区別する)

[入力モード]

グローバルコンフィグレーションモード

[説明]

ポリシーマップを生成する。ポリシーマップは、受信フレームに対する以下の処理をトラフィッククラス毎にまとめたものである。

- トラフィック分類
- プレマーキング
- メータリング
- ポリシング
- リマーキング

本コマンドで生成したポリシーマップは、**service-policy input** コマンドによって LAN/SFP+ポートおよび論理インターフェースに適用することができる。 これにより、ポリシーマップ内の各クラスマップによって受信フレームがトラフィッククラスに分類されるようになり、各トラフィックに対してユーザーの指定した QoS 処理が行われるようになる。

生成後、その内容を設定するポリシーマップモードに移動する。

no 形式で実行した場合、指定したポリシーマップを削除する。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

指定したポリシーマップが生成済みの場合、前回の設定に対して変更が行なわれる。 ただし、ポリシーマップが LAN/SFP+ポートおよび論理インターフェースに適用済みの場合、編集・削除することはできない。

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする。

- 10.1.0.0 のネットワークからのトラフィックを許可
- CIR:48kbps, CBS:12kbyte, EBS:12kbyte で、帯域クラスを分類
- Green:転送、Yellow:DSCP 値を 10 に書き換え、Red:破棄

[トラフィッククラスの定義]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.22 受信フレームに対するポリシーマップの適用

[書式]

service-policy input *name*
no service-policy *name*

[パラメーター]

name : 適用するポリシーマップ名

[入力モード]

インターフェースモード

[説明]

ポリシーマップを該当する LAN/SFP+ポートおよび論理インターフェースに適用する。

no 形式で実行した場合、LAN/SFP+ポートおよび論理インターフェースからポリシーマップを解除する。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

既にポリシーマップが LAN/SFP+ポートおよび論理インターフェースに適用済みの場合、エラーとなる。

ポリシーマップに関連付けられたクラスマップについて、LAN/SFP+ポートおよび論理インターフェースのトラストモードと対応しない設定が一つでも含まれていた場合、エラーとなる。 クラスマップの設定のうち、トラストモードによる適用制限があるコマンドは以下のとおり。

トラストモード	コマンド	制限内容
CoS	**set ip-dscp-queue**	使用不可
DSCP	**set cos-queue**	使用不可

トラストモード	コマンド	制限内容
Port Priority	**set cos**	使用不可
	set ip-precedence	
	set ip-dscp	
	set cos-queue	
	set ip-dscp-queue	
	police, remark-map	リマーキングが有効な組合せは使用不可(注 1)

注 1) リマーキングが有効な組合せとは、**police** コマンドの yellow-action または red-action が remark に設定されており、且つ、該当色の **remark-map** が設定されている場合を指す。

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ない。

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ない。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る。

[設定例]

LAN ポート #1 にポリシーマップ policy1 を適用する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

LAN ポート #1 からポリシーマップ policy1 を解除する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#no service-policy input policy1
```

9.2.23 プレマーキングの設定(CoS)

[書式]

set cos *value*
no set cos

[パラメーター]

value : <0 - 7>
プレマーキングで設定する CoS 値

[入力モード]

ポリシーマップ・クラスモード

[説明]

分類したトラフィッククラスの CoS 値を、指定した CoS 値に変更する。また、トラストモードに対応した送信キュー ID テーブルに基づき、送信キューの再割り当てを行う。

no 形式で実行した場合、トラフィッククラスに対する CoS 値のプレマーキング処理を削除する。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

プレマーキングは、送信キュー指定機能と併用することはできない。

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする

- 10.1.0.0 のネットワークからのトラフィックを許可
- 分類したトラフィッククラスを CoS 値"2"に変更する

[トラフィッククラスの定義]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set cos 2
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.24 プレマーキングの設定(TOS 優先度)

[書式]

set ip-precedence *value*
no set ip-precedence

[パラメーター]

value : <0 - 7>
プレマーキングで設定する TOS 優先度

[入力モード]

ポリシーマップ・クラスモード

[説明]

分類したトラフィッククラスの IP ヘッダの TOS 優先度(precedence)フィールド値を、指定した TOS 値に変更する。また、トラストモードに対応した送信キュー ID テーブルに基づき、送信キューの再割り当てを行う。

no 形式で実行した場合、トラフィッククラスに対する TOS 優先度のプレマーキング処理を削除する。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

プレマーキングは、送信キュー指定機能と併用することはできない。

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする

- 10.1.0.0 のネットワークからのトラフィックを許可
- 分類したトラフィッククラスを TOS 優先度"5"に変更する

[トラフィッククラスの定義]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set ip-precedence 5
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.25 プレマーキングの設定(DSCP)

[書式]

set ip-dscp *value*
no set dscp

[パラメーター]

value : <0 - 63>
プレマーキングで設定する DSCP 値

[入力モード]

ポリシーマップ・クラスモード

[説明]

分類したトラフィッククラスの DSCP 値を、指定した DSCP 値に変更する。また、トラストモードに対応した送信キュー ID テーブルに基づき、送信キューの再割り当てを行う。

no 形式で実行した場合、トラフィッククラスに対する DSCP 値のプレマーキング処理を削除する。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

プレマーキングは、送信キュー指定機能と併用することはできない。

RFC で推奨されていない DSCP 値へのプレマーキング/リマーキングは、合計 4 種類までを使用できる。RFC で推奨される DSCP 値は、下表のとおり。

PHB	DSCP 値	RFC
default	0	2474
Class Selector	0, 8, 16, 24, 32, 40, 48, 56	2474
Assured Forwarding	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38	2597
Expedited Forwarding(EF)	46	2598

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする

- 10.1.0.0 のネットワークからのトラフィックを許可
- 分類したトラフィッククラスを DSCP 値"10"に変更する

[トラフィッククラスの定義]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.26 個別ポリサーの設定(シングルレート)

[書式]

police [single-rate] *CIR CBS EBS* **yellow-action** *action* **red-action** *action*
no police

[キーワード]

single-rate : シングルレートポリサーを使用する

[パラメーター]

CIR : <1 - 102300000>
トラフィックレート(kbps)

CBS : <11 - 2097120>
適合トークンバケットのバーストサイズ(kbyte)

EBS : <11 - 2097120>
超過トークンバケットのバーストサイズ(kbyte)

action : 帯域クラスに分類されたパケットの動作

設定値	動作
transmit	転送
drop	破棄
remark	リマーキング(CoS/TOS/DSCP)

[入力モード]

ポリシーマップ・クラスモード

[説明]

分類したトラフィッククラスに対して、個別ポリサー(シングルレート)を設定する。

既に **police** コマンドで設定が行われている場合は、内容を更新する。

メータリングは、シングルレート・3 カラーマーカー(RFC2697)に基づいて行い、分類した帯域クラスに対して、以下の処理を指定することができる。

- Green : 転送のみ(指定不可)
- Yellow : 転送、破棄、リマーキングから選択
- Red : 破棄、リマーキングから選択

  ただし、リマーキングは、Yellow, Red のどちらか一方のみ指定することができる。

リマーキングの詳細設定は、**remark-map** コマンド(ポリシーマップ・クラスモード)で行う。 *action* が"remark"に設定されたのにかかわらず、その帯域クラスに対するリマーキングの詳細設定がなかった場合、リマーキングは無効となる。この場合、初期設定(Yellow:転送、Red:破棄)が適用される。

no 形式で実行した場合、メータリング・ポリシング・リマーキングの処理を削除する。

集約ポリサー(**police-aggregate** コマンド)との併用はできない。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする

- 10.1.0.0 のネットワークからのトラフィックを許可
- CIR:48kbps, CBS:12kbyte, EBS:12kbyte で、帯域クラスを分類
- Green:転送、Yellow:DSCP 値を 10 に書き換え、Red:破棄

[トラフィッククラスの定義]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.27 個別ポリサーの設定(ツインレート)

[書式]

police twin-rate *CIR PIR CBS PBS* **yellow-action** *action* **red-action** *action*

no police

[キーワード]

twin-rate : ツインレートポリサーを使用する

[パラメーター]

CIR : <1 - 102300000>

トラフィックレート(kbps)

PIR : <1 - 102300000>

ピークトラフィックレート(kbps)。CIR より小さい値は指定できない。

CBS : <11 - 2097120>

適合トークンバケットのバーストサイズ(kbyte)

PBS : <11 - 2097120>

ピークトークンバケットのバーストサイズ(kbyte)

action : 帯域クラスに分類されたパケットの動作

設定値	動作
transmit	転送
drop	破棄
remark	リマーキング(CoS/TOS/DSCP)

[入力モード]

ポリシーマップ・クラスモード

[説明]

分類したトラフィッククラスに対して、個別ポリサー(ツインレート)を設定する。

既に **police** コマンドで設定が行われている場合は、内容を更新する。

メータリングは、ツインレート・3 カラーマーカー(RFC2698)に基づいて行い、分類した帯域クラスに対して、以下の処理を指定することができる。

- Green : 転送のみ(指定不可)
- Yellow : 転送、破棄、リマーキングから選択
- Red : 破棄、リマーキングから選択

ただし、リマーキングは、Yellow, Red のどちらか一方のみ指定することができる。

リマーキングの詳細設定は、**remark-map** コマンド(ポリシーマップ・クラスモード)で行う。 *action* が"remark"に設定されたのにかかわらず、その帯域クラスに対するリマーキングの詳細設定がなかった場合、リマーキングは無効となる。この場合、初期設定(Yellow:転送、Red:破棄)が適用される。

no 形式で実行した場合、メータリング・ポリシング・リマーキングの処理を削除する。

集約ポリサー(**police-aggregate** コマンド)との併用はできない。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする

- 10.1.0.0 のネットワークからのトラフィックを許可
- CIR:48kbps, PIR:96kbps, CBS:12kbyte, PBS:12kbyte で、帯域クラスを分類
- Green:転送、Yellow:DSCP 値を 10 に書き換え、Red:破棄

[トラフィッククラスの定義]

