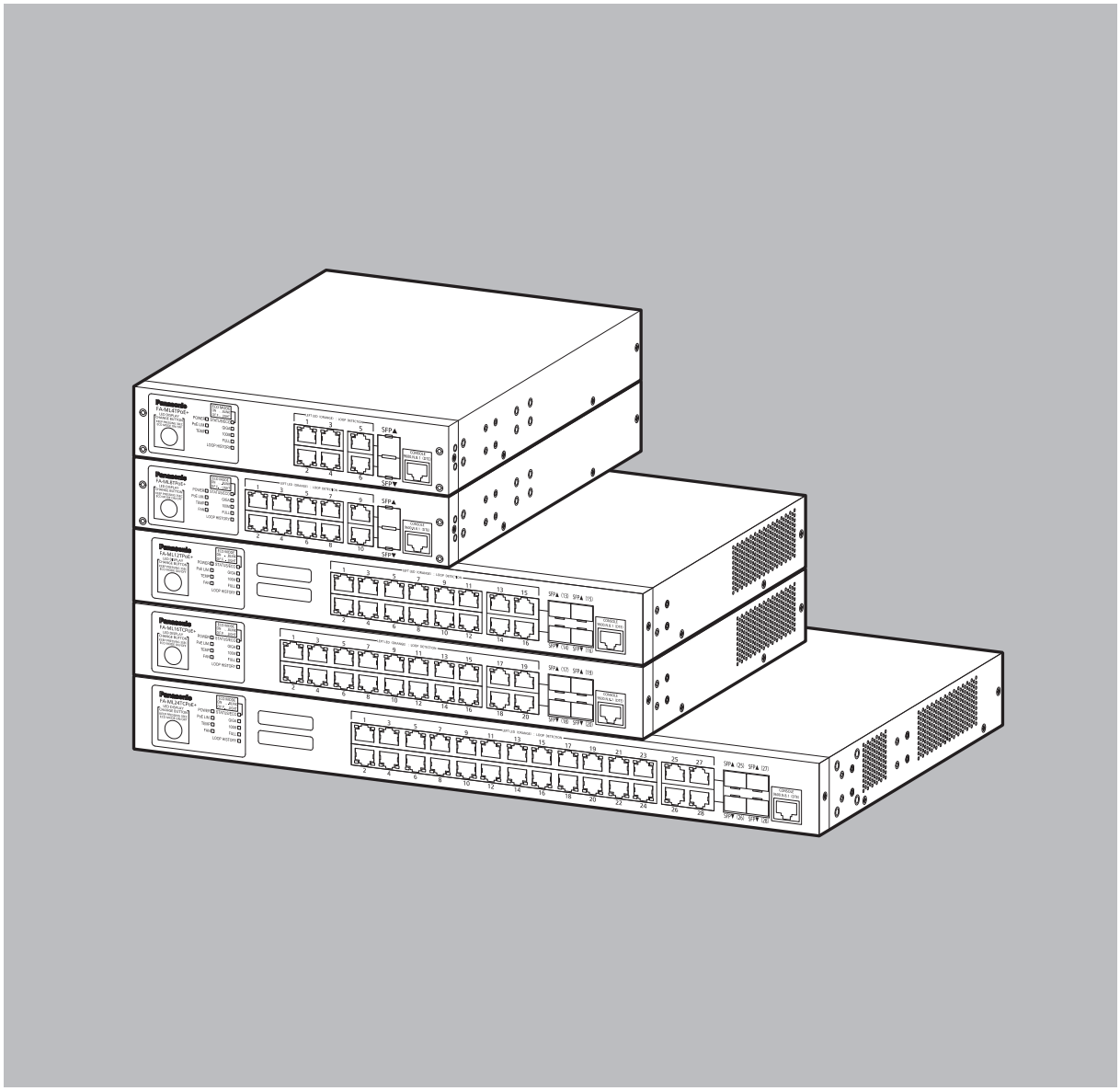
Panasonic

レイヤ２スイッチングハブ

WEB リファレンス

品番 PN230493N/PN230893
PN231293/PN231692
PN232492



本 WEB リファレンスは、以下の機種を対象としております。

品名	品番	ファームウェアバージョン
FA-ML4TPoE+	PN230493N	2.0.4.00 以上
FA-ML8TPoE+	PN230893	2.0.4.00 以上
FA-ML12TPoE+	PN231293	2.0.4.00 以上
FA-ML16TCPoE+	PN231692	2.0.4.00 以上
FA-ML24TCPoE+	PN232492	2.0.4.00 以上

各機種の対応機能は、商品仕様書をご覧ください。

目次

1 はじめに

本装置は WEB で設定をすることが可能です。

- WEB 設定を使用する場合、本装置に事前に CLI コマンドで以下①②③の設定が必要です。
  ① IP アドレスを設定。(192.168.0.101 は例です。)
  FA-ML#configure terminal
  FA-ML(config)#interface vlan 1
  FA-ML(config-if)#ip address 192.168.0.101 255.255.255.0
  ② http サーバ機能を有効化。
  FA-ML(config)#ip http server
  ③特権レベル 15 のユーザを作成。
  FA-ML(config)#username manager password manager privilege 15

- WEB ブラウザに①で設定した IP アドレスを入力し、③で設定したユーザ名、パスワードを入力すると、本装置にログインできます。

- ポップアップブロッカを使用している場合は、無効になっていることを確認してください。

- 管理ステーションで IPv6 インタフェースを使用している場合は、IPv6 リンクローカルアドレスではなく IPv6 グローバルアドレスを使用してブラウザから本装置にアクセスしてください。

- 操作なしで 10 分経過すると、自動でログアウトとなります。ログアウトまでの時間は設定 (セッションタイムアウト) により変更できます。

- 本リファレンスで使用している設定画面例は、実際の画面と異なる場合があります。

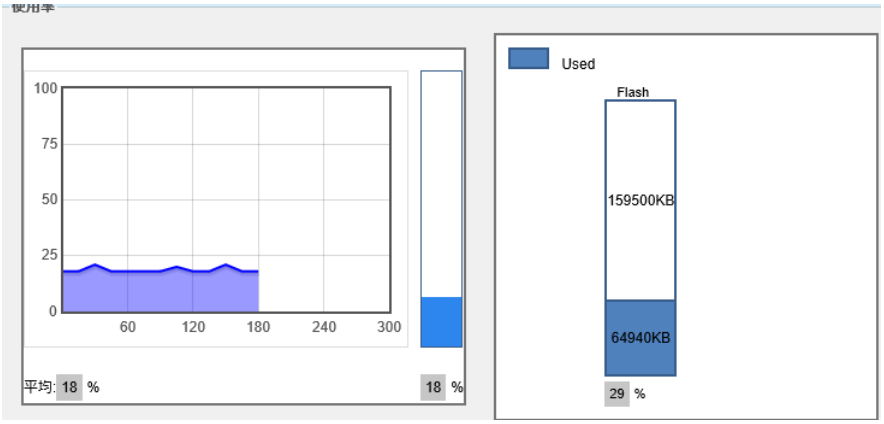
- 一部の画面は本リファレンスで説明していません。実際の画面の表示に従い、ご使用ください。

1.1 デバイス情報

ログインすると、最初にデバイス情報が表示されます。

パラメータ	概要
デバイスタイプ	FA-MLXXTPoE
システム名	デバイスのホスト名。
システムロケーション	デバイスの物理的な場所。
システム管理者	デバイスの連絡先。
ブート PROM バージョン	ブート PROM のバージョン。
ファームウェアバージョン	スイッチ用のバージョン
ハードウェアバージョン	ハードウェア用のバージョン。
MAC アドレス	ベース MAC アドレス。
IP アドレス	このデバイスの IP アドレス。
マスク	このデバイスのマスク。
ゲートウェイ	このデバイスのゲートウェイ。
システム時間	このデバイスのシステム時間。
シリアルナンバー	このデバイスのシリアル番号。

CPU、フラッシュの情報も以下のように表示されます。



2 システム

2.1 システム情報設定

システム設定を入力するには：

[システム] > [システム情報設定] に進みます。

パラメータ	概要
システム名	デバイスのシステム名を入力します。文字、数字、ハイフンのみを使用できます。ハイフンは先頭または末尾には使用できません。他の記号、句読点文字、またはスペースは使用できません。
システムロケーション	デバイスの物理的な場所を入力します。
システム管理者	デバイスの連絡先担当者の名前を入力します。
ウォッチドッグ	ウォッチドッグ機能を有効 / 無効にします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

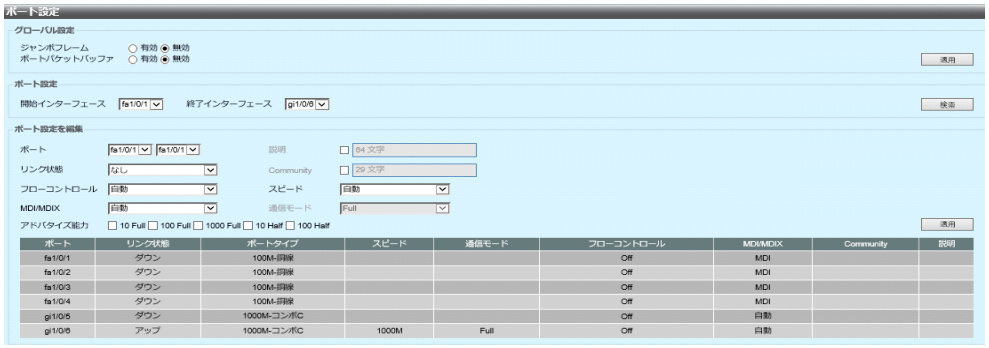
2.2 ポートコンフィグレーション

2.2.1 ポート設定

[ポート設定] ページには、グローバル設定とポートごとの設定が表示されます。このページは **[適用]** ボタンで選択、設定できます。

[ポート設定] テーブルを表示するには：

[システム] > [ポート設定] > [ポート設定] に進みます。



「グローバル設定」でジャンボフレームを有効または無効に設定します。次に、**[適用]** を押します。
「グローバル設定」でパケットバッファの拡張を有効または無効に設定します。次に、**[適用]** を押します。
「ポート設定」で [開始インターフェース]/[終了インターフェース] を設定します。次に、**[検索]** を押します。

「ポート設定の編集」で、ポートごとの設定を行うには：

[システム] > [ポートコンフィグレーション] > [ポート設定] に進みます。
選択したポート範囲のポート設定が表示されます。

パラメータ	概要
開始インターフェース / 終了インターフェース	ポート番号の範囲を選択します。
リンク状態	デバイスの再起動時に必要なポートの状態として、アップまたはダウンを選択します。
フローコントロール	802.3x フローコントロールの [オフ] または [自動]/[オン]（フル Duplex モード時のみ）を選択します。
MDI/MDIX	ポートの *Media Dependent Interface*（MDI）/*Media Dependent Interface with Crossover*（MDIX）の状態。 以下のオプションがあります。 • *MDIX* — ポートの送受信ペアをスワップします。 • *MDI* — ストレートスルーケーブルを使用して、このデバイスをステーションに接続します。 • *自動* — 別のデバイスに接続する正しいピンアウトを自動で検出するように、このデバイスを設定します。
説明	ユーザ定義によるポート名またはコメントを選択、入力します。
コミュニティ	ポートコミュニティ番号を選択して入力します。
スピード	ポートスピードを設定します。テーブルに表示されているポートタイプは利用可能なスピードです。スピードを設定するには、自動 /10M/100M/1000M/10G を選択できます。
通信モード	ポートの通信モードを設定します。このフィールドは、[スピード] フィールドで [自動] を選択していない場合のみに設定できます。ポートスピードは 10M または 100M に設定します。ポートスピードが 1G のときは、通信モードは常にフルです。 以下のオプションがあります。 • *ハーフ* — このポートはデバイスとクライアント間の送信を一度に 1 方向のみサポートします。 • *フル* — このポートはデバイスとクライアント間の送信を双方向同時にサポートします。
アドバタイズ能力	[スピード] を [自動] に設定したときスピードによりアドバタイズされる機能を選択します。 以下のオプションがあります。 • *10 Half* — ハーフ Duplex モードで 10Mbps のスピード。 • *10 Full* — フル Duplex モードで 10Mbps のスピード。 • *100 Half* — ハーフ Duplex モードで 100Mbps のスピード。 • *100 Full* — フル Duplex モードで 100Mbps のスピード。 • *1000 Full* — フル Duplex モードで 1000Mbps のスピード。

[適用] を押してランニングコンフィグレーションファイルを更新します。

2.2.2 エラーリカバリ設定

このページでは、自動リカバリ時間の経過後に、エラー状態によりシャットダウンしたポートが自動で有効に戻るように設定できます。

エラーリカバリ設定を指定するには：

[システム] > [ポート設定] > [エラーリカバリ設定] に進みます。

[適用] を押してグローバル設定とランニングコンフィグレーションファイルを更新します。

パラメータ	概要
自動復旧間隔	自動でエラーが回復する時間を指定します。
停止理由	• **ポートセキュリティ** — ポートセキュリティのためポートがシャットダウンしたとき自動エラーリカバリを有効にするように設定します。 • **802.1x** — 802.1x–802.1x によってポートがシャットダウンしたとき自動エラーリカバリを有効にするように設定します。 • **ACL 拒否** — ACL 拒否により自動エラーリカバリが有効になるように設定します。 • **STP BPDU ガード** — STP BPDU ガードによってポートがシャットダウンしたとき自動エラーリカバリが有効になるように設定します。 • **STP ループバックガード** — STP ループバックガードによってポートがシャットダウンしたとき自動エラーリカバリが有効になるように設定します。 • **UDLD** — UDLD によってポートがシャットダウンしたとき自動エラーリカバリが有効になるように設定します。 • **ループ検知・遮断** — ループバック検出によってポートがシャットダウンしたとき自動エラーリカバリが有効になるようにします。 • **ストームコントロール** — ストームコントロールによってポートがシャットダウンしたとき自動エラーリカバリが有効になるように設定します。

2.2.3 ループバック検出設定

ループバック検出（LBD）を用いて、ループパケットによるループが送信されたときループを防ぎます。デバイスが以前に送信された同じループプロトコルパケットを再び受信すると、このポートはユーザ設定に応じてブロックされるかシャットダウンされます。

ループプロトコルパケットの受信後にループを検出すると、ポートがブロック（ブロッキング状態）またはシャットダウン（シャットダウン状態）されます。デバイスはシステムログに記録し、トラップをトリガします。

ループ検知状態の定義は以下のようになります。

- **フォワーディング状態** — 通常のフォワーディング状態。独自のループバックフレームを検知すると、ループ検知状態に移行します。ループ検知状態は 2 つのモードでサポートされます（シャットダウン状態、ブロッキング状態）。
- **ブロッキング状態** — ポートブロッキング状態。以下のフレームのみを受け入れ、CPU へ転送します。他のフレームは必ず破棄されます。回復タイマを使用します。「独自のループバックフレーム」と「パナソニック PSDN プロトコル、BPDU、LACP、RRP」
- **シャットダウン状態** — ポートシャットダウン状態。ポートの管理状態は「ダウン」に設定されます。回復タイマを使用します。

ポートリカバリは以下のように定義されます。

- **回復タイマ** — このパラメータはユーザが変更できます（デフォルトは 60 秒）。回復時間を過ぎると、ポート状態またはポート管理のアクションが実行されます。

ループ検知モードは以下のように定義されます。

- **シャットダウンモード** —
  (a) ループを検出すると、受信したポートは「シャットダウン状態」になります。
  (b) ポートにより送信されたループ検知フレームをそのポートが受信すると、ポートは直ちに「シャットダウン状態」になります。その後、ポートは「ブロッキング状態」に設定されます。
  (c) 回復タイマの残り時間が 30 秒になると、「シャットダウンしていない状態」に変わります（ポート管理：アップ）。
  (d) 30 秒間にポートにより送信されたループ検知フレームをそのポートが受信しないと、ポートは「フォワーディング状態」になります。

- ブロッキングモード —
  (a) ループを検出すると、受信したポートは「ブロッキング状態」になります。
  (b) 回復時間の間にポートにより送信されたループ検知フレームをそのポートが受信しないと、ポートは「フォワーディング状態」になります。

他の機能との関係：
- LBD が有効なポートで RRP を有効にする場合は、この設定は失敗します。
- RRP が有効なポートで LBD を有効にする場合は、この設定は失敗します。

2.2.4 ループ検知機能の有効化・無効化

グローバル設定またはポートごとの設定により、ループ検知機能を有効または無効にできます。

ループが検知されると、スイッチは以下のアクションを実行します。

- ブロッキング / シャットダウン状態が受信ポートで設定されます。
- SYSLOG にこのループ情報が含まれます。

2.2.5 デフォルト設定

- グローバルループ検知・遮断状態 : 有効
- ポート：ポート fa1/0/1
- ループ検知・遮断状態：
  ダウンリンクポート：有効、アップリンクポート（コンボポート）：無効
- 復旧時間：60 秒
- モード：ブロック

ループバック検知を設定するには：

[システム] > [ポート設定] > [ループバック検出設定] に進みます。

[グローバルループ検知・遮断状態] フィールドで **[有効]** または **[無効]** を設定し、ループ検知機能を有効または無効にします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

[ポート] フィールドで **[ポート]** または **[LAG]** を設定し、設定対象のポートを選別します。

[ループ検知・遮断状態] で **[有効]** または **[無効]** を設定します。

[復旧時間] フィールドに秒単位の時間を入力します。

[モード] フィールドで **[ブロック]** または **[シャットダウン]** を設定します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

2.3 PoE 設定

2.3.1 PoE 条件設定

[PoE 条件設定] ページでは、PoE に関する装置共通の設定を行います。

[PoE 条件設定] テーブルを表示するには：
[システム] > [PoE 設定] > [PoE 条件設定] に進みます。

[画面の説明]

最大供給可能電力	この装置から給電可能な最大電力量が表示されます。	
Fan Speed Level	ファンの回転速度を設定します。（ファンレス製品は対象外です。） 設定値は High (工場出荷時) / Low1 /Low2 /Stop です。	
現在の供給電力	この装置からの現在の供給電力量が表示されます。	
Trap 送出用閾値	Trap を送信するための供給電力の閾値が表示されます。	
供給可能電力 超過時動作	供給電力が [最大供給可能電力] を超えた場合の給電方法が表示されます。	
	直前に接続したポートへの給電をしない	[最大供給可能電力] を超えた直前に接続されたポートへの給電を停止します。(工場出荷時設定)
	優先度が低いポートへの給電を停止する	[優先度] が一番低いポートへの給電を停止します。 [優先度] が同じ場合、ポート番号が大きいポートへの給電を停止します。
Fan Failure SNMP Trap Status	Fan Failure SNMP Trap 状態を設定できます。(ファンレス製品は対象外です。)	
PoE SNMP Trap Status	PoE SNMP Trap 状態を設定できます。	

[適用] を押してランニングコンフィグレーションファイルを更新します。

2.3.2 PoE ポート設定

[PoE ポート設定] ページでは、ポート毎の給電設定を行います。

[PoE ポート設定] テーブルを表示するには：
[システム] > [PoE 設定] > [PoE ポート設定] に進みます。

画面の説明

パラメータ	概要	
開始インターフェース / 終了インターフェース	ポート番号の範囲を選択します。	
給電設定	Up	給電を行います。
	Down	給電を行いません。
優先度	High	Critical の次に給電を行います。
	Critical	最優先で給電を行います。
	Low	優先給電を行いません
最大供給電力 (3000 to 30000 mW, 0:Auto)	最大供給電力を設定します。 0 を設定すると、クラスに基づき最大供給電力を設定します。	

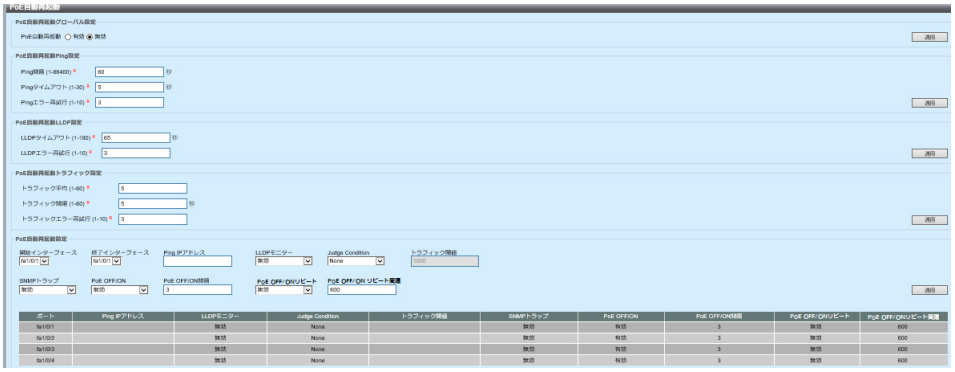
[適用] を押してランニングコンフィグレーションファイルを更新します。

パラメータ	概要	
ポート	ポート番号が表示されます。	
給電設定	給電可能かどうか表示されます。	
	Up	給電できます。
	Down	給電できません。
スケジューラ	PoE スケジューラ機能の状態が表示されます。 (対応予定)	
	ON	PoE スケジューラで PoE への給電が ON になったことを表します。
	OFF	PoE スケジューラで PoE への給電が OFF になったことを表します。
	-	PoE スケジューラが動作していないことを表します。
状態	給電の状態が表示されます。	
	Powered	給電を行っていることを表します。
	Not Powered	給電を行っていないことを表します。
	Overload	供給電力量の上限を超えた給電要求がされたために給電が停止されていることを表します。
レイヤ	接続機器が対応しているクラシフィケーション方式を表示します。	
	1	物理レイヤクラシフィケーションに対応しています。(IEEE802.3af 方式)
	2	LLDP を用いたデータリンクレイヤクラシフィケーション (DLLC) に対応しています。(IEEE802.3at 方式)
クラス	クラシフィケーションにより検出された Class 値が表示されます。	
優先度	給電の優先順位が表示されます。	
	Critical	最優先されることを表します。
	High	Critical の次に優先されることを表します。
	Low	優先されないことを表します。
最大供給電力 (mW)	供給電力の上限が表示されます。(200mW 単位) 「Auto」は、値がレイヤとクラスに従って計算されることを表します。	
電力 (mW)	供給電力が表示されます。(100mw 単位)	
電圧 (V)	電圧値が表示されます。(1V 単位)	
電流 (mA)	電流値が表示されます。(1mA 単位)	

2.3.3 PoE 自動再起動

[PoE 自動再起動] ページでは、PoE の自動再起動設定を行います。

[PoE ポート設定] テーブルを表示するには：
[システム] > [PoE 設定] > [PoE 自動再起動] に進みます。



[適用] を押してランニングコンフィグレーションファイルを更新します。

パラメータ	概要	
PoE 自動再起動	無効	PoE オートリブート無効 (工場出荷設定)
	有効	PoE オートリブート有効
Ping 間隔 (1-86400)	PoE オートリブートに使用する Ping 監視の間隔を秒単位で設定します。 (工場出荷設定 60)	
Ping タイムアウト (1-30)	PoE オートリブートに使用する Ping 監視のタイムアウトを秒単位で設定します。(工場出荷設定 5)	
Ping エラー再試行 (1-10)	PoE オートリブートに使用する Ping 監視のエラー発生時の再試行回数を設定します。(工場出荷設定 3)	
LLDP タイムアウト (1-180)	PoE オートリブートに使用するオートリブート LLDP 監視タイムアウトを秒単位で設定します。(工場出荷設定 65)	
LLDP エラー再試行 (1-10)	PoE オートリブートに使用するオートリブート LLDP 監視エラー時の再試行回数を設定します。(工場出荷設定 3)	
トラフィック平均 (1-60)	装置内部のトラフィック平均値算出間隔を設定します。(工場出荷設定 5)	

パラメータ	概要	
トラフィック間隔 (1-60)	トラフィック監視間隔を秒単位で設定します。(工場出荷設定 5)	
トラフィックエラー再試行 (1-10)	トラフィックエラー時の再試行回数を設定します。(工場出荷設定 3)	
開始インターフェース / 終了インターフェース	ポート番号の範囲を選択します。	
Ping IP アドレス	PoE オートリブートに使用する Ping の IP アドレスを設定します。	
LLDP モニター	無効	PoE オートリブート LLDP 監視無効 (工場出荷設定)
	有効	PoE オートリブート LLDP 監視有効
Judge Condition	None	通信料による PoE 端末異常判定無効 (工場出荷設定)
	Below	通信量が閾値を下回った場合に、PoE 端末を異常と判定します。
	Over	通信量が閾値を上回った場合に、PoE 端末を異常と判定します。
トラフィック閾値	通信量の閾値を bps で設定します。(0 ～ 100000000	
SNMP トラップ	無効	PoE オートリブート異常判定時の SNMP トラップ通知無効 (工場出荷設定)
	有効	PoE オートリブート異常判定時の SNMP トラップ有効
PoE OFF/ON	無効	PoE オートリブート異常判定時の PoE 給電 PoE OFF/ON 無効 (工場出荷設定)
	有効	PoE オートリブート異常判定時の PoE 給電 PoE OFF/ON 有効
PoE OFF/ON 間隔	PoE オートリブート異常判定時の PoE 給電 OFF/ON 繰り返し間隔を秒単位で設定します。(工場出荷設定 3)	

パラメータ	概要	
PoE OFF/ON リピート	無効	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し無効 (工場出荷設定)
	有効	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し有効
PoE OFF/ON リピート間隔	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し間隔を秒単位で設定します。(1-86400)	

[画面の説明]

パラメータ	概要	
ポート	ポート番号を表示します。	
Ping IP アドレス	PoE オートリブートに使用する Ping の IP アドレスを表示します。	
LLDP モニター	無効	LLDP モニター無効
	有効	LLDP モニター有効
Judge Condition	None	通信料による PoE 端末異常判定無効
	Below	通信量が閾値を下回った場合に、PoE 端末を異常と判定します。
	Over	通信量が閾値を上回った場合に、PoE 端末を異常と判定します。
トラフィック間隔	通信量監視間隔を表示します。	
SNMP トラップ	無効	PoE オートリブート異常判定時の SNMP トラップ通知無効
	有効	PoE オートリブート異常判定時の SNMP トラップ通知有効

パラメータ	概要	
PoE OFF/ON	無効	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し無効
	有効	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し有効
PoE OFF/ON 間隔	PoE オートリブート異常判定時の PoE 給電 OFF/ON 繰り返し間隔を表示します。	
PoE OFF/ON リピート	無効	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し無効
	有効	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し有効
PoE OFF/ON リピート間隔	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し間隔を表示します。	

2.3.4 PoE スケジューラスケジュール情報

[PoE スケジューラスケジュール情報] ページでは、PoE スケジューラのスケジュール情報を表示します。

[PoE スケジューラスケジュール情報] テーブルを表示するには :
[システム] > [PoE 設定] > [PoE スケジューラスケジュール情報] に進みます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

[画面の説明]

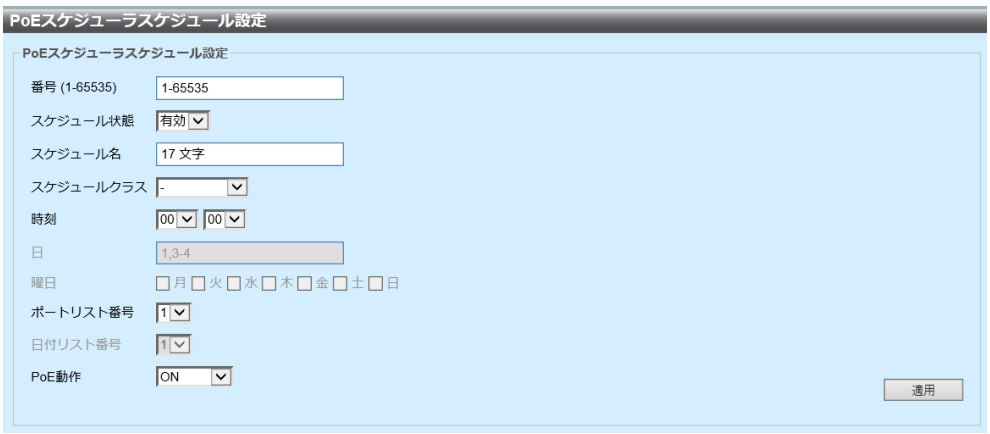
パラメータ	概要	
PoE スケジューラ グローバル設定状態	PoE スケジューラの設定状態が表示されます。	
	有効	PoE スケジューラを有効にします。
	無効	PoE スケジューラを無効にします。
PoE スケジューラ動作状態	PoE スケジューラの動作状態が表示されます。	
	Enalbe	PoE スケジューラ動作有効
	Disable	PoE スケジューラ動作無効 PoE スケジューラ機能は SNTP 機能で SNTP サーバと時刻同期する必要があります。 SNTP サーバとの同期が 3 回連続行えない場合、PoE スケジューラ機能で実行された PoE ポート状態は実行前の状態に自動的に復旧します。
表示順	指定した順番で一覧表示を並べ替えます。	
	番号	PoE スケジュールがインデックス番号順に表示されます。
	次回スケジュール実行時間	PoE スケジュールが次回実行時間順に表示されます。

パラメータ	概要	
番号	PoE スケジュールのインデックス番号が表示されます。 各エントリの [削除] をクリックすると、該当の PoE スケジュールを削除します。	
スケジュール名	PoE スケジュール名称が表示されます。	
スケジュールクラス	PoE スケジュールのクラスが表示されます。	
	毎日	毎日指定された時刻にスケジュールを実行します。
	毎週	毎週指定された曜日と時刻にスケジュールを実行します。
	毎月	毎月指定された日時にスケジュールを実行します。
	日付リスト	ユーザが指定した日時にスケジュールを実行します。
ポートリスト	PoE スケジュールが実行されるポートリストのインデックス番号が表示されます。	
PoE 動作	PoE スケジュールのアクションが表示されます。	
	ON	PoE を ON にします。
	OFF	PoE を OFF にします。
	OFF/ON	PoE を OFF/ON（再起動）します。
スケジュール状態	該当の PoE スケジュールの状態が表示されます。	
	Enable	該当の PoE スケジュールを有効にします。
	Disable	該当の PoE スケジュールを無効にします。
次回スケジュール実行時間	次回のスケジュールが実行される日時が表示されます。	

2.3.5 PoE スケジューラスケジュール設定

[PoE スケジューラスケジュール設定] ページでは、PoE スケジューラのスケジュール設定を行います。

[PoE スケジューラスケジュール設定] テーブルを表示するには：
[システム] > [PoE 設定] > [PoE スケジューラスケジュール設定] に進みます。



[適用] を押してランニングコンフィグレーションファイルを更新します。

[画面の説明]

パラメータ	概要	
番号	PoE スケジュールのインデックス番号が表示されます。	
スケジュール状態	該当の PoE スケジュールの状態が表示されます。	
	Enable	該当の PoE スケジュールを有効にします。
	Disable	該当の PoE スケジュールを無効にします。
スケジュール名	PoE スケジュール名称が表示されます。	
スケジュールクラス	PoE スケジュールのクラスが表示されます。	
	毎日	毎日指定された時刻にスケジュールを実行します。
	毎週	毎週指定された曜日と時刻にスケジュールを実行します。
	毎月	毎月指定された日時にスケジュールを実行します。
	日付リスト	ユーザが指定した日時にスケジュールを実行します。
時刻	PoE スケジュールが実行される時刻が表示されます。	
日	PoE スケジュールが実行される日（月単位）が表示されます。	

パラメータ	概要	
曜日	PoE スケジュールが実行される曜日（週単位）が表示されます。	
ポートリスト番号	PoE スケジュールが実行されるポートリストのインデックス番号が表示されます。	
日付リスト番号	PoE スケジュールが実行される日付リストのインデックス番号が表示されます。	
PoE 動作	PoE スケジュールのアクションが表示されます。	
	ON	PoE を ON にします。
	OFF	PoE を OFF にします。
	OFF/ON	PoE を OFF/ON（再起動）します。

2.3.6 PoE スケジューラポートリスト情報

[PoE スケジューラポートリスト情報] ページでは、PoE スケジューラのポートリストを表示します。

[PoE スケジューラポートリスト情報] テーブルを表示するには :
[システム] > [PoE 設定] > [PoE スケジューラポートリスト情報] に進みます。

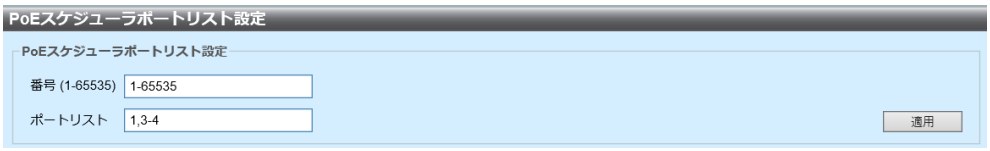
[画面の説明]

パラメータ	概要
番号	ポートリストのインデックス番号が表示されます。 各エントリの [削除] をクリックすると、該当のポートリストを削除します。
ポートリスト	ポートリストが表示されます。

2.3.7 PoE スケジューラポートリスト設定

[PoE スケジューラポートリスト設定] ページでは、PoE スケジューラのポートリスト設定を行います。

[PoE スケジューラポートリスト設定] テーブルを表示するには：
[システム] > [PoE 設定] > [PoE スケジューラポートリスト設定] に進みます。



[適用] を押してランニングコンフィグレーションファイルを更新します。

[画面の説明]

パラメータ	概要
番号	ポートリストのインデックス番号が表示されます。
ポートリスト	ポートリストが表示されます。

2.3.8 PoE スケジューラ日付リスト情報

[PoE スケジューラ日付リスト情報] ページでは、PoE スケジューラの日付リストを表示します。

[PoE スケジューラ日付リスト情報] テーブルを表示するには :
[システム] > [PoE 設定] > [PoE スケジューラ日付リスト情報] に進みます。

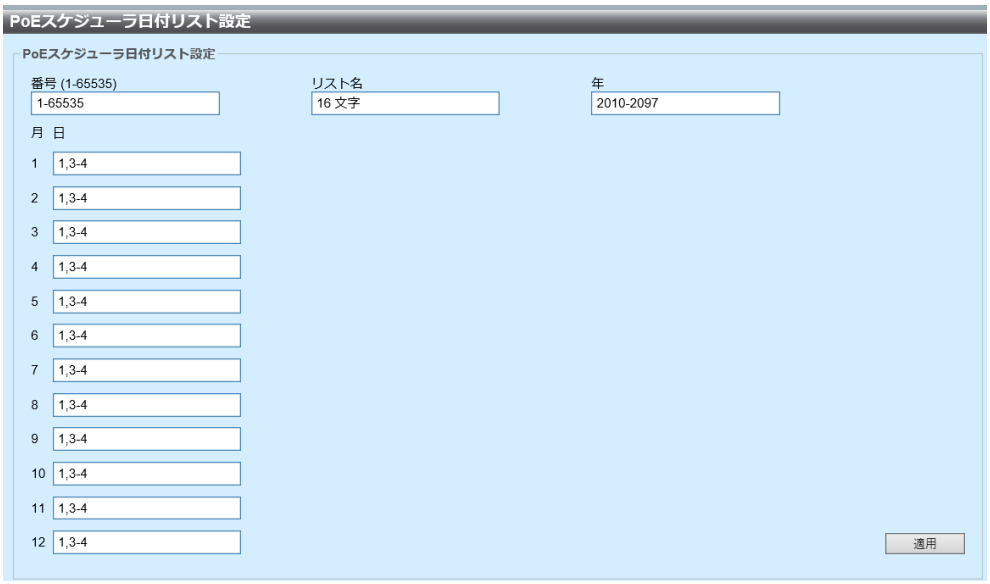
[画面の説明]

パラメータ	概要
番号	各エントリの [削除] をクリックすると、該当の日付リストを削除します。
年	日付リストが実行される年が表示されます。
月日	日付リストが実行される月日が表示されます。

2.3.9 PoE スケジューラ日付リスト設定

[PoE スケジューラ日付リスト設定] ページでは、PoE スケジューラの日付リスト設定を行います。

[PoE スケジューラ日付リスト設定] テーブルを表示するには :
[システム] > [PoE 設定] > [PoE スケジューラ日付リスト設定] に進みます。



[適用] を押してランニングコンフィグレーションファイルを更新します。

[画面の説明]

パラメータ	概要
番号	日付リストのインデックス番号が表示されます。
日付リスト名	日付リストの名称が表示されます。
年	日付リストに設定される年が表示されます。
月	日付リストに設定される月が表示されます。
日	日付リストに設定される日が表示されます。

2.3.10 ポート別 PoE スケジュール情報

[ポート別 PoE スケジュール情報] ページでは、設定済みのポート別 PoE スケジュール情報を表示します。

[ポート別 PoE スケジュール情報] テーブルを表示するには：
[システム] > [PoE 設定] > [ポート別 PoE スケジュール情報] に進みます。

[画面の説明]