```
SWP2(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-group 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police twin-rate 48 96 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.28 個別ポリサーのリマーキングの設定

[書式]

remark-map *color type value*
no remark-map

[パラメーター]

color : リマーキングを行う帯域クラス

設定値	説明
yellow	帯域クラス Yellow のリマーキング設定を行う
red	帯域クラス Red のリマーキング設定を行う

type : リマーキング種別

設定値	説明
cos	CoS リマーキング
ip-precedence	TOS 優先度リマーキング
ip-dscp	DSCP リマーキング

value : <0 - 7>

CoS, TOS 優先度のリマーキング値

: <0 - 63>

DSCP リマーキング値

[入力モード]

ポリシーマップ・クラスモード

[説明]

個別ポリサーで分類した帯域クラス Yellow, Red に対するリマーキング動作の設定を行う。また、トラストモードに対応した送信キュー ID テーブルに基づき、送信キューの再割り当てを行う。

リマーキングは、CoS 値、TOS 優先度、DSCP 値のいずれかを選択することができる。

no 形式で実行した場合、リマーキング設定を削除する。

リマーキングを行うためには、本コマンドの設定のほか、**police** コマンド(ポリシーマップ・クラスモード)で該当する帯域クラスのアクションを"remark"に設定しておく必要がある。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

リマーキングは、プレマーキングや送信キューの指定と併用することができる。

RFC で推奨されていない DSCP 値へのプレマーキング/リマーキングは、4 種類までをユーザー定義値として使用することができる。RFC で推奨される DSCP 値は、下表のとおり。

PHB	DSCP 値	RFC
default	0	2474
Class Selector	0, 8, 16, 24, 32, 40, 48, 56	2474
Assured Forwarding	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38	2597
Expedited Forwarding(EF)	46	2598

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする

- 10.1.0.0 のネットワークからのトラフィックを許可
- CIR:48kbps, CBS:12kbyte, EBS:12kbyte で、帯域クラスを分類
- Green:転送、Yellow:DSCP 値を 10 に書き換え、Red:破棄

[トラフィッククラスの定義]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police 48 12 12 yellow-action remark red-action drop
SWP2(config-pmap-c)#remark-map yellow ip-dscp 10
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.29 集約ポリサーの生成

[書式]

aggregate-police *name*
no aggregate-police *name*

[パラメーター]

name : 集約ポリサー名称 (20 文字以下、大文字小文字を区別する)

[入力モード]

グローバルコンフィグレーションモード

[説明]

集約ポリサーを生成する。既に生成済みの場合は、その内容を編集する。

コマンドが成功すると、集約ポリサーの内容を編集する集約ポリサーモードに遷移する。

no 形式で実行すると、集約ポリサーを削除する。

以下の場合、集約ポリサーの内容を変更することはできない(集約ポリサーモードに遷移しない)。

- 集約ポリサーの設定されたクラスマップを含むポリシーマップが LAN/SFP+ポートおよび論理インターフェースに適用されている

以下の場合、集約ポリサーを削除することはできない。

- **police-aggregate** コマンドにより、集約ポリサーがトラフィッククラスに設定されている

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

集約ポリサー"AGP-01"を生成する

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#
```

9.2.30 集約ポリサーの設定(シングルレート)

[書式]

police [single-rate] *CIR CBS EBS* **yellow-action** *action* **red-action** *action*
no police

[キーワード]

single-rate : シングルレートポリサーを使用する

[パラメーター]

CIR : <1 - 102300000>
トラフィックレート(kbps)

CBS : <11 - 2097120>

適合トークンバケットのバーストサイズ(kbyte)

EBS : <11 - 2097120>

超過トークンバケットのバーストサイズ(kbyte)

action : 帯域クラスに分類されたパケットの動作

設定値	動作
transmit	転送
drop	破棄
remark	リマーキング(CoS/TOS/DSCP)

[入力モード]

集約ポリサーモード

[説明]

集約ポリサーに、シングルレートポリサーの設定を行う。

no 形式で実行した場合、メータリング・ポリシング・リマーキングの処理を削除する。

メータリングは、シングルレート・3 カラーマーカー(RFC2697)に基づいて行い、分類した帯域クラスに対して、以下の処理を指定することができる。

- Green : 転送のみ(指定不可)
- Yellow : 転送、破棄、リマーキングから選択
- Red : 破棄、リマーキングから選択

  ただし、リマーキングは、Yellow, Red のどちらか一方のみ指定することができる。

リマーキングの詳細設定は、**remark-map** コマンド(集約ポリサーモード)で行う。 *action* が"remark"に設定されたのにかかわらず、その帯域クラスに対するリマーキングの詳細設定がなかった場合、リマーキングは無効となる。この場合、初期設定(Yellow:転送、Red:破棄)が適用される。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

集約ポリサー "AGP-01" を作成する。

- CIR:48kbps, CBS:12kbyte, EBS:12kbyte とし、SrTCM によるメータリングを実行
- Yellow:DSCP 値を 10 に書き換え、Red:破棄

[集約ポリサーの作成]

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#police single-rate 48 12 12 yellow-action remark red-action
drop
SWP2(config-agg-policer)#remark-map yellow ip-dscp 10
SWP2(config-agg-policer)#exit
```

9.2.31 集約ポリサーの設定(ツインレート)

[書式]

police twin-rate *CIR PIR CBS PBS* **yellow-action** *action* **red-action** *action*

no police

[キーワード]

twin-rate : ツインレートポリサーを使用する

[パラメーター]

CIR : <1 - 102300000>

トラフィックレート(kbps)

PIR : <1 - 102300000>

ピークトラフィックレート(kbps)。CIR より小さい値は指定できない。

CBS : <11 - 2097120>

適合トークンバケットのバーストサイズ(kbyte)

PBS : <11 - 2097120>

ピークトークンバケットのバーストサイズ(kbyte)

action : 帯域クラスに分類されたパケットの動作

設定値	動作
transmit	転送
drop	破棄
remark	リマーキング(CoS/TOS/DSCP)

[入力モード]

集約ポリサーモード

[説明]

集約ポリサーに、ツインレートポリサーの設定を行う。

no 形式で実行した場合、メータリング・ポリシング・リマーキングの処理を削除する。

メータリングは、ツインレート・3 カラーマーカー(RFC2698)に基づいて行い、分類した帯域クラスに対して、以下の処理を指定することができる。

- Green : 転送のみ(指定不可)
- Yellow : 転送、破棄、リマーキングから選択
- Red : 破棄、リマーキングから選択

  ただし、リマーキングは、Yellow, Red のどちらか一方のみ指定することができる。

リマーキングの詳細設定は、**remark-map** コマンド(集約ポリサーモード)で行う。 *action* が"remark"に設定されたのにかかわらず、その帯域クラスに対するリマーキングの詳細設定がなかった場合、リマーキングは無効となる。この場合、初期設定(Yellow:転送、Red:破棄)が適用される。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

集約ポリサー "AGP-01" を作成する。

- CIR:48kbps, PIR:96kbps, CBS:12kbyte, PBS:12kbyte とし、TrTCM によるメータリングを実行
- Yellow:DSCP 値を 10 に書き換え、Red:破棄

[集約ポリサーの作成]

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#police twin-rate 48 96 12 12 yellow-action remark red-
action drop
SWP2(config-agg-policer)#remark-map yellow ip-dscp 10
SWP2(config-agg-policer)#exit
```

9.2.32 集約ポリサーのリマーキングの設定

[書式]

remark-map *color type value*

no remark-map

[パラメーター]

color : リマーキングを行う帯域クラス

設定値	説明
yellow	帯域クラス Yellow のリマーキング設定を行う
red	帯域クラス Red のリマーキング設定を行う

type : リマーキング種別

設定値	説明
cos	CoS リマーキング
ip-precedence	TOS 優先度リマーキング
ip-dscp	DSCP リマーキング

value : <0 - 7>

CoS, TOS 優先度のリマーキング値

: <0 - 63>

DSCP リマーキング値

[入力モード]

集約ポリサーモード

[説明]

集約ポリサーで分類した帯域クラス Yellow, Red に対するリマーキング動作の設定を行う。また、トラストモードに対応した送信キュー ID テーブルに基づき、送信キューの再割り当てを行う。

リマーキングは、CoS 値、TOS 優先度、DSCP 値のいずれかを選択することができる。

no 形式で実行した場合、リマーキング設定を削除する。

リマーキングを行うためには、本コマンドの設定のほか、**police** コマンド(集約ポリサーモード)で該当する帯域クラスのアクションを"remark"に設定しておく必要がある。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

リマーキングは、プレマーキングや送信キューの指定と併用することができる。

RFC で推奨されていない DSCP 値へのプレマーキング/リマーキングは、4 種類までをユーザー定義値として使用することができる。RFC で推奨される DSCP 値は、下表のとおり。

PHB	DSCP 値	RFC
default	0	2474
Class Selector	0, 8, 16, 24, 32, 40, 48, 56	2474
Assured Forwarding	10, 12, 14, 18, 20, 22, 26, 28, 30, 34, 36, 38	2597
Expedited Forwarding(EF)	46	2598

[設定例]

集約ポリサー "AGP-01" にリマーキングの設定を行う。

- CIR:48kbps, PIR:96kbps, CBS:12kbyte, PBS:12kbyte とし、TrTCM によるメータリングを実行
- Yellow:DSCP 値を 10 に書き換え、Red:破棄

[集約ポリサーの作成]

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#police twin-rate 48 96 12 12 yellow-action remark red-
action drop
SWP2(config-agg-policer)#remark-map yellow ip-dscp 10
SWP2(config-agg-policer)#exit
```