パラメータ	概要	
ポート番号	表示対象のポート番号を指定します。	
番号	PoE スケジュールのインデックス番号が表示されます。	
スケジュールクラス	PoE スケジュールのクラスが表示されます。	
	毎日	毎日指定された時刻にスケジュールを実行します。
	毎週	毎週指定された曜日と時刻にスケジュールを実行します。
	毎月	毎月指定された日時にスケジュールを実行します。
	日付リスト	ユーザが指定した日時にスケジュールを実行します。
日／曜日／月日	PoE スケジュールが実行される日（月単位）、曜日（週単位）、または月日が表示されます。	
PoE 動作	PoE スケジュールのアクションが表示されます。	
	ON	PoE を ON にします。
	OFF	PoE を OFF にします。
	OFF/ON	PoE を OFF/ON（再起動）します。
スケジュール状態	該当の PoE スケジュールの状態が表示されます。	
	有効	該当の PoE スケジュールを有効です。
	無効	該当の PoE スケジュールを無効です。

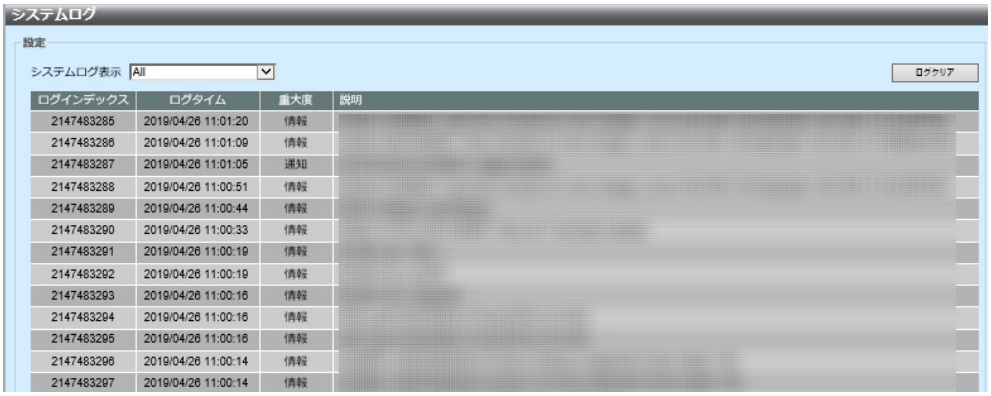
2.4 システムログ

以下のように、2 種類のログを記述できます。

- RAM に保存されるログ（再起動後、または電源オフで消去されます）。
- フラッシュメモリに保存されるログ（ユーザが手動で実行するコマンドによりクリアできます）。

ログメッセージに重大度を設定し、設定したレベルより高い重大度のログを SYSLOG サーバに送信できます。

ログのエントリを表示するには、**[システム] > [システムログ] > [システムログ]** に進みます。



ページ上部に以下が表示されます。

- **システムログ表示** — ログのタイプ：All、LoopDetection、AAA

すべてのログをクリアするには、**[ログクリア]** を押します。

2.4.1 ログ設定

重大性レベルには 7 段階あり、ログメッセージごとに次のように設定できます。例えば、「%INIT-N-message: …」というログメッセージの重大性は、**N**（情報）のレベルになります。

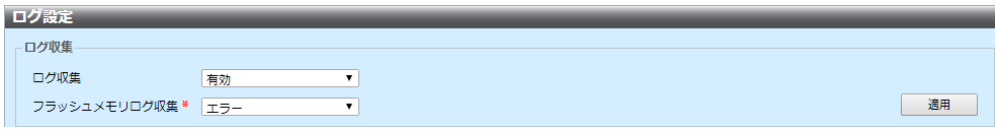
- **緊急** — システムは使用できません。
- **アラート** — アクションが必要です。
- **クリティカル** — システムは致命的な状態です。
- **エラー** — システムはエラー状態です。
- **ワーニング** — システムの警告が発生しました。
- **通知** — システムは適切に機能していますが、システムの通知が発生しました。
- **情報** — デバイス情報。
- **デバッグ** — イベントについての詳細情報。

デバイスでは重大性が高いイベントが保存されます。重大性が低いイベントは保存されません。

例えば、**エラー**を設定すると、それ以上の重大性レベルのログ（緊急、警告、クリティカル、エラー）がすべて保存されます。それより低い重大性のログ（警告、通知、情報、デバッグ）は保存されません。

グローバルなログパラメータを設定するには：

[システム] > [システムログ] > [ログ設定] に進みます。



パラメータ	概要
ログ収集	ログを有効または無効に設定します。
フラッシュメモリログ収集	RAM に保存されるメッセージの重大性レベルを設定します。

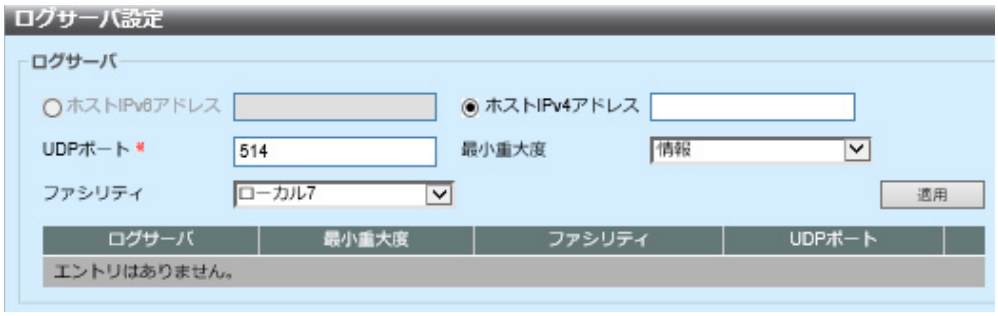
[適用] を押してランニングコンフィグレーションファイルを更新します。

2.4.2 ログサーバ設定

このページでは、リモート SYSLOG サーバにログメッセージを送信する必要がある場合に、使用するリモート SYSLOG サーバを設定できます（重大性含む）。

SYSLOG サーバを設定するには：

[システム] > [システムログ] > [ログサーバ設定] に進みます。



パラメータ	概要
ホスト **IPv4** アドレス	SYSLOG メッセージが送信されるサーバのソースインタフェース（IPv4 アドレス）を設定します。
ホスト **IPv6** アドレス	SYSLOG メッセージが送信されるサーバのソースインタフェース（IPv6 アドレス）を設定します。
UDP ポート	UDP ポートを設定します。
ファシリティ	ファシリティ — 1 ～ 7 のローカル値のいずれかを選択します。2 回目の値を割り当てると、最初の値は無効になります。
最小重大度	送信されるシステムログメッセージの最小レベルを設定します。

[適用] を押してランニングコンフィグレーションファイルを更新します。
SYSLOG サーバが追加されます。

2.5 時間

ネットワーク上のすべてのデバイスでは、システム時刻を同期させます。これはネットワーク時間の同期のために欠かせません。イベントログ時の管理、セキュリティ、ネットワークデバッギングに関係するからです。システム時間が時刻と同期していないと、セキュリティやネットワーク使用量のログファイルの追跡が困難になり、セキュリティ違反やネットワーク使用量の追跡時にデバイス間でログファイルを正確に相関できなくなります。

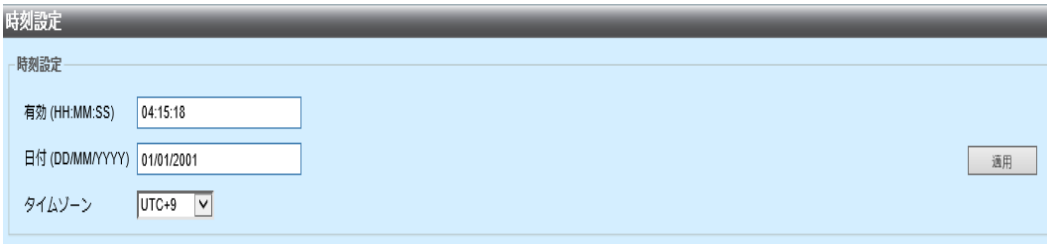
時間の同期によって、共有ファイルシステム間の差異を削減できます。時間を修正して統一させるには、デバイスでの時間設定が重要です。

NOTE デバイスでは Simple Network Time Protocol（SNTP）がサポートされており、有効にするとデバイスは SNTP クライアントとして機能し、システム時間を SNTP サーバと自動で同期します。

2.6 時刻設定

絶対的なタイムレンジを設定するには：

[システム] > [時間と SNTP] > [時刻設定] に進みます。



デバイスの時間と日付が表示されます。

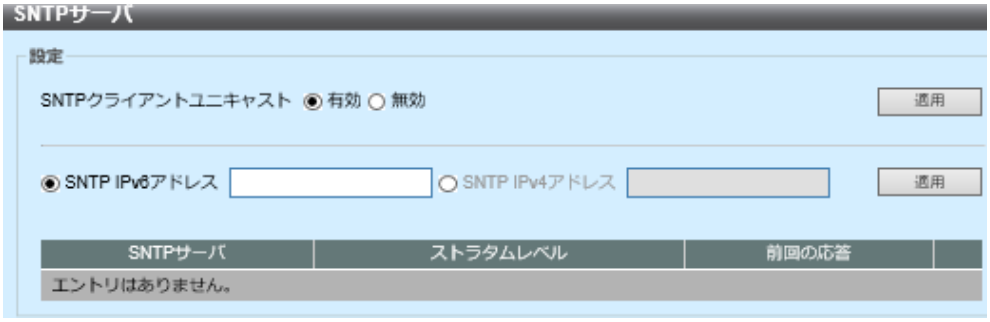
パラメータ	概要
時間（HH:MM:SS）	時間を設定します。例：04:15:18
日付（DD/MM/YYYY）	日付を設定します。例：01/01/2001
タイムゾーン	タイムゾーンを設定します。例：UTC+9

[適用] を押してランニングコンフィグレーションファイルを更新します。

2.7 SNTP サーバ

SNTP サーバを IPv6 または IPv4 に設定するには：

[システム] > [時間と SNTP] > [SNTP サーバ] に進みます。



デバイスのタイムレンジが表示されます。

SNTP クライアントユニキャストで有効または無効を設定します。

パラメータ	概要
SNTP IPv6 アドレス	SNTP IPv6 サーバアドレスを設定します。
SNTP IPv4 アドレス	SNTP IPv4 サーバアドレスを設定します。

[適用] を押します。

2.8 時間範囲

タイムレンジを設定し、以下のコマンドタイプと関連付け、タイムレンジ内に適用できます。

- ACL
- 8021X ポート認証
- ポート設定

いずれかのタイムレンジに達する時点で、関連するコマンドの機能が無効になります。

デバイスでは最大 10 のタイムレンジがサポートされます。

すべての時間指定はローカル時間として解釈されます（夏時間はこれに影響しません）。タイムレンジの入力値が目的の時間に有効になるように、システム時間を設定する必要があります。

時間範囲機能は以下のために使用できます。

- （例）業務時間中などにコンピュータのネットワークアクセスを制限します。それ以降はネットワークポートがロックされ、他のネットワークへのアクセスがブロックされます（「ポート設定」と「リンクアグリゲーション」を参照）。

タイムレンジを設定するには：

[システム] > [タイムレンジ] に進みます。

デバイスのタイムレンジが表示されます。

パラメータ	概要
タイムレンジ名	新しいタイムレンジ名を設定します。
開始時間	開始時間を設定するには、タイムレンジが始まる時間と日付を入力します。
終了時間	終了時間を設定するには、タイムレンジが終わる時間と日付を入力します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

3 管理

3.1 IP アドレス

IP アドレスページでは、IP アドレスを弊社スイッチに簡単に設定できます。
IP アドレス簡単設定ページは、以下の場合に便利です。

- 設定者が PC について詳しくない。
- キープアライブのチェックに ping 応答を使用できる。

3.1.1 IP アドレス簡単設定プロトコル設定

[管理] > [IP アドレス] > [IP アドレス簡単設定] に進みます。

[IP アドレス簡単設定インタフェース] フィールドで、オプションのいずれかを設定します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

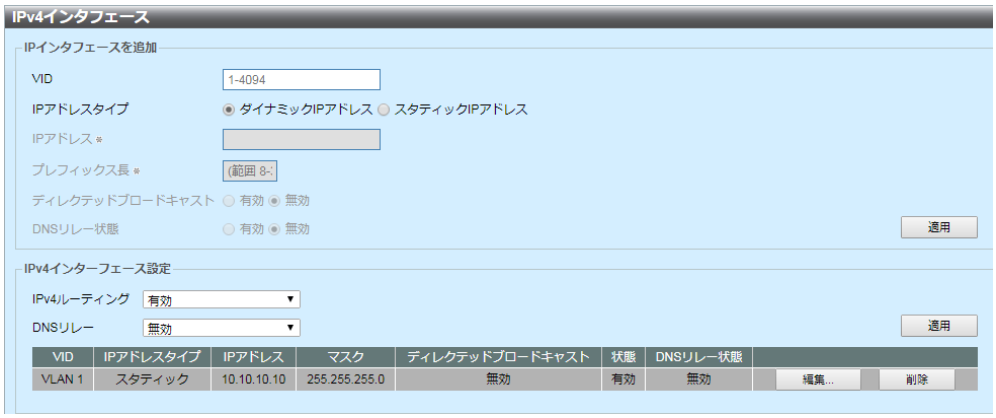
3.1.2 IPv4 インタフェース

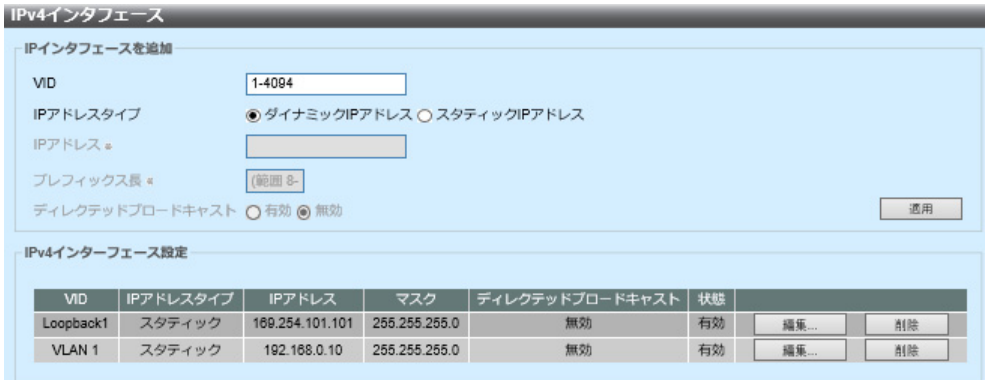
[IPv4 インタフェース] ページを用いて、デバイスの管理 IP アドレスを設定します。この IP アドレスは、VLAN、ループバックインタフェースに設定できます。

NOTE デバイスソフトウェアは、ポートまたは LAG に設定されている IP アドレスごとに VLAN ID（VID）を 1 つずつ消費します。デバイスは、4094 から開始して最初の未使用の VID を使用します。

IPv4 アドレスを設定するには：

[L3 機能] > [インタフェース] > [IPv4 インタフェース] に進みます。





IPv4 ルーティングを有効にするには、[IPv4 ルーティング] フィールドで **[有効]** を選択します。
DNS リレーを有効にするには、[DNS リレー] フィールドで **[有効]** を選択します。

[IPv4 インターフェース設定] ブロックの **[適用]** を押してランニングコンフィグレーションファイルを更新します。

IPv4 インタフェース設定テーブルには以下のフィールドが表示されます。

パラメータ	概要
VID	VLAN ID。
IP アドレスタイプ	以下の 2 つのパラメータがあります。 • *[ダイナミック IP アドレス]* — DHCP サーバから受信したアドレスです。 • *[スタティック IP アドレス]* — スタティック IP アドレスはユーザが手動で入力します。
IP アドレス	IP アドレスを入力します。
プレフィックス長	プレフィックス長（8 ～ 30）を入力します。
ディレクテッドブロードキャスト	ディレクデッドブロードキャストの物理ブロードキャストへの変換を有効または無効にします。
DNS リレー状態	DNS リレーを有効または無効にします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

> **注意** システムが、バックアップマスターが存在するいずれかのスタッキングモードにある場合、スタッキングマスターのスイッチオーバー中にネットワークから切断されないようにするために、**IP** アドレスをスタティックアドレスとして設定することを推奨します。これは、バックアップマスターがスタックの制御を引き継いだ場合に、**DHCP** を使用していると、スタックの元のマスターだったユニットから受信したものとは異なる **IP** アドレスを受信する可能性があるからです。

3.1.3 IPv6 インタフェース

IPv6 インタフェースは VLAN に設定できます。

IPv6 インタフェースを設定するには：

[L3 機能] > [インタフェース] > [IPv6 インタフェース] に進みます。

以下のフィールドに入力します。

パラメータ	概要
VID	特定の VLAN を選択します。

以下のパラメータが表示されます。

パラメータ	概要
インタフェース	インタフェース名。
状態	DHCPv6 クライアントが有効か無効かが表示されます。
自動設定	ネイバーから送信されたルータ広告に基づいて自動設定されたアドレスが表示されます。
IPv6 リダイレクト	ICMP IPv6 リダイレクトメッセージが有効か無効かが表示されます。これらのメッセージは、そのデバイスではなく別のデバイスにトラフィックを送信するように他のデバイスに通知するものです。

[適用] を押して、選択した VLAN で IPv6 処理を有効にします。

[削除] を押して、このインタフェース VLAN の IPv6 アドレスを削除することもできます。

3.2 PPS 設定

PPS（Power to Progress SDN）は、ネットワークを構成する複数の装置を一つのソフトウェアで管理し、運用や設定を容易にするための機能です。この機能を用いることで、PPS アプリケーション（別売）から本装置を制御することが可能となります。PPS アプリケーション（別売）から管理できる内容については、PPS アプリケーションの取扱説明書をご参照ください。

ご注意

- 起動後、Standalone の状態で 1 時間経過すると自動的に PPSP 機能を停止します。1 時間経過後、PPS コントローラを認識させるには機器の PPSP 機能を再起動、または機器の再起動を行ってください。
- 本機能を無効にした場合、PPS コントローラから管理できる内容が制限されます。
- 多拠点の機器（IP セグメントを超えた機器）への設定変更等をする場合は PPSP に対応した当社製レイヤ 3 スイッチングハブにて仮想リンク転送先 IP アドレスの設定が必要です。

3.2.1 PPS 設定

このページでは、PPS の基本設定を行います。

[管理] > [PPS 設定] > [PPS 設定] に進みます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

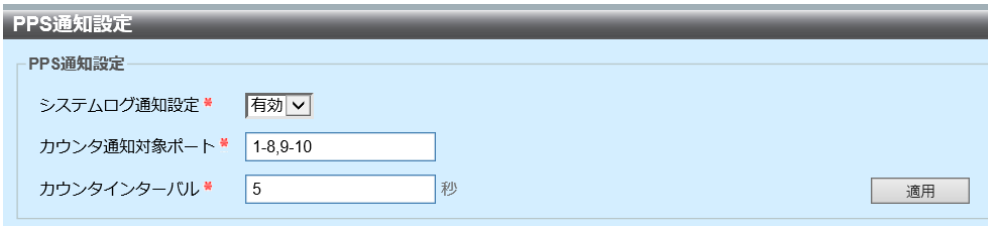
パラメータ	概要
PPS ステータス設定	PPS 機能を有効または無効に設定するか、リスタートを行います。
PPS スタート設定	PPS スタート状態を設定します。 **Standalone**ー PPS コントローラに管理されていない状態になります。 **CPNL**ー Controller Port Neightbor Lost 状態になり、コントローラを認識しているが、通信不可な状態になります。 Note. コントローラ ID が存在しない場合は、CPNL を選択しても Standalone 状態になります。
再送回数	生存確認を行うパケットの再送回数を設定します。再送回数は 1 ～ 5 回の範囲で指定します。
タイムアウト	生存確認のパケットに対する応答のタイムアウト値を設定します。タイムアウト値は 1 ～ 10 秒の範囲で設定します。
コントローラ ID	PPS コントローラの ID が表示されます。
コントローラ MAC アドレス	PPS コントローラの MAC アドレスが表示されます。

パラメータ	概要
PPS 状態	現在の PPS の動作状態が表示されます。
PPS ゲートウェイ	PPS ゲートウェイの MAC アドレスが表示されます。
コントローラポート	PPS コントローラとの通信に利用するポート番号が表示されます。
期限	PPS コントローラのの登録情報が削除されるまでの時間です。工場出荷時は 120 秒に設定されています。

3.2.2 PPS 通知設定

このページでは、PPS の通知設定を行います。

[管理] > [PPS 設定] > [PPS 通知設定] に進みます。



[適用] を押してランニングコンフィグレーションファイルを更新します。

パラメータ	概要
システムログ通知設定	PPS のシステムログ通知機能を有効または無効に設定します。
カウンタ通知対象ポート設定	PPS のカウンタ通知対象に使用するポートを設定します。
カウンタインターバル	カウンタインターバルの値を設定します。 値は１～１２０秒の範囲で設定します。

3.2.3 PPS ポート設定

このページでは、PPS のポート設定を行います。

[管理] > [PPS 設定] > [PPS ポート設定] に進みます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

パラメータ	概要
ポート	PPS ポート設定機能に使用するポートを指定します。
設定	PPS プライオリティの値を指定します。 値は 0 ～ 255 の範囲で指定します。
ポート	スイッチのポート番号が表示されます。
トランク	トランキングの設定状態をグループ番号で表示します。
リンク	各ポートのリンク状態をアップ / ダウンで表示します。
状態	各ポートの通信状態を表示されます。
設定	各ポートごとに設定された PPS の通信経路の自動判別に用いる優先度が表示されます。 工場出荷時は 128 が設定されています。
動作	各ポートごとに設定された PPS の通信経路の自動判別のための優先度が表示されます。

3.2.4 PPS ネイバー設定

このページでは、PPS のネイバー設定を行います。

[管理] > [PPS 設定] > [PPS ネイバー設定] に進みます。

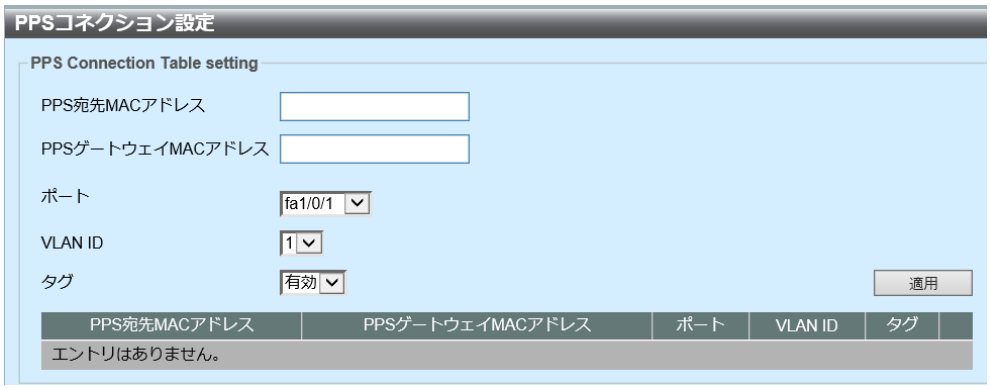
[適用] を押してランニングコンフィグレーションファイルを更新します。

パラメータ	概要
エージング時間	PPS 近接装置のエントリ保有時間を設定します。 値は 60 ～ 86400 秒の範囲で設定します。
MAC アドレス	PPS 近接装置の MAC アドレスが表示されます。
ポート	PPS 近接装置で通信に使用されているポート番号が表示されます。
期限	PPS 近接装置のエントリ保有時間が表示されます。

3.2.5 PPS コネクション設定

このページでは、PPS のコネクション設定を行います。

[管理] > [PPS 設定] > [PPS コネクション設定] に進みます。



[適用] を押してランニングコンフィグレーションファイルを更新します。

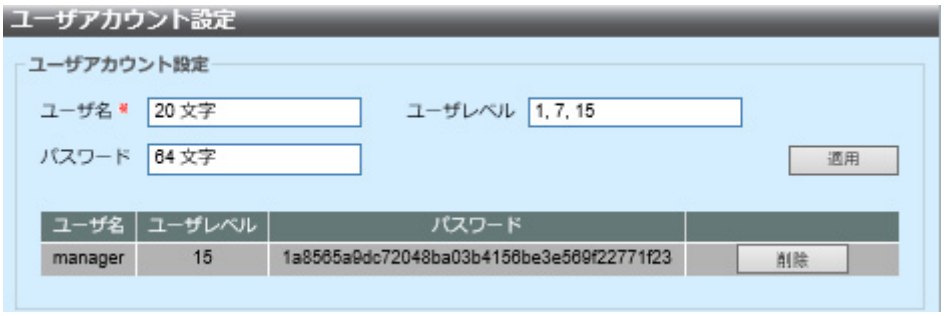
パラメータ	概要
PPS 宛先 MAC アドレス	PPS コネクションに追加する PPS 宛先 MAC アドレスを設定します。
PPS ゲートウェイ MAC アドレス	PPS コネクションに追加する PPS ゲートウェイ MAC アドレスを設定します。
ポート	PPS コネクションに追加するスイッチのポート番号を設定します。
VLAN ID	VLAN ID を設定します。 値は 1 ～ 4094 の範囲で設定します。
タグ	ゲートウェイに送信するパケットにタグをつける設定をします。有効 か 無効 を選択します。

3.3 ユーザアカウント設定

このページでは、ユーザを追加し、ユーザレベル（1/7/15）に応じてデバイスへのアクセスを許可することができます。

新規ユーザを追加するには：

[管理] > [ユーザアカウント設定] に進みます。



パラメータ	概要
ユーザ名	新しいユーザ名を 0 ～ 20 文字で入力します。UTF-8 文字は使用できません。
パスワード	パスワードを入力します（UTF-8 文字は使用できません）。パスワードの強度と複雑さが定義されている場合は、それに従います。
ユーザレベル	追加 / 編集するユーザレベルを設定します。 • *1（読み取り専用 CLI アクセス）— ユーザは GUI にアクセスできず、デバイス設定を変更できない CLI コマンドのみにアクセスできます。* • *7（読み取り / 制限付き書き込み CLI アクセス）*— ユーザは GUI にアクセスできず、デバイス設定を変更できる一部の CLI コマンドのみにアクセスできます。詳しくは *CLI* リファレンスガイドを参照してください。 • *15（読み書き管理アクセス）*— ユーザは GUI にアクセスでき、デバイスを設定できます。

[適用] を押してランニングコンフィグレーションファイルに更新を追加します。選択したユーザを削除するには **[削除]** を押し、ランニングコンフィグレーションファイルを更新します。

3.4 パスワード復旧

パスワード復旧を設定するには：

[管理] > [パスワード復旧] に進みます。

これを有効にすると、デバイスのコンソールポートへの物理アクセス権限を持つエンドユーザはブートメニューに入りパスワード復旧プロセスをトリガできます。システムの起動が終わると、パスワード認証なしにデバイスにログインできます。デバイスにログインするのは、コンソール経由でのみ、コンソールが物理アクセスによってデバイスに接続されている場合に限り許可されます。

これが無効の場合、ブートメニューへのアクセスは可能でパスワード復旧プロセスをトリガできます。

すべてのコンフィグレーションファイルとユーザファイルがシステム起動プロセスで削除され、適切なログメッセージが端末に対して生成されます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

3.5 SNMP

3.5.1 SNMP について

3.5.1.1 SNMP バージョンとワークフロー

デバイスの SNMP エージェントは SNMPv1、v2、v3 をサポートします。またシステムイベントをレポートし、サポート対象の MIB（Management Information Base）で定義されるトラップを使用しレシーバをトラップします。

3.5.1.2 SNMPv1 と v2

デバイスへのアクセスを管理するために、コミュニティエントリのリストが定義されます。各コミュニティエントリは*コミュニティ文字列*とそのアクセス特権で構成されます。デバイスは、正しい権限と正しい動作をともなうコミュニティを指定する SNMP イベントに対してのみ応答します。

SNMP エージェントはデバイスを管理する変数を維持します。それは *Management Information Base*（MIB）で定義されます。

NOTE セキュリティ脆弱性の問題のため、SNMPv3 の使用を推奨します。
セキュリティ上の理由から、デフォルトで SNMP は無効です。

3.6 エンジン ID

エンジン ID は SNMPv3 エンティティによって一意に使用されます。SNMP エージェントは権威 SNMP エンジンとみなされます。つまり、エージェントは受信されたメッセージ（Get、GetNext、GetBulk、Set）に応答しマネージャにトラップを送信します。エージェントのローカル情報はメッセージのフィールドにカプセル化されます。

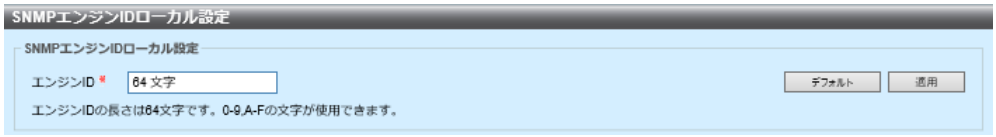
各 SNMP エージェントは、SNMPv3 メッセージ交換で使われるローカル情報を維持します。デフォルトの SNMP エンジン ID には、エンタープライズ番号とデフォルトの MAC アドレスが含まれています。このエンジン ID は、ネットワーク内のどのデバイスもエンジン ID が異なるように、一意である必要があります。

ローカル情報は 4 つの読み取り専用 MIB 変数に保存されます（snmpEngineId、snmpEngineBoots、snmpEngineTime、snmpEngineMaxMessageSize）。

> **注意** **エンジン ID を変更すると、設定済みの全ユーザとグループがクリアされます。**

SNMP エンジン ID を設定するには：

[管理] > [SNMP] > [エンジン ID ローカル設定] に進みます。



パラメータ	概要
デフォルト	これを押すと、デバイスで生成されたエンジン ID を使用します。デフォルトのエンジン ID はデバイスの MAC アドレスに基づいており、標準に準じて次のように定義されます。 • *最初の 4 つのオクテット* — 第 1 ビット = 1、残りは IANA Enterprise Number。 • *5 番目のオクテット* — 3 に設定し後続の MAC アドレスを示します。 • *最後の 6 つのオクテット* — デバイスの MAC アドレス。
エンジン ID	ローカルデバイスのエンジン ID を入力します。フィールド値は 16 進数文字列（範囲：10 ～ 64）です。16 進数文字列の各バイトは、2 桁の 16 進数で表されます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

3.7 ビュー

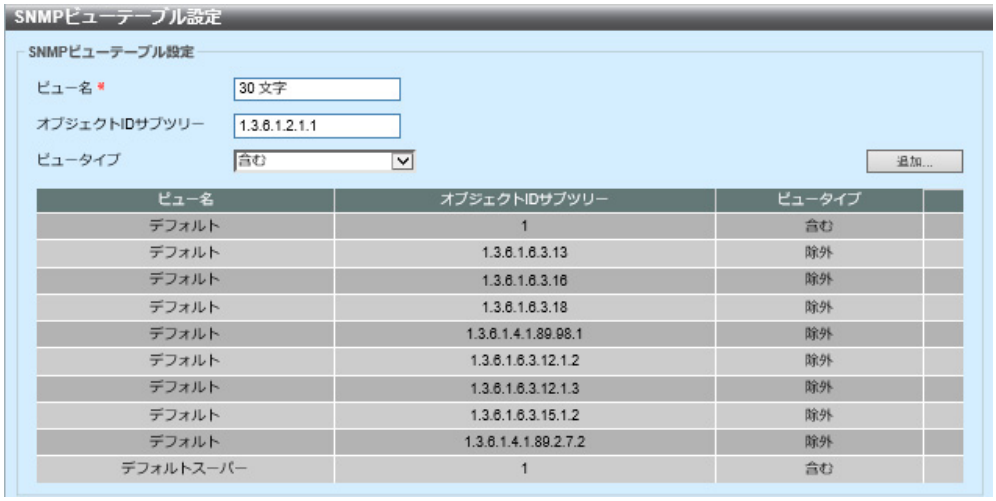
ビューは、MIB サブツリーのリスト用のユーザ定義によるラベルです。各サブツリー ID は、関係するサブツリーのルートの*オブジェクト識別子*（OID）によって定義されます。わかりやすい名前を使用して目的のサブツリーのルートを指定するか、または OID を入力できます。

各サブツリーは、定義されるビューに含まれるかまたは除外されます。

このページでは SNMP ビューを作成、削除できます。デフォルトのビュー（Default または DefaultSuper）は削除できません。

SNMP を設定するには：

[管理] > [SNMP] > [SNMP ビューテーブル設定] に進みます。



パラメータ	概要
ビュー名	ビュー名を入力します（0 ～ 30 文字）。
オブジェクト ID サブツリー	ビューに含まれるか排除される MIB ツリーのノードを設定します。
ビュータイプ	ノードが [含む] かまたは [除外] かを選択します。

[追加] を押してランニングコンフィグレーションファイルを追加、更新します。

3.8 グループ

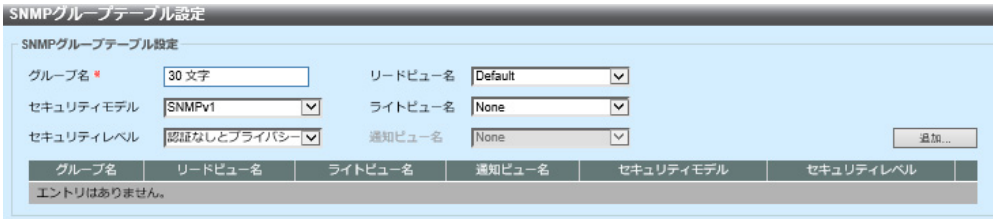
SNMPv1 と SNMPv2 はセキュアではありません。コミュニティ文字列は SNMP フレームを含めて送信します。コミュニティ文字列はパスワードのように機能して、SNMP エージェントへのアクセスを取得します。ただし、フレームとコミュニティ文字列はいずれも暗号化されます。

SNMPv3 は、受信した通知を各ユーザが読み書きできるコンテンツを提供、管理します。リード / ライト特権とセキュリティレベルは、グループで定義する必要があります。SNMP ユーザまたはコミュニティと関連付けられる場合に使用可能になります。

NOTE 非デフォルトのビューをグループと関連付けるには、最初に [ビュー] ページでビューを作成します。

SNMP グループを作成するには：

[管理] > [SNMP] > [SNMP グループテーブル設定] に進みます。



パラメータ	概要
グループ名	新しいグループ名を入力します。
セキュリティモデル	グループに加えられる SNMP バージョン、SNMPv1、v2 または v3 を設定します。
セキュリティレベル	グループに加えられるセキュリティレベルを選択します。SNMPv1 と SNMPv2 は認証または暗号化のいずれもサポートしません。SNMPv3 を選択する場合は、以下のいずれかを選択します。 • *認証なしとプライバシーなし（認証と暗号化のいずれもなし）* — 認証または暗号化のいずれのセキュリティレベルもグループに割り当てられません。 • *認証とプライバシーなし（認証あり、暗号化なし）* — SNMP メッセージを認証し、SNMP メッセージのオリジンを確実に認証済みにします。ただし暗号化は行われません。 • *認証とプライバシー（認証と暗号化）* — SNMP メッセージを認証し暗号化します。

パラメータ	概要
ビュー	ビューをグループの読み取り、書き込み、通知アクセス特権のいずれかに関連付けるように設定し、グループによる読み取り、書き込み、通知アクセス先の MIB ツリーのスコープを制限します。 • *読み取り* — 管理アクセスは読み取り専用です。それ以外の場合、このグループに関連付けられるユーザまたはコミュニティは、SNMP 自体を制御するもの以外のすべての MIB を読み取ることができます。 • *書き込み* — 管理アクセスは書き込みです。それ以外の場合、このグループに関連付けられるユーザまたはコミュニティは、SNMP を制御するもの以外のすべての MIB に書き込むことができます。 • *通知* — 利用可能なトラップコンテンツを、選択されたビューに含まれるものに制限します。それ以外の場合、トラップのコンテンツに制限はありません。これは SNMPv3 のみで選択できます。

[追加] を押してランニングコンフィグレーションファイルを更新します。

3.9 ユーザ

SNMP ユーザは、ログイン資格情報（ユーザ名、パスワード、認証方法）と、グループとエンジン ID との関係でユーザが実行するコンテキストとスコープによって設定されます。

設定済みユーザにはグループの属性があり、関連するビューで設定されたアクセス特権がともないます。

グループはネットワークを管理して、アクセス権を単一ユーザでなくユーザグループに割り当てます。

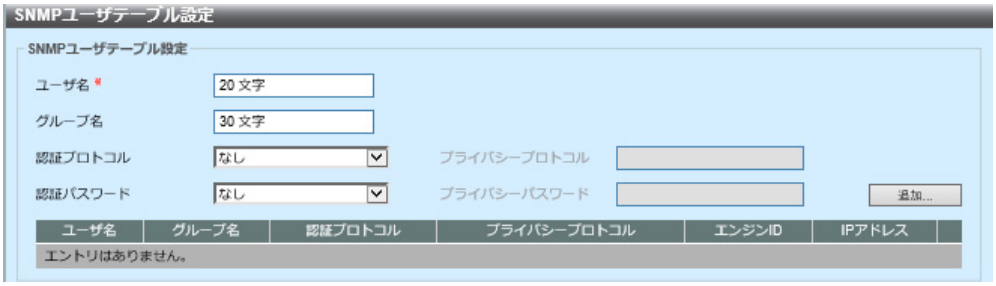
単一ユーザを 1 つのグループとすることもできます。

SNMPv3 ユーザを設定するには、最初に以下が必要です。

- 最初に [エンジン ID] ページでエンジン ID を設定する必要があります。
- [グループ] ページに SNMPv3 グループが必要です。

SNMP ユーザを表示して新規ユーザを定義するには：

[管理] > [SNMP] > [SNMP ユーザテーブル設定] に進みます。



このページには既存のユーザが表示されます。

パラメータ	概要
ユーザ名	ユーザの名前を設定します。
グループ名	SNMP ユーザが属する SNMP グループを設定します。 SNMP グループは [グループ] ページで定義されます。 注：削除されたグループのユーザは残りますが、非アクティブになります。
認証プロトコル	認証プロトコルを以下のように設定します。グループに認証が必要ない場合は、ユーザは認証を設定できません。 • *なし* — ユーザ認証は不要です。 • *MD5 パスワード* — MD5 認証方法によるキー生成のためのパスワード。 • *SHA* パスワード — SHA（Secure Hash Algorithm）認証方法によるキー生成のためのパスワード。
認証パスワード	MD5 または SHA パスワードのいずれにもよらずに認証を行う場合、ローカルユーザパスワードを**プレーンテキスト**で入力します（ASCII 文字 32 文字まで）。
プライバシープロトコル	[なし] または [DES]（データ暗号化標準規格）を設定します。 • *なし* — パスワードは暗号化されません。 • *DES* — パスワードは DES により暗号化されます。
プライバシーパスワード	DES 暗号化キーの 16 バイト（厳密に 16 進数文字 32 文字であること）を入力します（DES 暗号化方法を選択した場合のみ必要です）。

[追加 ...] を押して保存し、ランニングコンフィグレーションファイルを更新します。

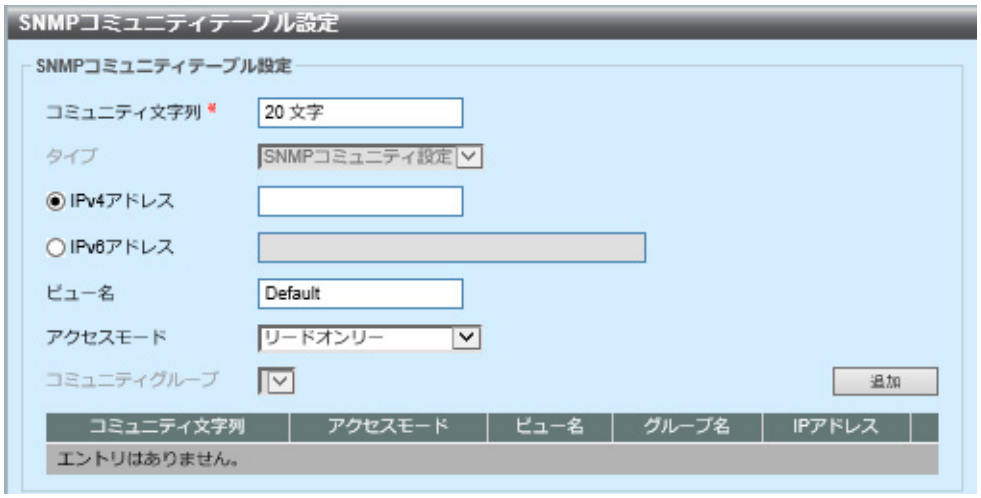
3.10 コミュニティ

SNMPv1 と SNMPv2 のアクセス権は、[コミュニティ] ページでコミュニティを定義して管理します。コミュニティ名は、SNMP 管理ステーションとデバイス間の共有パスワードの一種です。SNMP 管理ステーションの認証に使用します。

コミュニティは SNMPv1 と v2 のみで定義されます。これは SNMPv3 がコミュニティでなくユーザとの間で機能するからです。ユーザは、割り当てられたアクセス権を持つグループに属します。

SNMP コミュニティを設定するには：

[管理] > [SNMP] > [SNMP コミュニティテーブル設定] に進みます。



このページには、設定された SNMP コミュニティとそのプロパティも表示されます。

パラメータ	概要
コミュニティ文字列	デバイスへの管理ステーションの認証に使用されるコミュニティ名を入力します。
タイプ	コミュニティまたはコミュニティグループを設定します。
IPv4 アドレス	SNMP 管理ステーションの IPv4 アドレスを設定します。
IPv6 アドレス	SNMP 管理ステーションの IPv6 アドレスを設定します。
ビュー名	SNMP ビュー名を設定します。

パラメータ	概要
アクセスモード	このコミュニティタイプでは、どのグループへの接続もありません。コミュニティアクセスレベル（読み取り専用、読み書き、または SNMP 管理）の選択のみが可能です。オプションでそれを特定のビューに関連付けることができます。デフォルトでこの設定が MIB 全体に適用されます。これを選択する場合は、以下のフィールドを入力します。 • リードオンリー — 管理アクセスが読み取り専用に制限されます。コミュニティに変更を加えることはできません。 • リード ライト — 管理アクセスは読み取り / 書き込みです。デバイス設定に変更を加えることができますが、コミュニティにはできません。 • SNMP アドミン — ユーザには、すべてのデバイス設定オプションへのアクセス権とコミュニティを編集する権限もあります。SNMP 管理は、SNMP MIB を除くすべての MIB のリードライトと同等です。SNMP 管理は SNMP MIB へのアクセスに必要になります。
コミュニティグループ	[タイプ] を [グループタイプ] に設定する場合にグループを設定します。

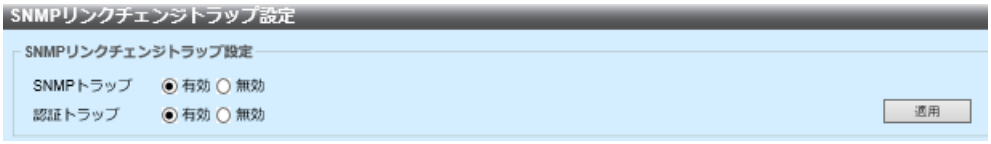
[追加] を押して SNMP コミュニティを定義しランニングコンフィグレーションファイルを更新します。

3.11 リンクチェンジトラップ

[Trap Configuration] ページでは、デバイスからの SNMP 通知の送信を設定できます。SNMP 通知の受信者は、[ホスト] ページで設定できます。

トラップを設定するには：

[管理] > [SNMP] > [SNMP リンクチェンジトラップ設定] に進みます。



[SNMP トラップ] フィールドで **[有効]** または **[無効]** を設定し、デバイスが SNMP 通知を送信できるように指定します。

[認証トラップ] フィールドで **[有効]** または **[無効]** を設定し、SNMP 認証失敗の通知を有効にします。

[適用] を押して SNMP トラップ設定を保存し、ランニングコンフィグレーションファイルを更新します。

3.12 ホスト

トラップメッセージが生成され、RFC 1215 の定義に従いシステムイベントをレポートします。システムは、サポート対象の MIB で定義されたトラップを生成できます。

トラップレシーバ（通知受信者）は、デバイスによってトラップメッセージが送信されるネットワークノードです。通知受信者のリストは、トラップメッセージのターゲットとして定義されます。

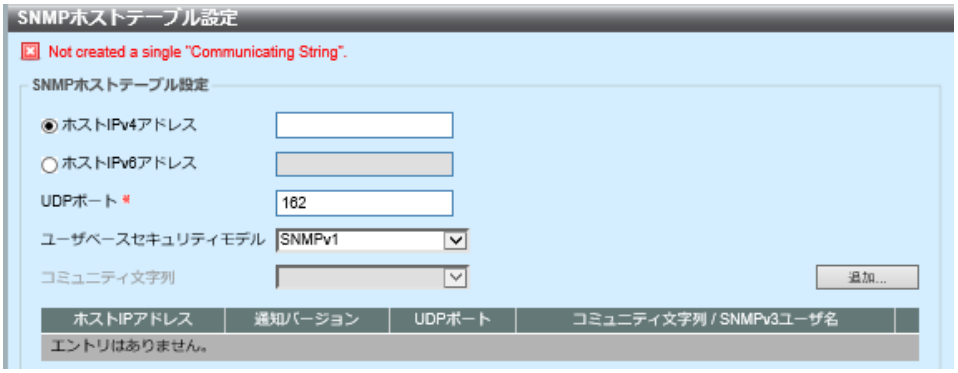
トラップレシーバのエントリには、ノードの IP アドレスと、トラップメッセージに含まれるバージョンに対応する SNMP 資格情報が含まれています。トラップメッセージ送信を必要とするイベントが発生すると、そのメッセージが通知受信者テーブルに含まれているすべてのノードに送信されます。

[ホスト] ページでは、SNMP 通知の送信先と各送信先に送付される SNMP 通知のタイプを設定し（トラップまたは情報）、通知の属性を設定できます。

SNMP 通知は、デバイスから SNMP 管理ステーションに送信されるメッセージで、リンクアップ / リンクダウンなど特定のイベントが発生したことを示します。

SNMPv1、2、3 で受信者を設定するには：

[管理] > [SNMP] > [SNMP ホストテーブル設定] に進みます。



パラメータ	概要
ホスト **IPv4** アドレス	IPv4SNMP サーバとの通信の情報メッセージでソース IPv4 アドレスとして使われる IPv4 アドレスを持つソースインタフェースを入力します。
ホスト **IPv6** アドレス	IPv6SNMP サーバとの通信のトラップメッセージでソース IPv6 アドレスとして使われる IPv6 アドレスを持つソースインタフェースを入力します。

パラメータ	概要
UDP ポート	通知に使われる UDP ポートを入力します（デフォルトは 162）。
ユーザベースセキュリティモデル	トラップ SNMP バージョン v1/v2/v3 を選択します。
コミュニティ文字列	プルダウンからトラップ管理のコミュニティ文字列を設定します。

[適用] を押して SNMP ホスト設定を保存し、ランニングコンフィグレーションファイルを更新します。

3.13 RMON

RMON（リモートネットワークモニタリング）では、SNMP エージェントがトラフィック統計情報を所定の期間にわたり予防的にモニタリングし、SNMP マネージャにトラップを送信できます。ローカルの SNMP エージェントは、事前に定義された閾値と実際のリアルタイムのカウンタを比較し、アラームを生成します。このとき、セントラル SNMP 管理プラットフォームによるポーリングの必要はありません。ネットワークのベースラインに対して正しい閾値を設定している限り、これは予防的管理に効果的なメカニズムです。

RMON では、SNMP マネージャがデバイスに頻繁にポーリングして情報を得る必要がないのでデバイスとマネージャ間のトラフィックを減らすことができ、またデバイスはイベントが発生した時点でそれをレポートするのでマネージャは状態レポートを適時に取得できます。

このような機能により、以下のアクションを実行できます。

- 現在の統計情報の表示（カウンタ値がクリアされた時刻から）。また所定の期間でこれらのカウンタの値を収集し、収集したデータのテーブルを表示できます。そこでは収集した各セットが [*ヒストリ*] ページでの 1 行になります。

- カウンタ値で関心のある変更、例えば「所定数の遅延コリジョンに到達」（[アラーム] ページで指定）を定義し、このイベントが発生したとき何のアクションを実行するかを指定します（ログ、トラップ、またはログとトラップ）

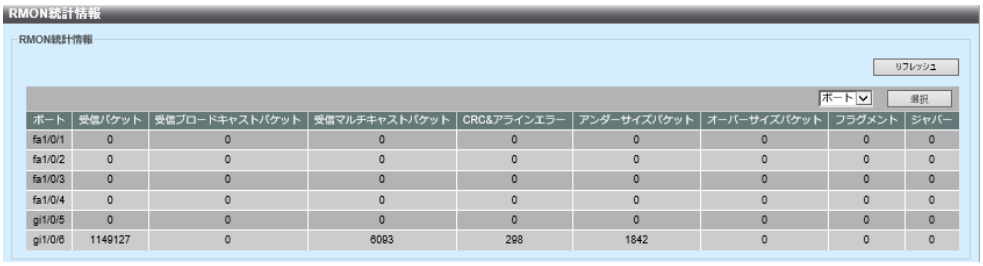
3.13.1 統計

このページにはパケットサイズについての詳細情報、物理レイヤのエラーについてや RMON 標準に準じた情報が表示されます。大きすぎるパケットは以下の基準で Ethernet フレームとして定義されます。

- パケット長が MRU バイトサイズより大きい。
- コリジョンイベントが検出されていない。
- 遅延コリジョンイベントが検出されていない。
- 受信（Rx）エラーイベントが検出されていない。
- パケットに有効な CRC がある。

RMON 統計情報を表示、および / またはリフレッシュレートを設定するには：

[管理] > [RMON] > [統計] に進みます。



すべての Ethernet 統計情報が表示されます。**[選択]** を押して [ポート]/[LAG] を選択することもできます。

[リフレッシュ] を押してすべてのインタフェース統計情報をリフレッシュします。

NOTE 以下のフィールドのいずれかにエラー数（0 以外）が表示される場合は、[**最終アップデート**] 時間が表示されます。

パラメータ	概要
受信パケット	受信した優良パケット数。マルチキャストパケットとブロードキャストパケットを含みます。
受信ブロードキャストパケット	受信した優良ブロードキャストパケット数。この数にマルチキャストパケット数は含まれません。
受信マルチキャストパケット	受信した優良マルチキャストパケット数。
CRC& アラインエラー	発生した CRC エラーとアラインメントエラー数。
アンダーサイズパケット	受信した小さすぎるパケット数（64 オクテット未満）。

パラメータ	概要
オーバーサイズパケット	受信した大きすぎるパケット数（1518 オクテット超）。
フラグメント	64 オクテット未満の長さ（フレーミングビットは除外し、FCS オクテットは含める）で受信し、整数のオクテットを持つ無効な FCS（フレーム検査シーケンス）（FCS Error）または非整数のオクテットを持つ無効な FCS（Alignment Error）のいずれかであるパケットの総数。
ジャバー	1518 オクテットを超える長さ（フレーミングビットは除外し、FCS オクテットは含める）で受信し、整数のオクテットを持つ無効な FCS（フレーム検査シーケンス）（FCS Error）または非整数のオクテットを持つ無効な FCS（Alignment Error）のいずれかであるパケットの総数。

3.13.2 ヒストリ

RMON 機能は、インタフェースごとに統計情報をモニタリングできます。

[ヒストリ] ページでは、サンプリング頻度、保存するサンプルの量、データ収集元のポートを定義します。

データをサンプリング、保存するとそれが [ヒストリ] ページに表示されます。参照するには **[ヒストリ]** ページをクリックします。

RMON のコントロール情報を設定するには：

[**管理**] > [**RMON**] > [**ヒストリ**] に進みます。

パラメータ	概要
ポート	ヒストリサンプルの取得元になるインタフェースを設定します。
保存するサンプルの最大数	保存するサンプルの数を入力します。デフォルトは 50 です。
ポーリング間隔	ポートからサンプルを収集する時間を秒で入力します。 フィールド範囲は 1 ～ 3600 です。デフォルトは 1800 です。
オーナー	RMON 情報を要求した RMON ステーションまたはユーザを入力します（160 文字未満）。

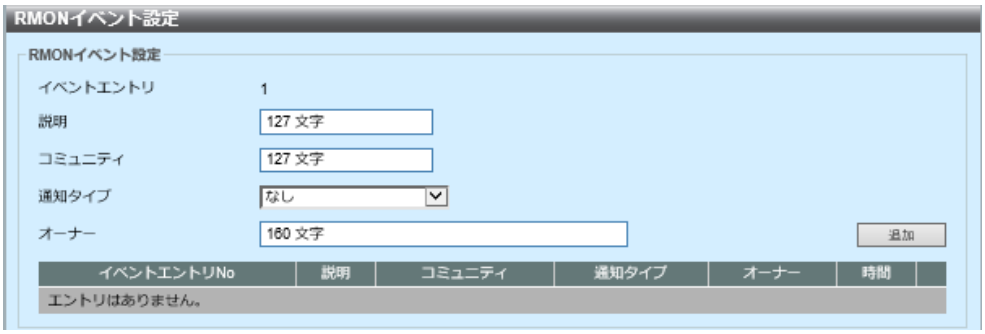
[追加] を押して、[ヒストリ] ページにエントリを追加し、ランニングコンフィグレーションファイルを更新します。

3.13.3 イベント

アラームがトリガされたとき何が発生するかを設定します。ログとトラップのあらゆる組み合わせが可能です。

RMON イベントを設定するには：

[管理] > [RMON] > [イベント] に進みます。



パラメータ	概要
イベントエントリ	イベントエントリの数値が表示されます。
説明	イベントの名前を入力します。
コミュニティ	含める SNMP コミュニティの文字列を入力します。
通知タイプ	このイベントのアクションタイプを以下の値で設定します。 • *なし* — アラームが作動したときアクションは起こりません。 • *ログ（イベントログテーブル）* — アラームがトリガされたとき、イベントログテーブルにログエントリを追加します。 • *トラップ（SNMP マネージャと Syslog サーバ）* — アラームが作動したとき、リモートログサーバにトラップを送信します。 • *ログとトラップ* — アラームが作動したとき、イベントログテーブルにログエントリを追加し、リモートログサーバにトラップを送信します。
オーナー	デバイスを入力するか、イベントを定義したユーザを入力します。

[追加] を押して RMON イベントを保存し、ランニングコンフィグレーションファイルを更新します。

3.13.4 アラーム

このページでは、サンプリング間隔と、各種カウンタまたはエージェントが維持する他の SNMP オブジェクトカウンタにより生成される例外イベントの閾値を設定できます。上昇閾値 / 下降閾値の両方をアラームで設定する必要があります。

- 上昇閾値：この閾値を超えると、対の下降閾値を超えるまで上昇イベントは生成されません。
- 下降アラーム：このアラームが発生すると、上昇閾値を超えたとき次のアラームが発生します。

1 つまたは複数のアラームは 1 つのイベントにバインドされ、アラーム発生時に実行されるアクションを示します。

アラームカウンタは、絶対値によりモニタリングするかまたはカウンタ値の変化（差分）によってモニタリングできます。

RMON アラームを設定するには：

[管理] > [RMON] > [アラーム] に進みます。

パラメータ	概要
ポート	RMON 統計情報が表示されるインタフェースのタイプを設定します。
間隔	アラーム間隔時間を秒で入力します。
カウンタ名	測定する発生タイプを示す MIB 変数を設定します。
サンプルタイプ	アラームを生成するサンプリング方法を設定します。 • *アブソリュート* — 閾値を超えるとアラームが生成されます。 • *差分* — 前回サンプリングした値を現在の値から差し引きます。値の差を閾値と比較します。閾値を超えた場合にアラームが生成されます。
上限閾値	上昇閾値アラームのトリガ値を入力します。
下降閾値	下降閾値アラームをトリガする値を入力します（デフォルトは 100）。

パラメータ	概要
上限超過時イベント	上限超過時イベントがトリガされたとき実行されるイベントを設定します（値は 1 ～ 65535）。
下限超過時イベント	下限超過時イベントがトリガされたとき実行されるイベントを設定します（値は 1 ～ 65535）。
オーナー	アラームを受信するユーザまたはネットワーク管理システムの名前を入力します（最大 160 文字）。

[適用] を押して RMON アラームを保存し、ランニングコンフィグレーションファイルを更新します。

3.14 Telnet/Web

このページではデバイスで Telnet または Web を有効にできます。
Telnet と Web の初期設定は無効です。

Telnet/Web サービスを設定するには：

[管理] > [Telnet/Web] に進みます。

[HTTP サービス] または [Telnet サービス] フィールドで **[Web]** または **[Telnet]** を、ポート番号を指定して有効にするかまたは無効にします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

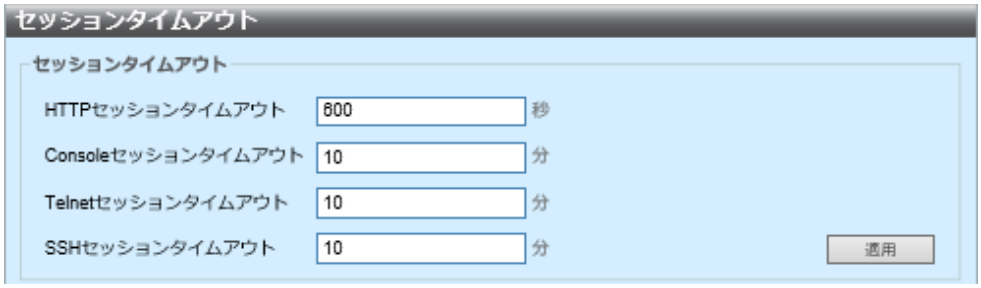
3.15 セッションタイムアウト

セッションタイムアウトでは、管理セッションがタイムアウトするまでアイドルを継続できる時間間隔を設定します。以下のセッションのいずれかをもう一度確立するには再度ログインする必要があります。

- HTTP セッションタイムアウト
- Console セッションタイムアウト
- Telnet セッションタイムアウト
- SSH セッションタイムアウト

各種セッションのセッションタイムアウトを設定するには：

[管理] > [セッションタイムアウト] に進みます。



セッションのタイプごとにタイムアウトを対応するリストから入力します。HTTP セッションタイムアウトのデフォルトのタイムアウト値は 600 秒、その他は 10 分です。

[適用] を押してランニングコンフィグレーションファイルを更新します。

3.16 DNS

DNS（Domain Name System）はドメイン名を IP アドレスに変換しホストの場所とアドレス情報を特定するために使用します。

DNS クライアントとしてのデバイスは、1 台または複数の設定済み DNS サーバを介してドメイン名を IP アドレスに解決します。

3.16.1 DNS 設定

[DNS 設定] ページを使用して、DNS サーバを設定しデバイスのデフォルトのドメインを設定できます。

[管理] > [DNS] > [DNS 設定] に進みます。

以下のパラメータを設定します。

パラメータ	概要
IP ドメイン検索	DNS クライアントとしてデバイスを有効にするように設定します。DNS クライアントは 1 台または複数の設定済み DNS サーバを介して、DNS 名を IP アドレスに解決できます
ポーリング間隔	デバイスが DNS クエリの応答を待つ時間を秒で入力します (デフォルトは 2 秒)。

[適用] を押してランニングコンフィグレーションファイルを更新します。

以下のパラメータのいずれかを入力します。

パラメータ	概要
ネームサーバ IPv4	DNS サーバの IPv4 アドレスを入力します。
ネームサーバ IPv6	DNS サーバの IPv6 アドレスを入力します。

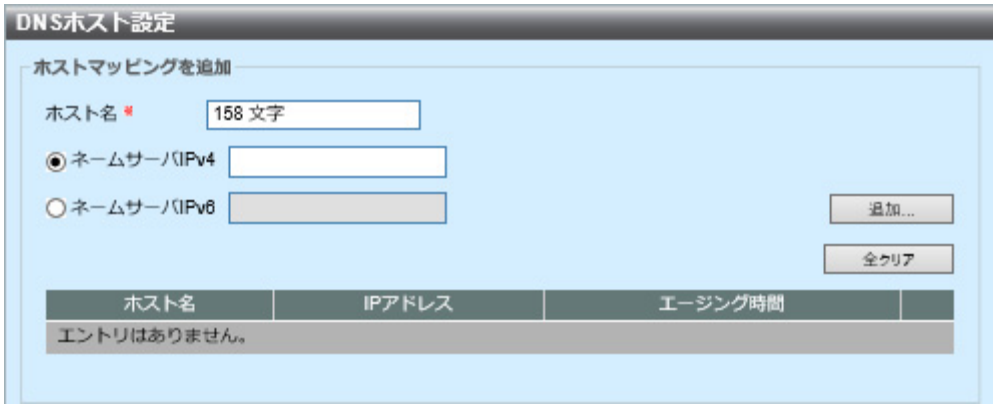
[追加 ...] を押してランニングコンフィグレーションファイルを更新します。

3.16.2 ホストマッピング

ホストの名前 /IP アドレスのマッピングは、ホストマッピングテーブルに保存されます。
名前解決は、常にスタティックエントリのチェックによって始まり、外部 DNS サーバへのリクエスト送信によって終わります。
ホスト名ごとに DNS サーバあたり 8 つの IP アドレスがサポートされます。

ホスト名とその IP アドレスを追加するには：

[管理] > [DNS] > [ホストマッピング] に進みます。



必要に応じて、**[全クリア]** を押しテーブル内の全エントリをクリアします。

パラメータ	概要
ホスト名	ユーザ定義のホスト名または完全修飾名を入力します。ホスト名は、ASCII 文字 A ～ Z（大文字小文字の区別なし）、数字の 0 ～ 9、下線、ハイフンに制限されます。ピリオド（.）はラベルの区切りに使用します。
ネームサーバ IPv4	1 つのアドレスまたは 8 つまでの関連する IP アドレスを入力します。
ネームサーバ IPv6	1 つのアドレスまたは 8 つまでの関連する IPv6 アドレスを入力します。

[追加 ...] を押してランニングコンフィグレーションファイルを更新します。

3.17 ファイルシステム

3.17.1 ファイルディレクトリ

[ファイルディレクトリ] ページには、システムにあるシステムファイルが表示されます。

NOTE 表示されるファイルは、スタックにユニット 2 台がある場合はマスターユニットから読み込まれたものです。

[管理] > [ファイルシステム] > [ファイルディレクトリ] に進みます。

3.17.2 ファームウェアの操作

[ファームウェア操作] ページを使用して以下を実行できます。

- ファームウェアイメージの更新
- バックアップファームウェアイメージの更新
- アクティブイメージとバックアップイメージのスワップ

ファイル転送では以下の方法がサポートされます。

- ブラウザが備える機能を使用する HTTP/HTTPS
- TFTP。TFTP サーバが必要

スタック内の各ユニットのソフトウェアイメージは、スタックが正しく機能するように同一でなければなりません。スタック内の各ユニットは以下のいずれかの方法でアップグレードできます。

- デバイスをスタックに加える前にデバイスのファームウェアを手動でアップグレードできます（推奨）。
- 新たに追加したユニットにマスターと同じファームウェアがなければ、スタックマスターはそのユニットのファームウェアを自動でアップグレードします。

デバイスには 2 つのファームウェアイメージが保存されています。イメージの 1 つは*アクティブイメージ*、もう 1 つのイメージは*非アクティブイメージ*として識別されます。

デバイスのファームウェアを更新するとき、新しいファームウェアは常に非アクティブイメージを上書きします。新しいファームウェアをデバイスにアップロードすると、次回の起動時に新規バージョンが使用されます。再起動後は、旧バージョンが非アクティブバージョンになります。

HTTP/HTTPS または TFTP を使用してファームウェアを更新またはバックアップするには：

[管理] > [ファイルシステム] > [ファームウェア操作] に進みます。

以下の情報を表示します。

パラメータ	概要
アクティブなファームウェアファイル名	現在のアクティブなファームウェアファイルを表示します。
アクティブなファームウェアバージョン	アクティブなファームウェアファイルの現行バージョンを表示します。

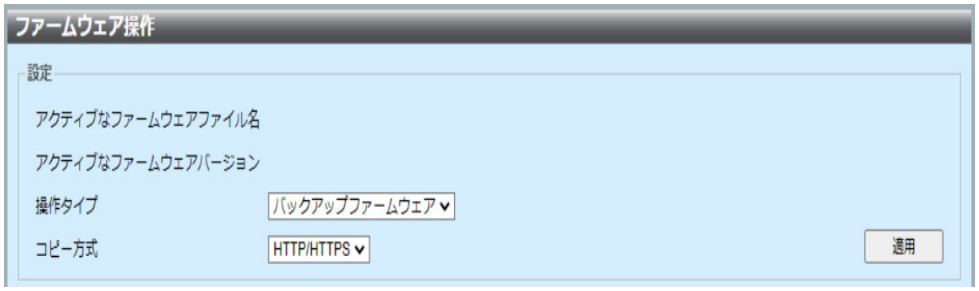
以下のパラメータを設定します。

パラメータ	概要
操作タイプ	[アップデートファームウェア]、[バックアップファームウェア]、または [スワップイメージ] を設定します。
コピー方式	**[HTTP/HTTPS]** または **[TFTP]** を選択します。
ファイル名	[参照] を押して、更新するファイルを選択します。

[適用] を押します。

3.17.2.1 TFTP を使用してファームウェアを更新またはバックアップするには :

[管理] > [ファイルシステム] > [ファームウェア操作] に進みます。



以下の情報を表示します。

パラメータ	概要
アクティブなファームウェアファイル名	現在のアクティブなファームウェアファイルを表示します。
アクティブなファームウェアバージョン	アクティブなファームウェアファイルの現行バージョンを表示します。

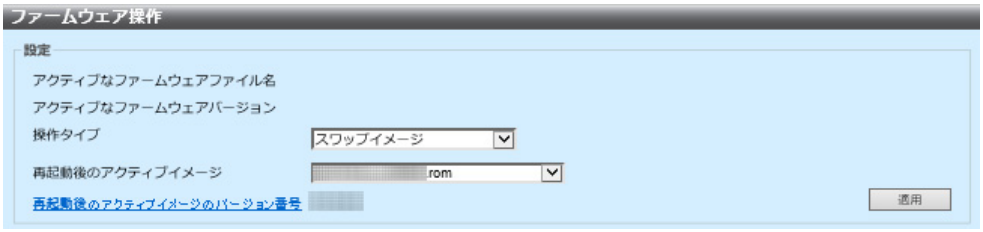
以下のパラメータを設定します。

パラメータ	概要
操作タイプ	[アップデートファームウェア] または [バックアップファームウェア] を設定します。
コピー方式	**TFTP** として設定します。
Server IP Address	TFTP サーバを **IP** アドレスで指定するかどうかを設定します。
ディスティネーション	名前を入力します。

[適用] を押して操作を開始します。

3.17.2.2 イメージファイルをスワップするには :

[管理] > [ファイルシステム] > [ファームウェア操作] に進みます。



以下の情報を表示します。

パラメータ	概要
アクティブなファームウェアファイル名	現在のアクティブなファームウェアファイルを表示します。
アクティブなファームウェアバージョン	アクティブなファームウェアファイルの現行バージョンを表示します。

以下のパラメータを設定します。

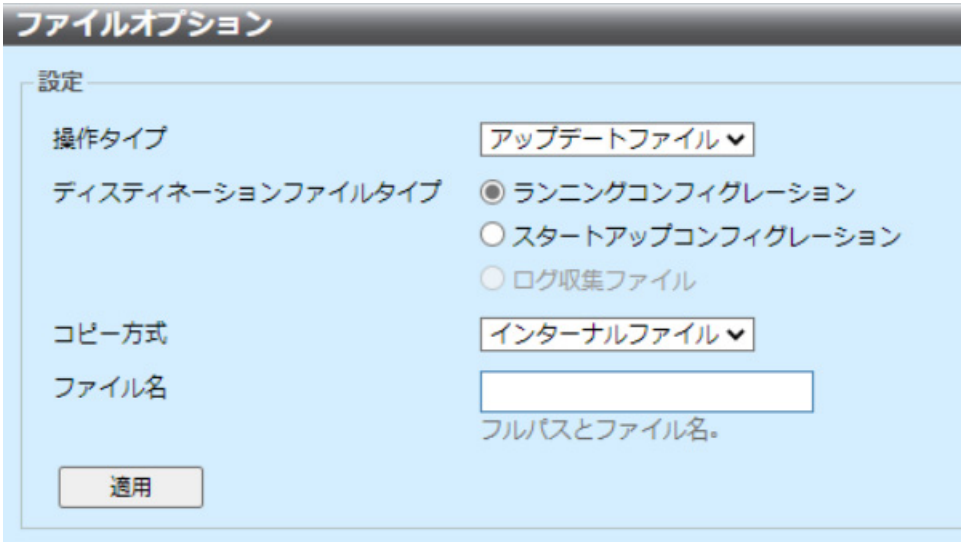
パラメータ	概要
操作タイプ	スワップイメージとして設定します。

[適用] を押し、成功メッセージが表示されたら、新しいファームウェアを直ちに再読み込みする場合は **[再起動]** を押します。

3.17.3 ファイルオプション

設定データの保存ができます。

[管理] > [ファイルシステム] > [ファイルオプション]



3.18 再起動

設定を変更すると（例：ジャンボフレームを有効にする）、システムを再起動しないとその変更が有効になりません。一方で、デバイスを再起動するとランニングコンフィグレーションファイルが削除されるので、デバイスを再起動する前にランニングコンフィグレーションファイルを起動コンフィグレーションファイルに保存することが重要です。

デバイスを再起動するには：

[管理] > [再起動] に進みます。

[工場出荷時のデフォルトに戻す][スタートアップコンフィグレーションファイルをクリア][再起動] フィールドのうち、一つを有効にし **[再起動]** ボタンを押すと、デバイスを再起動します。

パラメータ	概要
工場出荷時のデフォルトに戻す	設定を工場出荷時の状態にします。
スタートアップコンフィグレーションファイルをクリア	起動設定をクリアします。
再起動	デバイスを再起動します。起動コンフィグレーションファイルに未保存の情報は失われます。
再起動	デバイスを再起動します。このプロセスでは、アクティブイと非アクティブのイメージ、ミラーコンフィグレーションファイルとローカリゼーションファイルを除き、すべての情報が消去されます。 スタックユニット ID は自動に設定されます。

4 L2 機能

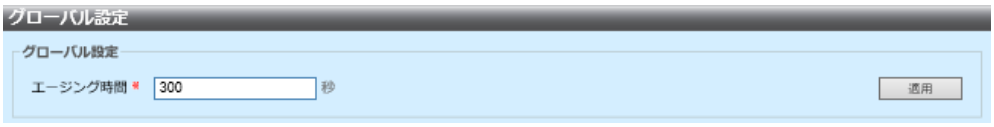
4.1 FDB

デバイスはスタティック / ダイナミック MAC アドレスで最大 16K をサポートします。

4.2 グローバル設定

グローバル設定を行うには：

[L2 機能] > [FDB] > [グローバル設定] に進みます。



パラメータ	概要
エージング時間	エージング時間（秒）を入力します。エージング時間はユーザ定義による値です（デフォルトは **300** 秒）。

[適用] を押してランニングコンフィグレーションファイルを更新します。

4.3 ユニキャストスタティック FDB

スタティック MAC アドレスがデバイスの特定の物理インタフェースと VLAN に割り当てられます。このアドレスが別のインタフェースで検出されると、それは無視され、アドレステーブルに記述されません。

[L2 機能] > [FDB] >[ユニキャストスタティック FDB] に進みます。

現在定義されているスタティックアドレスが表示されます。

パラメータ	概要
ポート /LAG	エントリのインタフェース（ポートまたは LAG）を設定します。
VID	ポートの VLAN ID を設定します。
MAC アドレス	インタフェースの MAC アドレスを入力します。

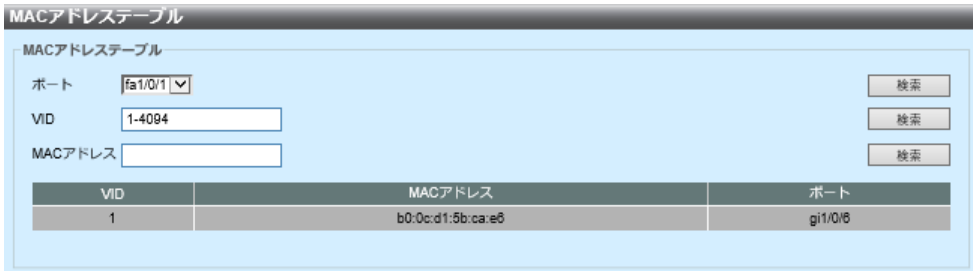
[適用] を押してエントリを追加しテーブルに表示します。

4.4 MAC アドレステーブル

予約された範囲（IEEE 標準に従う）に属する送信先 MAC アドレスを含むフレームがデバイスに届いたとき、そのフレームを破棄するかブリッジすることができます。

MAC アドレステーブルで 1 つまたはすべてのエントリを表示するには：

[L2 機能] > [FDB] >[MAC アドレステーブル] に進みます。



MAC アドレスが表示されます。

パラメータ	概要
ポート	テーブルのクエリを行うインタフェースを設定します。
VID	テーブルのクエリを行う VLAN ID を入力します（有効な値は 1 ～ 4094）。
MAC アドレス	予約する MAC アドレスを入力します。

4.5 VLAN

4.5.1 VLAN 設定

4.5.1.1 VLAN 設定ワークフロー

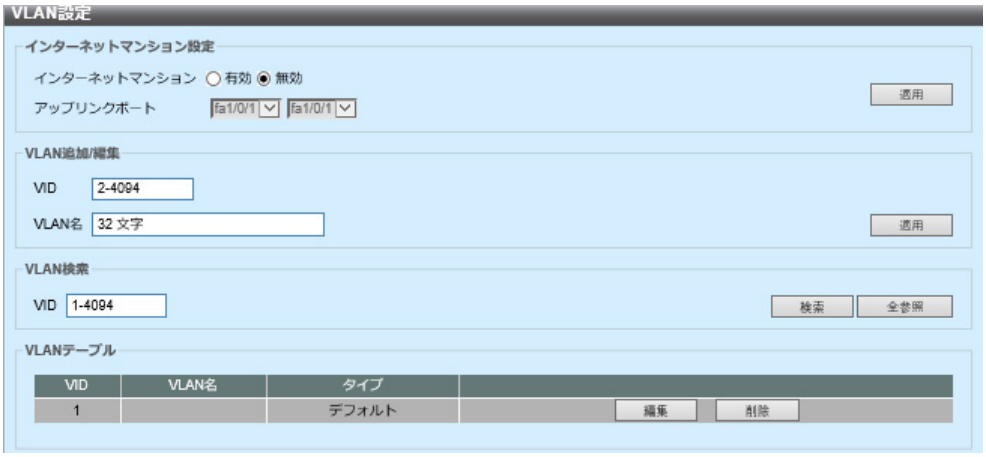
VLAN を設定するには：

2. 「VLAN 設定」セクションの説明に従い、必要な VLAN を作成 / 編集 / 検索します。
3. ポートに対して目的の VLAN 関連の設定を行い、「*インタフェース設定*」セクションの説明に従いインタフェースで QinQ を有効にします。
4. 「*インタフェース設定*」セクションの説明に従い、VLAN にインタフェースを割り当てます。
5. 「*インタフェース設定*」セクションの説明に従い、全インタフェースの現在の VLAN ポートメンバシップを表示します。
6. 必要に応じて、「VLAN バインディング」セクションの説明に従い、VLAN グループを設定します。