9.2.33 集約ポリサーの表示

[書式]

show aggregate-police [*name*]

[パラメーター]

name : 集約ポリサー名。省略時はすべての集約ポリサーが対象となる。

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

集約ポリサーの内容を表示する。表示内容は、**show class-map** コマンドで表示される police セクションと同様。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

集約ポリサー"AGP-01"の内容を表示する。

```
SWP2#show aggregate-police AGP-01

     Aggregator-Police Name: AGP-01
         Mode: TrTCM
         average rate (48 Kbits/sec)
         peak rate (96 Kbits/sec)
         burst size (12 KBytes)
         peak burst size (16 KBytes)
         yellow-action (Transmit)
         red-action (Drop)
```

9.2.34 集約ポリサーの適用

[書式]

police-aggregate *name*
no police-aggregate *name*

[パラメーター]

name : 適用する集約ポリサー

[入力モード]

ポリシーマップ・クラスモード

[説明]

トラフィッククラスに対して、集約ポリサーを設定する。

no 形式で実行した場合、トラフィッククラスに対する集約ポリサーの設定を削除する。

個別ポリサー(ポリシーマップ・クラスモードの **police single-rate, police twin-rate** コマンド)との併用はできない。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

ポリシーマップ"policy1"の 2 つのトラフィッククラス"class1", "class2"に対して、集約ポリサー"AGP-01"を適用する

- CIR:48kbps, CBS:12kbyte, EBS:12kbyte とし、SrTCM によるメータリングを実行
- Yellow:DSCP 値を 10 に書き換え、Red:破棄

[集約ポリサーの作成]

```
SWP2(config)#aggregate-police AGP-01
SWP2(config-agg-policer)#police single-rate 48 12 12 yellow-action remark red-action
drop
SWP2(config-agg-policer)#remark-map yellow ip-dscp 10
SWP2(config-agg-policer)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#police-aggregate AGP-01
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#class class2
SWP2(config-pmap-c)#police-aggregate AGP-01
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.35 メータリングカウンターの表示

[書式]

show qos metering-counters [*ifname*]

[パラメーター]

ifname : LAN/SFP+ポートおよび論理インターフェース名。省略時は全ポートを対象とする。

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

指定した LAN/SFP+ポートおよび論理インターフェースにおける、すべてのポリサー(個別ポリサー/集約ポリサー)のメータリング統計情報を表示する。

表示される統計情報は以下のとおり。

項目	説明
Green Bytes	帯域クラス Green に分類されたバイト数
Yellow Bytes	帯域クラス Yellow に分類されたバイト数
Red Bytes	帯域クラス Red に分類されたバイト数

カウントの開始は、LAN/SFP+ポートおよび論理インターフェースにポリシーマップを適用した時点を起点とする。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

LAN ポート #1 のメータリング統計情報を表示する。

```
SWP2#show qos metering-counters port1.1
Interface: port1.1(policy1)

  ****** Individual ******
  Class-map         : class1
      Green Bytes   : 178345
      Yellow Bytes  : 0
      Red Bytes     : 0

  ****** Aggregate *******
  Aggregate-policer: AGP-01
  Class-map         : class2
                      class3
      Green Bytes   : 28672
      Yellow Bytes  : 2048
      Red Bytes     : 51552
```

9.2.36 メータリングカウンターのクリア

[書式]

clear qos metering-counters [*ifname*]

[パラメーター]

ifname : LAN/SFP+ポートおよび論理インターフェース名。省略時は全ポートを対象とする。

[入力モード]

特権 EXEC モード

[説明]

指定した LAN/SFP+ポートおよび論理インターフェースにおける、すべてのポリサー(個別ポリサー/集約ポリサー)のメータリング統計情報をクリアする。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

LAN ポート #1 のメータリング統計情報をクリアする。

```
SWP2#clear qos metering-counter port1.1
```

9.2.37 送信キューの指定(CoS-Queue)

[書式]

set cos-queue *value*

no set cos-queue

[パラメーター]

value : <0 - 7>

送信キュー ID に対応した CoS 値

[入力モード]

ポリシーマップ・クラスモード

[説明]

分類したトラフィッククラスに送信キューを割り当てる。

送信キューの指定には CoS 値を使用し、「CoS-送信キュー ID 変換テーブル」に基づいた送信キューが割り当てられる。

no 形式で実行した場合、トラフィッククラスに対する送信キューの指定を無効にする。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

送信キュー指定は、プレマーキングと併用することはできない。

CoS による送信キューの指定は、CoS トラストモード専用となる。ポリシーマップに、本コマンドを含むクラスマップが一つでも含まれる場合、そのポリシーマップは CoS トラストモード以外のポートには適用できない。

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする

- 10.1.0.0 のネットワークからのトラフィックを許可
- 分類したトラフィッククラスは送信キュー 3(CoS:3)に変更する

[トラフィッククラスの定義]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set cos-queue 3
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.38 送信キューの指定(DSCP-Queue)

[書式]

set ip-dscp-queue *value*

no set ip-dscp-queue

[パラメーター]

value : <0 - 63>

送信キュー ID に対応した DSCP 値

[入力モード]

ポリシーマップ・クラスモード

[説明]

分類したトラフィッククラスに送信キューを割り当てる。

送信キューの指定には DSCP 値を使用し、「DSCP-送信キュー ID 変換テーブル」に基づいた送信キューが割り当てられる。

no 形式で実行した場合、トラフィッククラスに対する送信キューの指定を無効にする。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

送信キュー指定は、プレマーキングと併用することはできない。

DSCP による送信キューの指定は、DSCP トラストモード専用となる。ポリシーマップに、本コマンドを含むクラスマップが一つでも含まれる場合、そのポリシーマップは DSCP トラストモード以外のポートには適用できない。

[設定例]

LAN ポート #1 の受信フレームに対して以下の設定をする

- 10.1.0.0 のネットワークからのトラフィックを許可
- 分類したトラフィッククラスは送信キュー 3(DSCP:24)に変更する

[トラフィッククラスの定義]

```
SWP2(config)#access-list 1 permit any 10.1.0.0 0.0.255.255 any
SWP2(config)#class-map class1
SWP2(config-cmap)#match access-list 1
SWP2(config-cmap)#exit
```

[ポリシーの設定]

```
SWP2(config)#policy-map policy1
SWP2(config-pmap)#class class1
SWP2(config-pmap-c)#set ip-dscp-queue 24
SWP2(config-pmap-c)#exit
SWP2(config-pmap)#exit
SWP2(config)#interface port1.1
SWP2(config-if)#service-policy input policy1
```

9.2.39 ポリシーマップ情報の表示

[書式]

show policy-map [*name*]

[パラメーター]

name : ポリシーマップ名。省略時、すべてのポリシーマップ情報が表示される。

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

指定したポリシーマップの情報を表示する。表示内容は以下。

項目	説明
Policy-Map Name	ポリシーマップ名
State	ポリシーマップの適用状態(attached/detached)
Class-Map Name	クラスマップ情報。詳細は **show class-map** コマンドを参照のこと
Match	分類条件 - Match Access-List (アクセスリスト ID) - Match ethertype (Ethernet Type) - Match vlan (VLAN ID) - Match vlan-range (VLAN ID) - Match CoS (CoS 値) - Match IP precedence (TOS 優先度) - Match IP DSCP (DSCP 値)

項目	説明
Set	プレマーキング設定、送信キュー指定 - Set CoS (プレマーキング設定：CoS 値) - Set IP precedence (プレマーキング設定：TOS 優先度) - Set IP DSCP (プレマーキング設定：DSCP 値) - Set CoS-Queue (送信キュー指定：CoS) - Set IP-DSCP-Queue (送信キュー指定：DSCP)
Police	メータリング／ポリシング／リマーキング設定 ※詳細は以下を参照

メータリング／ポリシング／リマーキング設定の詳細は以下のとおり。

項目		説明
Aggregator-Police Name		集約ポリサー名称(設定されている場合のみ)
Mode		メータリングアルゴリズム(SrTCM/TrTCM)
SrTCM のみ表示	average rate	トラフィックレート(Kbits/sec)
	burst size	適合トークンパケットのバーストサイズ(KBytes)
	excess burst size	超過トークンパケットのバーストサイズ(KBytes)
TrTCM のみ表示	average rate	トラフィックレート(Kbits/sec)
	peak rate	ピークトラフィックレート(Kbits/sec)
	burst size	適合トークンパケットのバーストサイズ(KBytes)
	peak burst size	ピークトークンパケットのバーストサイズ(KBytes)
yellow-action		帯域クラス Yellow に対する動作(transmit/drop/remark)
red-action		帯域クラス Red に対する動作(drop/remark)

- Match と Set は、設定されているものが一つだけ表示される。
- Match と Set と Police は、対応するコマンド(match, set, police)が設定されていない場合は表示されない。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

ポリシーマップ"policy1"の情報を表示する。