4.5.1.2 VLAN 設定

1 つまたは複数の VLAN を作成するには：

[L2 機能] > [VLAN] > [VLAN 設定] に進みます。



[VLAN 追加 / 編集] ブロックで 1 つまたは複数の VLAN を**追加 / 編集**します。

パラメータ	概要
インターネットマンション	インターネットマンションの有効、無効を設定します。（工場出荷設定：無効）
アップリンクポート	インターネットマンションの有効時、アップリンクポートを最大 2 ポートまで指定します。
VID	追加または編集する VLAN の値または値の範囲を入力します（2 ～ 4094）。
VLAN 名	表示する VLAN 名を入力します（1 ～ 32 文字）。

[適用] を押して VLAN を作成または編集します。

[VLAN 検索] ブロックで **[VID]** を入力し VLAN を検索します。

[VLAN 検索] ブロックで **[検索]** または **[全参照]** を押して VLAN を検索します。

VLAN テーブルの各行で **[編集]** または **[削除]** を押し、その VLAN を編集または削除します（VLAN 1 は編集のみ可能）。

4.5.1.3 インタフェース設定

このページでは、VLAN 関連情報の設定を表示して有効にします。

VLAN 設定を行うには：

[L2 機能] > [VLAN] > [インタフェース設定] に進みます。

テーブルの表示をポートまたは LAG に指定するには、[ポート] または [LAG] を設定し **[選択]** を押します。

パラメータ	概要
ポート	[ポート] または [LAG] を設定します。
VID モード	VLAN のインタフェースモードを設定します。以下のオプションがあります。 • *アクセス* — インタフェースは 1 つの VLAN のタグなしメンバです。このモードで設定されるポートはアクセスポートと呼ばれます。 • *トランク* — インタフェースは 1 つの VLAN のみのタグなしメンバであり、ゼロまたはそれ以上の VLAN のタグ付きメンバとなります。このモードで設定されるポートはトランクポートと呼ばれます。 • *ハイブリッド* — インタフェースは IEEE802.1q 規格に定義される全機能をサポートできます。インタフェースは 1 つまたは複数 VLAN のタグ付きまたはタグなしメンバになります。 • *プライベート VLAN - ホスト* — インタフェースを孤立またはコミュニティとして設定します。次に、[セカンダリ VLAN - ホスト] フィールドで孤立またはコミュニティ VLAN を選択します。

パラメータ	概要
VID モード	• *プライベート VLAN* - プロミスキャス — インタフェースをプロミスキャスとして設定します。 • *VLAN マッピング* - *トンネル* — トンネル VLAN マッピングを設定します。 • *VLAN マッピング* - *1 対 1* — 1 対 1 の VLAN マッピングを設定します。
フレームタイプ	インタフェースが受信できるフレームタイプを以下のいずれかに設定します。設定されたフレームタイプ以外のフレームは入口で破棄されます。それらのフレームタイプはジェネラルモードでのみ利用できます。 • *全受付* — インタフェースは、タグなしフレーム、タグ付きフレーム、優先度タグフレームの全フレームタイプを受け付けます。 • *タグのみ受付* — インタフェースはタグ付きフレームのみを受け付けます。 • *アンタグのみ受付* — インタフェースはタグなしフレームと優先度フレームのみを受け付けます。
受信フィルタリング	有効または無効に設定します。
ネイティブ VLAN ステータス	有効または無効に設定します。
ネイティブ VID	ネイティブ VLAN ID の値を入力します（1 ～ 4094）。
モード	2 つのモードを割り当てることができます。 • *アンタグ* — タグなしとして定義します。 • *タグ* — タグ付きとして定義します。
VID	VLAN ID を入力します（1 ～ 4094）。

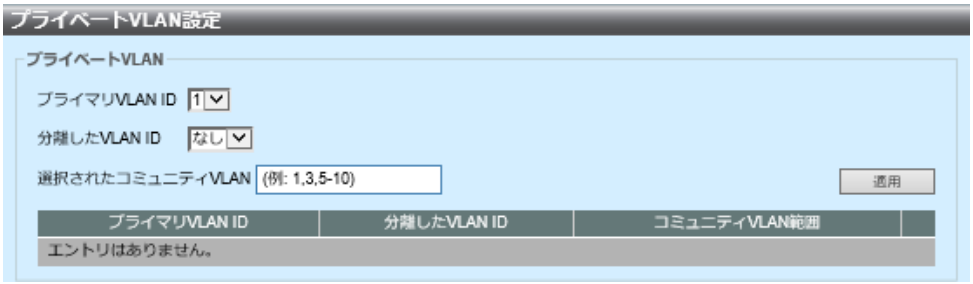
[適用] を押してランニングコンフィグレーションファイルを更新します。

4.6 プライベート VLAN 設定

[プライベート VLAN 設定] ページには、定義済みのプライベート VLAN が表示されます。

新しいプライベート VLAN を作成するには：

[L2 機能] > [VLAN] > [プライベート VLAN 設定] に進みます。



パラメータ	概要
プライマリ VLAN ID	[プライベート VLAN] で、プライマリ VLAN として定義する VLAN を設定します。プライマリ VLAN を使用して、プロミスキャスポートから孤立ポートとコミュニティポートへのレイヤ 2 接続を許可します。
分離した VLAN ID	孤立 VLAN を使用して、孤立ポートがプライマリ VLAN にトラフィックを送信できるようにします。
選択されたコミュニティ VLAN	コミュニティ VLAN にする VLAN を**選択されたコミュニティ VLAN** リストに移行します。コミュニティ VLAN を使用して、コミュニティポートからプロミスキャスポートおよび同じコミュニティのコミュニティポートへのレイヤ 2 接続を許可します。これは**コミュニティ VLAN 範囲**と呼ばれます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

4.7 GVRP 設定

VLAN を認識する隣接したデバイス間では、GVRP（Generic VLAN Registration Protocol）を使用して VLAN 情報を相互に交換できます。GVRP は GARP（Generic Attribute Registration Protocol ）に基づいており、VLAN 情報をブリッジネットワーク全体に伝搬します。

GVRP 機能を設定するには、GVRP ではタグ付けのサポートが必要なことから、ポートにジェネラルモードを割り当てる必要があります。

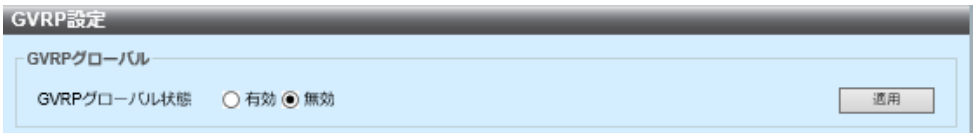
GVRP は、各ポートに加えてグローバルでも有効にする必要があります。有効にすると、GVRP は GPDU（GARP Packet Data Unit）を送受信します。定義済みの VLAN でもアクティブでない場合は伝搬されません。VLAN を伝搬するには、少なくとも 1 つのポートで VLAN が有効でなければなりません。

デフォルトで、GVRP はグローバルとポートの両方で無効です。

4.7.1 GVRP グローバル設定

GVRP グローバル設定を行うには：

[L2 機能] > [VLAN] > [GVRP 設定] に進みます。



[GVRP グローバル状態] で、GVRP をグローバルに有効にします。

[適用] を押してグローバル GVRP 状態を設定します。

4.7.2 GVRP ポート設定

インタフェースの GVRP を設定するには：

[L2 機能] > [VLAN] > [GVRP ポート設定] に進みます。

インタフェースまたはインタフェース範囲をインタフェースタイプ（ポートまたは LAG）とともに設定します。

[GVRP 状態] フィールドで有効または無効を設定します。

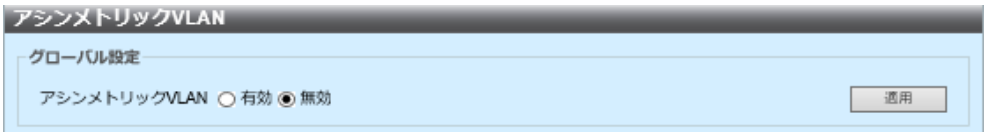
[適用] を押します。GVRP ポート設定が編集され、ランニングコンフィグレーションファイルに書き込まれます。

[選択] を押すと、ポートまたは LAG によってフィルタリングできます。

4.8 アシンメトリック VLAN

アシンメトリック VLAN 設定を行うには：

[L2 機能] > [VLAN] >[アシンメトリック VLAN] に進みます。



[アシンメトリック VLAN] でアシンメトリック VLAN を有効または無効に設定します。

[適用] を押して、アシンメトリック VLAN を有効または無効にします。

4.9 VLAN バインディング

VLAN グループは、レイヤ 2 ネットワーク上のトラフィックの負荷分散に使用します。

パケットはさまざまな分類に応じて VLAN に割り当てられます。

いくつかの分類スキームが定義されている場合、パケットは以下の順序で VLAN に割り当てられます。

パラメータ	概要
TAG	パケットがタグ付きの場合、VLAN はタグから取得されます。
MAC ベース VLAN	MAC ベース VLAN が定義されている場合、VLAN は入口インタフェースの送信元 MAC アドレスから VLAN へのマッピングから取得されます。
プロトコルベース VLAN	プロトコルベース VLAN が定義されている場合、VLAN は入口インタフェースの（Ethernet タイプの）プロトコルから VLAN へのマッピングから取得されます。
PVID	VLAN はポートのデフォルト VLAN ID から取得されます。

4.9.1 MAC VLAN プロファイル / バインディングについて

MAC ベース VLAN 分類により、パケットをその送信元 MAC アドレスに応じて分類できます。これにより、インタフェースごとに MAC アドレスから VLAN へのマッピングを定義できます。

いくつかの MAC ベース VLAN グループを定義できます。各グループには異なる MAC アドレスが含まれています。

これらの MAC ベースグループは特定のポート /LAG に割り当てることができます。MAC ベース VLAN グループは、同じポートで重複する MAC アドレス範囲を含むことはできません。

4.9.1.1 MAC ベース VLAN の設定方法

MAC ベース VLAN グループを定義するには：

1. MAC アドレスを VLAN グループ ID に割り当てます（[MAC VLAN プロファイル] ページを使用）。

2. 必要なインタフェースごとに以下を行います。
   a. VLAN グループを VLAN に割り当てます（[MAC VLAN バインディング] ページを使用）。インタフェースはジェネラルモードである必要があります。
   b. インタフェースが VLAN に属さない場合は、[インタフェース設定] ページでインタフェースを VLAN に手動で割り当てます。

4.9.1.2 MAC VLAN プロファイル

MAC アドレスを VLAN グループに設定するには：

[L2 機能] > [VLAN] > [VLAN グループ] > [MAC VLAN プロファイル] に進みます。

パラメータ	概要
MAC アドレス	VLAN グループに割り当てる MAC アドレスを入力します。 注： この値は他の VLAN グループに割り当てることはできません。
プレフィックスマスク	MAC アドレスのプレフィックスを入力します。
グループ **ID**	ユーザ作成による VLAN グループ ID 番号を入力します。

[適用] を押して、MAC アドレスを VLAN グループに割り当てます。

4.9.1.3 MAC VLAN バインディング

NOTE ポート /LAG はジェネラルモードである必要があります。

MAC ベース VLAN グループをインタフェース上の VLAN に設定するには：

[L2 機能] > [VLAN] > [VLAN グループ] > [MAC VLAN バインディング] に進みます。

パラメータ	概要
ポート	受信するトラフィックが経由する汎用インタフェース（ポート /LAG）を入力します。
グループ ID	VLAN グループを設定します。
VID	VLAN グループからのトラフィックの転送先となる VLAN を設定します。

[適用] を押して、VLAN への VLAN グループのマッピングを設定します。このマッピングはインタフェースを VLAN にダイナミックにバインドしません。インタフェースは VLAN に手動で追加する必要があります。

4.9.2 サブネット VLAN プロファイル / バインディングについて

サブネットベースのグループ VLAN 分類により、パケットをそのサブネットに応じて分類できます。これにより、インタフェースごとにサブネットから VLAN へのマッピングを定義できます。

複数のサブネットベース VLAN グループを定義できます。グループごとに異なるサブネットが含まれます。

これらのグループは特定のポート /LAG に割り当てることができます。サブネットベース VLAN グループは、同じポートで重複するサブネットの範囲を含むことはできません。

4.9.2.1 サブネットベース VLAN の設定方法

サブネットベース VLAN グループを設定するには：

1. サブネットベースのグループを設定します（[Subnet-based Groups] ページを使用）。
2. 必要なインタフェースごとに、サブネットベースのグループを VLAN に割り当てます（[サブネット VLAN プロファイル] ページを使用）。インタフェースには DVA（Dynamic VLAN）を割り当てられません。IS モードでは、デバイスがジェネラルモードでない場合でも設定を保存し、後から有効にできます。

> **NOTE** インタフェースが VLAN に属さない場合は、[インタフェース設定] ページでインタフェースを VLAN に手動で割り当てます。そうでないと、サブネットベースのグループから VLAN への設定は有効になりません。

4.9.2.2 サブネット VLAN プロファイル

サブネットベースのグループを追加するには：

[L2 機能] > [VLAN] > [VLAN グループ] > [サブネット VLAN プロファイル] に進みます。

パラメータ	概要
IP アドレス	サブグループのベースになる IP アドレスを入力します。
プレフィックスマスク	サブネットを定義するプレフィックスマスクを入力します。
グループ **ID**	グループ ID を入力します。

[適用] を押して、このグループを追加しランニングコンフィグレーションファイルを更新します。

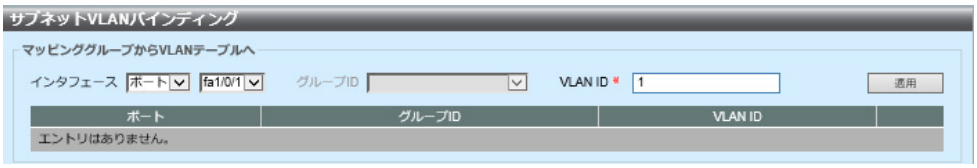
4.9.2.3 サブネット VLAN バインディング

各ポートがそれぞれの VLAN に関連付けられている状態で、いくつかのグループを 1 つのポートにバインドできます。

いくつかのグループを 1 つの VLAN にマッピングすることもできます。

サブネットグループを VLAN にマッピングするには：

[L2 機能] > [VLAN] > [VLAN グループ] > [サブネット VLAN バインディング] に進みます。



テーブルには現在定義されているマッピングが表示されます。

パラメータ	概要
ポート	プロトコルベースのグループに準じて、VLAN に割り当てるポートまたは LAG の番号を指定します。
グループ ID	プロトコルグループ ID。
VLAN ID	このインタフェースの指定されたグループが、ユーザ定義の VLAN ID に割り当てられます。

[適用] を押して、サブネットベースグループのポートを VLAN にマッピングし、ランニングコンフィグレーションファイルを更新します。

4.9.3 プロトコル VLAN バインディングについて

プロトコルのグループは、定義してからポートにバインドできます。ポートをプロトコルグループにバインドしたら、そのグループのプロトコルから生成されるすべてのパケットには、[Protocol-Based Groups] ページで設定される VLAN が割り当てられます。

4.9.3.1 プロトコルベース VLAN の設定方法

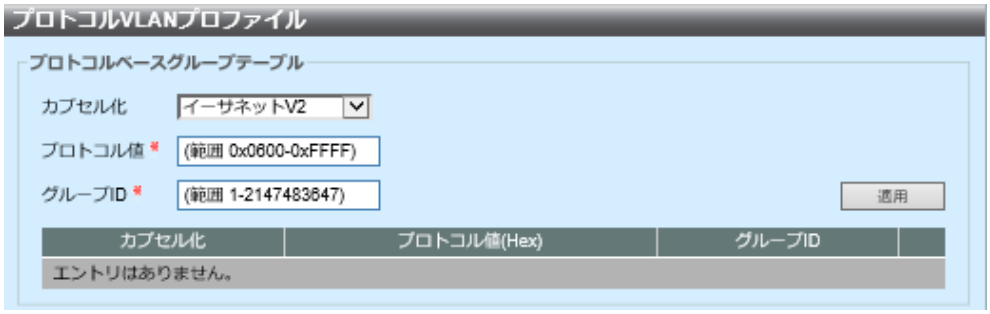
プロトコルベース VLAN グループを設定するには：

1. プロトコルグループを設定します（[プロトコル VLAN プロファイル] ページを使用）。
2. 必要なインタフェースごとに、プロトコルグループを VLAN に割り当てます（[インタフェース設定] ページを使用）。インタフェースはジェネラルモードである必要があります。またインタフェースには DVA（Dynamic VLAN）を割り当てられません。

4.9.3.2 プロトコル VLAN プロファイル

プロトコルセットを設定するには：

[L2 機能] > [VLAN] > [VLAN グループ] > [プロトコル VLAN プロファイル] に進みます。



このテーブルには以下の情報が表示されます。

パラメータ	概要
カプセル化	VLAN グループのベースとなるプロトコルを表示します。
プロトコル値	プロトコル値を 16 進数で表示します。
グループ ID	インタフェースが追加されるプロトコルグループ ID を表示します。

以下のパラメータを入力します。

パラメータ	概要
カプセル化	プロトコルパケットタイプ。以下のオプションがあります。 • *Ethernet V2* — これを選択する場合は、**[イーサネットタイプ]** を選択します。 • *LLC-SNAP (rfc1042)* — これを選択する場合は、**[プロトコル値]** を入力します。 • *LLC* — これを選択する場合は、**[DSAP-SSAP Values]** を選択します。
プロトコル値 (Hex)	LLC-SNAP（rfc 1042）カプセル化のプロトコルを入力します。
グループ ID	プロトコルグループ ID を入力します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

4.9.3.3 プロトコル VLAN バインディング

プロトコルグループをポートにマッピングするには、ポートがジェネラルモードで、ポートに DVA が設定されていないことが必要です（「インタフェース設定」を参照）。

各ポートがそれぞれの VLAN に関連付けられている状態で、いくつかのグループを 1 つのポートにバインドできます。

いくつかのグループを 1 つの VLAN にマッピングすることもできます。

プロトコルポートを VLAN にマッピングするには：

[L2 機能] > [VLAN] > [VLAN グループ] > [プロトコル VLAN バインディング] に進みます。

テーブルには、現在定義されているマッピング情報が表示されます。

パラメータ	概要
ポート	プロトコルベースのグループに準じて、VLAN に割り当てるポートまたは LAG の番号を指定します。
グループ ID	プロトコルグループ ID。
VID	インタフェースがユーザ定義の VLAN ID に割り当てられます。

[適用] を押して、プロトコルポートを VLAN にマッピングし、ランニングコンフィグレーションファイルを更新します。

4.10 音声 VLAN

LAN 上の IP フォンや VoIP エンドポイント、音声システムなどの音声デバイスは、同じ VLAN に配置されます。この VLAN は音声 VLAN と呼ばれます。音声デバイスが異なる音声 VLAN にある場合は、通信可能にするために IP（レイヤ 3）ルータが必要です。

デバイスは 1 つの音声 VLAN をサポートします。デフォルトでは、音声 VLAN は VLAN 1 です。音声 VLAN はデフォルトで VLAN 1 になります。異なる音声 VLAN は手動で設定できます。自動音声 VLAN が有効な場合は、ダイナミックに学習できます。

「Configuring VLAN Interface Setting」セクションに記述されている基本 VLAN 設定を使用するか、または音声関連の SmartPort マクロをポートに手動で適用することで、音声 VLAN にポートを手動で追加できます。または、デバイスが音声 VLAN OUI モードにあるかまたはデバイスで自動 SmartPort が有効であれば、ポートをダイナミックに追加することもできます。

4.10.1 ダイナミック音声 VLAN モード

デバイスは 2 つのダイナミック音声 VLAN モード、音声 VLAN OUI（Organization Unique Identifier）モードと自動音声 VLAN モードをサポートします。これら 2 つのモードは、音声 VLAN および / または音声 VLAN ポートメンバシップの設定方法に影響します。2 つのモードのどちらか 1 つのみを設定できます。

- **音声 VLAN OUI**
  音声 VLAN OUI モードでは、音声 VLAN は手動設定による VLAN でなければならず、デフォルトの VLAN は使用できません。

  デバイスが音声 VLAN OUI モードにあり、ポートが音声 VLAN に参加する候補として手動で設定されている場合、デバイスが設定済み音声 VLAN OUI のいずれかと一致する送信元 MAC アドレスを含むパケットを受信するのであれば、デバイスはポートを音声 VLAN にダイナミックに追加します。OUI は Ethernet MAC アドレスの最初の 3 バイトです。

OUI モードを使用する場合、デバイスは OUI に基づいて音声トラフィックのマッピングと注釈（CoS/802.1p）を追加で設定できます。

デフォルトで、すべてのインタフェースは CoS/802.1p で信頼されています。デバイスは、音声ストリームで検出される CoS/802.1p の値に基づいて QoS（quality of service）を適用します。自動音声 VLAN では、高度な QoS を使用して音声ストリームの値をオーバーライドできます。音声 VLAN OUI 音声ストリームでは QoS をオーバーライドできるのに加えて、音声 VLAN OUI で目的の CoS/802.1p の値を指定し注釈オプションを使用することにより、オプションで 802.1p の音声ストリームに注釈を付けることができます。

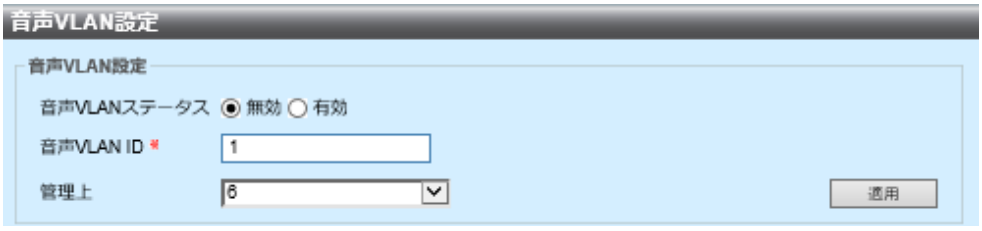
4.10.2 音声 VLAN の制約

以下の制約があります。

- 音声 VLAN は 1 つだけサポートされます。
- 音声 VLAN として定義される VLAN は削除できません。また音声 VLAN OUI には以下の制約が該当します。
- 音声 VLAN は DVA（Dynamic VLAN assignment）をサポートできません。
- 音声 VLAN モードが OUI の場合は、音声 VLAN はゲスト VLAN であってはなりません。音声 VLAN モードが自動の場合は、音声 VLAN はゲスト VLAN であってもかまいません。
- 音声 VLAN の QoS 意思決定は、ポリシー /ACL QoS の意思決定を除き、他の QoS 意思決定に優先します。
- 現在の音声 VLAN に候補ポートがない場合に限り、新しい VLAN ID を音声 VLAN に対して設定できます。
- 候補ポートのインタフェース VLAN はジェネラルモードまたはトランクモードになければなりません。
- 音声 VLAN の QoS は、音声 VLAN に参加している候補ポートと、スタティックポートに適用されます。
- FDB（Forwarding Database）による MAC アドレスの学習が可能な場合は、音声フローが受け入れられます（FDB に空きがなければアクションは何も起こりません）。

音声 VLAN グローバルを表示、設定するには：

[L2 機能] > [VLAN] > [音声 VLAN] > [音声 VLAN グローバル] に進みます。



パラメータ	概要
音声 VLAN ステータス	音声 VLAN を有効または無効にします。(デフォルトは無効)。

パラメータ	概要
音声 VLAN ID	音声 VLAN になる VLAN を入力します。 注： 音声 VLAN ID、CoS/802.1p、および / または DSCP に変更を加えると、デバイスが管理音声 VLAN をスタティック音声 VLAN としてアドバタイズする原因になります。外部音声 VLAN によってトリガされる *Auto* Voice VLAN Activation オプションを選択する場合は、デフォルト値を維持する必要があります（デフォルトは 1）。
管理上	LLDP-MED によって音声ネットワークポリシーとして使われる CoS 値を設定します（デフォルトは 6）。

[適用] を押して、VLAN グローバルをランニングコンフィグレーションファイルに更新します。

4.10.3 音声 VLAN OUI

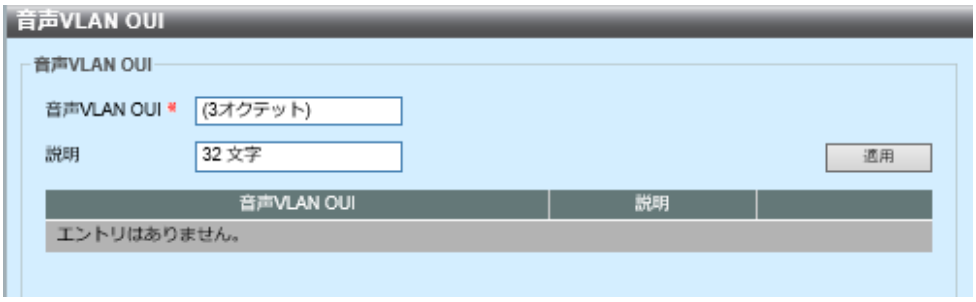
OUI は IEEE（Institute of Electrical and Electronics Engineers, Incorporated）RA（Registration Authority）によって割り当てられます。IP フォンのメーカー数は限られており著名でもあるので、既知の OUI 値によって、該当するフレームとそれらのフレームが検出されるポートが自動で音声 VLAN に割り当てられます。

OUI グローバルテーブルには最大 128 の OUI を保持できます。

[音声 VLAN OUI] ページを使用して、既存の OUI を表示し、新しい OUI を追加します。

音声 VLAN OUI を設定および / または新しい音声 VLAN OUI を追加するには：

[L2 機能] > [VLAN] > [音声 VLAN] > [音声 VLAN OUI] に進みます。



パラメータ	概要
音声 VLAN OUI	新しい OUI を入力します。
説明	OUI 名を入力します。

[適用] を押して、OUI を音声 VLAN OUI テーブルに追加します。

4.10.4 音声 VLAN ポート

インタフェースに音声 VLAN OUI を設定するには：

[L2 機能] > [VLAN] > [音声 VLAN] > [音声 VLAN ポート] に進みます。

パラメータ	概要
ポート / 開始インターフェース / 終了インターフェース	インタフェースまたはインタフェース範囲を選択します（ポートまたは LAG）。
ステータス	有効にする場合は、インタフェースは音声 VLAN OUI ベース音声 VLAN の候補ポートです。設定済み音声 VLAN OUI のいずれかと一致するパケットを受信するとき、ポートが音声 VLAN に追加されます。
モード	以下のオプションを設定します。 • *All* — 音声 VLAN に分類されるすべてのパケットに QoS 属性が適用されます。 • *MAC アドレス* — QoS 属性は IP フォンからのパケットのみに適用されます。

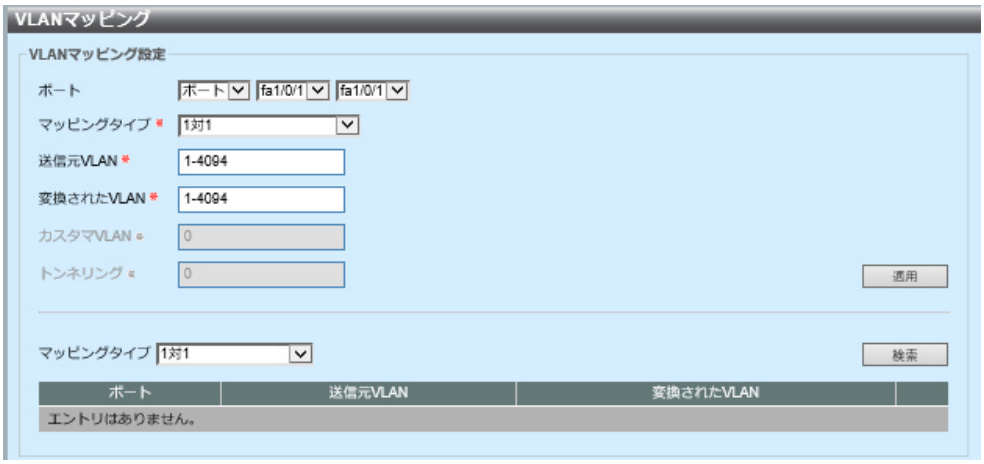
[適用] を押します。

4.11 VLAN トンネル

このセクションでは、VLAN トンネルの設定方法について説明します。

4.11.1 VLAN マッピング

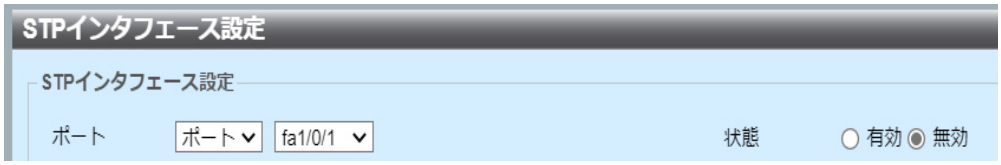
[L2 機能] > [VLAN トンネル] >[VLAN マッピング] に進みます。



パラメータ	概要
ポート	ポートまたは LAG により、インタフェースまたはインタフェース範囲を選択します。
マッピングタイプ	「1 対 1」またはトンネルマッピング」を選択します。
送信元 VLAN	元の VLAN ID を入力します（1 ～ 4094）。
変換された VLAN	変換された VLAN ID を入力します（1 ～ 4094）。

パラメータを入力後、**[適用]** を押します。

予め STP インターフェース設定画面で、ポートの状態を無効に設定しておく必要があります。



テーブルをフィルタリングするには、**[マッピングタイプ]** で「1 対 1」または「トンネルマッピング」を設定し、**[検索]** を押します。

4.12 STP

4.12.1 STP 状態 & グローバル設定

[STP 状態 & グローバル設定] ページには、STP、RSTP、または MSTP を有効にするパラメータが含まれています。

[STP インタフェース設定]、[RSTP インタフェース設定]、[MSTP プロパティ] の各ページを使用して、各モードをそれぞれ設定します。

STP 状態およびグローバル設定を行うには：

[L2 機能] > [STP] > [STP 状態 & グローバル設定] に進みます。

STP 設定：

パラメータ	概要
スパニングツリー状態	デバイスで有効または無効に設定します。
STP 操作モード	STP モード（**STP** または **RSTP** または **MSTP**）を設定します。
プライオリティ	プライオリティの値を設定します。BPDU を交換した後、プライオリティが最も低いデバイスがルートブリッジになります。すべてのブリッジのプライオリティが同じ場合は、それらの MAC アドレスを使用してルートブリッジが決まります。プライオリティの値は、4096 単位で設定します。例えば、4096、8192、12288... のようになります（デフォルトは 32768）。
ハロータイム	ルートブリッジが設定メッセージを待つ合間の間隔を秒単位で設定します（デフォルトは 2）。
最大エイジ	デバイスがデバイス自体の設定の再定義を行う前に、設定メッセージを受信しないまま待機できる間隔を秒単位で設定します（デフォルトは 20）。
フォワード遅延	ブリッジがパケット転送の前に学習状態のままになる間隔を秒単位で設定します。（デフォルトは 15）。

[適用] を押して設定をランニングコンフィグレーションファイルに保存します。

4.12.2 STP インタフェース設定

[STP インタフェース設定] ページでは、ポートごとに STP を設定し、指定ブリッジなどプロトコルが学習した情報を表示できます。

設定を指定して入力すると、それは STP プロトコルのすべてのフレーバで有効になります。

インタフェースで STP を設定するには：

[L2 機能] > [STP] > [STP インタフェース設定] に進みます。

インタフェースが表示されます。以下に、「ポートロール」の詳細情報を示します。

パラメータ	概要
ポートロール	インスタンスごとのロールを、ポートか LAG で表示します。このロールは、STP パスを可能にするために MSTP アルゴリズムによって割り当てられます。 • *ルート* — このインタフェースを介したパケット転送は、ルートデバイスにパケットを転送する最低のパスコストになります。 • *指定* — ブリッジを LAN に接続する際に経由されるインタフェース。MST インスタンスで LAN からルートブリッジへの最低ルートパスコストになります。 • *オルタネイト* — ルートインタフェースからルートデバイスへのオルタネイトパスを可能にするインタフェース。 • *バックアップ* — スパニングツリーリーブに向かう指定ポートパスのバックアップパスを可能にするインタフェース。バックアップポートは、2 つのポートがポイントツーポイントリンクによってループで接続されたときに発生します。バックアップポートは、1 つの LAN で共有セグメントへの接続が 2 つ以上確立されているときにも発生します。 • *無効* — インタフェースはスパニングツリーに参加しません。 • *バウンダリ* — このインスタンスのポートはバウンダリポートです。このポートは状態をインスタンス 0 から継承し、[STP インタフェース設定] ページで表示できます。

以下のパラメータを入力します。

パラメータ	概要
ポート	スパニングツリーを設定するポートまたは LAG の設定を行います。
状態	ポートで STP を有効または無効に設定します。
パスコスト	ルートパスコストへのポートコントリビューションを設定するか、またはシステムにより生成されるデフォルトのパスコストを使用します。

パラメータ	概要
エッジポート	ポートのファストリンク（有効 / 無効）を設定します。ポートでファストリンクモードが有効の場合、ポートリンクがアップのときポートは自動でフォワーディング状態に設定されます。ファストリンクは STP プロトコル収束を最適化します。以下のオプションがあります。 • *有効* — ファストリンクを直ちに有効にします。 • *自動* — インタフェースがアクティブになった数秒後にファストリンクを有効にします。これにより、ファストリンクを有効にする前に STP がループを解決できます。 • *無効* — ファストリンクを無効にします。 注：この値は [自動] に設定することを推奨します。これにより、ホストがデバイスに接続されている場合にはデバイスはポートをファストリンクモードに設定し、ホストが別のデバイスに接続されている場合にはポートを通常の STP ポートとして設定します。これによりループを回避できます。 MSTP モードではエッジポートは機能しません。
ルートガード	デバイスでルートガードを有効または無効に設定します。 ルートガードオプションは、ルートブリッジをネットワークに強制的に配置する方法になります。 ルートガードでは、この機能が有効なポートが指定ポートになります。通常は、ルートブリッジの 2 つ以上のポートが接続されていない限り、ルートブリッジのすべてのポートが指定ポートです。ブリッジがルートガード有効ポートで優位 BPDU を受信すると、ルートガードはこのポートを root-inconsistent の STP 状態に移行します。この root-inconsistent 状態は、実質的にリスニング状態と同じです。このポートを通じて転送されるトラフィックはありません。このように、ルートガードは強制的にルートブリッジの位置を決めます。
BPDU ガード	ポートの BPDU（Bridge Protocol Data Unit）転送機能を有効または無効に設定します。
優先度	ポートの優先度値を設定します。優先度値は、ブリッジで 2 つのポートがループ接続されているとき、ポートの選択に影響します。優先度は 0 ～ 240 の値で、16 単位で設定します（デフォルトは 128）。

[適用] を押してランニングコンフィグレーションファイルのインタフェース設定を更新します。

テーブルをフィルタリングするには、**[ポート]** または **[LAG]** を設定し、**[選択]** を押します。

4.12.3 RSTP インタフェース設定

RSTP（Rapid Spanning Tree Protocol）では、フォワーディングループを作成せずに STP 収束を迅速化できます。

[RSTP インタフェース設定] ページでは、ポートごとに RSTP を設定できます。このページで行う設定は、グローバル STP モードを RSTP または MSTP に設定しているときにアクティブになります。

RSTP 設定を入力するには：

[L2 機能] > [STP] > [STP 状態 & グローバル設定] に進みます。

[RSTP] を有効にします。

[L2 機能] > [STP] > [RSTP インタフェース設定] に進みます。[RSTP インタフェース設定] ページが表示されます。

ポートまたは LAG を設定します。

ポートまたは LAG とのインタフェースを設定します。

パラメータ	概要
ポート	インタフェースを設定し、ポートまたは LAG を指定します。
ポイントツーポイント操作状態	ポイントツーポイントリンク状態を設定します。フル Duplex に定義されたポートは、ポイントツーポイントポートリンクとみなされます。 • *有効* — この機能を有効にすると、ポートは RSTP エッジポートとして、直ちにフォワーディングモードになります（通常は 2 秒以内）。 • *無効* — ポートは RSTP のためのポイントツーポイントとはみなされません。このため、STP はポートで高速ではなく通常速度で機能します。 • *自動* — RSTP BPDU を使用してデバイスの状態を自動で決定します。