```
SWP2#show policy-map policy1

  Policy-Map Name: policy1
    State: attached

    Class-Map Name: class1
      Qos-Access-List Name: 1
      Police: Mode: SrTCM
              average rate (48 Kbits/sec)
              burst size (12 KBytes)
              excess burst size (12 KBytes)
              yellow-action (Remark [DSCP:10])
              red-action (Drop)
```

9.2.40 マップステータスの表示

[書式]

show qos map-status *type* [*name*]

[パラメーター]

type : 表示するマップ種別

設定値	説明
policy	ポリシーマップのステータス情報を表示
class	クラスマップのステータス情報を表示

name : 表示するポリシーマップ（またはクラスマップ）の名称。省略時はすべてのポリシーマップ（またはクラスマップ）が対象となる。

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

ポリシーマップやクラスマップのステータス情報を表示する。

本コマンドを使用することで、ポリシーマップがどの LAN/SFP+ポートおよび論理インターフェース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登録されているかなど、ポリシーマップやクラスマップの結合に関する情報を知ることができる。

表示内容は以下のとおり。

policy-map

項目	表示内容
input port	ポリシーマップが適用されている LAN/SFP+ポートおよび論理インターフェースの一覧
edit/erase	**policy-map/no policy-map** が実行可能かどうか
attach limitation	トラストモード毎の適用可否

class-map

項目	表示内容
policy-map asociation	クラスマップが登録されているポリシーマップの一覧
edit/erase	**class-map/no class-map** が実行可能かどうか
attach limitation	トラストモード毎の適用可否

ポリシーマップやクラスマップの設定内容は、**show policy-map**, **show class-map** コマンドで確認すること。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]

ポリシーマップ"policy1"のステータスを表示する。

```
SWP2#show qos map-status policy policy1
policy1 status
  input port            : port1.3

  edit/erase            : Disable

  attach limitation
    CoS trust mode           : Enable
    DSCP trust mode          : Enable
    Port-Priority trust mode : Disable
```

クラスマップ"class1"のステータスを表示する。

```
SWP2#show qos map-status class class1
class1 status
  policy-map association : policy1 (Detached)
```

```
edit/erase              : Disable

attach limitation
  CoS trust mode           : Enable
  DSCP trust mode          : Enable
  Port-Priority trust mode : Disable
```

9.2.41 送信キューのスケジューリング設定

[書式]

qos wrr-weight *queue-id weight*
no qos wrr-weight *queue-id*

[パラメーター]

queue-id : <0-7>
送信キュー ID

weight : <1-32>
WRR の重み

[初期設定]

no qos wrr-weight 0

no qos wrr-weight 1

no qos wrr-weight 2

no qos wrr-weight 3

no qos wrr-weight 4

no qos wrr-weight 5

no qos wrr-weight 6

no qos wrr-weight 7

[入力モード]
グローバルコンフィグレーションモード

[説明]
送信キューに対して、WRR(重み付きラウンドロビン)の重みづけ設定を行う。
スケジューリング方式は、すべての LAN/SFP+ポートおよび論理インターフェース共通の設定となる。
no 形式で実行した場合、送信キューは絶対優先(SP)方式となる。

[ノート]
本コマンドを実行するには、QoS を有効にしておくこと。

[設定例]
送信キュー#7,#6 を SP 方式 (7 が優先)、#5,#4,#3,#2,#1,#0 を WRR 方式 (5:5:5:2:1:1)とする。

```
SWP2(config)#no qos wrr-weight 7
SWP2(config)#no qos wrr-weight 6
SWP2(config)#qos wrr-weight 5 5
SWP2(config)#qos wrr-weight 4 5
SWP2(config)#qos wrr-weight 3 5
SWP2(config)#qos wrr-weight 2 2
SWP2(config)#qos wrr-weight 1 1
SWP2(config)#qos wrr-weight 0 1
```

9.2.42 トラフィックシェーピング(ポート単位)の設定

[書式]

traffic-shape rate kbps *CIR* **burst** *BC*
no traffic-shape rate

[パラメーター]

CIR : <18-1000000>

トラフィックレート(kbps)。丸め込みが発生するため、入力値に対して実際の適用値が異なる場合がある([ノート]参照)

BC : <4-16000>

バーストサイズ(kbyte)。4kbyte 単位での設定となる。

[初期設定]

no traffic-shape rate

[入力モード]

インターフェースモード

[説明]

ポートに対して、シェーピングを設定する。

no 形式で実行した場合、ポートシェーピングの設定は無効となる。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

トラフィックレートは丸め込みが発生するため、入力値に対して実際の適用値が異なる場合がある。

[設定例]

LAN ポート #1 からの送信を CIR:30016kbps, Bc:1876000byte に絞る。

```
SWP2(config)#interface port1.1
SWP2(config-if)#traffic-shape rate kbps 30016 burst 1876
```

9.2.43 トラフィックシェーピング(キュー単位)の設定

[書式]

traffic-shape queue *queue-id* **rate kbps** *CIR* **burst** *BC*

no traffic-shape queue *queue-id* **rate**

[パラメーター]

queue-id : <0-7>

送信キュー ID

CIR : <18-1000000>

トラフィックレート(kbps)。丸め込みが発生するため、入力値に対して実際の適用値が異なる場合がある([ノート]参照)

BC : <4-16000>

バーストサイズ(kbyte)。4kbyte 単位での設定となる。

[初期設定]

no traffic-shpe queue 0 rate

no traffic-shpe queue 1 rate

no traffic-shpe queue 2 rate

no traffic-shpe queue 3 rate

no traffic-shpe queue 4 rate

no traffic-shpe queue 5 rate

no traffic-shpe queue 6 rate

no traffic-shpe queue 7 rate

[入力モード]

インターフェースモード

[説明]

ポートの送信キューに対して、シェーピングを設定する。

no 形式で実行した場合、送信キューに対するシェーピングの設定は無効となる。

[ノート]

本コマンドを実行するには、QoS を有効にしておくこと。

トラフィックレートは丸め込みが発生するため、入力値に対して実際の適用値が異なる場合がある。

[設定例]

LAN ポート #1 のキュー #0 からの送信を CIR:10Mbps, Bc:64000byte に絞る。

```
SWP2(config)#interface port1.1
SWP2(config-if)#traffic-shape queue 0 rate kbps 10000 burst 64
```

9.3 フロー制御

9.3.1 フロー制御(IEEE 802.3x PAUSE の送受信)の設定(システム)

[書式]

flowcontrol *type*
no flowcontrol

[パラメーター]

type : フロー制御の動作

設定値	説明
enable	フロー制御を有効にする
disable	フロー制御を無効にする

[初期設定]

flowcontrol disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

システム全体のフロー制御(IEEE 802.3x PAUSE フレーム送受信)を有効にする。

no 形式で実行した場合、フロー制御を無効にする。

[ノート]

QoS 機能が有効なとき、システムのフロー制御を有効にすることはできない。

フロー制御を有効にした場合、自動的にテールドロップ機能は無効になる。

インターフェース毎のフロー制御は、システム側とインターフェース側のフロー制御設定をそれぞれ有効にした場合のみ動作する。

[設定例]

システムのフロー制御を有効にする。

```
SWP2(config)#flowcontrol enable
```

9.3.2 フロー制御(IEEE 802.3x PAUSE の送受信)の設定(インターフェース)

[書式]

flowcontrol *type*
no flowcontrol

[パラメーター]

type : フロー制御の動作

設定値	説明
auto	フロー制御の自動ネゴシエーションを有効にする
both	Pause フレームの送信/受信を有効にする
disable	フロー制御を無効にする

[初期設定]

flowcontrol disable

[入力モード]

インターフェースモード

[説明]

LAN/SFP+ポートのフロー制御(IEEE 802.3x PAUSE フレーム送受信)を有効にする。

no 形式で実行した場合、フロー制御を無効にする。

[ノート]

本コマンドは LAN/SFP+ポートにのみ設定可能。

システムのフロー制御が無効な場合動作しない。

PAUSE フレームの送信と受信は両方セットで有効/無効の設定となる。(送信と受信のどちらか一方のみを有効に設定することはできない)

中断要求時に本製品が送信する PAUSE フレームの中断時間は、0xFFFF(65535)とする。

[設定例]

LAN ポート #1 のフロー制御を有効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#flowcontrol both
```

LAN ポート #1 のフロー制御を無効にする。

```
SWP2(config)#interface port1.1
SWP2(config-if)#no flowcontrol
```

9.3.3 フロー制御の動作状態の表示

[書式]

show flowcontrol [inteface *ifname*]

[キーワード]

interface : 表示するインターフェースを指定する

[パラメーター]

ifname : LAN/SFP+ポート名。省略時は全インターフェースを対象とする。
表示するインターフェース

[入力モード]

非特権 EXEC モード、特権 EXEC モード

[説明]

フロー制御に関する情報(有効/無効, PAUSE フレームの送受信数)を表示する。

[ノート]

PAUSE フレーム送受信数は、該当ポートのフロー制御が有効となっている場合のみ表示される。

PAUSE フレーム送受信数は、**clear frame-counters** コマンド実行時にクリアされる。

[設定例]

LAN ポート #1 のフロー制御情報を表示する。

```
SWP2#show flowcontrol port1.1
Port        FlowControl       RxPause TxPause
```

```
---------   -----------       ------- -------
port1.1     Both                 4337       0
```

全ポートのフロー制御情報を表示する

```
SWP2#show flowcontrol
System flow-control: Enable
Port        FlowControl       RxPause TxPause
---------   -----------       ------- -------
port1.1     Both                 4337       0
port1.2     Disable                 -       -
port1.3     Both                    0    1732
port1.4     Disable                 -       -
port1.5     Disable                 -       -
port1.6     Disable                 -       -
port1.7     Disable                 -       -
port1.8     Disable                 -       -
```

9.4 ストーム制御

9.4.1 ストーム制御の設定

[書式]

storm-control *type* [*type*..] **level** *level*

no storm-control

[パラメーター]

type : ストーム制御タイプ

ストーム制御タイプ	説明
broadcast	ブロードキャストストーム制御を有効にする
multicast	マルチキャストストーム制御を有効にする
unicast	宛先不明のユニキャストフレームの制御を有効にする

level : <0.00-100.00>

閾値を帯域幅のパーセンテージで設定する
閾値は小数点以下第 2 位まで設定できる

[初期設定]

no storm-control

[入力モード]

インターフェースモード

[説明]

LAN/SFP+ポートに対しブロードキャストストーム制御、マルチキャストストーム制御および、宛先不明のユニキャストフレームの制御を有効にし、受信制限をかける。

閾値を超えて受信したフレームは破棄される。ただし、閾値が 100%の場合は受信制限はしない。閾値は全フレーム共通であり、個別には設定できない。

[設定例]

LAN ポート #1 のブロードキャストストーム制御とマルチキャストストーム制御を有効にし閾値 30%を設定する。

```
SWP2(config)#interface port1.1
SWP2(config-if)#storm-control broadcast multicast level 30
```

9.4.2 ストーム制御 受信上限値の表示

[書式]

show storm-control [*ifname*]

[パラメーター]

ifname	:	LAN/SFP+ポートのインターフェース名 表示するインターフェース

[初期設定]

なし

[入力モード]

非特権 EXEC モード、 特権 EXEC モード

[説明]

フレームの受信上限値を表示する。

インターフェース名を省略した場合は、全インターフェースが対象となる。

[設定例]

全インターフェースの設定状態を表示する。

```
SWP2#show storm-control
Port      BcastLevel    McastLevel    UcastLevel
port1.1     30.00%        30.00%       100.00%
port1.2     20.00%        20.00%        20.00%
port1.3    100.00%       100.00%       100.00%
port1.4    100.00%       100.00%       100.00%
port1.5     50.00%        50.00%       100.00%
port1.6    100.00%       100.00%       100.00%
port1.7    100.00%       100.00%        30.00%
port1.8    100.00%       100.00%        30.00%
```

第 10 章

アプリケーション

10.1 ローカル RADIUS サーバー

10.1.1 ローカル RADIUS サーバー機能の設定

[書式]

radius-server local enable [*port*]
radius-server local disable
no radius-server local

[パラメーター]

port : <1024-65535>
認証用 UDP ポート番号(省略時は 1812 とする)

[初期設定]

radius-server local disable

[入力モード]

グローバルコンフィグレーションモード

[説明]

ローカル RADIUS サーバー機能の有効/無効を設定する。
また、認証用 UDP ポート番号を変更することができる。
no 形式でコマンドを実行した場合は初期設定値に戻る。

[ノート]

ローカル RADIUS サーバー機能を使用するためには、最初に **crypto pki generate ca** コマンドでルート認証局を生成する必要がある。

[設定例]

ローカル RADIUS サーバー機能を有効にする。

```
SWP2(config)#radius-server local enable
```

10.1.2 アクセスインターフェースの設定

[書式]

radius-server local interface *interface*
no radius-server local interface

[パラメーター]

interface : VLAN インターフェース名

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

ローカル RADIUS サーバーへのアクセスを許可する VLAN インターフェースを設定する。
アクセスインターフェースは最大 7 件まで設定できる。
no 形式でコマンドを実行した場合は、指定したインターフェースを削除する。

[設定例]

VLAN #1 と VLAN #100 に接続している RADIUS クライアント(NAS)からのアクセスを許可する。

```
SWP2(config)#radius-server local interface vlan1
SWP2(config)#radius-server local interface vlan100
```

10.1.3 ルート認証局を生成

[書式]

crypto pki generate ca [*ca-name*]
no crypto pki generate ca

[パラメーター]

ca-name : 認証局名

認証局名の入力可能文字

- 3 文字以上 32 文字以内
- \ [ ] / " ? スペースを除く半角英数字・半角記号
- "DEFAULT"は指定不可

[初期設定]

なし

[入力モード]

グローバルコンフィグレーションモード

[説明]

クライアント証明書を発行するためのルート認証局を生成する。

認証局名を省略した場合は"YAMAHA_SWITCH"を使用する。

no 形式でコマンドを実行した場合は、指定したルート認証局を削除する。

[ノート]

ルート認証局を生成していない場合は、ローカル RADIUS サーバー機能は使用できない。

既にルート認証局が生成されている状態で異なる認証局名を設定した場合、ルート認証局は上書きされる。

ルート認証局を削除または上書きすると、発行済みのクライアント証明書はすべて無効となる。

ルート認証局が存在していても **crypto pki generate ca** 設定がないとルート認証局として使用できない。

[設定例]

認証局名が"MYRADIUS"のルート認証局を生成する。

```
SWP2(config)#crypto pki generate ca MYRADIUS
```

10.1.4 RADIUS コンフィグレーションモード

[書式]

radius-server local-profile

[入力モード]

グローバルコンフィグレーションモード

[説明]

RADIUS コンフィグレーションモードに移行する。

ローカル RADIUS サーバー機能の動作仕様を設定するためのモードである。

[設定例]

RADIUS コンフィグレーションモードに移行する。

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#
```

10.1.5 認証方式の設定

[書式]

authentication *mode* [*mode...*]
no authentication

[パラメーター]

mode : 認証方式

設定値	説明
pap	PAP 認証方式
peap	PEAP 認証方式
eap-md5	EAP-MD5 認証方式
eap-tls	EAP-TLS 認証方式
eap-ttls	EAP-TTLS 認証方式

[初期設定]

authentication pap peap eap-md5 eap-tls eap-ttls

[入力モード]

RADIUS コンフィグレーションモード

[説明]

ローカル RADIUS サーバーで使用する認証方式を指定する。

no 形式でコマンドを実行した場合は初期設定値に戻り、すべての認証方式が有効となる。

[ノート]

PEAP, EAP-TTLS 認証方式の内部認証方式として、MSCHAPv2 と MD5 をサポートする。

MD5 を使用する場合は、認証方式に eap-md5 を指定する必要がある。

[設定例]

使用する認証方式を PEAP, EAP-MD5 に制限する。

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#authentication peap eap-md5
```

10.1.6 RADIUS クライアント(NAS)の設定

[書式]

nas *host* key *secret*

no nas *host*

[キーワード]

key : RADIUS クライアント(NAS)との通信時に使用するパスワードを設定する

[パラメーター]

host : IP アドレス、または、IP ネットワークアドレス

設定値	説明
IPv4 アドレス(A.B.C.D)	0.0.0.1～223.255.255.255 のうち 127.0.0.1 を除いたもの
IPv4 ネットワークアドレス(A.B.C.D/M)	ネットワークマスクの範囲は 8～32 で、IP アドレスのホスト部は 0 となる
IPv6 アドレス(A:B:C::D)	ユニキャストアドレスのうち、未指定アドレス(::/128)、デフォルトルートアドレス(::/0)、ループバックアドレス(::1/128)を除いたもの
IPv6 ネットワークアドレス(A:B:C::D/M)	プレフィックス長は 1～128

secret : 共有パスワード

(128 文字以内、\ [ ] " ? スペースを除く半角英数字・半角記号)

[初期設定]

nas 127.0.0.1 key secret_local

[入力モード]

RADIUS コンフィグレーションモード

[説明]

RADIUS クライアントリストに RADIUS クライアント(NAS)を追加する。

最大登録数は 100 である。

no 形式でコマンドを実行した場合は、指定した RADIUS クライアントの設定を削除する。

[ノート]

本コマンドで設定した RADIUS クライアント(NAS)情報は、running-config、および、startup-config には表示されない。

また、通常の設定コマンドとは異なり、本コマンドを実行した時点で設定データとして保存される。

設定した RADIUS クライアント(NAS)情報は、**show radius-server local nas** コマンドで確認できる。

本機器のポート認証機能でローカル RADIUS サーバーを指定する場合は、以下を設定する必要がある。

```
SWP2(config)#radius-server host 127.0.0.1 key secret_local
```

[設定例]