[適用] をクリックしてランニングコンフィグレーションファイルを更新します。

テーブルをフィルタリングするには、**[ポート]** または **[LAG]** を設定し、**[選択]** を押します。

4.13 MST（Multiple Spanning Tree）について

MSTP（Multiple Spanning Tree Protocol）を使用して、さまざまなドメイン間（異なる VLAN 上）で STP ポート状態を分離します。例えば、VLAN A でのループにより 1 つの STP インスタンスでポート A がブロックされるとき、別の STP インスタンスで同じポートをフォワーディング状態にできます。[MSTP プロパティ] ページでは、グローバル MSTP 設定を指定できます。

MSTP を設定するには：

[STP 状態 & グローバル設定] ページの説明に従い、[STP 操作モード] を [MSTP] に設定します。

MSTP インスタンスを設定します。各 MSTP インスタンスは、インスタンスにマッピングされる VLAN からのパケットを橋渡しするループのないトポロジを計算し構築します。「VLAN MSTP インスタンス」セクションを参照してください。

どの MSTP インスタンスがどの VLAN でアクティブになるかを決定し、それに応じて各 MSTP インスタンスを VLAN に関連付けます。

4.13.1 MSTP プロパティ

MSTP プロパティは、各 VLAN グループについて個別のスパニングツリーを設定し、各スパニングツリーインスタンスで 1 つの可能なパスを除き他のすべてのオルタネイトパスをブロックします。MSTP では、複数の MSTI（MST instance）を実行可能な MST 領域を形成できます。複数の領域と他の STP ブリッジは、1 つの CST（Common Spanning Tree）を使用して相互接続されます。

MSTP は RSTP ブリッジと完全な互換性があるので、MSTP BPDU は RSTP ブリッジによって RSTP BPDU として解釈されます。これにより、RSTP ブリッジとの互換性が設定変更なく有効になることに加え、MSTP 領域外にあるどの RSTP ブリッジも、領域内の MSTP ブリッジの数に関わらず、その領域を 1 つの RSTP ブリッジとして認識するようになります。

2 つ以上のスイッチが同じ MST 領域に存在するためには、それらに同じ VLAN MST インスタンスのマッピング、同じ設定リビジョン番号、同じ領域名がある必要があります。

同じ MST 領域に存在するスイッチは、別の MST 領域からのスイッチによって分離されることはありません。それらが分離されると、その領域は 2 つの個別の領域になります。

このマッピングは [VLAN MSTP インスタンス] ページで設定できます。

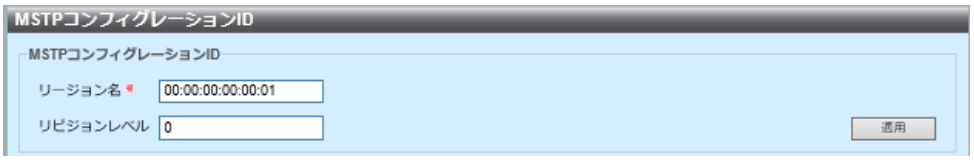
このページを使用する前に、システムが MSTP モードで動作しているかどうかを確認します。

MSTP を設定するには：

[L2 機能] > [STP] > [STP 状態 & グローバル設定] に進みます。

MSTP を有効にします。

[L2 機能] > [STP] > [MSTP プロパティ] に進みます。



パラメータ	概要
リージョン名	MSTP のリージョン名を設定します。
リビジョンレベル	現在の MST 設定のリビジョンを識別する符号なし 16 ビット数を設定します。このフィールドの設定範囲は 0 ～ 65535 です。

[適用] を押して、MSTP プロパティを定義しランニングコンフィグレーションファイルを更新します。

4.13.2 VLAN MSTP インスタンス

[VLAN MSTP インスタンス] ページでは、各 VLAN を MSTI（Multiple Spanning Tree Instance）にマッピングできます。同じ領域にあるデバイスでは、VLAN から MSTI へのマッピングが同じである必要があります。

NOTE 同じ MSTI を複数の VLAN にマッピングできますが、1 つの VLAN にマッピングできるのは 1 つの MST インスタンスだけになります。

このページ（およびすべての MSTP ページ）の設定は、システムの STP モードが MSTP の場合に適用されます。

インスタンスゼロに加えて 16 までの MST インスタンスを定義できます。

MST インスタンスのいずれかに明示的にマッピングされていない VLAN の場合、デバイスはそれらを CIST（Core and Internal Spanning Tree）インスタンスに自動でマッピングします。CIST インスタンスは MST インスタンス 0 です。

VLAN を MST インスタンスにマッピングする設定を行うには：

[L2 機能] > [STP] > [VLAN MSTP インスタンス] に進みます。

テーブルには以下の情報が表示されます。

パラメータ	概要
インスタンス ID	すべての MST インスタンスを表示します。
VLAN	その MST インスタンスに属するすべての VLAN を表示します。

VLAN を MSTP インスタンスに追加するには、MST インスタンスを選択し [編集] をクリックします。

パラメータ	概要
インスタンス ID	MST インスタンスを選択します。
VLAN	この MST インスタンスにマッピングされる VLAN を設定します。

[適用] を押して、MSTP と VLAN をマッピングしランニングコンフィグレーションファイルを更新します。

4.13.3 MSTP インタフェース設定

[MSTP インタフェース設定] ページでは、すべての MST インスタンスについてポート MSTP の設定を行い、現在プロトコルが学習している情報、例えば MST インスタンスごとの指定ブリッジなどを表示できます。

MST インスタンスのポートを設定するには：

[L2 機能] > [STP] > [MSTP インタフェース設定] に進みます。

以下の情報を表示します。

パラメータ	概要
ポート	MSTI 設定を行うインタフェース。
インタフェース優先度	指定されたインタフェースと MST インスタンスのポート優先度。
パスコスト	ルートパスコストに対するポートコントリビューションを **[ユーザ定義]** テキストボックスに入力するか、または **[デフォルトを使用]** を選択してデフォルト値を使用します。

パラメータ	概要
状態	特定の MST インスタンスの特定ポートの MSTP 状態。パラメータは以下のとおりです。 • *無効* — STP は現在無効です。 • *ブロッキング* — このインスタンスのポートは現在ブロックされており、トラフィックを転送すること（BPDU データは例外）または MAC アドレスを学習することはできません。 • *リスニング* — このインスタンスのポートはリスニングモードです。ポートはトラフィックを転送することおよび MAC アドレスを学習することはできません。 • *学習* — このインスタンスのポートは学習モードです。ポートはトラフィックを転送できませんが、新しい MAC アドレスを学習できます。 • *フォワーディング* — このインスタンスのポートはフォワーディングモードです。ポートはトラフィックを転送し新しい MAC アドレスを学習できます。 • *バウンダリ* — このインスタンスのポートはバウンダリポートです。インスタンス 0 から状態を継承します。
ポートロール	STP パスを可能にするため MSTP アルゴリズムによって割り当てられた、ポートごとのポートロールまたは LAG ロール、またはインスタンスごとの LAG。 • *ルート* — このインタフェースを介したパケット転送は、ルートデバイスにパケットを転送する最低のパスコストになります。 • *指定ポート* — ブリッジを LAN に接続する際に経由されるインタフェース。MST インスタンスで LAN からルートブリッジへの最低ルートパスコストになります。 • *オルタネイト* — ルートポートからルートブリッジへのオルタネイトパスを可能にするインタフェース。 • *バックアップ* — スパニングツリーリーブに向かう指定ポートパスのバックアップパスを可能にするインタフェース。バックアップポートは、2 つのポートがポイントツーポイントリンクによってループで接続されたときに発生します。バックアップポートは、1 つの LAN で共有セグメントへの接続が 2 つ以上確立されているときにも発生します。 • *無効* — インタフェースはスパニングツリーに参加しません。 • *バウンダリ* — このインスタンスのポートはバウンダリポートです。インスタンス 0 から状態を継承します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

4.14 リンクアグリゲーション

4.14.1 リンクアグリゲーションについて

LACP（Link Aggregation Control Protocol）は IEEE 規格（802.3az）の一部で、いくつかの物理ポートをまとめてバンドルし 1 つの論理チャネル（LAG）を形成できます。LAG は、帯域幅を増やしてポートの柔軟性を高め、2 つのデバイス間のリンク冗長性を向上させます。

2 タイプの LAG がサポートされます。

- **スタティック** — LACP が無効な場合は、その LAG はスタティックです。LAG のポートは手動で設定します。スタティック LAG に割り当てられたポートグループは、常にアクティブメンバです。LAG を手動で作成したら、LAG を編集しメンバを削除して（適用前であればメンバを追加し直すことが可能）[LACP] ボタンが編集用に利用可能になるまで、LACP オプションを追加または削除できません。
- **ダイナミック** — LACP が有効な場合は、その LAG はダイナミックです。ダイナミック LAG に割り当てられたポートグループは、候補ポートです。LACP は、どの候補ポートがアクティブメンバポートかを決定します。非アクティブの候補ポートはスタンバイポートであり、アクティブメンバポートのいずれかに不具合が発生した場合の代替ポートとなります。

4.14.1.1 LAG の特性

基本的に、LAG はシステムによって 1 つの論理ポートとして扱われます。特に、LAG には通常のポートと同じように、状態や速度といったポート属性があります。

デバイスでサポートする LAG の数は 32 で、1 つの LAG グループには最大 8 ポートを設定できます。

いずれの LAG にも以下の特性があります。

- LAG のすべてのポートは必ず同じメディアタイプになります。
- ある LAG に属するポートを、別の LAG に割り当てることはできません。
- スタティック LAG に割り当てられるポートは 8 つまでです。ダイナミック LAG には最大 16 ポートを候補ポートにすることができます。
- LAG にポートを追加すると、LAG の設定がそのポートに適用されます。LAG からポートを削除すると、ポートの元の設定が再び適用されます。
- スパニングツリーなどのプロトコルは、LAG の全ポートを 1 つのポートとみなします。

4.14.1.2 ロードバランス

LAG に転送されるトラフィックはアクティブメンバポート全体でロードバランスが行われるため、LAG の全アクティブメンバポートの総帯域幅に近い効果的な帯域幅を達成できます。

LAG のアクティブメンバポートでのトラフィックのロードバランスは、ハッシュベースの分散機能により管理されます。この機能ではレイヤ 2 またはレイヤ 3 パケットヘッダ情報に基づいて、ユニキャストとマルチキャストのトラフィックを分散します。

ロードバランスには 2 つの方式があります。

- **MAC アドレス** — 全パケットの宛先と送信元の MAC アドレスに基づきます。
- **IP と MAC アドレス** — IP パケットでは宛先と送信元の IP アドレス、非 IP パケットでは宛先と送信元の MAC アドレスに基づきます。

4.14.2 デフォルトの設定

デフォルトでは、ポートは LAG のメンバではなく、LAG を構成するための候補ポートでもありません。

4.14.3 スタティック LAG およびダイナミック LAG の設定方法

LAG を手動で作成すると、その LAG を編集しメンバを削除するまでは、LACP を作成または削除できません。LAG を編集しメンバを削除した後でのみ、[LACP] ボタンを使用して編集できるようになります。

スタティック LAG を設定するには、以下のアクションを実行します。

1. LAG で LACP を無効にして LAG をスタティックにします。**ポートリスト**からポートを選択して **LAG メンバ**リストに移動することで、8 つまでのポートをスタティック LAG に割り当てます。LAG のロードバランスアルゴリズムを選択します。これらのアクションを [LAG 管理] ページで実行します。
2. [LAG 設定] ページで、速度やフローコントロールなど LAG のさまざまな要素を設定します。

ダイナミック LAG を設定するには、以下のアクションを実行します。

1. LAG で LACP を有効にします。[LAG 管理] ページで**ポートリスト**からポートを選択して **LAG メンバ**リストに移動することで、16 までの候補ポートをダイナミック LAG に割り当てます。
2. [LAG 設定] ページで、速度やフローコントロールなど LAG のさまざまな要素を設定します。
3. [LACP] ページで、LACP の優先度と LAG のポートのタイムアウトを設定します。

4.14.4 LAG 管理

[LAG 管理] ページには、グローバル設定と LAG ごとの設定が表示されます。このページでは、グローバル設定を行い、目的の LAG を設定、編集することもできます。

LAG のロードバランスアルゴリズムを設定するには：

[L2 機能] > [リンクアグリゲーション] > [LAG 管理] に進みます。

以下の **[ロードバランスアルゴリズム]** のいずれかを設定します。

パラメータ	概要
MAC アドレス	全パケットの送信元および宛先 MAC アドレスによりロードバランスを実行します。
IP/MAC アドレス	IP パケットでは送信元と宛先 IP アドレスによって、非 IP パケットでは送信元と宛先 MAC アドレスによって、ロードバランスを実行します。

[適用] を押して、ロードバランスアルゴリズムをランニングコンフィグレーションファイルに保存します。

4.14.5 LAG 設定

[LAG 設定] ページには、全 LAG の現在の設定を示すテーブルが表示されます。ここでは、選択した LAG の設定を行い、サスペンデッド LAG をもう一度有効にできます。

LAG 設定を行う、またはサスペンデッド LAG をもう一度有効にするには：

[L2 機能] > [リンクアグリゲーション] > [LAG 設定] に進みます。

パラメータ	概要
LAG	LAG ID 番号を設定します。
説明	LAG 名またはコメントを入力します。
ステータス	選択した LAG にアップまたはダウンを設定します。
オートネゴシエーション	LAG でオートネゴシエーションを有効または無効にします。オートネゴシエーションは 2 つのリンクパートナ間のプロトコルで、LAG がその送信速度とフローコントロールをパートナにアドバタイズできるようになります（フローコントロールのデフォルトは無効）。リンクアグリゲーションの両側でオートネゴシエーションを有効のままにするか、またはリンク速度が同一であることを確認して両側で無効にすることを推奨します。
アドバタイズ	LAG のアドバタイズを [最大能力] にするかどうかを設定します。
フローコントロール	LAG でフローコントロールを **[有効]** または **[無効]** または **[オートネゴシエーション]** に設定します。
保護された LAG	LAG を分離レイヤ 2 の保護されたポートにします。

[追加] を押してランニングコンフィグレーションファイルを更新します。

4.14.6 LACP

ダイナミック LAG は LACP に対応しており、LACP は LAG に定義されたすべての候補ポートで機能します。

4.14.6.1 LACP 優先度とルール

8 つ以上の候補ポートで構成されるダイナミック LAG では、LACP システム優先度と LACP ポート優先度の両方を使用して、どの候補ポートがアクティブメンバポートとなるかを決定します。

LAG の選択された候補ポートはすべて、同じリモートデバイスに接続されます。ローカルとリモートのスイッチの両方に、LACP システムの優先度があります。

以下のアルゴリズムを使用して、LACP ポート優先度がローカルまたはリモートのいずれのデバイスから取得されるかを決定します。ローカルの LACP システム優先度をリモートの LACP システム優先度と比較します。最も優先度が高いデバイスによって、LAG に対する候補ポート選択が制御されます。両方の優先度が同じ場合は、ローカルとリモートの MAC アドレスを比較します。最小の MAC アドレスを持つデバイスの優先度に応じて、LAG に対する候補ポート選択が制御されます。

1 つのダイナミック LAG には、同じタイプの Ethernet ポートを最大 16 ポート設定できます。最大 8 ポートをアクティブにでき、最大 8 ポートをスタンバイモードにできます。ダイナミック LAG に 9 ポート以上がある場合、リンクの制御末端にあるデバイスはポート優先度を利用して、どのポートが LAG にバンドルされ、どのポートがホットスタンバイモードになるかを決定します。他のデバイス（リンクの制御末端でない）のポート優先度は無視されます。

以下に、ダイナミック LACP のアクティブなポートまたはスタンバイポートの選択に使用するその他のルールを示します。

- 最高速度のアクティブメンバとは異なる速度で機能するリンクまたはハーフ Duplex で機能するリンクは、スタンバイになります。ダイナミック LAG のすべてのアクティブポートは、同じボーレートで機能します。
- リンクのポート LACP 優先度が現在アクティブのリンクメンバの優先度より低く、アクティブメンバの数がすでに最大数に達している場合は、リンクは非アクティブになりスタンバイモードになります。

4.14.6.2 リンクパートナなしの LACP

LACP で LAG を作成できるようにするには、両方のリンク末端のポートで LACP の設定を行う必要があります。これにより両ポートは LACP PDU を送信し、受信した PDU を処理します。

ただし、1 つのリンクパートナで一時的に LACP の設定が行われない場合があります。そのようなケースには、例えば、リンクパートナがデバイス上にあり、そのデバイスが Auto-config プロトコルを使用して設定を受信するプロセスにある場合があります。このデバイスのポートはまだ LACP に設定されていません。LAG がリンクアップしないと、デバイスはいつまでも設定されない状態のままです。類似のケースはデュアル NIC のネットワーク起動コンピュータ（PXE など）でも発生し、このようなコンピュータは起動しなければ LAG 設定を受信しません。

LACP が設定されたいくつかのポートがあり、リンクが 1 つ以上のポートに通じながらそれらのポートでリンクパートナから LACP 応答がない場合は、リンクが通じている最初のポートが LACP LAG に追加されアクティブになります（他のポートは非候補になります）。このように、例えば、ネイバーデバイスが DHCP を使用してその IP アドレスを取得し、自動設定を使用して設定を取得することができます。

4.14.6.3 LACP 設定

[LACP] ページを使用して、LAG の候補ポートを設定し、ポートごとの LACP パラメータを設定します。

すべての要素が同じ状態で、可能な最大アクティブポート数（8）を超える候補ポート数が LAG に設定されている場合、デバイスは最高優先度のデバイスのダイナミック LAG からポートをアクティブとして選択します。

NOTE LACP 設定は、ダイナミック LAG のメンバでないポートには関係ありません。

LACP 設定を定義するには：

[L2 機能] > [リンクアグリゲーション] > [LACP] に進みます。

[LACP システム優先度] を入力します。

パラメータ	概要
ポート	タイムアウトと優先度の値を割り当てるポート番号を選択します。
LACP ポート優先度	ポートの LACP 優先度値を入力します。 値が 1 の場合が最も高い優先度となります。
LACP タイムアウト	連続的な LACP PDU の送受信の時間間隔。LACP PDU の定期的な送信を選択します。この送信は、LACP タイムアウトの設定に応じて、[ロング] または [ショート] の送信速度で発生します。

[追加] をクリックしてランニングコンフィグレーションファイルを更新します。

4.15 マルチキャスト

4.15.1 マルチキャストフォワーディングについて

マルチキャストフォワーディングでは、1 対多の情報提供が可能です。マルチキャストアプリケーションは、コンテンツ全体の受信を必要としない複数クライアントに対する情報提供に便利です。代表的なアプリケーションには、送信の途中でクライアントがチャネルに参加し送信終了前にチャネルから離脱できる、ケーブル TV 的なサービスがあります。

該当するポートのみにデータを転送することで、リンク上の帯域幅とホストリソースを節約できます。

すべてのマルチキャストフレームは、デフォルトの設定で VLAN の全ポートに対してフラッディングされます。該当するポートのみに選択的に転送し、[プロパティ] ページで [ブリッジマルチキャストフィルタリングステータス] を有効にすることにより残りのポートでマルチキャストをフィルタリング（ドロップ）できます。

MFDB（Multicast Forwarding Data Base）は関連する VLAN を定義します。マルチキャストフィルタリングは、すべてのトラフィックで強制的に行われます。

マルチキャストメンバシップを表す一般的な方法は (S,G) の表記で、ここで S はデータのマルチキャストストリームを送信する（シングルの）ソース、G は IPv4 または IPv6 グループアドレスです。マルチキャストクライアントが特定マルチキャストグループのどのソースからでもマルチキャストトラフィックを受信できる場合、これは (*,G) として保存されます。

以下のマルチキャストフレーム転送方式のいずれかを設定できます。

パラメータ	概要
MAC グループアドレス	Ethernet フレームの宛先 MAC アドレスに基づきます。 注：1 つまたは複数の IP マルチキャストグループアドレスを、1 つの MAC グループアドレスにマッピングできます。MAC グループアドレスに基づく転送は、ストリームのレシーバを持たないポートに転送される IP マルチキャストストリームになります。
IP グループアドレス	IP パケット (*,G) の宛先 IP アドレスに基づきます。
送信元固有 IP グループアドレス	IP パケット (S,G) の宛先 IP アドレスと送信元 IP アドレスの両方に基づきます。

(S,G) は IGMPv3 と MLDv2 によってサポートされる一方、IGMPv1/2 と MLDv1 は単なるグループ ID である (*.G) のみをサポートします。

デバイスは最大で 256 のスタティックおよびダイナミックのマルチキャストグループアドレスをサポートします。

VLAN ごとにフィルタリングオプションの 1 つのみを設定できます。

4.15.2 一般的なマルチキャスト設定

マルチキャスト対応のレイヤ 2 スイッチはマルチキャストパケットを LAN 内の登録済みノードに転送する一方、マルチキャストルータはマルチキャストパケットを IP サブネット間でルーティングします。

以降の設定で、ルータは IGMP/MLD クエリを定期的に送信します。一般的な設定には、マルチキャストストリームをプライベートおよび / またはパブリック IP ネットワーク間で転送するルータ、IGMP/MLD スヌーピング機能を持つデバイス、およびマルチキャストストリームの受信を目的とするマルチキャストクライアントが含まれます。

4.15.3 マルチキャストの機能

レイヤ 2 マルチキャストサービスでは、レイヤ 2 スイッチは特定のマルチキャストアドレスにアドレス指定された 1 つのフレームを受信します。そのフレームのコピーを作成し、それらのコピーは該当するそれぞれのポートに転送されます。

デバイスが IGMP/MLD スヌーピングに対応しており、マルチキャストストリームのフレームを受信する場合、デバイスは、IGMP/MLD ジョインメッセージを使用してマルチキャストストリームを受信するように登録されたすべてのポートにマルチキャストフレームを転送します。

システムには、各 VLAN のマルチキャストグループのリストが維持されており、これにより各ポートが受信するマルチキャスト情報が管理されます。マルチキャストグループとその受信ポートは、IGMP または MLD プロトコルスヌーピングを使用してスタティックに設定またはダイナミックに学習できます。

4.15.4 IGMP/MLD スヌーピングのマルチキャスト登録

マルチキャスト登録は、マルチキャスト登録プロトコルとリスニングプロセスに応答します。プロトコルは IPv4 では IGMP、IPv6 では MLD です。

デバイスの VLAN で IGMP/MLD スヌーピングが有効の場合、デバイスに接続された VLAN とネットワーク上のマルチキャストルータから受信する IGMP/MLD パケットを分析します。

ホストが IGMP/MLD メッセージを使用してオプションの特定ソースからのマルチキャストストリーム受信の登録を行うことをデバイスが学習する場合、デバイスはその登録を MFDB に追加します。

以下のバージョンがサポートされます。

- IGMP v1/v2/v3
- MLD v1/v2

> **NOTE** デバイスはダイナミック VLAN で IGMP/MLD スヌーピングをサポートしません。ただし、スタティック VLAN のみで IGMP/MLD スヌーピングをサポートします。

IGMP/MLD スヌーピングをグローバルまたは 1 つの VLAN で有効にできる場合、すべての IGMP/MLD パケットは CPU に転送されます。CPU は着信するパケットを分析し以下を判定します。

- どのポートがどの VLAN のどのマルチキャストグループへの参加を要求しているか。
- どのポートが、IGMP/MLD クエリを生成するマルチキャストルータ（Mrouter）に接続されているか。
- どのポートが PIM、DVMRP、または IGMP/MLD クエリプロトコルを受信しているか。

これらの VLAN は [IGMP/MLD スヌーピング IP マルチキャストグループ] ページに表示されます。

特定のマルチキャストグループへの参加を要求するポートは、ホストが参加を望むグループを指定する IGMP/MLD レポートを発行します。これにより、MFDB（Multicast Forwarding Data Base）へのフォワーディングエントリが作成されます。

4.15.5 IGMP スヌーピングクエリア

IGMP/MLD スヌーピングクエリアを使用して、マルチキャストルータがない場合にスヌーピングスイッチのレイヤ 2 マルチキャストドメインをサポートします。例えば、ローカルサーバはマルチキャストコンテンツを提供しますが、ネットワーク上のルータ（ある場合）はマルチキャストをサポートしません。

デバイスは、バックアップクエリアとして、または通常の IGMP クエリアが存在しない状況における IGMP クエリアとして設定できます。デバイスは完全な機能の IGMP クエリアではありません。

デバイスは、IGMP クエリアとして有効な場合、マルチキャストルータから IGMP トラフィック（クエリ）が検出されない状態で 60 秒が経過した後に始動します。他の IGMP クエリアがある場合、デバイスは標準のクエリア選択プロセスの結果に基づいて、クエリ送信を停止する（または停止しない）場合があります。

IGMP/MLD クエリアアクティビティの速度は、IGMP/MLD スヌーピング対応スイッチに合わせる必要があります。クエリは、スヌーピングテーブルのエージング時間と整合するレートで送信されるものとします。クエリがエージング時間を下回るレートで送信されると、サブスクライバはマルチキャストパケットを受信できません（[IGMP/MLD スヌーピング IP マルチキャストグループ] ページを参照）。

IGMP/MLD クエリアエレクションメカニズムが無効の場合、60 秒後に IGMP/MLD スヌーピングクエリアが有効になってから、ジェネラルクエリメッセージが送信されます。他のクエリアがない場合、ジェネラルクエリメッセージの送信を開始します。別のクエリアが検出される場合は、ジェネラルクエリメッセージの送信を停止します。

IGMP/MLD スヌーピングクエリアは、別のクエリアがあるかどうかを確認するクエリを以下の間隔で送信し、ない場合はジェネラルクエリメッセージの送信を再開します。

クエリパッシブ間隔 = ロバストネス * クエリ間隔 + 0.5* クエリ応答間隔

NOTE VLAN に IPM マルチキャストルータ 1 台がある場合は、IGMP/MLD クエリア選択メカニズムを無効にすることを推奨します。

4.15.6 マルチキャストアドレスのプロパティ

マルチキャストアドレスのプロパティは以下のとおりです。

- 各 IPv4 マルチキャストアドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。
- IPv6 マルチキャストアドレスは FF00:/8 です。
- IP マルチキャストグループアドレスをレイヤ 2 マルチキャストアドレスにマッピングするには：
  - IPv4 については、IPv4 アドレスの下位 23 ビットに、01:00:5e のプレフィックスを加えることでマッピングされます。標準では、IP アドレスの上位 9 ビットは無視され、この上位ビットの値のみが異なるすべての IP アドレスが同じレイヤ 2 アドレスにマッピングされます。これは使用される下位 23 ビットが同じであるためです。例えば、234.129.2.3 は MAC マルチキャストグループアドレス 01:00:5e:01:02:03 にマッピングされます。最大 32 の IP マルチキャストグループアドレスを、同じレイヤ 2 アドレスにマッピングできます。
  - IPv6 については、マルチキャストアドレスの下位 32 ビットに、33:33 のプレフィックスを加えることでマッピングされます。例えば、IPv6 マルチキャストアドレス FF00:1122:3344 はレイヤ 2 マルチキャスト 33:33:11:22:33:44 にマッピングされます。

4.15.7 IGMP/MLD プロキシ

IGMP/MLD プロキシはシンプルな IP マルチキャストプロトコルです。

IGMP/MLD プロキシを使うことで、エッジデバイスなどのデバイス上のマルチキャストトラフィックを複製できます。また、このようなデバイスの設計と実装を大幅に簡素化できます。より複雑なマルチキャストルーティングプロトコル、例えば PIM（Protocol Independent Multicast）または DVMRP（Distance Vector Multicast Routing Protocol）などはサポートしないことによって、デバイスのコストと運用諸経費の両方を削減できます。もう 1 つの利点は、プロキシデバイスがコアネットワークルータによって使用されるマルチキャストルーティングプロトコルに依存しなくなることです。このため、プロキシデバイスをあらゆるマルチキャストネットワークで簡単に展開できます。

4.15.7.1 IGMP/MLD プロキシツリー

IGMP/MLD プロキシは、ロバストマルチキャストルーティングプロトコルを実行する必要がない、シンプルなツリートポロジで機能します。学習グループのメンバシップ情報とプロキシグループのメンバシップ情報に基づいてシンプル IPM ルーティングプロトコルを使用し、その情報に基づいてマルチキャストパケットを転送することで十分です。

各プロキシデバイスでは、ツリーはダウンストリームインタフェースとアップストリーム指定によって手動で設定する必要があります。プロキシするツリートポロジにも適用される IP アドレッシングスキームは、プロキシデバイスが IGMP/MLD クエリア選定で選ばれてマルチキャストトラフィックを転送できるように設定する必要があります。ツリー内では、プロキシデバイスを除く他のマルチキャストルータは存在できず、ツリーのルートは広範なマルチキャストインフラストラクチャに接続されることが想定されます。

プロキシデバイスが IGMP/MLD に基づくフォワーディングを実行する場合、このデバイスには 1 つのアップストリームインタフェースと 1 つまたは複数のダウンストリームインタフェースがあります。これらの指定は明示的に設定されます。各インタフェースがどのタイプかを判定するプロトコルはありません。デバイスのダウンストリームインタフェースでは、プロキシデバイスは IGMP/MLD のルータ部分を実行し、デバイスのアップストリームインタフェースで IGMP/MLD のホスト部分が実行されます。

1 つのツリーのみをサポートします。

4.15.7.2 フォワーディングルールとクエリア

適用されるルールには以下があります。

- プロキシデバイスがインタフェース上でクエリアの場合に限り、アップストリームインタフェースで受信されるマルチキャストパケットは、パケットを要求するすべてのダウンストリームインタフェースで転送されます。
- デバイスがインタフェース上でクエリアでない場合、プロキシデバイスはダウンストリームインタフェースで受信されるマルチキャストパケットをドロップします。
- プロキシデバイスがクエリアとなるダウンストリームインタフェースで受信されるマルチキャストパケットは、アップストリームインタフェース上で転送され、さらにパケットを要求するダウンストリームインタフェースでプロキシデバイスがクエリアの場合に限りそれらすべてのダウンストリームインタフェース上で転送されます。

4.15.7.3 ダウンストリームインターフェースの保護

IGMP/MLD ツリーのインタフェースに着信する IP マルチキャストトラフィックは、デフォルトで転送されます。ダウンストリームインタフェースに着信する IP マルチキャストトラフィックの転送を無効にすることができます。グローバルで無効にすること、および特定のダウンストリームインタフェースで無効にすることができます。

4.16 プロパティ

マルチキャストフィルタリングを有効にして、転送方式を選択するには：

[L2 機能] > [マルチキャスト] > [プロパティ] に進みます。

[ブリッジマルチキャストフィルタリングステータス] を設定しフィルタリングを有効にします。

[適用] を押してグローバル設定をランニングコンフィグレーションファイルに設定します。

パラメータ	概要
VLAN ID	転送方式を選択する VLAN ID を設定します。
IPv4 転送方式	IPv4 アドレスの転送方式として、以下のいずれかを設定します。 • *MAC グループアドレス* — MAC マルチキャストグループアドレスに従いパケットを転送します。 • *IP グループアドレス* — IPv4 マルチキャストグループアドレスに従いパケットを転送します。 • *送信元固有 IP グループアドレス* — 送信元 IPv4 アドレスと IPv4 マルチキャストグループアドレスに従いパケットを転送します。VLAN で IPv4 アドレスを設定する場合、IPv4 マルチキャストのオペレーショナル転送方式は IP グループアドレスになります。

パラメータ	概要
IPv6 転送方式	IPv6 アドレスの転送方式として以下のいずれかを設定します。 • *MAC グループアドレス* — MAC グループアドレスに従いパケットを転送します。 • *IP グループアドレス* — IP グループアドレスに従いパケットを転送します。VLAN で IPv6 アドレスを設定する場合、IPv6 マルチキャストに運用可能な転送方式は IP グループアドレスになります。 • *送信元固有 IP グループアドレス* — 送信元 IP グループアドレスに従いパケットを転送します。VLAN で IPv6 アドレスを設定する場合、IPv6 マルチキャストのオペレーショナル転送方式は IP グループアドレスになります。 注： IPv6 IP グループアドレスモードと送信元固有 IP グループアドレスモードでは、デバイスは宛先マルチキャストアドレスの 4 バイトと送信元アドレスについてのみ照合します。宛先マルチキャストアドレスでは、グループ ID の最後の 4 バイトのみが照合されます。送信元アドレスでは、最後の 3 バイトと最後から 5 番目のバイトが照合されます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

4.17 MAC グループアドレス

このページには以下の機能が含まれています。

- 特定の VLAN ID または特定の MAC アドレスグループについて、MFDB（Multicast Forwarding Data Base）にクエリを行い、その情報を表示します。このデータは IGMP/MLD スヌーピングによってダイナミックに取得するか、または手動の入力でスタティックに取得します。
- 宛先 MAC アドレスに基づいてスタティックフォワーディング情報を提供する、MFDB へのスタティックエントリを作成または削除します。
- 各 VLAN ID と MAC アドレスグループのメンバであるすべてのポート /LAG を表示し、トラフィックがそこに転送されるか否かを入力します。

MAC マルチキャストグループを作成、編集、表示するには：

[L2 機能] > [マルチキャスト] > [MAC グループアドレス] に進みます。

パラメータ	概要
VID	グループの VLAN ID を設定します。
MAC グループアドレス	マルチキャストグループの MAC アドレスを設定します。MAC グループアドレスが指定されていない場合、ページには選択した VLAN からの全 MAC グループアドレスが含まれています。
ポート	Port/LAG とインタフェース / インタフェース範囲を設定します。
タイプ	各インタフェースとマルチキャストグループの関連付けの方法。 • *なし* — ポートが現在この VLAN でこのマルチキャストグループのメンバでないことを定義します。 • *スタティック* — マルチキャストグループへのインタフェースをスタティックメンバとして定義します。 • *禁止* — ポートがこの VLAN でこのマルチキャストグループに参加できないことを定義します。

[適用] を押して、MAC マルチキャストグループアドレスをランニングコンフィグレーションファイルに追加し、下のテーブルに表示します。

[削除] または **[クリア]** を押してスタティック MAC グループアドレスを削除またはクリアします。

4.18 IP マルチキャストグループアドレス

[IP マルチキャストグループアドレス] ページと [MAC グループアドレス] ページは類似していますが、マルチキャストグループは IP アドレスによって定義される点が異なります。

[IP マルチキャストグループアドレス] ページでは、IP マルチキャストグループのクエリと作成を実行できます。

IP マルチキャストグループを設定、表示するには：

[L2 機能] > [マルチキャスト] > [IP マルチキャストグループアドレス] に進みます。

テーブルには、スヌーピングによって学習されたすべての IP マルチキャストグループアドレスが表示されます。

パラメータ	概要
IPv4/IPv6	IPv4 または IPv6 アドレスタイプを入力します。
VID	追加されるグループの VLAN ID を指定します。
IP マルチキャストグループメンバ指定	IP マルチキャストグループメンバ指定の有効、無効を設定します。
IP マルチキャストグループメンバ	IP マルチキャストグループメンバをポート番号または LAG のグループ番号で指定します。
特定ソースアドレス指定	特定のソースアドレスを指定して IP マルチキャストグループを設定するときに有効にします。有効にした場合は [送信元 IP アドレス] フィールドにアドレスを指定します。指定しない場合、エントリは (*,G) エントリ（任意の IP ソースからの IP グループアドレス）として作成されます。
送信元 IP アドレス	[ソース固有] を有効にする場合に含めるソースアドレスを指定します。

[適用] を押して IP マルチキャストグループを作成し、このデバイスを更新します。

IP マルチキャストグループアドレスの登録を削除するには、アドレスを選択して **[削除]** を押します。

4.19 IPv4 マルチキャスト設定

4.19.1 IGMP スヌーピング

選択的な IPv4 マルチキャストフォワーディングをサポートするために、

- ブリッジマルチキャストフィルタリングを有効にします（[プロパティ] ページで）。
- [IGMP スヌーピング] ページでは、IGMP スヌーピングをグローバルに有効にするか、該当する各 VLAN で有効にします。

IGMP スヌーピングを有効にして、VLAN でデバイスを IGMP スヌーピングとして認識するには：

[L2 機能] > [マルチキャスト] > [IPv4 マルチキャストコンフィグレーション] > [IGMP スヌーピング] に進みます。

[IGMP スヌーピング] の [IGMP スヌーピング状態] が有効の場合、ネットワークトラフィックをモニタリングするデバイスは、どのホストがマルチキャストトラフィックの受信を要求したかを判定できます。デバイスは、IGMP スヌーピングとブリッジマルチキャストフィルタリングの両方が有効な場合に限り、IGMP スヌーピングを実行します。

IGMP スヌーピングテーブルには、各 VLAN ID の IGMP スヌーピング状態が表示されます。

パラメータ	概要
VID	VLAN ID を表示します。
VLAN Name	VLAN 名を表示します。
ステータス	IGMP スヌーピングが有効かどうか、実際に VLAN で実行しているかどうかを表示します。

[グローバル設定] の [IGMP スヌーピング状態] を有効 / 無効にするには、**[適用]** を押してランニングコンフィグレーションファイルを更新します。

4.19.2 IGMP スヌーピング VLAN ステータス設定

特定の VLAN で IGMP を設定するには：

[L2 機能] > [マルチキャスト] > [IPv4 マルチキャストコンフィグレーション] > [IGMP スヌーピング] に進みます。

IGMP を有効にする各 VLAN を表示します。

パラメータ	概要
VID	IGMP スヌーピングを定義（[有効] または [無効] に）する VLAN。

インタフェースを設定し、**[編集]** を押します。上記 [VID] フィールドに値を入力します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