IP アドレス 192.168.100.101、共有パスワード"abcde"の RADIUS クライアント(NAS)を追加する。

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#nas 192.168.100.101 key abcde
```

10.1.7 認証ユーザーの設定

[書式]

user *userid password* [vlan *vlan-id*] [mac *mac-address*] [ssid *ssid*] [name *name*] [mail *mail-address*] [auth *type*] [expire *date*]

no user *userid*

[キーワード]

vlan	:	ダイナミック VLAN 用の VLAN を設定する
mac	:	認証端末を特定したい場合に端末の MAC アドレスを指定する
ssid	:	接続している SSID を特定したい場合に SSID を指定する
name	:	ユーザー名称を設定する
mail	:	クライアント証明書の配布先メールアドレスを設定する
auth	:	認証方式タイプを設定する
expire	:	クライアント証明書の有効期限を設定する(認証方式タイプが EAP-TLS の場合のみ有効)

[パラメーター]

userid : ユーザー ID

(3 文字以上 32 文字以内、"DEFAULT"は指定不可)

認証方式	入力可能文字
EAP-MD5, EAP-TTLS, PEAP, PAP	\ [ ] " ? スペースを除く半角英数字・半角記号
EAP-TLS	\ [ ] / : * | < > " ? スペースを除く半角英数字・半角記号

password : パスワード

(32 文字以内、\ [ ] " ? スペースを除く半角英数字・半角記号)

vlan-id : <1-4094>

ダイナミック VLAN 用の VLAN 番号

mac-address : hhhh.hhhh.hhhh (h は 16 進数)

認証端末(ユーザー)の MAC アドレス

ssid : 接続先 SSID

(32 文字以内、\ [ ] " ? スペースを除く半角英数字・半角記号)

name : ユーザー名

(32 文字以内、" ? スペースを除く半角英数字・半角記号)

mail-address : メールアドレス

(256 文字以内、半角英数と _ - . @)

type : 認証方式タイプ

設定値	説明
pap	PAP 認証方式 (ユーザー ID とパスワードを使用するタイプ)
peap	PEAP, EAP-MD5, EAP-TTLS 認証方式 (ユーザー ID とパスワードを使用するタイプ)
eap-tls	EAP-TLS 認証方式 (証明書を使用するタイプ)

省略時は eap-tls とする

date : 日付(省略時は 2037/12/31 とする)

(YYYY/MM/DD 現在日付から 2037/12/31 まで)

[初期設定]

なし

[入力モード]

RADIUS コンフィグレーションモード

[説明]

RADIUS サーバーで認証するユーザーを登録する。

最大登録数は 2000 である。

no 形式でコマンドを実行した場合は、指定したユーザーを削除する。

認証方式に EAP-TLS を指定した場合、**certificate user** コマンドでクライアント証明書の発行が必要となる。

また、パスワードやクライアント証明書の有効期限を変更した場合も、再度クライアント証明書の発行が必要となる。

クライアント証明書を発行済みのユーザーを削除する場合、自動的にクライアント証明書の失効処理を行う。

[ノート]

本コマンドで設定したユーザー情報は、running-config、および、startup-config には表示されない。

また、通常の設定コマンドとは異なり、本コマンドを実行した時点で設定データとして保存される。

設定したユーザー情報は、**show radius-server local user** コマンドで確認できる。

mac キーワードで指定する MAC アドレスは、RADIUS クライアント(NAS)が Calling-Station-Id を通知してきた場合に使用される。

ssid キーワードで指定する SSID は、RADIUS クライアント(NAS)が Called-Station-Id を通知してきた場合に使用される。

[設定例]

認証ユーザーを登録する。

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#user yamaha secretpassword mac 00a0.de00.0001 auth peap name
YamahaTaro
```

10.1.8 再認証間隔の設定

[書式]

reauth interval *time*
no reauth interval

[パラメーター]

time : <3600,43200,86400,604800>
再認証間隔の秒数

[初期設定]

reauth interval 3600

[入力モード]

RADIUS コンフィグレーションモード

[説明]

RADIUS クライアント(NAS)に通知する再認証間隔を設定する。

再認証間隔として使用するか否かについては、RADIUS クライアント(NAS)側に委ねられる。

no 形式でコマンドを実行した場合は初期設定に戻す。

[設定例]

再認証間隔を 604800 秒に設定する。

```
SWP2(config)#radius-server local-profile
SWP2(config-radius)#reauth interval 604800
```

10.1.9 ローカル RADIUS サーバーへの設定データ反映

[書式]

radius-server local refresh

[入力モード]

特権 EXEC モード

[説明]

ローカル RADIUS サーバーに現在の設定を反映させる。

RADIUS 関連の設定を変更した場合は、必ず本コマンドを実行しローカル RADIUS サーバーへデータ更新させる必要がある。

[ノート]

本コマンドを実行した場合、ローカル RADIUS サーバーはデータを反映させるために一時的に動作を中断し反映後に再開する

[設定例]

ローカル RADIUS サーバーに、現在の設定を反映させる。

```
SWP2#radius-server local refresh
```

10.1.10 クライアント証明書の発行

[書式]

certificate [mail] **user** [*userid*]

[キーワード]

mail : クライアント証明書の発行と同時にユーザーへ添付メールを送付する。

[パラメーター]

userid : ユーザー ID

(3 文字以上 32 文字以内、"DEFAULT"は指定不可)

認証方式	入力可能文字
EAP-MD5, EAP-TTLS, PEAP, PAP	\ [ ] " ? スペースを除く半角英数字・半角記号
EAP-TLS	\ [ ] / : * | < > " ? スペースを除く半角英数字・半角記号

[入力モード]

特権 EXEC モード

[説明]

EAP-TLS 認証方式を指定しているユーザーのクライアント証明書を発行する。

ユーザー ID を省略した場合は、下記の条件に合致するすべてのユーザーのクライアント証明書を一括発行する。

- クライアント証明書を一度も発行していないユーザー
- パスワード、クライアント証明書の有効期限を変更したユーザー
- 認証方式を EAP-TLS へ変更したユーザー

認証方式を EAP-TLS から EAP-TLS 以外に変更したユーザーは、自動的にクライアント証明書を失効させる。

mail キーワードを指定した場合、**user** コマンドで設定しているメールアドレスへクライアント証明書を送付する。

メールの件名と本文については、証明書送付時のメール設定(**mail send certificate** コマンド)のテンプレートに従う。

メールアドレスが設定されていない場合はメール送信しない。

[ノート]

クライアント証明書は 1 ユーザーにつき 2 通まで発行できる。2 通以上発行した場合は古いのものから順番に失効する。

クライアント証明書の一括発行は時間がかかるためバックグランドで行っており、発行中でもコマンド実行は可能である。

ただし、以下のコマンドについては実行できないように制限をかけている。

- crypto pki generate ca
- no crypto pki generate ca
- nas
- user
- certificate user
- certificate mail user
- certificate revoke

[設定例]

クライアント証明書を一括発行する。

```
SWP2#certificate user
```

10.1.11 クライアント証明書の発行中断

[書式]

certificate abort

[入力モード]

特権 EXEC モード

[説明]

クライアント証明書の一括発行を中断させる。

再度 **certificate user** コマンドを実行することでクライアント証明書の発行を再開できる。

[設定例]

クライアント証明書の一括発行を中断させる。

```
SWP2#certificate abort
```

10.1.12 クライアント証明書の失効

[書式]

certificate revoke user *userid*
certificate revoke id *certificate-id*

[キーワード]

user	:	指定したユーザーのクライアント証明書を失効させる
id	:	指定したクライアント証明書 ID のクライアント証明書を失効させる

[パラメーター]

userid : ユーザー ID

(3 文字以上 32 文字以内、"DEFAULT"は指定不可)

認証方式	入力可能文字
EAP-MD5, EAP-TTLS, PEAP, PAP	\ [ ] " ? スペースを除く半角英数字・半角記号
EAP-TLS	\ [ ] / : * | < > " ? スペースを除く半角英数字・半角記号

certificate-id : クライアント証明書 ID

"ユーザー ID"-"シリアル番号"の組み合わせ

[入力モード]

特権 EXEC モード

[説明]

指定したユーザーまたはクライアント証明書 ID のクライアント証明書を失効させる。

クライアント証明書が失効された場合、その証明書を使った認証は失敗する。

[ノート]

クライアント証明書 ID(certificate-id)は、**show radius-server local certificate list** コマンドで確認できる。

[設定例]

ユーザー ID "Taro" のクライアント証明書を失効させる。

```
SWP2#certificate revoke user Taro
```

クライアント証明書 ID "Taro-DF598EE9B44D22CC" のクライアント証明書を失効させる。

```
SWP2#certificate revoke id Taro-DF598EE9B44D22CC
```

10.1.13 クライアント証明書のエクスポート(メール送信)

[書式]

certificate export mail all compress
certificate export mail user *userid* **compress**

[キーワード]

all	:	すべてのユーザーにクライアント証明書をメール送信する
user	:	指定したユーザーにクライアント証明書をメール送信する
compress	:	ZIP ファイルに圧縮する

[パラメーター]

userid : ユーザー ID

(3 文字以上 32 文字以内、"DEFAULT"は指定不可)

認証方式	入力可能文字
EAP-MD5, EAP-TTLS, PEAP, PAP	\ [ ] " ? スペースを除く半角英数字・半角記号
EAP-TLS	\ [ ] / : * | < > " ? スペースを除く半角英数字・半角記号

[入力モード]

特権 EXEC モード

[説明]

クライアント証明書をメール添付して各ユーザーにメール送信する。

送付するクライアント証明書は、各ユーザーのパスワードで圧縮した ZIP ファイルである。

メールアドレスが設定されていないユーザーに対しては、メールの送信が行われない。

メールを送信するには、事前にメールの送信先サーバーやメールの件名などをメールテンプレートに設定し、 **mail send certificate** コマンドで、送信時に使用するメールテンプレート ID を設定しておく必要がある。

[ノート]

メール送信されるクライアント証明書は、最新の 1 通のみである。

[設定例]

ユーザー ID Yamaha のクライアント証明書をメール送信する。

```
SWP2#certificate export mail user Yamaha
```

10.1.14 RADIUS クライアント(NAS)の表示

[書式]

show radius-server local nas *host*

[パラメーター]

host : IP アドレス、または、IP ネットワークアドレス

設定値	説明
IPv4 アドレス(A.B.C.D)	0.0.0.1～223.255.255.255 のうち 127.0.0.1 を除いたもの
IPv4 ネットワークアドレス(A.B.C.D/M)	ネットワークマスクの範囲は 8～32 で、IP アドレスのホスト部は 0 となる
IPv6 アドレス(A:B:C::D)	ユニキャストアドレスのうち、未指定アドレス(::/128)、デフォルトルートアドレス(::/0)、ループバックアドレス(::1/128)を除いたもの
IPv6 ネットワークアドレス(A:B:C::D/M)	プレフィックス長は 1～128

[入力モード]

特権 EXEC モード

[説明]

RADIUS クライアント(NAS)の一覧を表示する。

[設定例]

IP アドレスが"192.168.100.0/24"の RADIUS クライアント(NAS)を表示する。

```
SWP2#show radius-server local nas 192.168.100.0/24
host                                    key
------------------------------------------------------------------------------
------------------
192.168.100.0/24                        abcde
```

10.1.15 認証ユーザー情報の表示

[書式]

show radius-server local user [detail *userid*]

[キーワード]

detail : 指定したユーザーの詳細情報表示する

[パラメーター]

userid : ユーザー ID

(3 文字以上 32 文字以内、"DEFAULT"は指定不可)

認証方式	入力可能文字
EAP-MD5, EAP-TTLS, PEAP, PAP	\ [ ] " ? スペースを除く半角英数字・半角記号
EAP-TLS	\ [ ] / : * | < > " ? スペースを除く半角英数字・半角記号

[入力モード]

特権 EXEC モード

[説明]

ユーザー情報を表示する。

[設定例]

ユーザー情報の一覧を表示する。

```
SWP2#show radius-server local user
Total     1

userid                           name                                 vlan mode
-------------------------------------------------------------------------------
00a0de001080                     YamahaTaro                              1 eap-md5
```

ユーザー ID が"00a0de000001"のユーザー情報を表示する。

```
SWP2#show radius-server local user detail 00a0de000001
Total     1

userid      : 00a0de000001
password    : secretpassword
mode        : eap-tls
vlan        : 10
MAC         : 00a0.de00.0001
SSID        :
name        : YamahaTaro
mail-address: test.com
expire date : 2037/12/31
certificated: Not
```

10.1.16 クライアント証明書の発行状態表示

[書式]

show radius-server local certificate status

[入力モード]

特権 EXEC モード

[説明]

クライアント証明書発行処理の状態を表示する。

発行状態	内容
done	クライアント証明書の発行が完了または未発行
processing	クライアント証明書を発行中
aborted	certificate abort コマンドなどによってクライアント証明書の発行を中断

[設定例]

クライアント証明書発行処理の状態を表示する。

```
SWP2#show radius-server local certificate status
certificate process: done.
```

10.1.17 クライアント証明書のリスト表示

[書式]

show radius-server local certificate list [**detail** *userid*]

[キーワード]

detail	:	詳細一覧表示を出力する

[パラメーター]

userid	:	ユーザー ID (3 文字以上 32 文字以内、"DEFAULT"は指定不可)

認証方式	入力可能文字
EAP-MD5, EAP-TTLS, PEAP, PAP	\ [ ] " ? スペースを除く半角英数字・半角記号
EAP-TLS	\ [ ] / : * | < > " ? スペースを除く半角英数字・半角記号

[入力モード]

特権 EXEC モード

[説明]

発行済クライアント証明書のリストを表示する。

userid を指定した場合は、そのユーザーの詳細情報を表示する。

[設定例]

特定ユーザーの発行済クライアント証明書を表示をする。

```
SWP2#show radius-server local certificate list detail Yamaha

userid                              certificate number
enddate
-------------------------------------------------------------------------------
--------
Yamaha                              Yamaha-DF598EE9B44D22CC
2018/12/31
                                    Yamaha-DF598EE9B44D22CD
2019/12/31
```

10.1.18 クライアント証明書の失効リスト表示

[書式]

show radius-server local certificate revoke

[入力モード]

特権 EXEC モード

[説明]

失効処理されたクライアント証明書のリストを表示する。

失効理由	内容
revoked	手動による失効
expired	有効期限切れによる失効

[設定例]

クライアント証明書の失効リストを表示をする。

```
SWP2#show radius-server local certificate revoke
```

```
userid                          certificate number
reason
-------------------------------------------------------------------------------
--------
Yamaha                          Yamaha-DF598EE9B44D22CC
expired
                                Yamaha-DF598EE9B44D22CD
revoked
```

索引

A

aaa authentication auth-mac 161
aaa authentication auth-web 161
aaa authentication dot1x 160
access-group (IPv4) 281
access-group (IPv6) 283
access-group (MAC) 286
access-list (IPv4) 279
access-list (IPv6) 282
access-list (MAC) 284
access-list description (IPv4) 281
access-list description (IPv6) 283
access-list description (MAC) 285
action 128
aggregate-police 311
arp 238
arp-ageing-timeout 238
arp-ageing-timeout request 239
auth clear-state time (インターフェースモード) 179
auth clear-state time (グローバルコンフィグレーションモード) 179
auth dynamic-vlan-creation 168
auth guest-vlan 168
auth host-mode 166
auth no-response-authorized 174
auth order 167
auth radius attribute nas-identifier 174
auth reauthentication 167
auth timeout quiet-period 169
auth timeout reauth-period 169
auth timeout server-timeout 170
auth timeout supp-timeout 170
auth-mac auth-user 164
auth-mac enable 163
auth-mac static 165
auth-web enable 165
auth-web redirect-url 178
authentication 328
auto-ip 235

B

backup-config 36
banner motd 34

C

cable-diagnostics tdr execute interface 46
certificate abort 333
certificate export mail 334
certificate revoke 334
certificate user 332
channel-group mode 151
class 298
class-map 298
clear access-list counters 287
clear arp-cache 238
clear auth state 178
clear auth statistics 177
clear boot list 40
clear cable-diagnostics tdr 47
clear counters 146
clear ip dhcp snooping binding 230
clear ip dhcp snooping statistics 231
clear ip igmp snooping 272
clear ipv6 dhcp client 250
clear ipv6 mld snooping 278
clear ipv6 neighbors 254
clear lacp counters 156
clear lldp counters 120
clear logging 60
clear mac-address-table dynamic 185
clear qos metering-counters 316
clear spanning-tree detected protocols 211
clear ssh host 98
clear ssh-server host key 95
clear system-diagnostics on-demand 46
clear test cable-diagnostics tdr 47
cli-command 129
clock set 47
clock summer-time date 50
clock summer-time recurring 50
clock timezone 48
cold start 131
copy running-config startup-config 35
crypto pki generate ca 328

D

description 135
description (schedule) 128
dns-client 256
dns-client domain-list 258
dns-client domain-name 257
dns-client name-server 257
dot1x control-direction 162
dot1x max-auth-req 163
dot1x port-control 162

E

eee 137
enable password 31
erase backup-config 39
erase startup-config 39
errdisable auto-recovery 182
exec-timeout 55

F

find switch start 133
find switch stop 133
firmware-update execute 124
firmware-update http-proxy 123
firmware-update reload-time 126
firmware-update revision-down enable 125
firmware-update timeout 125
firmware-update url 123
flowcontrol (インターフェースモード) 323
flowcontrol (グローバルコンフィグレーションモード) 323

H

hostname 130
http-server 88
http-server access 90
http-server interface 89
http-server language 91
http-server login-timeout 91
http-server secure 88

I

instance 211

instance priority 213
instance vlan 212
interface reset 144
ip address 232
ip address dhcp 233
ip dhcp snooping (インターフェースモード) 223
ip dhcp snooping (グローバルコンフィグレーションモード) 222
ip dhcp snooping information option 225
ip dhcp snooping information option allow-untrusted 226
ip dhcp snooping information option format remote-id 226
ip dhcp snooping information option format-type circuit-id 226
ip dhcp snooping limit rate 228
ip dhcp snooping logging 228
ip dhcp snooping subscriber-id 227
ip dhcp snooping trust 224
ip dhcp snooping verify mac-address 224
ip forwarding 239
ip igmp snooping 262
ip igmp snooping check ra 266
ip igmp snooping check tos 266
ip igmp snooping check ttl 265
ip igmp snooping fast-leave 263
ip igmp snooping mrouter interface 264
ip igmp snooping mrouter-port data-suppression 269
ip igmp snooping querier 264
ip igmp snooping query-interval 265
ip igmp snooping report-forward 268
ip igmp snooping report-suppression 268
ip igmp snooping version 267
ip route 235
ipv6 242
ipv6 address 243
ipv6 address autoconfig 243
ipv6 address dhcp 244
ipv6 address pd 245
ipv6 dhcp client nd-prefix 250
ipv6 dhcp client pd 246
ipv6 forwarding 254
ipv6 mld snooping 272
ipv6 mld snooping fast-leave 273
ipv6 mld snooping mrouter interface 273
ipv6 mld snooping querier 274
ipv6 mld snooping query-interval 274
ipv6 mld snooping report-suppression 276
ipv6 mld snooping version 275
ipv6 nd accept-ra-default-routes 247
ipv6 neighbor 253
ipv6 route 251