4.20 IPv6 マルチキャスト設定

4.20.1 MLD スヌーピング

選択的な IPv6 マルチキャストフォワーディングをサポートするために、

- ブリッジマルチキャストフィルタリングを有効にします（[プロパティ] ページで）。
- [MLD スヌーピング] ページでは、MLD スヌーピングをグローバルに有効にするか、該当する各 VLAN で有効にします。

MLD スヌーピングを有効にして VLAN で設定するには：

[L2 機能] > [マルチキャスト] > [IPv6 マルチキャストコンフィグレーション] > [MLD スヌーピング] に進みます。

[MLD スヌーピング] がグローバルで有効の場合、ネットワークトラフィックをモニタリングするデバイスは、どのホストがマルチキャストトラフィックの受信を要求したかを判定できます。デバイスは、MLD スヌーピングとブリッジマルチキャストフィルタリングの両方が有効な場合に限り、MLD スヌーピングを実行します。

MLD スヌーピングテーブルが表示されます。表示されるフィールドについては、以下の [Edit] ページで説明します。さらに、以下のフィールドが表示されます。

パラメータ	概要
VID	VLAN ID を表示します。
VLAN 名	VLAN 名を表示します。
ステータス	MLS スヌーピングが有効かどうか、実際に VLAN で実行しているかどうかを表示します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

NOTE MLD スヌーピングタイマ設定、例えばクエリロバストネス、クエリ間隔などの変更は、すでに作成済みのタイマには反映されません。

4.20.2 MLD VLAN ステータス設定

特定の VLAN で MLD を設定するには：

[L2 機能] > [マルチキャスト] > [IPv6 マルチキャストコンフィグレーション] > [MLD スヌーピング] に進みます。

MLD を有効にする各 VLAN を表示します。

パラメータ	概要
VID	MLD スヌーピングを定義（**[有効]** または **[無効]** に）する VLAN。

インタフェースを設定し、**[編集]** を押します。上記 [VID] フィールドに値を入力します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

4.21 IGMP/MLD スヌーピング IP マルチキャストグループ

このページには、IGMP/MLD メッセージから学習した IPv4 および IPv6 グループアドレスが表示されます。

このページの情報と [MAC グループアドレス] ページの情報には相違がある場合があります。例えば、システムフィルタは MAC ベースのグループに準じ、ポートがマルチキャストグループ 224.1.1.1 と 225.1.1.1 への参加を要求し、両方とも同じ MAC マルチキャストアドレス 01:00:5e:01:01:01 にマッピングされるとします。この場合、MAC マルチキャストのページには 1 つのエントリがある一方、このページには 2 つのエントリがあります。

IP マルチキャストグループのクエリを行うには：

[L2 機能] > [マルチキャスト] > [IGMP/MLD スヌーピング IP マルチキャストグループ] に進みます。

検索するスヌーピンググループのタイプ（[IGMP] または [MLD]）を設定します。

[検索] を押します。各マルチキャストグループに対して以下のフィールドが表示されます。

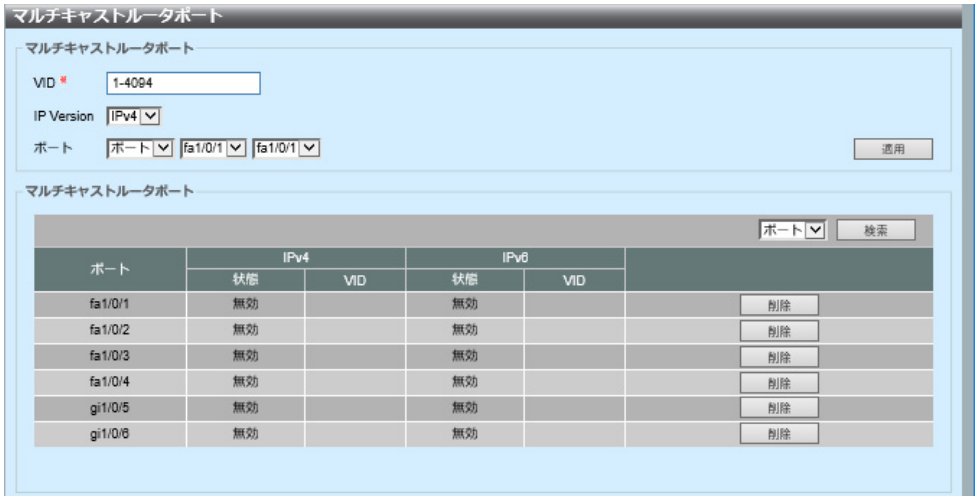
パラメータ	概要
VID	VLAN ID
グループアドレス	マルチキャストグループ MAC アドレスまたは IP アドレス。
ソースアドレス	すべての指定されたグループポートの送信元アドレス。
含まれるポート	マルチキャストストリームの送信先ポートのリスト。
除外ポート	グループに含まれないポートのリスト。
互換性モード	デバイスがその IP グループアドレスで受信するホストからの最も古い登録 IGMP/MLD バージョン。

4.22 マルチキャストルータポート

マルチキャストルータ（Mrouter）ポートは、マルチキャストルータに接続するポートです。デバイスがマルチキャストストリームと IGMP/MLD 登録メッセージを転送する場合、マルチキャストルータポート番号をメッセージに含みます。これは、マルチキャストルータがマルチキャストストリームを順次転送し登録メッセージを他のサブネットに伝搬できるようにするために必要です。

マルチキャストルータポートをスタティックに設定、またはマルチキャストルータに接続されているポートをダイナミックに検出して表示するには：

[L2 機能] > [マルチキャスト] > [マルチキャストルータポート] に進みます。



パラメータ	概要
VID	ルータポートの VLAN ID を設定します。
IP Version	マルチキャストルータがサポートする IP バージョンを設定します。
ポート	ポートまたは LAG のいずれを表示するか設定します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

[検索] を押して、ポートまたは LAG をフィルタリングして表示します。

4.23 全フォワード

ブリッジマルチキャストフィルタリングを有効にすると、登録済みマルチキャストグループへのマルチキャストパケットが IGMP スヌーピングと MLD スヌーピングに基づいてポートに転送されます。ブリッジマルチキャストフィルタリングを無効にすると、すべてのマルチキャストパケットが対応する VLAN にフラッディングされます。

[全フォワード] ページでは、特定の VLAN からマルチキャストストリームを受信するポートおよび / または LAG を設定します。この機能は、マルチキャストの [プロパティ] ページでブリッジマルチキャストフィルタリングを有効にする必要があります。もし無効にすると、すべてのマルチキャストトラフィックがデバイスのポートにフラッディングされます。

あるポートに接続しているデバイスが IGMP および / または MLD をサポートしない場合は、そのポートをスタティックに（手動で）全フォワードに設定できます。

IGMP メッセージと MLD メッセージを除くマルチキャストパケットは、全フォワードとして定義されているポートに常に転送されます。設定は、選択した VLAN のメンバであるポートのみに反映されます。

全フォワードのマルチキャストを設定するには：

[L2 機能] > [マルチキャスト] > [全フォワード] に進みます。

パラメータ	概要
VLAN ID	ポート /LAG の VLAN ID を表示するように設定します。
インタフェースタイプ	ポートまたは LAG を表示するように設定します。

[検索] を押して、すべてのポート /LAG の状態を表示します。

全フォワードとして定義するポート /LAG を以下の値で設定します。

パラメータ	概要
ポート	ポート /LAG インタフェースを設定します。
マルチキャスト受信設定	このインタフェースで受信されるマルチキャストを設定します。 • *スタティック* — ポートはすべてのマルチキャストストリームを受信します。 • *禁止* — IGMP/MLD スヌーピングによりポートがマルチキャストグループに参加するように指定した場合でも、ポートはマルチキャストストリームを受信できません。 • なし — マルチキャスト受信を行いません。

[適用] を押してランニングコンフィグレーションファイルを更新します。

4.24 未登録マルチキャスト

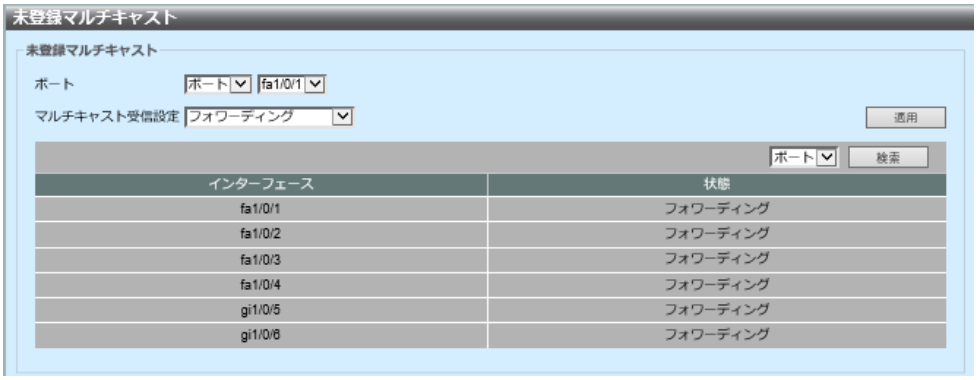
この機能により、ユーザは、要求（登録）されたマルチキャストグループのみを受信し、ネットワークで転送される可能性がある他の（未登録の）マルチキャストグループは受信しません。

未登録のマルチキャストフレームは、通常、VLAN の全ポートに転送されます。

未登録のマルチキャストストリームを受信または拒絶（フィルタリング）するように、ポートを設定できます。この設定は、ポートがそのメンバである（またはメンバになる）どの VLAN でも有効になります。

未登録のマルチキャストの設定を行うには：

[L2 機能] > [マルチキャスト] > [未登録マルチキャスト] に進みます。



[ポート] または **[LAG]** を設定し、テーブルの表示をフィルタリングします。

[検索] を押します。

[未登録マルチキャスト] の以下の設定を行います。

パラメータ	概要
ポート	ポート /LAG インタフェースを設定します。
マルチキャスト受信設定	インタフェースのフォワーディング状態を以下の値で設定します。 • *フォワーディング* — 選択したインタフェースへの未登録マルチキャストフレームのフォワーディングを有効にします。 • *フィルタリング* — 選択したインタフェースに対する未登録マルチキャストフレームのフィルタリング（拒絶）を有効にします。

[適用] を押して設定を保存しランニングコンフィグレーションファイルを更新します。

4.25 LLDP（Link Layer Discovery Protocol）

LLDP は、直接接続された LLDP 対応ネイバーのリンクレイヤプロトコルで、LLDP 自体とその機能をアドバタイズします。デフォルトの設定では、デバイスはそのすべてのインタフェースに LLDP アドバタイズを定期的に送信し、着信する LLDP パケットを必要に応じてプロトコルによって処理します。LLDP では、アドバタイズはパケットでの TLV（タイプ（Type）、長さ（Length）、値（Value））としてエンコードされます。

NOTE LLDP は、ポートが LAG として設定されているかどうかを区別しません。1 つの LAG に複数のポートがある場合、LLDP はそれらのポートが LAG であることを考慮せずに、各ポートでパケットを送信します。

LLDP の機能は、インタフェースの STP 状態に依存しません。

インタフェースが 802.1x ポートアクセスコントロールとして有効になっている場合、デバイスは、そのインタフェースが認証および許可されている場合に限り、そのインタフェースとの間で LLDP パケットを送受信します。

ポートがミラーリングのターゲットである場合、LLDP はポートをダウン状態とみなします。

NOTE LLDP は、直接接続された LLDP 対応デバイスのリンクレイヤプロトコルで、LLDP 自体とその機能をアドバタイズします。LLDP 対応デバイスが直接接続されておらず LLDP 非対応デバイスで切り離されている環境での展開では、LLDP 非対応デバイスが受信 LLDP パケットをフラッディングする場合に限り、LLDP 対応デバイスは他のデバイスからアドバタイズを受信できます。LLDP 非対応デバイスが VLAN-aware フラッディングを実行する場合、LLDP 対応の各デバイスはそれらが同じ VLAN にある場合に限りデバイス同士で互いを検知できます。LLDP 非対応デバイスが LLDP パケットをフラッディングする場合は、1 つの LLDP 対応デバイスが複数のデバイスからアドバタイズを受信する場合があります。

4.25.1 LLDP について

LLDP プロトコルによって、ネットワーク管理を強化し異なるベンダ環境でのトラブルシューティングを行うことができます。LLDP は、ネットワークデバイスが自らを他のシステムにアドバタイズし発見した情報を保存する方法を標準化します。

デバイスに LLDP プロトコルがあることで、そのデバイスの設定、ID、機能を隣接するデバイスにアドバタイズできます。またそれらのデバイスはそのデータを MIB（Management Information Base）に保存します。このネットワーク管理システムは、これらの MIB データベースにクエリを行うことで、ネットワークのトポロジをモデル化します。

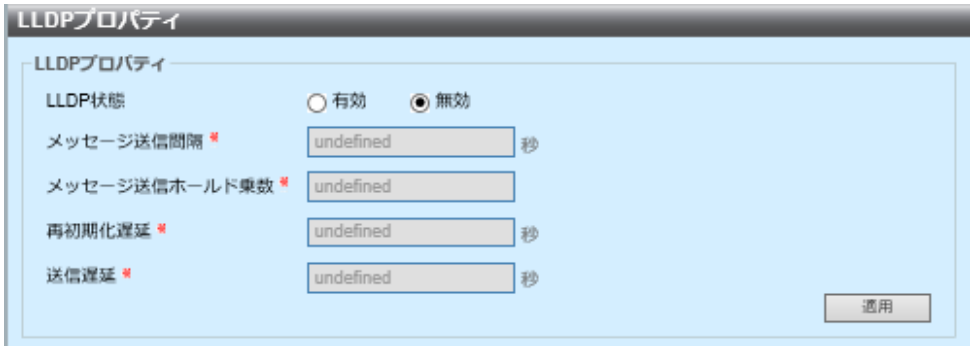
LLDP はリンクレイヤプロトコルです。デフォルト値を使用した設定では、デバイスはすべての着信 LLDP パケットをプロトコルの要求に従って終了、処理します。

4.25.2 プロパティ

LLDP 汎用パラメータを入力して、例えばタイマおよび機能の設定をグローバルに有効または無効にできます。

LLDP のプロパティを設定するには：

[L2 機能] > [LLDP] > [プロパティ] に進みます。



パラメータ	概要
LLDP 状態	デバイスで LLDP を有効にするように設定します（デフォルトで無効）。
メッセージ送信間隔	LLDP アドバタイズ更新が送信されるレート（秒）を入力します。
メッセージ送信ホールド乗数	LLDP パケットが破棄されるまで保持される時間の長さを入力します。TLV アドバタイズ間隔の倍数単位で測定されます。例えば、TLV アドバタイズ間隔が 30 秒でホールド乗数が 4 の場合、LLDP パケットは 120 秒後に破棄されます。
再初期化遅延	LLDP の有効または無効サイクルに続き、LLDP の無効化と再初期化の間に経過する時間（秒）を入力します。
送信遅延	LLDP ローカルシステム MIB での変化による連続的な LLDP フレーム送信間に経過する時間の長さ（秒）を入力します。

[適用] を押してランニングコンフィグレーションファイルに変更を追加しファイルを更新します。

4.25.3 ポート設定

このページでは、ポートごとに SNMP と LLDP の通知をアクティブにできます。

LLDP-MED TLV をアドバタイズするには、[LLDP MED ポート設定] ページの設定を行い、デバイスの管理アドレス TLV を設定します。

LLDP ポート設定を行うには：

[L2 機能] > [LLDP] > [ポート設定] に進みます。

このページには、ポート LLDP 情報が表示されます。

[編集] を押してポートごとの設定を行います。

パラメータ	概要
管理状態	以下の LLDP パブリッシングオプションを設定します。 • *Tx のみ* — パブリッシングは行いますが検出は行いません。 • *Rx のみ* — 検出は行いますがパブリッシングは行いません。 • *Tx & Rx* — パブリッシングと検出を行います。 • *無効* — このポートで LLDP が無効であることを示します。
SNMP 通知	[有効] に設定すると、SNMP 通知の受信者に通知を送信します。
広告モード	以下のパラメータのいずれかを設定し、デバイスの IP 管理アドレスをアドバタイズします。 • *自動アドバタイズ* — ソフトウェアはアドバタイズする管理アドレスをデバイスの全 IP アドレスから自動で選択します。IP アドレスが複数の場合、ソフトウェアはダイナミック IP アドレスのうち最小の IP アドレスを選択します。ダイナミックアドレスがない場合、ソフトウェアはスタティック IP アドレスのうち最小の IP アドレスを選択します。 • *なし* — 管理 IP アドレスをアドバタイズしません。 • *マニュアルアドバタイズ* — アドバタイズする管理 IP アドレスを設定します。このオプションは、デバイスに複数の IP アドレスが設定されている場合に推奨します。
IP アドレス	マニュアルアドバタイズを選択した場合は、表示されるアドレスから管理 IP アドレスを選択します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

4.25.4 LLDP MED ポート設定

各ポートで LLDP MED を設定するには：

[L2 機能] > [LLDP] > [LLDP MED ポート設定] に進みます。

パラメータ	概要
ポート	ポートを設定します。
LLDP MED 状態	有効または無効を設定します。
SNMP 通知	有効または無効を設定します。

[適用] を押してランニングコンフィグレーションファイルに設定を書き込みます。

4.25.5 LLDP ローカル情報

ポートでアドバタイズされる LLDP ローカルポート状態を表示するには：

[L2 機能] > [LLDP] > [LLDP ローカル情報] に進みます。

どのポートについて以下の情報を表示するかを設定できます。

4.25.5.1 グローバル

パラメータ	概要
ポート ID サブタイプ	ポート識別子のタイプ。
ポート ID	ポート識別子。
ポート説明	ポートの概要。

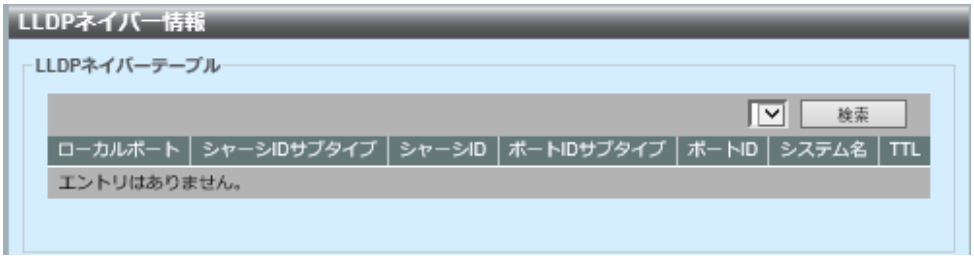
4.25.6 LLDP ネイバー情報

このページには、隣接するデバイスから受信する情報が含まれています。

タイムアウト後は情報は削除されます。このタイムアウトはネイバーから受信した Time To Live TLV（ネイバーから LLDP PDU が受信されなかった時間）の値に基づきます。

LLDP ネイバー情報を表示するには：

[L2 機能] > [LLDP] > [LLDP ネイバー情報] に進みます。



パラメータ	概要
ローカルポート	ネイバーの接続先となるローカルポートの番号。
シャーシ ID サブタイプ	シャーシ ID のタイプ（例えば MAC アドレス）。
シャーシ ID	802 LAN 隣接デバイスシャーシの識別子。
ポート ID サブタイプ	ポート識別子のタイプ。
ポート ID	ポート識別子。
システム名	パブリッシングされるデバイス名。
TTL	このネイバーの情報が削除されるまでの時間（秒）。

[検索] を押します。

4.25.7 LLDP 統計

このページには、ポートごとの LLDP 統計情報が表示されます。

LLDP 統計を表示するには：

[L2 機能] > [LLDP] > [LLDP 統計] に進みます。

パラメータ	概要
ポート	ポート識別子。
総計	送信されたフレームの総数。
廃棄総計	廃棄されたフレームの総数。
エラー総計	エラーが発生したフレームの総数。
受信総計	受信されたフレームの総数。
TLV 破棄総計	廃棄された TVL フレームの総数。
未知の TLV 総計	不明な TVL フレームの総数。

4.26 リングプロトコル（RRP）

4.26.1 はじめに

この機能は「リングトポロジ」によって使用され、2 種類のノードがあります。ノードの 1 つは「マスタノード」、もう 1 つは「トランジットノード」です。「マスタノード」には特定のポートが 2 種類あります。ポートの 1 つは「プライマリポート」、もう 1 つは「セカンダリポート」です。「マスタノード」は「プライマリポート」からコントロールフレームを送信します。このとき、「マスタノード」の「セカンダリポート」が、それ自体が送信したコントロールフレームを受信する場合、「マスタノード」はトポロジが「リング」であると判定します。そして、「マスタノード」の「セカンダリポート」はすべての非コントロールフレームを廃棄します。これにより、ネットワークループは発生しません。

「リングトポロジ」または「トランジットノードのアクシデント」で「リンクダウン」が発生すると、「マスタノード」は「セカンダリポート」を直ちにブロック解除し、「冗長ルート」が使用されます。「メインルート」から「冗長ルート」への変更にかかる時間は「1 秒」未満です。

「リングトポロジ」が復旧すると、「メインルート」がもう一度使用されます。「メインルート」に復旧するまでの時間は「1 秒」未満です。

RRP 機能を使用する場合、DUT は STP 機能も同時に使用します。

RRP 機能の用語：

パラメータ	概要
RRP ドメイン	RRP ドメインは識別子のグループです。システムが複数ドメインを使用する場合、論理的には複数の「リングトポロジ」を含むことができます。
マスタノード	このノードには 2 種類の状態があります。それらは「プライマリポート」と「セカンダリポート」です。 • *プライマリポート* — このポートは「ヘルスチェック」のコントロールフレームを送信します。このポートには 4 種類のポート状態があります。それらは「未知」、「ブロッキング」、「ダウン」、「フォワーディング」です。ユーザは、他の RRP ドメインで使われるポートをプライマリポートに設定できます。

パラメータ	概要
	マスタノードの「プライマリポートの役割」は常に「アップストリーム」です。 *未知*：RRP ドメインは設定されません。 *ブロッキング*：コントロールフレームは受信されますが、非コントロールフレームは受信されません。 *ダウン*：このポートはリンクダウンです。 *フォワーディング*：このポートはすべてのフレームを受信して転送します。 • *セカンダリポート* — このポートは「ヘルスチェック」のコントロールフレームを送信します。このポートには 4 種類のポート状態があります。それらは、「未知」、「ブロッキング」、「ダウン」、このポートはコントロールフレームを受信します。このポートが「ヘルスチェック」のコントロールフレームを受信する場合、このノードはこのトポロジが「リングトポロジ」であると判定します。このポートには 4 種類のポート状態があります。それらは「未知」、「ブロッキング」、「ダウン」、「フォワーディング」です。ユーザは、他の RRP ドメインで使われるポートをセカンダリポートに設定できます。 マスタノードの「セカンダリポートの役割」は常に「ダウントリーム」です。 *未知*：RRP ドメインは設定されません。 *ブロッキング*：コントロールフレームは受信されますが、非コントロールフレームは受信されません。 *ダウン*：このポートはリンクダウンです。 *フォワーディング*：このポートはすべてのフレームを受信して転送します。 このノードには 3 種類の状態があります。それらは「IDLE」、「完了」、「失敗」です。 • *IDLE 状態* — RRP 機能が「無効」の場合、ノードの状態は「IDLE」です。 • *完了状態* — このノードが「リングトポロジ」を判定すると、ノードはこの状態にトランジットします。 • *失敗状態* — このノードが「非リングトポロジ」を判定すると、ノードの状態が「失敗」になります。

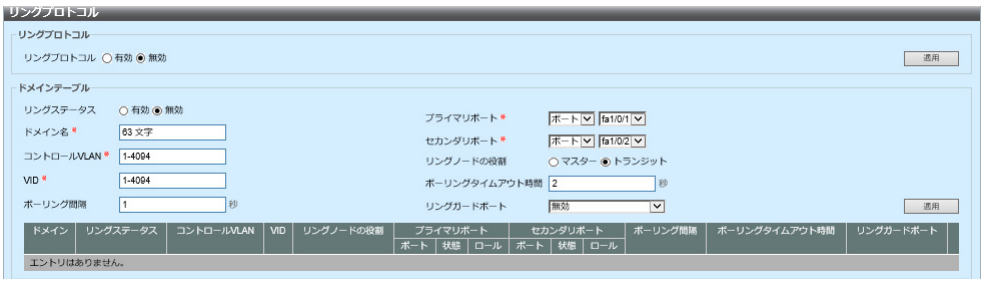
パラメータ	概要
トランジットノード	このノードには 2 種類の状態があります。それらは「プライマリポート」と「セカンダリポート」です。ただし、「プライマリポート」と「セカンダリポート」に違いはありません。 • *プライマリポートとセカンダリポート* — これらのポートは「リングトポロジ」に接続する必要があります。また、これらのポートには 4 種類のポート状態があります。それらは「未知」、「ブロッキング」、「ダウン」、「フォワーディング」です。さらに、各ポートには「アップストリーム」と「ダウンストリーム」の 2 種類のロールがあります。ユーザは、他の RRP ドメインで使われるポートをプライマリポートまたはセカンダリポートに設定できます。 *未知*：RRP ドメインは設定されません。 *ブロッキング*：コントロールフレームは受信されますが、非コントロールフレームは受信されません。 *ダウン*：このポートはリンクダウンです。 *フォワーディング*：このポートはすべてのフレームを受信して転送します。 *アップストリーム*：このロールは、このポートが「マスタノード」の「フォワーディング」ポート状態に最短であることを示します。また、このポートは「ヘルスチェック」のコントロールフレームを受信します。 *ダウンストリーム*：このロールは、このポートが「マスタノード」の「フォワーディング」ポート状態に最も遠いことを示します。また、このポートは「ヘルスチェック」のコントロールフレームを送信します。 このノードには 3 種類の状態があります。それらは「IDLE」、「リンクアップ」、「リンクダウン」、「事前転送」です。 *IDLE 状態*：RRP 機能が「無効」の場合、ノードの状態は「IDLE」です。 *リンクアップ状態*：このノードで「プライマリポート」と「セカンダリポート」の両方が「リンクアップ」の場合、ノードはこの状態にトランジットします。 *リンクダウン状態*：このノードで「プライマリポート」または「セカンダリポート」のいずれかが「リンクダウン」の場合、ノードはこの状態にトランジットします。 *事前転送状態*：このノードでポートの「リンクダウン」が復旧すると、ノードはこの状態にトランジットし「リングトポロジ」が復旧します。
コントロール VLAN	全ノードにこの VLAN があります。コントロールフレームは、「コントロール VLAN」を使用して送信する必要があります。この VLAN は各 RRP ドメインで 1 つのみでなければなりません。この VLAN で送信されるコントロールフレームは、「802.1Q 優先度 = 7（最高）」です。

パラメータ	概要
データ VLAN	全ノードにこの VLAN があります。非コントロールフレームは、「データ VLAN」を使用して送信する必要があります。この VLAN には多くの VLAN がある可能性があります。VLAN ID は各 RRP ドメインで重複する場合があります。
ポーリング間隔	「マスタノード」は「ヘルスチェック」のコントロールフレームをこの間隔で送信します。デフォルト値は 1（秒）です。
Fail Period	「マスタノード」がこの時間内に「ヘルスチェック」のコントロールフレームを受信しない場合、「マスタノード」は「非リングトポロジ」と判定します。デフォルト値は 2（秒）です。

4.26.2 RRP の設定

リングプロトコル（RRP）を有効にして設定するには：

[L2 機能] > [リングプロトコル] に進みます。



[リングプロトコル] オプションを有効にします。

[適用] を押して、ランニングコンフィグレーションファイルに設定を保存しファイルを更新します。

リングプロトコルのドメインテーブルを追加するには：

[リングステータス] を有効に設定します。

以下のフィールドを入力します。

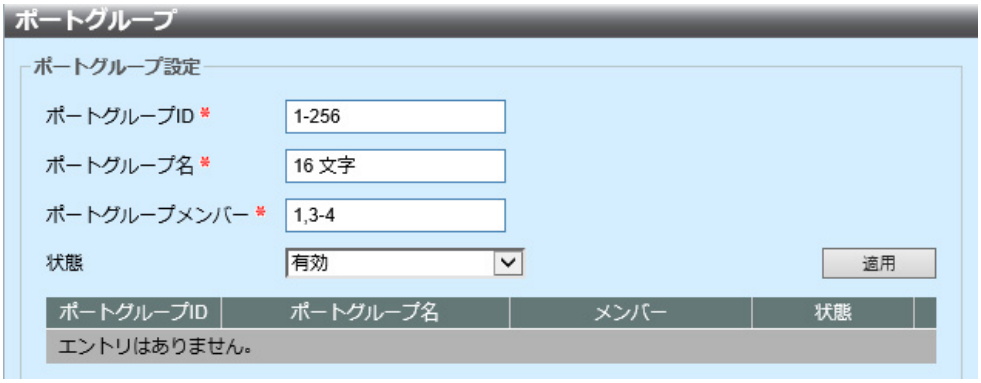
パラメータ	概要
リングステータス	このドメインを有効または無効にします。
ドメイン名	RRP ドメイン名を作成します。
コントロール VLAN	現在のドメインのコントロール VLAN ID を指定します。
VID	現在のドメインのデータ VLAN ID リストを指定します。
ポーリング間隔	ポーリング間隔を設定します。
プライマリポート	現在のドメインのプライマリポートを指定します。
セカンダリポート	現在のドメインのセカンダリポートを指定します。
リングノードの役割	リングノードの役割のマスタまたはトランジットを指定します。
故障期間	ポーリングまたは故障期間の間隔を設定します。
リングガードポート	無効 / プライマリ / セカンダリ / 両方のガードモードを設定します。

[適用] を押してリングプロトコルを追加し、ランニングコンフィグレーションファイルを更新します。

4.26.3 ポートグループ

このデバイスに接続されている全デバイスを表示するには：

[L2 機能] > [ポートグループ] に進みます。



パラメータ	概要
ポートグループ ID	ポートグループ ID を設定します。
ポートグループ名	ポートグループ名を設定します。
ポートグループメンバー	ポートグループメンバーを設定します。
状態	

5 L3 機能

5.1 ARP

デバイスでは、デバイスに直接接続された IP サブネットに存在する既知のすべてのデバイスの ARP（Address Resolution Protocol）テーブルが維持されます。直接接続された IP サブネットとは、デバイスの IPv4 インタフェースが接続されているサブネットを指します。デバイスは、ローカルデバイスにパケットを送信 / ルーティングする必要がある場合に、ARP テーブルを検索してそのデバイスの MAC アドレスを取得します。

ARP テーブルには、スタティックアドレスとダイナミックアドレスが両方含まれます。スタティックアドレスは手動で設定され、エージアウトしません。ダイナミックアドレスは、デバイスが受信した ARP パケットから作成され、設定された時間が経過するとエージアウトします。

NOTE これらのマッピング情報は、生成されたトラフィックをルーティングしたり転送したりするために使用されます。

5.1.1 Gratuitous ARP

[L3 機能]> [ARP] > [Gratuitous ARP] に進みます。

以下の値を設定します。

パラメータ	概要
IP Gratuitous ARP 状態	IP Gratuitous ARP 状態を有効 / 無効にします。
Gratuitous ARP トラップ状態	Gratuitous ARP トラップ状態を有効 / 無効にします。
IP Gratuitous ARP Dad-Reply 状態	IP Gratuitous ARP Dad-Reply 状態を有効 / 無効にします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

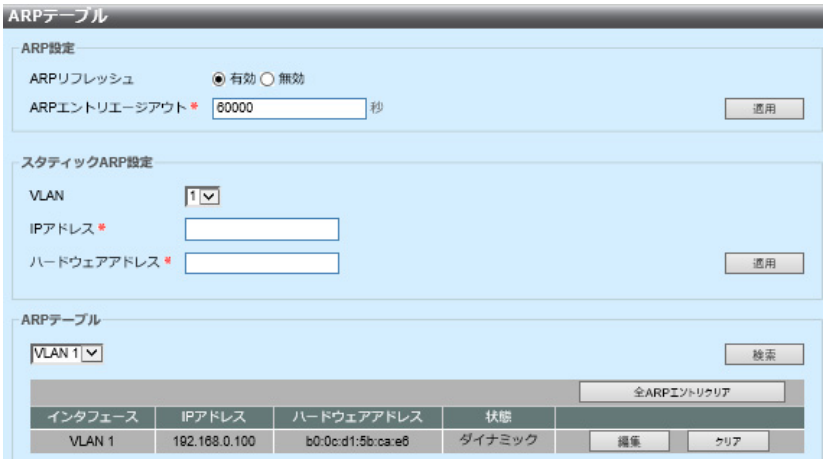
VLAN インタフェースを設定するには、**[編集]** を押して以下のフィールドを設定します。

パラメータ	概要
インタフェース名	インタフェース名を入力します。
間隔時間	間隔タイプを入力します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

5.1.2 スタティック ARP

[L3 機能] > [ARP] > [ARP テーブル] に進みます。



[ARP 設定] ブロックで以下の値を設定できます。

パラメータ	概要
ARP リフレッシュ	ARP リフレッシュを有効 / 無効にします。
ARP エントリエージアウト	ダイナミックアドレスが ARP テーブルに存続できる時間を秒単位で入力します。ダイナミックアドレスは、テーブル内での存続時間が ARP エントリエージアウト時間を経過するとエージアウトします。エージアウトしたダイナミックアドレスはテーブルから削除され、再学習された場合のみテーブルに戻されます。 ARP エントリエージアウト時間。エージアウトしたダイナミックアドレスはテーブルから削除され、再学習された場合のみテーブルに戻されます。

[適用] を押してランニングコンフィグレーションファイルの ARP グローバル値を更新します。

[Status ARP] ブロックで以下の値を設定できます。

パラメータ	概要
VLAN	ポートに VLAN インタフェースを設定できます。デバイスに設定されている IPv4 インタフェースのリストから目的のインタフェースを選択します。
IP アドレス	ローカルデバイスの IP アドレスを入力します。
ハードウェアアドレス	ローカルデバイスの MAC アドレスを入力します。

[適用] を押してランニングコンフィグレーションファイルの VLAN 設定を更新します。

下部のテーブルには、以下の情報が表示されます。

パラメータ	概要
インタフェース	IP デバイスが存在する、直接接続された IP サブネットの IPv4 インタフェース。
IP アドレス	IP デバイスの IP アドレス。
ハードウェアアドレス	IP デバイスの MAC アドレス。

VLAN/IP アドレス / ハードウェアアドレスの値を設定するには、**[編集]** を押して STEP3/4 に従います。

各 VLAN 設定を表示するには、**[検索]** を押してテーブルをフィルタリングします。

すべての ARP エントリを削除するには、**[ARP テーブルエントリをクリア]** を押します。テーブル内の ARP エントリがすべてクリアされます。

5.2 インタフェース

IP インタフェースアドレスは、ユーザが手動で設定することも、DHCP サーバにより自動的に設定することもできます。このセクションでは、デバイスの IP アドレスを手動で定義する方法、またはデバイスを DHCP クライアントにして定義する方法について説明します。

＜条件＞

トラフィックの MTU は 9000 バイトに制限されます。

デフォルトでは、IPv4 アドレス設定は空の状態です。

DHCP クライアントであるデバイスは、DHCPv4 サーバからの DHCPv4 応答で IPv4 アドレスを受信すると、ARP（Address Resolution Protocol）パケットを送信して、その IP アドレスが固有であることを確認します。IPv4 アドレスが使用中であることが ARP 応答で示された場合、デバイスは、アドレスを提供した DHCP サーバに DHCPDECLINE メッセージを送信し、別の DHCPDISCOVER パケットを送信してこのプロセスをやり直します。

60 秒以内に DHCPv4 応答が返されない場合、デバイスは DHCPDISCOVER クエリを引き続き送信し、デフォルトの空の IPv4 アドレスを使用します。

同じ IP サブネット上で複数のデバイスによって同一の IP アドレスが使用されている場合、IP アドレスのコリジョンが起こります。アドレスのコリジョンが起こった場合、DHCP サーバや、デバイスとの間でコリジョンが生じているデバイスに対して管理上のアクションが必要になります。

事前に定義されたデフォルトルートは提供されません。デバイスをリモート管理するには、デフォルトルートを定義する必要があります。DHCP によって割り当てられるすべてのデフォルトゲートウェイは、デフォルトルートとして保存されます。これに加え、デフォルトルートを手動で定義することもできます。デフォルトルートは [*IPv6 ルート*] ページで定義します。

デバイスは複数の IP アドレスを保持できます。各 IP アドレスは、指定したポート、LAG、または VLAN に割り当てることができます。これらの IP アドレスは、[IPv4 インタフェース] ページおよび [IPv6 インタフェース] ページで設定します。デバイスには、そのすべての IP アドレスで対応するインタフェースから到達できます。

本書では、デバイスに設定または割り当てられたすべての IP アドレスを管理 IP アドレスと呼びます。

<IPv6 に関して >

IPv6（Internet Protocol version 6）は、パケット交換インターネットワーク用のネットワークレイヤプロトコルです。IPv6 は IPv4 の後継プロトコルとして設計されました。

IPv6 では、アドレスサイズが 32 ビットから 128 ビットに拡張され、IP アドレス割り当ての柔軟性が向上しています。IPv6 アドレスは、8 グループの 4 桁の 16 進数値として表記されます。0 のみのグループを省略して「::」に置き換えた省略形を使用することもできます。

IPv6 ノードが IPv4 専用のネットワークを介して他の IPv6 ノードと通信するには、仲介マッピングメカニズムが必要です。このメカニズムはトンネルと呼ばれ、IPv6 専用のホストが IPv4 サービスに到達したり、分離した IPv6 ホストおよびネットワークが IPv4 インフラストラクチャを介して IPv6 ノードに到達したりできるようにします。

デバイスは、IPv6 フレームを IPv6 イーサタイプにより検出することができます。

このデバイスは、ターゲットエンドステーションまたはより宛先に近いルータである場合があります。フォワーディングメカニズムでは、ネクストホップデバイスの MAC アドレスを宛先 MAC アドレスとし、受信した L3 パケットは（基本的に）変更されず、その前後に L2 フレームが再構築されます。

システムは、スタティックルーティングおよびネイバー探索メッセージ（IPv4 の ARP メッセージと同様）を使用して、適切なフォワーディングテーブルとネクストホップアドレスを構築します。

ルートは、2 台のネットワークデバイス間のパスを定義します。ユーザが追加するルーティングエントリはスタティックルートです。ユーザが明示的に削除するまでシステムで維持および使用され、ルーティングプロトコルによって変更されることはありません。スタティックルートの更新が必要な場合は、ユーザが明示的に行う必要があります。ネットワークでルーティングループが形成されないようにするのはユーザの責任です。

スタティック IPv6 ルートは以下のいずれかです。

- 直接接続されたルート。すなわち、宛先がデバイスのインタフェースに直接接続されているため、パケットの宛先（インタフェース）がネクストホップアドレスとして使用されます。

- 再帰ルート。ネクストホップのみが指定され、送信インタフェースはネクストホップから導き出されます。

同様に、ネクストホップデバイス（直接接続されたエンドシステムなど）の MAC アドレスは、ネットワーク探索によって自動的に導き出されます。ただし、この動作はユーザがネイバーテーブルに手動でエントリを追加することによりオーバーライドしたり補足したりできます。

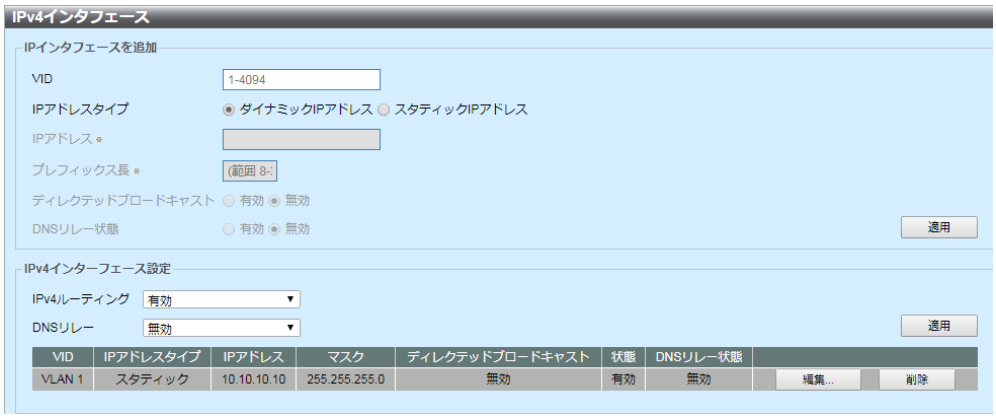
5.2.1 IPv4 インタフェース

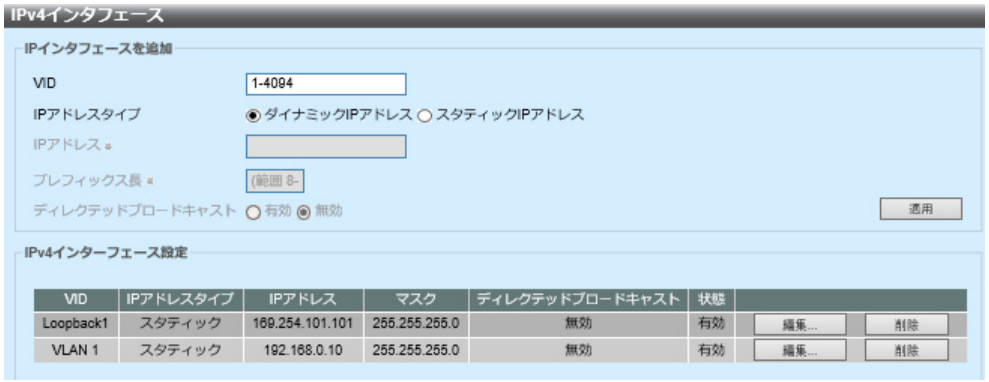
[IPv4 インタフェース] ページを用いて、デバイスの管理 IP アドレスを設定します。この IP アドレスは、VLAN、ループバックインタフェースに設定できます。

NOTE デバイスソフトウェアは、ポートまたは LAG に設定されている IP アドレスごとに VLAN ID（VID）を 1 つずつ消費します。デバイスは、4094 から開始して最初の未使用の VID を使用します。

IPv4 アドレスを設定するには：

[L3 機能] > [インタフェース] > [IPv4 インタフェース] に進みます。





IPv4 ルーティングを有効にするには、[IPv4 ルーティング] フィールドで **[有効]** を選択します。
DNS リレーを有効にするには、[DNS リレー] フィールドで **[有効]** を選択します。

[IPv4 インターフェース設定] ブロックの **[適用]** を押してランニングコンフィグレーションファイルを更新します。

IPv4 インタフェース設定テーブルには以下のフィールドが表示されます。

パラメータ	概要
VID	VLAN ID。
IP アドレスタイプ	以下の 2 つのパラメータがあります。 • *[ダイナミック IP アドレス]* — DHCP サーバから受信したアドレスです。 • *[スタティック IP アドレス]* — スタティック IP アドレスはユーザが手動で入力します。
IP アドレス	IP アドレスを入力します。
プレフィックス長	プレフィックス長（8 ～ 30）を入力します。
ディレクテッドブロードキャスト	ディレクデッドブロードキャストの物理ブロードキャストへの変換を有効または無効にします。
DNS リレー状態	DNS リレーを有効または無効にします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

> **注意** システムが、バックアップマスターが存在するいずれかのスタッキングモードにある場合、スタッキングマスターのスイッチオーバー中にネットワークから切断されないようにするために、**IP** アドレスをスタティックアドレスとして設定することを推奨します。これは、バックアップマスターがスタックの制御を引き継いだ場合に、**DHCP** を使用していると、スタックの元のマスターだったユニットから受信したものとは異なる **IP** アドレスを受信する可能性があるからです。

5.2.2 IPv6 インタフェース

IPv6 インタフェースは VLAN に設定できます。

IPv6 インタフェースを設定するには：

[L3 機能] > [インタフェース] > [IPv6 インタフェース] に進みます。

以下のフィールドに入力します。

パラメータ	概要
VID	特定の VLAN を選択します。

以下のパラメータが表示されます。

パラメータ	概要
インタフェース	インタフェース名。
状態	DHCPv6 クライアントが有効か無効かが表示されます。
自動設定	ネイバーから送信されたルータ広告に基づいて自動設定されたアドレスが表示されます。
IPv6 リダイレクト	ICMP IPv6 リダイレクトメッセージが有効か無効かが表示されます。これらのメッセージは、そのデバイスではなく別のデバイスにトラフィックを送信するように他のデバイスに通知するものです。

[適用] を押して、選択した VLAN で IPv6 処理を有効にします。

[削除] を押して、このインタフェース VLAN の IPv6 アドレスを削除することもできます。

5.3 IPv4 フォワーディングテーブル

IPv4 フォワーディングテーブルを表示するには：

[L3 機能] > [IPv4 フォワーディングテーブル **]** に進みます。

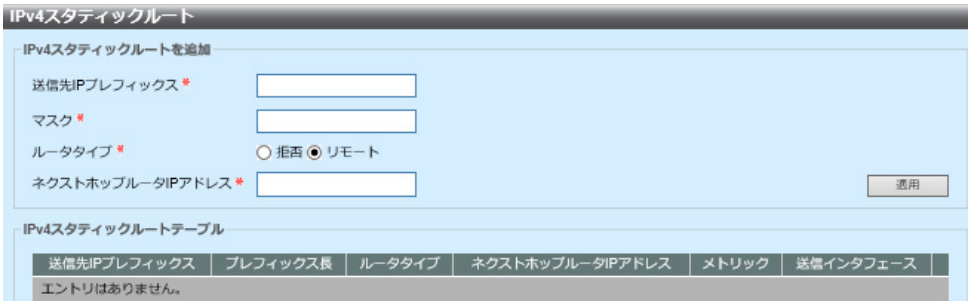
[IPv4 フォワーディングテーブル **]** に情報が表示されます。

5.4 IPv4 スタティックルート

このページでは、デバイスの IPv4 スタティックルートを設定したり表示したりできます。トラフィックのルーティング時には、最長プレフィックスマッチ（LPM アルゴリズム）に従ってネクストホップが決定されます。宛先 IPv4 アドレスが IPv4 スタティックルートテーブルの複数のルートに一致することがあります。この場合、デバイスは、一致したルートのうちサブネットマスクが最大のルート、すなわち最長プレフィックスマッチのルートを使用します。複数のデフォルトゲートウェイが定義されている場合、設定されているすべてのデフォルトゲートウェイのうち、最小の IPv4 アドレスが使用されます。

IP スタティックルートを設定するには：

[L3 機能] > [IPv4 スタティックルート] に移動します。



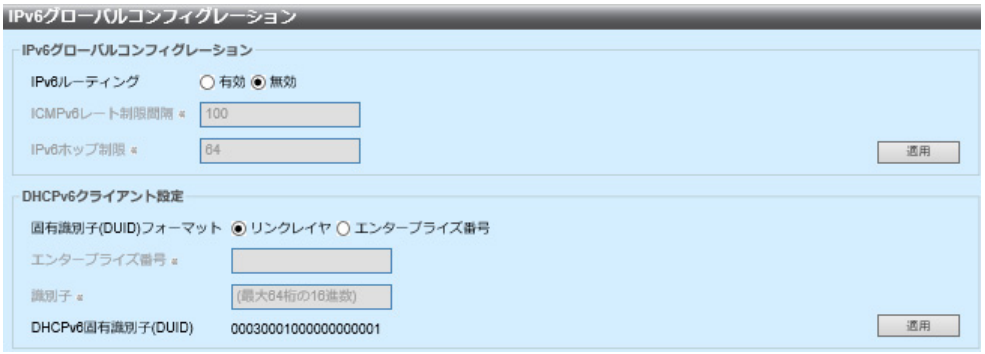
パラメータ	概要
送信先 IP プレフィックス	宛先 IP アドレスのプレフィックスを入力します。
マスク	マスクを設定します。
ルータタイプ	以下のようにルートタイプを設定します。 • *[拒否]* — ルートを拒否し、すべてのゲートウェイ経由での宛先ネットワークへのルーティングを停止します。この場合、このルートの宛先 IP を持つフレームが着信すると、ドロップされます。 • *[リモート]* — ルートがリモートパスであることを示します。
ネクストホップルータ IP アドレス	ルート上のネクストホップ IP アドレスまたは IP エイリアスを入力します。 注： デバイスが DHCP サーバから自身の IP アドレスを取得する、直接接続された IP サブネットを経由するスタティックルートを設定することはできません。

[適用] を押してランニングコンフィグレーションファイルを更新します。

5.5 IPv6 グローバルコンフィグレーション

IPv6 グローバルパラメータおよび DHCPv6 クライアント設定を設定するには：

[L3 機能] > [IPv6 グローバルコンフィグレーション] に進みます。



[IPv6 グローバル設定] ブロックで以下のパラメータを入力します。

パラメータ	概要
IPv6 ルーティング	IPv6 ルーティングを有効または無効にします。これを有効にしない場合、デバイスはホストとして（ルータとしてではなく）機能し、管理パケットを受信できますがパケットを転送することはできません。ルーティングが有効な場合、デバイスは IPv6 パケットを転送できます。 IPv6 ルーティングを有効にすると、auto-config 処理により、デバイスインタフェースに以前割り当てられたアドレスが、ネットワーク上のルータから送信される RA から削除されます。
ICMPv6 レート制限間隔	ICMP エラーメッセージの生成頻度を入力します（デフォルトは 100）。
IPv6 ホップ制限	最終的な宛先に到達するまでにパケットが通過できる中間ルータの最大数を入力します。パケットが次のルータに転送されるたびに、ホップ制限が減少します。ホップ制限が 0 になると、パケットは破棄されます。これにより、パケットが永久に転送されるのを防ぎます（デフォルトは 64）。

[適用] を押して IPv6 グローバルパラメータを更新します。

[DHCPv6 クライアント設定] ブロックで以下のパラメータを入力します。

パラメータ	概要
固有識別子 (DUID) フォーマット	これは、DHCP サーバがクライアントを指定するために使用する DHCP クライアントの識別子です。以下のいずれかの形式を使用できます。 • *[リンクレイヤ]* — （デフォルト）。このオプションを選択した場合、デバイスの MAC アドレスが使用されます。 • *[エンタープライズ番号]* — IANA によって管理される、ベンダが登録したプライベートエンタープライズ番号。 • *[エンタープライズ番号]* — ベンダが登録した番号を設定します。
識別子	ベンダが定義した 16 進数文字列。文字数が偶数でない場合、右側にゼロが追加されます。16 進数の文字は、2 文字ごとにピリオドまたはコロンで区切ることができます（最大 64 文字の 16 進数文字）。
DHCPv6 固有識別子 (DUID)	選択した識別子が表示されます。

[適用] を押して DHCPv6 クライアント設定を更新します。

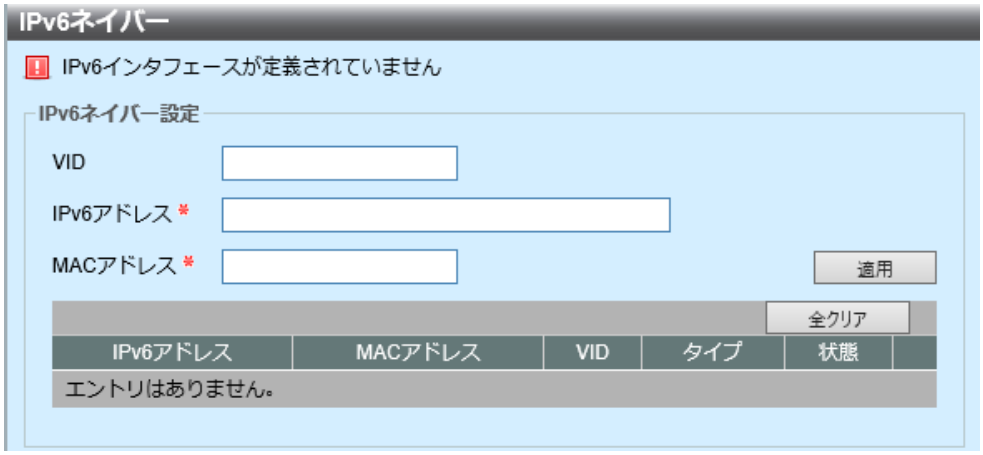
5.6 IPv6 ネイバー

このページでは、IPv6 ネイバーのリストを設定したり表示したりできます。IPv6 ネイバーテーブル（探索キャッシュ）には、デバイスと同じ IPv6 サブネット上にあるネイバーの IPv6 MAC アドレスが表示されます。このテーブルは IPv4 の ARP テーブルに相当します。デバイスは、ネイバーと通信する必要がある場合に、IPv6 ネイバーテーブルを使用して、ネイバーの IPv6 アドレスに基づいて MAC アドレスを特定します。

このページには、自動的に検出または手動で設定されたネイバーのエントリと、ネイバーの接続先インタフェース、ネイバーの IPv6 アドレスと MAC アドレス、エントリタイプ（スタティックまたはダイナミック）、およびネイバーの状態が表示されます。

IPv6 ネイバーを設定するには：

[L3 機能] > [IPv6 ネイバー] に進みます。



以下の値がテーブルに表示されます。

パラメータ	概要
IPv6 アドレス	ネイバーの IPv6 アドレス。
MAC アドレス	指定した IPv6 アドレスにマッピングされている MAC アドレス。
VID	近傍 IPv6 インタフェースの VLAN ID。
タイプ	ネイバー探索キャッシュ情報のエントリタイプ（スタティックまたはダイナミック）。

パラメータ	概要
状態	IPv6 ネイバーの状態が以下の値で示されます。 • *[不完全な]* — アドレス解決の処理中です。ネイバーはまだ応答していません。 • *[Reachable]* — ネイバーは到達可能であることがわかっています。 • *[失効]* — 以前既知だったネイバーが現在到達不能になっています。トラフィックの送信が必要になるまで、ネイバーの到達可能性を確認するためのアクションは実行されません。 • *[遅延]* — 以前既知だったネイバーが現在到達不能になっています。インタフェースは、事前に定義された遅延時間にわたって [遅延] 状態になります。到達可能性の確認が受信されない場合、状態は [プローブ] に変更されます。 • *[プローブ]* — ネイバーが到達可能かどうかが不明になったため、到達可能性を確認するためにユニキャストネイバー要請プローブを送信しています。

テーブルのすべてのエントリをクリアするには、IPv6 ネイバーテーブルの **[全クリア]** ボタンを押します。

以下のパラメータを入力します。

パラメータ	概要
VID	近傍 IPv6 インタフェースの VLAN ID。
IPv6 アドレス	有効な IPv6 ネットワークアドレスを入力します。
MAC アドレス	上記の IPv6 アドレスにマッピングされている MAC アドレスを入力します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

5.7 IPv6 デフォルトルータリスト

このページでは、デフォルト IPv6 ルータアドレスを設定したり表示したりできます。このリストには、デバイスが非ローカルトラフィック（空の場合も含む）に使用するデフォルトルータの候補ルータが表示されます。デバイスは、このリストからルータをランダムに選択します。デバイスがサポートするスタティック IPv6 デフォルトルータは 1 つです。デバイスの IPv6 インタフェースには、ダイナミックデフォルトルータからルータ広告が送信されています。

IP アドレスを削除 / 追加すると、以下のイベントが起こります。

- IP インタフェースを削除すると、すべてのデフォルトルータ IP アドレスが削除されます。ダイナミック IP アドレスは削除できません。
- ユーザ定義のアドレスを複数挿入しようとすると、アラートメッセージが表示されます。
- リンクローカルタイプ（すなわち「fe80:」）以外のアドレスを挿入しようとすると、アラートメッセージが表示されます。

デフォルトルータを設定するには：

[L3 機能] > [IPv6 デフォルトルータリスト] に進みます。

テーブルに各デフォルトルータについて以下のような情報が表示されます。

パラメータ	概要
インタフェース名	デフォルトルータが存在する送信 IPv6 インタフェース。
デフォルトルータ IPv6 アドレス	リンクローカル IP アドレス。
タイプ	設定では以下の 2 つのオプションが使用されます。 • *[スタティック]*— デフォルトルータは [追加] ボタンからこのテーブルに手動で追加されました。 • *[ダイナミック]*— デフォルトルータは動的に設定されました。

パラメータ	概要
メトリック	このホップのコスト。

スタティックデフォルトルータを変更するには、テーブルのいずれかのエントリの **[編集]** を押します。
[IPv6 スタティック / デフォルトルート] ブロックで以下のパラメータを入力します。

パラメータ	概要
ネクストホップタイプ	パケットが送信される次の宛先の IP アドレス。これには以下のタイプがあります。 • *[グローバル]* — 他のネットワークから到達および認識可能なグローバルユニキャスト IPv6 タイプの IPV6 アドレス。 • *[リンクローカル]* — 単一のネットワークリンク上のホストを一意に識別する IPv6 インタフェース / アドレス。リンクローカルアドレスのプレフィックスは **FE80** です。このタイプのアドレスはルーティングできず、ローカルネットワーク上での通信にのみ使用できます。サポートされるリンクローカルアドレスは 1 つのみです。リンクローカルアドレスがインタフェースにすでに存在する場合、このエントリにより、設定されているアドレスが置き換わります。
インタフェース名	送信リンクローカルインタフェースが表示されます。
デフォルトルータ IPv6 アドレス	スタティックデフォルトルータの IP アドレス。
メトリック	このホップコストの数値を入力します。

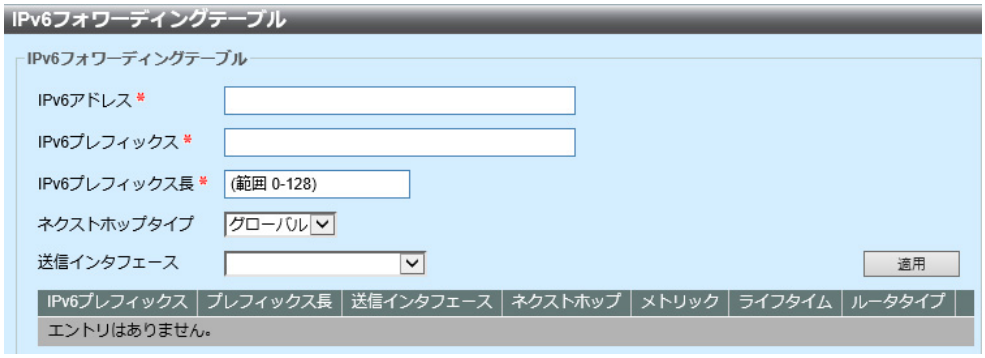
[適用] を押してランニングコンフィグレーションファイルを更新します。

5.8 IPv6 ルート

IPv6 ルートテーブルには、設定されているさまざまなルートが表示されます。これらのルートの 1 つはデフォルトルート（IPv6 アドレス：0）で、IPv6 デフォルトルータリストから選択されたデフォルトルータを使用して、デバイスと同じ IPv6 サブネット上にない宛先デバイスにパケットを送信します。また、テーブル内のデフォルトルートには、ICMP リダイレクトメッセージを使用して IPv6 ルータから受信した ICMP リダイレクトルートであるダイナミックルートも含まれます。ICMP リダイレクトメッセージは、デフォルトルータが、デバイスが通信しようとしている IPv6 サブネットにトラフィックをルーティングしていない場合に送信されます。

IPv6 ルートを表示するには：

[L3 機能] > [IPv6 ルート] に移動します。



テーブルに以下のパラメータが表示されます。

パラメータ	概要
IPv6 プレフィックス	宛先 IPv6 サブネットアドレスの IP ルートのプレフィックス。
プレフィックス長	宛先 IPv6 サブネットアドレスの IP ルートのプレフィックス長。プレフィックス長の前にはスラッシュが付きます。
送信インタフェース	パケットをルーティングするために使用されるインタフェース。
ネクストホップ	パケットのルーティング先のアドレスタイプ。通常、これは近傍ルータのアドレスです。以下のいずれかの値が表示されます。 • *[グローバル]* — 他のネットワークから到達および認識可能なグローバルユニキャスト IPV6 タイプの IPv6 アドレスです。
メトリック	このルートと、IPv6 ルータテーブルにある同じ宛先の他のルートを比較するために使用されます。すべてのデフォルトルートには同じ値が設定されます。

パラメータ	概要
ライフタイム	削除前にパケットを送信および再送信できる期間。
ルータタイプ	宛先への接続方法に関するエントリを取得するために、以下の方法を使用できます。 • *[S]（スタティック）* — エントリは手動で設定されました。 • *[I]（ICMP リダイレクト）* — エントリは、ICMP リダイレクトメッセージを使用して IPv6 ルータから受信した ICMP リダイレクトダイナミックルートです。 • *[ND]（ルータ広告）* — エントリはルータ広告メッセージから取得されました。

テーブル内のエントリの **[編集]** を押して、[IPv6 フォワーディングテーブル] ブロックで値を入力します。

パラメータ	概要
IPv6 アドレス	ルートの IPv6 アドレスを追加します。
IPv6 プレフィックス	宛先 IPv6 サブネットアドレスの IP ルートのプレフィックス。
プレフィックス長	宛先 IPv6 サブネットアドレスの IP ルートのプレフィックス長。プレフィックス長の前にはスラッシュが付きます。
ネクストホップタイプ	パケットのルーティング先のアドレスタイプ。通常、これは近傍ルータのアドレスです。以下のいずれかの値が表示されます。 • *[グローバル]* — 他のネットワークから到達および認識可能なグローバルユニキャスト IPv6 タイプの IPV6 アドレスです。
送信インタフェース	パケットをルーティングするために使用されるインタフェース。

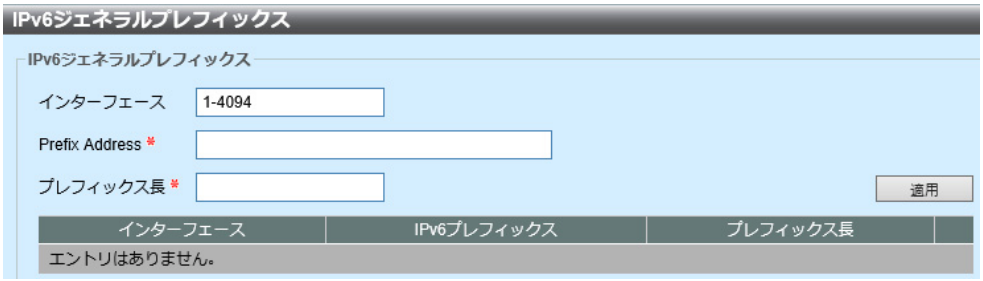
[適用] を押してランニングコンフィグレーションファイルを更新します。

5.9 IPv6 ルータコンフィグレーション

5.9.1 IPv6 プレフィックス

デバイスのインタフェースでアドバタイズするプレフィックスを設定するには：

[L3 機能] > [IPv6 ルータコンフィグレーション] > [IPv6 プレフィックス] に進みます。



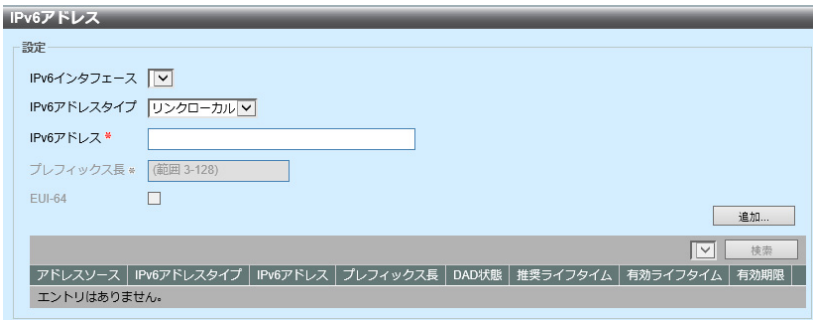
パラメータ	概要
インターフェース	インタフェースの VLAN ID を入力します（1 ～ 4096）。
Prefix Address	IPv6 ジェネラルプレフィックスの IPv6 アドレスを入力します。
プレフィックス長	IPv6 プレフィックス長を入力します。この値は、プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を表す 10 進数です。10 進値の前にスラッシュを付ける必要があります。

[適用] を押してランニングコンフィグレーションファイルを更新します。

5.10 IPv6 アドレス

IPv6 アドレスとインタフェースを関連付けるには：

[L3 機能] > [IPv6 アドレス] に進みます。



パラメータ	概要
IPv6 インタフェース	IPv6 アドレスを定義するインタフェース。* が表示されている場合、IPv6 インタフェースは設定されているが有効になっていないことを意味します。
IPv6 アドレスタイプ	追加する IPv6 アドレスのタイプを選択します。 • *[リンクローカル]* — 1 つのネットワークリンク上にあるホストを一意に識別する IPv6 アドレス。リンクローカルアドレスのプレフィックスは **FE80** です。このタイプのアドレスはルーティングできず、ローカルネットワーク上での通信にのみ使用できます。サポートされるリンクローカルアドレスは 1 つのみです。リンクローカルアドレスがインタフェースにすでに存在する場合、このエントリにより、設定されているアドレスが置き換わります。 • *[グローバル]* — 他のネットワークから到達および認識可能なグローバルユニキャスト IPV6 タイプの IPv6 アドレスです。 • *[エニーキャスト]* — IPv6 アドレスのエニーキャストアドレス。これは、通常はそれぞれ異なるノードに属している一連のインタフェースに割り当てられるアドレスです。エニーキャストアドレスに送信されたパケットは、使用中のルーティングプロトコルの定義に従い、エニーキャストアドレスで指定された最近接インタフェースに配信されます。 注： IPv6 アドレスが ISATAP インタフェースに存在する場合、エニーキャストは使用できません。

パラメータ	概要
IPv6 アドレス	デフォルトのリンクローカルアドレスとマルチキャストアドレスに加え、デバイスは、受信したルータ広告に基づいてインタフェースにグローバルアドレスを自動的に追加します。デバイスでは、インタフェースで最大 128 個のアドレスがサポートされます。各アドレスは、16 ビット値をコロンで区切って 16 進数形式で指定した有効な IPv6 アドレスである必要があります。 各トンネルタイプには以下のアドレスタイプを追加できます。 • *手動トンネル* へ — グローバルアドレスまたはエニーキャストアドレス • *ISATAP トンネル* へ — EUI-6 によるグローバルアドレス • *6to4 トンネル* — なし
プレフィックス長	グローバル IPv6 プレフィックス長（0 ～ 128）は、プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を表します。
EUI-64	グローバル IPv6 アドレスのインタフェース ID 部分をデバイスの MAC アドレスに基づいて EUI-64 形式で指定するように選択できます。

[追加] を押してランニングコンフィグレーションファイルを更新します。

テーブルで特定のエントリ情報をフィルタリングするには、**[検索]** を押します。

6 QoS

QoS（Quality of Service）機能をネットワーク全体に適用することにより、必要な基準に従ってネットワークトラフィックに優先度を設定し、重要性の高いトラフィックを優先的に処理することができます。

6.1 QoS の概要

QoS 機能は、ネットワークのパフォーマンスを最適化するために使用します。

QoS では以下の機能が提供されます。

- 以下のようなアトリビュートに基づいて、受信トラフィックをトラフィッククラスに分類します。
  - デバイス設定
  - 入力インタフェース
  - パケットの内容
  - これらのアトリビュートの組み合わせ
    QoS では以下のような処理が行われます。

パラメータ	概要
トラフィックの分類	受信トラフィックは、パケットの内容やポートに基づいて特定のトラフィックフローに分類されます。この分類はアクセスコントロールリストに従って行われ、ACL 基準を満たしているトラフィックに対してのみ、CoS または QoS 分類が実行されます。
ソフトウェアキューへの割り当て	各受信パケットはフォワーディングキューに割り当てられます。パケットは、そのパケットが属するトラフィッククラスの機能として特定のキューに送信されます。「キュー」を参照してください。
その他のトラフィッククラス	処理アトリビュート — 帯域幅管理などさまざまなクラスに QoS メカニズムが適用されます。

6.1.1 QoS 全般

[QoS プロパティ] ページで、信頼するヘッダフィールドのタイプを入力します。[CoS/802.1p キュー] ページで、そのフィールドのすべての値に対して出力キューを割り当て、どのキューからフレームを送信するかを指定します（信頼モードが CoS/802.1p か DSCP かによって異なる）。

6.1.2 QoS モード

すべてのインタフェースに対して以下のいずれかのモードを設定します。

- **無効モード** – トラフィックは 1 つのベストエフォートキューにマッピングされます。すなわち、トラフィックタイプ間で優先度に優劣はありません。
- **QoS 基本モード**（サービスクラス）
  同じクラスのトラフィックは同じように扱われ、受信フレームに指定された QoS 値に基づいて出力ポートで出力キューを決定する単一の QoS アクションが実行されます。QoS 値には以下の値が使用されます。
  - レイヤ 2：レイヤ 2 では、VPT（VLAN 優先度タグ）802.1p 値
  - レイヤ 3：レイヤ 3 では、IPv4 の場合は DSCP（Differentiated Service Code Point）値、IPv6 の場合の場合は TC（トラフィッククラス）値

  基本モードのデバイスでは、外部で割り当てられたこの QoS 値が信頼されます。パケットに外部で割り当てられた QoS 値により、そのパケットのトラフィッククラスと QoS が決まります。
  信頼するヘッダフィールドは、[QoS プロパティ] ページで入力します。また、[CoS/802.1p キュー] ページまたは [DSCP 変換マップ] ページ（それぞれ信頼モードが CoS/ 802.1p または DSCP の場合）で、そのフィールドのすべての値に対して、フレームを送信する出力キューを割り当てます。
- **QoS 拡張モード**（フローごとの QoS（Quality of Service））
  フローごとの QoS は、クラスマップやポリサーで構成されます。
  - クラスマップはフロー内のトラフィックの種類を定義するもので、複数の ACL から成ります。ACL に一致するパケットはそのフローに属します。
  - ポリサーは、設定された QoS をフローに適用するものです。フローの QoS 設定は、出力キュー、DSCP 値または CoS/802.1p 値、およびプロファイル外（超過）トラフィックに対するアクションで構成されます。

モードを上記のいずれかのモードに変更すると、以下のように動作が変化します。

- QoS を無効にした場合：シェーパおよびキュー設定（WRR/SP 帯域幅設定）がデフォルト値にリセットされます。その他すべてのユーザ設定はそのまま維持されます。
- QoS 基本モードから拡張モードに変更した場合：基本モードの QoS 信頼モード設定は維持されません。
- QoS 拡張モードから他のモードに変更した場合：ポリシープロファイル定義およびクラスマップが削除されます。インタフェースに直接バインドされている ACL は、バインドされたままになります。

6.2 全般

6.2.1 QoS プロパティ

このページでは、QoS モード（無効、基本、または拡張）を設定できます。
また、各インタフェースのデフォルト CoS 優先度を定義できます。

QoS モードを設定するには：

[QoS] > [一般] > [QoS プロパティ] に進みます。

パラメータ	概要
無効	QoS を無効にします。
基本	QoS を基本モードで有効にします。
拡張	QoS を拡張モードで有効にします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

指定したデフォルト CoS 番号をポート /LAG インタフェースに設定するには、
[適用] を押します。

テーブルの以下のフィールドに表示されるポートまたは LAG をフィルタリングするには、**[選択]** を押します。

パラメータ	概要
ポート	インタフェースタイプ。
デフォルト **CoS**	デフォルトの CoS は 0 です。 VLAN タグが設定されていない受信パケットのデフォルト VPT 値。 デフォルト値 0 は、基本モードが設定され、QoS 基本モードの [グローバル設定] ページで信頼モードとして CoS が選択されている場合にのみ、タグなしフレームに適用されます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.2.2 キュー

最も優先度の高いキューの番号は 8 です。最も優先度の低いキューの番号は 1 です。

キューでのトラフィックの処理を決定する方式には、絶対優先（SP）と重み付きラウンドロビン（WRR）の 2 つがあります。

- **絶対優先（SP）** — 出力トラフィックは、最も優先度の高いキュー内のものが最初に送信されます。これより優先度の低いキュー内のトラフィックは、優先度が最高のキューの送信が完了してから送信されるため、番号が最も大きいキューのトラフィックに対して最も高い優先度が与えられます。
- **重み付きラウンドロビン（WRR）** — キューから送信されるパケット数はキューの重みに比例します（重みが大きいキューほど送信されるフレームが多くなる）。例えば、キューの最大数が 4 個で、そのすべてが WRR で処理され、デフォルトの重みを使用している場合、キュー 1 では帯域幅の 2/15（すべてのキューが飽和し、輻輳が発生していると仮定）、キュー 2 では 3/15、キュー 3 では 4/15、キュー 4 では 6/15 がそれぞれ使用されます。デバイスで使用される WRR アルゴリズムのタイプは、標準的な DWRR（Deficit WRR）ではなく、SDWRR（Shaped Deficit WRR）です。

キューイングモードは [キュー] ページで変更できます。キューイングモードが絶対優先の場合、優先度によってキューの処理順序が設定されます。まず、キュー 4 またはキュー 8（最も優先度の高いキュー）が処理され、そのキューの処理が完了した後に、番号が次に高いキューに進みます。

キューイングモードが重み付きラウンドロビンの場合、キューはそのキューに割り当てられた帯域幅を消費するまで処理され、その後、次のキューが処理されます。

優先度の低いキューに WRR を割り当て、優先度の高いキューは絶対優先のままにすることもできます。この場合、絶対優先キューのトラフィックは、常に WRR キューのトラフィックよりも先に送信されます。WRR キューのトラフィックは必ず、絶対優先キューが空になった後に転送されます（各 WRR キューから送信されるトラフィックの相対量はその重みによって決まる）。

優先度方式を設定し、WRR 値を入力するには：

[QoS] > [一般] > [キュー] に移動します。

[WRTD] フィールドでキューイングモードを設定します。

パラメータ	概要
有効	絶対優先（SP）として設定します。
無効	WRR として設定し、キューに割り当てる WRR 重みを入力します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