L

l2-mcast flood 261
l2-mcast snooping tcn-query 262
l2-unknown-mcast (インターフェースモード) 260
l2-unknown-mcast (グローバルコンフィグレーションモード) 260
l2-unknown-mcast forward link-local 261
l2ms filter enable 120
lacp multi-speed 155
lacp port-priority 160
lacp system-priority 154
lacp timeout 155
led-mode default 131
line con 54
line vty 54
lldp auto-setting 108
lldp interface enable 115
lldp run 106
lldp system-description 107
lldp system-name 107
lldp-agent 108
logging facility 58
logging format 57
logging host 57
logging stdout info 60
logging trap debug 58
logging trap error 59
logging trap informational 59
loop-detect (インターフェースモード) 219
loop-detect (グローバルコンフィグレーションモード) 218
loop-detect blocking 220
loop-detect blocking interval 221
loop-detect reset 221

M

mac-address-table ageing-time 184
mac-address-table learning 184
mac-address-table static 185
mail certificate expire-notify 104
mail notify trigger 100
mail send certificate 103
mail send certificate-notify 103
mail server smtp host 98
mail server smtp name 99
mail template 100
management interface 56
match access-list (QoS) 299
match access-list (VLAN) 288
match cos 300
match ethertype 301
match ip-dscp 300
match ip-precedence 300
match vlan 302
match vlan-range 302
mdix auto 137
mirror interface 139
mru 136
mtu 240
multiple-vlan group name 199
multiple-vlan transfer ympi 199

N

nas 329
ntpdate interval 53
ntpdate oneshot 53
ntpdate server 52

P

pass-through eap 180
password-encryption 31
ping 241
ping6 255
police single-rate (ポリシーマップ・クラスモード) 307
police single-rate (集約ポリサーモード) 311
police twin-rate (ポリシーマップ・クラスモード) 308
police twin-rate (集約ポリサーモード) 312
police-aggregate 315
policy-map 303
port-channel load-balance 157
port-security enable 180
port-security mac-address 181
port-security violation 181
private-vlan 188
private-vlan association 189
proav profile-type 134

Q

qos cos 291
qos cos-queue 295
qos dscp-queue 296

qos enable 290
qos port-priority-queue 296
qos queue sent-from-cpu 297
qos trust 292
qos wrr-weight 321

R

radius-server deadtime 173
radius-server host 171
radius-server key 173
radius-server local enable 327
radius-server local interface 327
radius-server local refresh 332
radius-server local-profile 328
radius-server retransmit 172
radius-server timeout 172
reauth interval 332
region 213
reload 131
remark-map (ポリシーマップ・クラスモード) 310
remark-map (集約ポリサーモード) 313
restart 131
revision 213
rmon 70
rmon alarm 74
rmon clear counters 78
rmon event 73
rmon history 72
rmon statistics 71

S

save 36
save logging 60
schedule 126
schedule template 129
send from 101
send notify wait-time 102
send server 101
send subject 102
send to 101
service terminal-length 56
service-policy 304
set cos 305
set cos-queue 317
set ip-dscp 306
set ip-dscp-queue 317
set ip-precedence 306
set lldp 109
set management-address-tlv 109
set msg-tx-hold 114
set timer msg-fast-tx 113
set timer msg-tx-interval 112
set timer reinit-delay 113
set too-many-neighbors limit 115
set tx-fast-init 114
sflow 79
sflow agent 79
sflow collector 80
sflow collector max-datagram-size 80
sflow max-header-size 81
sflow polling-interval 81
sflow sampling-rate 81
sfp-monitor rx-power 148
show access-group 288
show access-list 287
show aggregate-police 314
show arp 237
show auth statistics 176
show auth status 175
show auth supplicant 176
show backup-config 38
show boot 39
show cable-diagnostics tdr 47
show class-map 302
show clock 51
show config(show running-config) 37
show ddm status 147
show dhcp lease 234
show dipsw 133
show disk-usage 42
show dns-client 258
show eee capabilities interface 138
show eee status interface 138
show environment 41
show errdisable 183
show error port-led 132
show etherchannel 152
show etherchannel status 158
show firmware-update 125
show flowcontrol 324
show frame-counter 145
show http-server 89
show interface 141
show interface brief 143
show inventory 40
show ip dhcp snooping 229
show ip dhcp snooping binding 230
show ip dhcp snooping interface 229
show ip dhcp snooping statistics 230
show ip forwarding 240
show ip igmp snooping groups 270
show ip igmp snooping interface 271
show ip igmp snooping mrouter 270
show ip interface 233
show ip route 236
show ip route database 237
show ip route summary 237
show ipv6 dhcp interface 249
show ipv6 forwarding 254
show ipv6 interface 248
show ipv6 mld snooping groups 277
show ipv6 mld snooping interface 277
show ipv6 mld snooping mrouter 276
show ipv6 neighbors 253
show ipv6 route 252
show ipv6 route database 252
show ipv6 route summary 253
show l2ms 121
show lacp sys-id 154
show lacp-counter 156
show led-mode 132
show lldp interface 116
show lldp neighbors 118
show logging 60
show loop-detect 221
show mac-address-table 186
show mac-address-table count 187
show mail information 104
show memory 42
show mirror 140
show ntpdate 53
show policy-map 318
show port-security status 182
show process 42
show qos 293
show qos interface 293
show qos map-status 320
show qos metering-counters 316
show qos queue-counters 294
show radius-server 177
show radius-server local certificate list 337
show radius-server local certificate revoke 337

show radius-server local certificate status 336
show radius-server local nas 335
show radius-server local user 336
show rmon 76
show rmon alarm 78
show rmon event 77
show rmon history 77
show rmon statistics 76
show running-config 37
show sflow 82
show sflow sampling 82
show snmp community 69
show snmp group 70
show snmp user 70
show snmp view 69
show spanning-tree 207
show spanning-tree mst 216
show spanning-tree mst config 216
show spanning-tree mst instance 217
show spanning-tree statistics 209
show ssh-server 92
show ssh-server host key 95
show startup-config 38
show static-channel-group 150
show storm-control 325
show system-diagnostics 45
show tech-support 43
show telnet-server 84
show test cable-diagnostics tdr 47
show tftp-server 87
show tx-queue-monitor 149
show users 34
show vlan 200
show vlan access-map 290
show vlan filter 290
show vlan multiple-vlan 201
show vlan private-vlan 200
show y-unos 106
shutdown 135
snapshot delete 122
snapshot enable 121
snapshot save 122
snapshot trap terminal 122
snmp-server access 68
snmp-server community 65
snmp-server contact 64
snmp-server enable trap 63
snmp-server group 66
snmp-server host 61
snmp-server location 64
snmp-server startup-trap-delay 62
snmp-server user 67
snmp-server view 65
spanning-tree 203
spanning-tree bpdu-filter 204
spanning-tree bpdu-guard 205
spanning-tree edgeport 207
spanning-tree forward-time 202
spanning-tree instance 214
spanning-tree instance path-cost 215
spanning-tree instance priority 214
spanning-tree link-type 204
spanning-tree max-age 202
spanning-tree mst configuration 211
spanning-tree path-cost 206
spanning-tree priority (インターフェースモード) 206
spanning-tree priority (グローバルコンフィグレーションモード) 203
spanning-tree shutdown 201
speed-duplex 136
ssh 97
ssh-client 97
ssh-server 92
ssh-server access 93
ssh-server client alive 96
ssh-server host key generate 94
ssh-server interface 93
static-channel-group 150
storm-control 325
switchport access vlan 191
switchport mode access 190
switchport mode private-vlan 194
switchport mode trunk 191
switchport multiple-vlan group 198
switchport private-vlan host-association 194
switchport private-vlan mapping 195
switchport trunk allowed vlan 192
switchport trunk native vlan 193
switchport voice cos 197
switchport voice dscp 197
switchport voice vlan 196
system-diagnostics on-demand execute 46

T

telnet 85
telnet-client 86
telnet-server 83
telnet-server access 84
telnet-server interface 84
terminal length 55
test cable-diagnostics tdr interface 46
tftp-server 86
tftp-server interface 87
tlv-select basic-mgmt 110
tlv-select ieee-8021-org-specific 111
tlv-select ieee-8023-org-specific 111
tlv-select med 112
traceroute 242
traceroute6 256
traffic-shape queue rate 322
traffic-shape rate 321
tx-queue-monitor usage-rate (インターフェースモード) 149
tx-queue-monitor usage-rate (グローバルコンフィグレーションモード) 148

U

user 330
username 32
username privilege 33

V

vlan 188
vlan access-map 288
vlan database 187
vlan filter 289

W

write 36

Y

y-unos enable 105