WRR について以下の値を入力します。

パラメータ	概要
キュー ID	キュー番号。
WRR 重み	WRR を設定した場合、キューに割り当てる WRR 重みを入力します。

[適用] を押してランニングコンフィグレーションファイルを更新するか、**[全クリア]** を押してデフォルト値に戻します。

6.2.3 CoS/802.1p キュー

このページでは、出力キューに CoS/802.1p 優先度をマッピングします。[CoS/802.1p to Queue Table] ブロックで、受信パケットの VLAN タグ内の 802.1p 優先度に基づいて、そのパケットの出力キューを定義します。受信パケットにタグが設定されていない場合、入力ポートに割り当てられたデフォルト CoS/802.1p 優先度が 802.1p 優先度として使用されます。

以下は、キューが 8 個ある場合のデフォルトマッピングです。

802.1p 値 （0 ～ 7、7 が最高）	キュー （8 個のキュー 1 ～ 8、8 が最高の優先度）	7 個のキュー （8 がスタック制御トラフィックに使用される最高の優先度）のスタック	備考
0	1	1	バックグラウンド
1	2	1	ベストエフォート
2	3	2	エクセレント エフォート
3	6	5	重要なアプリケーション - LVS 電話の SIP
4	5	4	ビデオ
6	8	7	インターワーク制御 LVS 電話の RTP
7	7	6	ネットワーク制御

CoS/802.1p 値とキューのマッピング（[CoS/802.1p キューテーブル])、キュースケジュール方式、および帯域幅の割り当て（[帯域幅] ページ）を変更することにより、ネットワークで目標とする QoS を達成できます。

キューへの CoS/802.1p 値のマッピングは、以下のいずれかの条件が満たされている場合にのみ適用できます。

- デバイスが QoS 基本モードで、かつ CoS/802.1p 信頼モードの場合
- デバイスが QoS 拡張モードで、かつ CoS/802.1p により信頼されたフローにパケットが属している場合

CoS 値をキュー ID 番号にマッピングするには：

[QoS] > [一般] > [CoS/802.1p キュー] に進みます。

パラメータ	概要
802.1p	出力キューに割り当てる 802.1p 優先度タグ値を設定します（0：最低の優先度、7：最高の優先度）。
出力キュー	802.1p 優先度のマッピング先の出力キューを設定します（1 ～ 8）（1：最低の優先度、8：最高の優先度）。

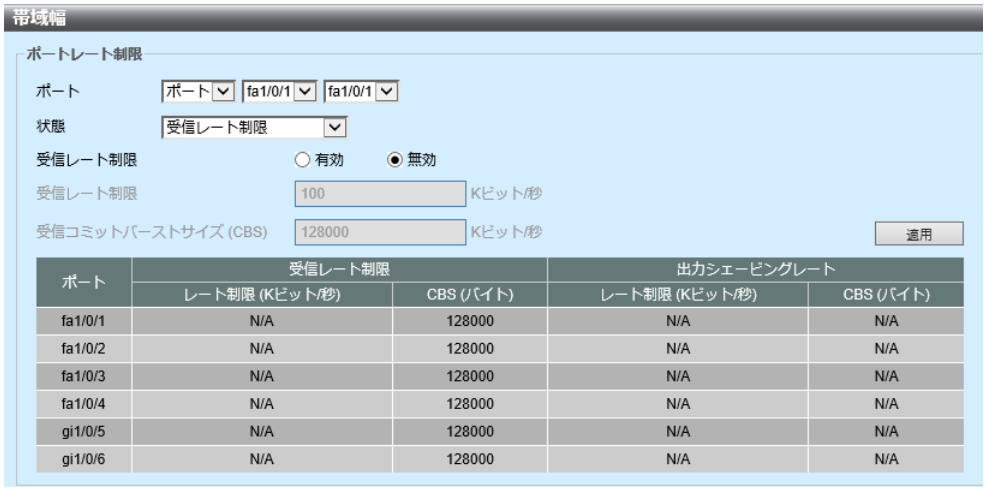
[適用] を押してランニングコンフィグレーションファイルを更新します。

6.2.4 帯域幅

このページでは、各インタフェースの帯域幅情報を確認できます。

帯域幅情報を設定および表示するには：

[QoS] > [一般] > [帯域幅] に進みます。



ポート	受信レート制限		出力シェーピングレート	
	レート制限 (Kビット/秒)	CBS (バイト)	レート制限 (Kビット/秒)	CBS (バイト)
fa1/0/1	N/A	128000	N/A	N/A
fa1/0/2	N/A	128000	N/A	N/A
fa1/0/3	N/A	128000	N/A	N/A
fa1/0/4	N/A	128000	N/A	N/A
gi1/0/5	N/A	128000	N/A	N/A
gi1/0/6	N/A	128000	N/A	N/A

テーブルには、各インタフェースの入出力のレートとバーストが表示されます。

- **入力**：
  - *[レート制限 (K ビット / 秒)]* — 入力レート制限が表示されます。
  - *[受信コミットバーストサイズ (CBS)]* — 入力インタフェースのピークバーストサイズ（データのバイト数）。
- **出力**：
  - *[レート制限 (K ビット / 秒)]* — 出力シェーピングレートが表示されます。
  - *[出力コミットされたバーストサイズ (CBS)]* — 出力インタフェースのピークバーストサイズ（データのバイト数）。

インタフェースタイプとして **[ポート]** または **[LAG]** を設定します。

[状態] で、入力対象を [入力] および [出力] から選択します。

パラメータ	概要
入力（状態）	入力レート制限を有効にするには、[状態] を [入力] に設定します。
受信レート制限（K ビット / 秒）	入力インタフェースで許可する帯域幅の最大量を入力します。

パラメータ	概要
受信コミットバーストサイズ (CBS)	受信インタフェースのデータのピークバーストサイズをバイト単位で入力します。帯域幅が許容された制限を一時的に超えた場合でも、このデータ量を送信できます。このフィールドは、インタフェースがポートの場合のみ使用できます。
出力（状態）	出力レート制限を有効にするには、[状態] を [出力] に設定します。 • **[出力シェーピングレート（K ビット / 秒）]** — 出力インタフェースの最大帯域幅を入力します。 • **[出力コミットされたバーストサイズ (CBS)]** — 出力インタフェースのデータのピークバーストサイズをバイト単位で入力します。帯域幅が許容された制限を一時的に超えた場合でも、このデータ量を送信できます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.2.5 キュー出力制限

送信レートをポートごとに制限するには、[帯域幅] ページで設定します。

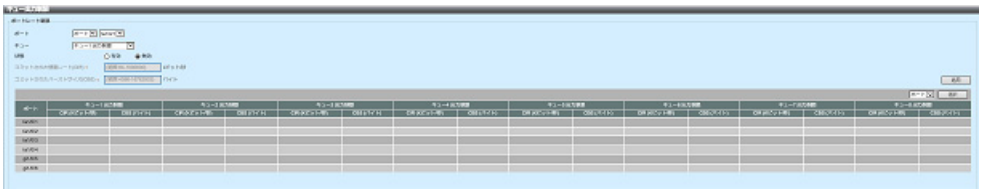
選択した出力フレームの送信レートをキューごと、ポートごとに制限することもできます。出力レート制限は、出力負荷を制限することによって実行されます。

管理フレーム以外のすべてのフレームが制限の対象になります。レートの計算では、制限されないフレームが無視され、そのフレームのサイズは制限の合計に含まれません。

キュー出力制限のレートは無効にできます。

キュー出力制限を設定するには：

[QoS] > [一般] > [キュー出力制限] に移動します。



各キュー、各ポートのレート制限とバーストサイズが表示されます。

インタフェースタイプでフィルタリングするには、**[ポート]** または **[LAG]** を指定して **[選択]** を押します。

各キューに対して以下の値を入力する必要があります。

パラメータ	概要
ポート	インタフェースタイプとして [ポート] または [LAG] を設定します。
キュー	出力制限を有効にするキュー（キュー 1 ～キュー 8）を設定します。
状態	ポートレート制限を有効または無効に設定します。
コミットされた情報レート (CIR)	最大レート（CIR）を K ビット / 秒（Kbps）単位で入力します。 CIR は、送信可能な平均最大データ量です。
コミットされたバーストサイズ (CBS)	ピークバーストサイズ（CBS）をバイト単位で入力します。 CBS は、バーストが CIR を超えた場合に送信できるデータの最大バーストです。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.3 QoS 基本モード

6.3.1 はじめに

QoS 基本モードでは、ネットワーク上の特定のドメインを信頼されたドメインとして定義できます。このドメイン内のパケットは、そのパケットに必要なサービスのタイプを知らせるために、802.1p 優先度や DSCP でマークされます。そのドメイン内のノードはこれらのフィールドを使用して、パケットを特定の出力キューに割り当てます。初期のパケット分類およびこれらのフィールドのマーキングは、信頼されたドメインに入るときに行われます。

6.3.2 QoS 基本モードの設定方法

QoS 基本モードの設定方法は以下のとおりです。

1. [QoS プロパティ] ページを使用してシステムに基本モードを設定します。
2. [グローバル設定] ページを使用して信頼動作を設定します。デバイスでは、CoS/802.1p 信頼モードと DSCP 信頼モードがサポートされます。CoS/802.1p 信頼モードでは、VLAN タグ内の 802.1p 優先度が使用されます。DSCP 信頼モードでは、IP ヘッダ内の DSCP 値が使用されます。

受信パケットの CoS マークを信頼すべきではない例外的なポートがある場合は、[インタフェース設定] ページを使用して、そのポートで QoS 状態を無効にします。

[インタフェース設定] ページでは、グローバルに設定された信頼モードをポートで有効または無効にできます。ポートで信頼モードを無効にすると、そのポートの入力パケットはすべてベストエフォートで転送されます。受信パケット内の CoS/802.1p 値や DSCP 値を信頼できないポートでは、信頼モードを無効にすることを推奨します。無効にしない場合、ネットワークのパフォーマンスに悪影響が及ぶ可能性があります。

6.3.3 グローバル設定

このページでは、デバイスで信頼モードを有効にできます。

この設定は、QoS モードが基本モードの場合にアクティブになります。QoS ドメインに入ってくるパケットは、QoS ドメインのエッジで分類されます。

信頼モードを設定するには：

[QoS] > [QoS 基本モード] > [グローバル設定] に移動します。

デバイスが基本モードの場合、**[トラストモード]** を設定します。パケットの CoS レベルおよび DSCP タグが別々のキューにマッピングされている場合、設定する信頼モードによってパケットがどのキューに割り当てられるかが決まります。

パラメータ	概要
CoS/802.1p	トラフィックは、VLAN タグ内の VPT フィールドまたはポートごとのデフォルト CoS 値（受信パケットに VLAN タグがない場合）に基づいてキューにマッピングされます。VPT とキューの実際のマッピングは、[CoS/802.1p キュー] ページで設定できます。
DSCP	すべての IP トラフィックは、IP ヘッダ内の DSCP フィールドに基づいてマッピングされます。 DSCP とキューの実際のマッピングは、[DSCP to Queue] ページで設定できます。IP トラフィック以外のトラフィックは、ベストエフォートキューにマッピングされます。
CoS/802.1p-DSCP	CoS または DSCP のいずれか設定されているもの。

受信パケット内の元の DSCP 値を DSCP オーバーライドテーブルに入力された新しい値で上書きするには、**[受信 DSCP の上書き]** を設定します（「DSCP 変換マップ」を参照）。[受信 DSCP の上書き] を有効にすると、デバイスでは出力キューイングに新しい DSCP 値が使用されます。また、パケット内の元の DSCP 値が新しい DSCP 値で置き換えられます。

NOTE フレームは、元の DSCP 値ではなく、書き換えられた新しい値を使用して出力キューにマッピングされます。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.3.4 インタフェース設定

このページでは、デバイスの各ポートに QoS を設定できます。この設定による動作は以下のとおりです。

- **インタフェースで無効にした場合** — ポートのインバウンドトラフィックはベストエフォートキューにマッピングされ、分類 / 優先度設定は行われません。
- **インタフェースで有効にした場合** — ポートでは、システム全体に設定されている信頼モード（CoS/802.1p 信頼モードまたは DSCP 信頼モードのいずれか）に基づいて、ポートに入るときにトラフィックの優先度が設定されます。

インタフェースごとの QoS 設定を行うには：

[QoS] > [QoS 基本モード] > [インタフェース設定] に進みます。

インタフェースタイプとして **[ポート]** または **[LAG]** を設定します。

[QoS 状態] を有効または無効にします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.4 QoS 拡張モード

6.4.1 はじめに

ACL に一致し、通過が許可されたフレームには、その通過を許可した ACL 名のラベルが暗黙的に付けられます。これらのフローには、拡張モードの QoS アクションを適用できます。

QoS 拡張モードでは、デバイスにより、フローごとの QoS をサポートするためにポリシーが使用されます。ポリシーとその要素には以下の特性と関係があります。

- ポリシーは 1 つ以上のクラスマップで構成されます。
- クラスマップは、それに関連付けられている 1 つ以上の ACL に基づいてフローを定義します。クラスマップ内の、許可（転送）アクションが設定された ACL ルール（ACE）に一致したパケットのみが同じフローに属すると見なされ、これらのパケットに同じ QoS が適用されます。すなわち、ポリシーには、それぞれユーザ定義の QoS が設定された 1 つ以上のフローが含まれます。
- クラスマップ（フロー）の QoS は、それに関連付けられているポリサーによって適用されます。ポリサーには、シングルポリサーと集約ポリサーの 2 つのタイプがあります。各ポリサーには、QoS 仕様が設定されます。シングルポリサーは、ポリサーの QoS 仕様に基づいて、1 つのクラスマップ、すなわち 1 つのフローに QoS を適用します。集約ポリサーは、1 つ以上のクラスマップ、すなわち 1 つ以上のフローに QoS を適用します。集約ポリサーでは、異なるポリシーのクラスマップをサポートできます。

  2 レート 3 カラー（2R3C）機能がサポートされます。この機能により、すべてのポリサーが 2 つの閾値を持つことができます。最初の閾値に達すると、ユーザ設定の超過時アクションが実行されます。2 番目の閾値に達すると、ユーザ設定の違反時アクションが実行されます（「集約ポリサー」ページを参照）。
- フローごとの QoS は、ポリシーを目的のポートにバインドすることによりフローに適用されます。ポリシーとそのクラスマップは 1 つ以上のポートにバインドできますが、各ポートにバインドできるポリシーは 1 つまでです。

NOTE

- 集約ポリサーとシングルポリサーは、デバイスがレイヤ 2 モードで動作している場合に使用できます。
- ACL は、ポリシーに関係なく、1 つ以上のクラスマップに設定できます。
- 1 つのクラスマップが属することのできるポリシーは 1 つのみです。
- シングルポリサーに関連付けられたクラスマップが複数のポートにバインドされている場合、ポートごとにシングルポリサーのインスタンスが独自に保持され、各ポートでは相互に独立した状態でそれぞれのインスタンスによって QoS がクラスマップ（フロー）に適用されます。
- 集約ポリサーは、ポリシーやポートに関係なく、集約されたすべてのフローに QoS を適用します。

拡張 QoS 設定は、以下の 3 つの部分で構成されます。

- 照合するルールの定義。1 つのルールグループに一致したすべてのフレームは、1 つのフローとして見なされます。
- ルールに一致した各フロー内のフレームに適用するアクションの定義。
- 1 つ以上のインタフェースへの、ルールとアクションの組み合わせのバインディング。

6.4.2 QoS 拡張モードの設定方法

QoS 拡張モードに設定するには、以下の手順に従います。

1. [QoS プロパティ] ページを使用してシステムに拡張モードを設定します。[グローバル設定] ページで信頼モードを設定します。パケットの CoS レベルおよび DSCP タグが別々のキューにマッピングされている場合、設定する信頼モードによってパケットがどのキューに割り当てられるかが決まります。
   - 内部の DSCP 値が受信パケットで使用されているものと異なる場合、[Out-of-Profile DSCP Mapping] ページを使用して外部値を内部値にマッピングします。これにより、[DSCP Remarking] ページが開きます。
2. 「ACL Configuration」の手順に従って ACL を作成します。
3. ACL が指定されている場合、[クラスマッピング] ページを使用してクラスマップを作成し、そのクラスマップに ACL を関連付けます。
4. [ポリシーテーブル] ページを使用してポリシーを作成し、[ポリシークラスマップ] ページでポリシーに 1 つ以上のクラスマップを関連付けます。必要に応じて、クラスマップをポリシーに関連付けるときにポリサーをクラスマップに割り当てて、QoS を指定することもできます。
   - **シングル** – [ポリシーテーブル] ページおよび [クラスマッピング] ページで、クラスマップにシングルポリサーを関連付けるポリシーを設定します。そのポリシー内でシングルポリサーを定義します。
   - **集約** – [集約ポリサー] ページを使用して、各フローに対して、一致したすべてのフレームを同じポリサー（集約ポリサー）に送信する QoS アクションを設定します。[ポリシーテーブル] ページを使用して、クラスマップに集約ポリサーを関連付けるポリシーを作成します。
5. [ポリサーバインディング] ページを使用して、ポリシーをインタフェースにバインドします。

6.4.3 グローバル設定

このページでは、デバイスで信頼モードを有効にできます。QoS ドメインに入ってくるパケットは、QoS ドメインのエッジで分類されます。

信頼設定を指定するには：

[QoS] > [QoS 拡張モード] > [グローバル設定] に進みます。

デバイスが拡張モードの場合、**[トラストモード]** を設定します。パケットの CoS レベルおよび DSCP タグが別々のキューにマッピングされている場合、設定する信頼モードによってパケットがどのキューに割り当てられるかが決まります。

パラメータ	概要
CoS/802.1p	トラフィックは、VLAN タグ内の VPT フィールドまたはポートごとのデフォルト CoS 値（受信パケットに VLAN タグがない場合）に基づいてキューにマッピングされます。VPT とキューの実際のマッピングは、[CoS/802.1p キュー] ページで設定できます。
DSCP	IP トラフィックは、IP ヘッダ内の DSCP フィールドに基づいてマッピングされます。 DSCP とキューの実際のマッピングは、[DSCP to Queue] ページで設定できます。IP トラフィック以外のトラフィックは、ベストエフォートキューにマッピングされます。
CoS/802.1p-DSCP	IP 以外のトラフィックには CoS 信頼モードを設定し、IP トラフィックには DSCP 信頼モードを設定します。

[グローバル設定] フィールドで、インタフェースにデフォルトモード状態（[信頼できる] または [信頼できない] のいずれか）を設定します。これにより、拡張 QoS で基本的な QoS 機能が提供され、拡張 QoS で CoS/DSCP をデフォルトで信頼できるようになります（ポリシーの作成は不要）。

DSCP オーバーライドテーブルに従って受信パケット内の元の DSCP 値を新しい値で上書きするには、**[受信 DSCP の上書き]** を設定します。[受信 DSCP の上書き] を有効にすると、デバイスでは出力キューイングに新しい DSCP 値が使用されます。また、パケット内の元の DSCP 値が新しい DSCP 値で置き換えられます。

NOTE フレームは、元の DSCP 値ではなく、書き換えられた新しい値を使用して出力キューにマッピングされます。

[受信 DSCP の上書き] を有効にした場合、**[DSCP 変換マップ]** を押して DSCP を再設定します。

[適用] を押します。

6.4.4 DSCP 変換マップ

クラスマップ（フロー）にポリサーを割り当てた後、フローのトラフィック量が QoS 指定の制限を超えた場合に実行するアクションを定義できます。フローの QoS 制限超過を引き起こしたトラフィックの部分は*プロファイル外パケット*と呼ばれます。

プロファイル外 DSCP に超過時 / 違反時アクションが設定されている場合、デバイスでは、プロファイル外 DSCP マッピングテーブルに基づいて、プロファイル外 IP パケットの元の DSCP 値が新しい値に再マッピングされます。また、これらのパケットの出力キューと新しい値を使用してリソースが割り当てられます。さらに、プロファイル外パケットの元の DSCP 値が新しい DSCP 値で物理的に置き換えられます。

プロファイル外 DSCP の超過時アクションを使用するために、プロファイル外 DSCP マッピングテーブルで DSCP 値を再マッピングできます。工場出荷時の設定では、テーブル内の DSCP 値によってパケットがそれ自身に再マッピングされるため、この操作を行わないと、アクションが null になります。

この機能により、信頼された QoS ドメイン間で交換される受信トラフィックの DSCP タグが変更されます。あるドメインで使用されている DSCP 値を変更すると、そのタイプのトラフィックの優先度が、他のドメインで使用されている DSCP 値に対して設定され、同じタイプのトラフィックとして識別されるようになります。

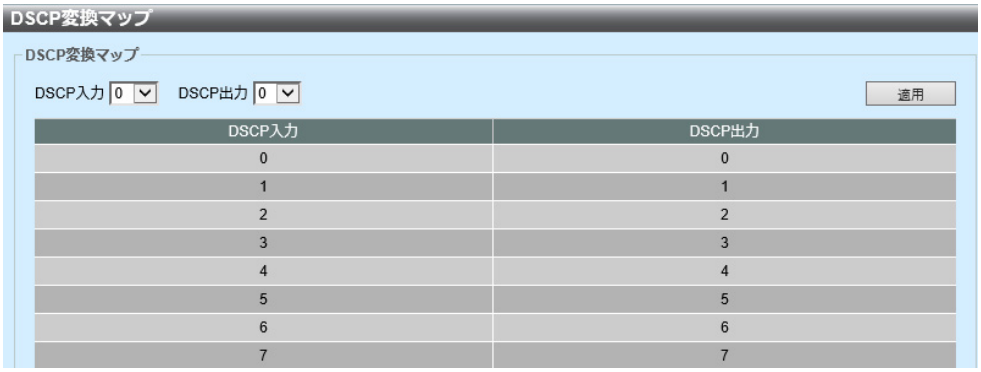
これらの設定はシステムが QoS 拡張モードのときにアクティブになり、有効にすると、グローバルにアクティブになります。

例えば、シルバー、ゴールド、およびプラチナの 3 つのサービスレベルがあり、これらのレベルをマークするために、それぞれ 10、20、30 の DSCP 受信値が使用されているとします。同じ 3 つのサービスレベルを持つが、使用している DSCP 値が 16、24、および 48 である別のサービスプロバイダにこのトラフィックが転送される場合、**DSCP 変換マップ**により、受信値はマッピングされている送信値に変更されます。

デバイスに出入りするトラフィックの DSCP 値は以下のように設定できます。

DSCP 値をマッピングするには：

[QoS] > [QoS 拡張モード] > [DSCP 変換マップ] に進みます。



[DSCP 入力] または **[DSCP 出力]** に、受信値をマッピングする値を設定します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.4.5 クラスマッピング

クラスマップは、そのクラスマップに定義されている ACL（アクセスコントロールリスト）を使用してトラフィックフローを定義するもので、MAC ACL、IP ACL、および IPv6 ACL を組み合わせることもできます。クラスマップは、match-all または match-any でパケット基準に一致するように設定します。パケットとの一致はファーストフィット方式で処理されます。すなわち、最初に一致したクラスマップに関連付けられているアクションが、システムで実行されるアクションになります。同じクラスマップに一致したパケットは、同じフローに属するものと見なされます。

NOTE クラスマップを定義した時点では、QoS には何の影響もありません。これは、後でクラスマップを使用するための中間的なステップです。

より複雑なルールセットが必要な場合、ポリシーと呼ばれるスーパーグループに複数のクラスマップをグループ化できます（「ポリシーテーブル」ページを参照）。

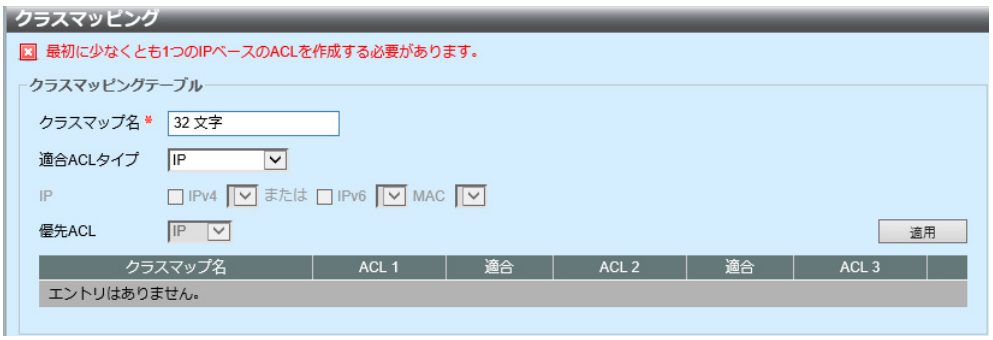
NOTE 同じクラスマップ内では、MAC ACL と、フィルタリング条件として宛先 IPv6 アドレスを持つ IPv6 ACE とを組み合わせて使用することはできません。

[クラスマッピング] ページには、定義されているクラスマップと、それぞれを構成する ACL が表示され、クラスマップを追加または削除することができます。

クラスマップを指定するには：

[QoS] > [QoS 拡張モード] > [クラスマッピング] に移動します。

各クラスマップについて、定義されている ACL がその相互関係とともに表示されます。最大 3 つの ACL をそれぞれの **[適合]**（**[AND]** または **[Or]**）とともに確認できます。[適合] は ACL 相互の関係を表し、クラスマップは 3 つの ACL を And または Or で組み合わせた結果になります。



パラメータ	概要
クラスマップ名	新しいクラスマップの名前を入力します。
適合 ACL タイプ	パケットが、クラスマップで定義されているフローに属するものと見なされるために一致する必要のある基準。以下のオプションがあります。 • *[IP]* — パケットは、クラスマップに定義されている IP ベースの ACL のいずれかに一致する必要があります。 • *[MAC]* — パケットは、クラスマップ内の MAC ベースの ACL に一致する必要があります。 • *[IP と MAC]* — パケットは、クラスマップ内の IP ベースの ACL および MAC ベースの ACL の両方に一致する必要があります。 • *[IP または MAC]* — パケットは、クラスマップ内の IP ベースの ACL または MAC ベースの ACL のいずれかに一致する必要があります。
IP	クラスマップに IPv4 ベースの ACL を設定します。
IPv4/IPv6	クラスマップに IPv4/IPv6 ベースの ACL を設定します。
MAC	クラスマップに MAC ベースの ACL を設定します。
優先 ACL	パケットを最初に照合する ACL（IP ベースの ACL または MAC ベースの ACL）を設定します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.4.6 集約ポリサー

事前に定義されたルールセットに一致するトラフィックのレートを測定したり、ポートで許可されるファイル転送トラフィックのレート制限などの制限を適用したりできます。

ポリサーを実行するには、クラスマップ内の ACL を使用して目的のトラフィックを照合する必要があります。また、ポリサーを使用することで、一致したトラフィックに QoS を適用できます。

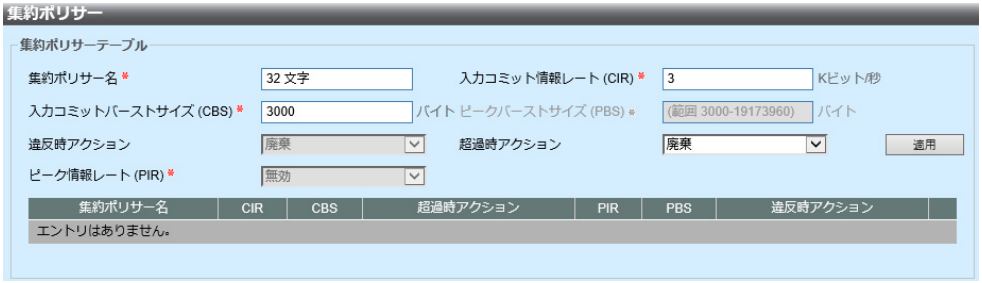
ポリサーには QoS 仕様を設定でき、以下のように動作します。

- **集約ポリサー** — 集約ポリサーは、1 つ以上のクラスマップ、すなわち 1 つ以上のフローに QoS を適用します。集約ポリサーには、それぞれ異なるポリシーの複数のクラスマップを設定できます。集約ポリサーは、ポリシーやポートに関係なく、集約されたすべてのフローに QoS を適用します。「集約ポリサー」ページを参照してください。
  集約ポリサーは、ポリサーが複数のクラスで共有される場合に指定します。特定のポートのポリサーを別のデバイスの他のポリサーと共有することはできません。
- **シングル（標準）ポリサー** — シングルポリサーは、ポリサーの QoS 仕様に基づいて、1 つのクラスマップ、すなわち 1 つのフローに QoS を適用します。シングルポリサーに関連付けられたクラスマップが複数のポートにバインドされている場合、ポートごとにシングルポリサーのインスタンスが独自に保持され、互いに独立している複数のポートでそれぞれのインスタンスによって QoS がクラスマップ（フロー）に適用されます。「ポリシーテーブル」ページを参照してください。

クラスマップへのポリサーの割り当ては、クラスマップをポリシーに追加するときに行います。集約ポリサーは、[集約ポリサー] ページで作成する必要があります。

集約ポリサーを設定するには：

[QoS] > [QoS 拡張モード] > [集約ポリサー] に進みます。



パラメータ	概要
集約ポリサー名	集約ポリサー名を入力します。
入力コミットバーストサイズ (CBS)	CIR を超えた場合のピークバーストサイズをバイト単位で入力します。「帯域幅」ページを参照してください。
違反時アクション	ピークサイズを超えた場合のアクションとして以下のいずれかのアクションを設定します。 • *[廃棄]* — ピークサイズに違反しているフレームをドロップします。 • *[プロファイル外 DSCP]* — 以前設定されていた DSCP 値に基づく DSCP 値により、ピークサイズに違反しているフレームをマークします。
ピーク情報レート (PIR)	ピークバーストサイズを超えた場合のアクションを有効にするように設定します。
入力コミット情報レート (CIR)	許可される最大帯域幅をビット / 秒単位で入力します。「帯域幅」ページを参照してください。
ピークバーストサイズ (PBS)	ピークバーストサイズをバイト単位で入力します。
超過時アクション	CIR を超えた分の受信パケットに対して実行するアクションを設定します。以下の値を設定できます。 • *[廃棄]* — 定義された CIR 値を超えた分のパケットをドロップします。 • *[プロファイル外 DSCP]* — プロファイル外 DSCP マッピングテーブルに基づいて、定義された CIR 値を超えた分のパケットの DSCP 値を再マッピングします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.4.7 ポリシーテーブル

このページには、デバイスに指定されている拡張 QoS ポリシーが表示されます。ポリシーを作成および削除することもできます。インタフェースにバインドされているポリシーのみがアクティブになります。「ポリサーバインディング」ページを参照してください。

各ポリシーは以下の要素で構成されます。

- ACL から成る 1 つ以上のクラスマップ。これによりトラフィックフローが定義されます。
- トラフィックフローに QoS を適用する 1 つ以上の集約。

ポリシーを追加した後、クラスマップを追加できます。

QoS ポリシーを作成するには：

[QoS] > [QoS 拡張モード] > [ポリシーテーブル] に進みます。

定義されているポリシーが表示されます。

[ポリシー名] フィールドに、新しいポリシーの名前を入力します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.4.8 ポリシークラスマップ

1 つのポリシーに 1 つ以上のクラスマップを追加することができます。クラスマップでは、同じトラフィックフローに属していると見なすパケットのタイプを定義します。
ポリシーにクラスマップを作成するには：

[QoS] > [QoS 拡張モード] > [ポリシークラスマップ] に進みます。

パラメータ	概要
ポリシー名	クラスマップの追加先のポリシー。
ポリサータイプ	ポリシーのポリサータイプを選択します。以下のオプションがあります。 • *[なし]* – ポリシーを使用しません。 • *[シングル]* – ポリシーのポリサーはシングルポリサーです。 • *[集約]* – ポリシーのポリサーは集約ポリサーです。
クラスマップ名	ポリシーに関連付ける既存のクラスマップ（作成については、「クラスマッピング」を参照）を設定します。
アクションタイプ	一致したすべての入力パケットの CoS/802.1p 値や DSCP 値に関するアクションを設定します。 • *[デフォルトの信頼モード]* – 入力パケットの CoS/802.1p 値や DSCP 値が無視されるなど、一致したパケットはベストエフォートで送信されます。 • *[常に信頼]* – このオプションを設定すると、デバイスでは、一致したパケットの DSCP および CoS/802.1p が信頼されます。パケットが IP パケットの場合、パケットはその DSCP 値と DSCP キューテーブルに基づいて出力キューに入れられます。それ以外の場合、パケットの出力キューは、パケットの CoS/802.1p 値と CoS/802.1p キューテーブルに基づいて決められます。

[ポリサータイプ] が [集約] の場合、**[集約ポリサー]** を設定します。

[ポリサータイプ] が [シングル] の場合、以下の QoS パラメータを入力します。

パラメータ	概要
入力コミット情報レート (CIR)	CIR を Kbps 単位で入力します。CIR については、「帯域幅」ページを参照してください。
入力コミットバーストサイズ (CBS)	CBS をバイト単位で入力します。「帯域幅」ページを参照してください。
超過時アクション	CIR を超えた分の受信パケットに割り当てるアクションを以下から設定します。 • *[廃棄]* — 定義された CIR 値を超えた分のパケットをドロップします。 • *[プロファイル外 DSCP]* — 定義された CIR を超えた分の IP パケットは、プロファイル外 DSCP マッピングテーブルから得られる新しい DSCP で転送されます。
ピーク強制	ピークバーストサイズを超えた場合のアクションを有効にするように設定します。
ピーク情報レート (PIR)	ピークトラフィックレート（PIR）を k ビット / 秒（kbps）単位で入力します。
ピークバーストサイズ (PBS)	ピークバーストサイズ（PBS）を k ビット / 秒（kbps）単位で入力します。
違反時アクション	ピークサイズを超えた場合のアクションを以下のように設定します。 • *[廃棄]* — ピークサイズに違反しているフレームをドロップします。 • *[プロファイル外 DSCP]* — 以前設定されていた DSCP 値に基づく DSCP 値により、ピークサイズに違反しているフレームをマークします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

6.4.9 ポリサーバインディング

このページには、どのポートにどのポリシープロファイルがバインドされているかが表示されます。ポリシーは、入力 / 出力ポリシーとしてインタフェースにバインドできます。特定のポートにバインドしたポリシープロファイルは、そのポートでアクティブになります。1 つのポート、1 つの方向に設定できるポリシープロファイルは 1 つのみですが、1 つのポリシーを複数のポートにバインドすることができます。

ポリシーをポートにバインドすると、トラフィックがフィルタリングされ、そのポリシーで定義されているフローに属するトラフィックに QoS が適用されます。

ポリシーを設定するには、まず、そのポリシーをすべてのバインド先ポートから削除（バインド解除）する必要があります。

> **NOTE** ポートにはポリシーまたは ACL をバインドできますが、両方をバインドすることはできません。

ポリシーバインディングを指定するには：

[QoS] > [QoS 拡張モード] > [ポリサーバインディング] に進みます。

必要に応じて **[ポート]** または **[LAG]** を設定します。

入力インタフェースまたはポリシーについて以下の値を入力します。

パラメータ	概要
入力ポリシーバインディング	入力ポリシーとインタフェースのバインディングを有効にします。
ポリシー名	バインドする入力ポリシーを設定します。

出力インタフェースまたはポリシーについて以下の値を入力します。

パラメータ	概要
出力ポリシーバインディング	出力ポリシーとインタフェースのバインディングを有効にします。
ポリシー名	バインドする出力ポリシーを設定します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

7 ACL

アクセスコントロールリストは一種のセキュリティメカニズムです。ACL の定義は、特定の QoS（Quality of Service）の対象となるトラフィックフローを定義するためのメカニズムの 1 つとして機能します。前の「QoS」セクションを参照してください。

ネットワーク管理者は ACL を使用することにより、入力トラフィックに対してパターン（フィルタおよびアクション）を定義できます。ACL がアクティブになっているポートまたは LAG からデバイスに入ってくるパケットは、通過が許可または拒否されます。

7.1 はじめに

アクセスコントロールリスト（ACL）は、分類用のフィルタとアクションが順番に並べられたリストです。1 つの分類ルールとそのアクションを組み合わせたものは、アクセスコントロール要素（ACE）と呼ばれます。

各 ACE は、トラフィックグループを区別するフィルタと、それに関連付けられたアクションで構成されます。1 つの ACL には、受信フレームの内容と照合される複数の ACE を含めることができます。フィルタに内容が一致したフレームには、拒否アクションまたは許可アクションが適用されます。

1 つのポートまたは 1 つの ACL に設定できる ACE は最大 256 個です。

パケットが ACE フィルタに一致すると、システムによりその ACE のアクションが実行され、ACL の処理が停止されます。パケットが ACE フィルタに一致しない場合、次の ACE が処理されます。どの ACE フィルタにも一致することなく ACL のすべての ACE が処理された場合、別の ACL が存在するときは、その ACL が同様に処理されます。

NOTE 関連するすべての ACL のどの ACE にも一致しなかった場合、パケットはドロップされます（デフォルトアクション）。このようにデフォルトではドロップアクションが実行されるため、デバイス自体に送信される管理トラフィック（HTTP/SNMP/Telnet）など、必要なトラフィックを許可する ACE を ACL に明示的に追加する必要があります。例えば、ACL の条件に一致しなかったすべてのパケットが破棄されないようにするには、すべてのトラフィックを許可する最低優先度の ACE を ACL に明示的に追加する必要があります。

ACL がバインドされているポートで IGMP/MLD を有効にする場合は、IGMP/MLD パケットをデバイスに転送する ACE フィルタを ACL に追加します。そうしないと、そのポートで IGMP/MLD スヌーピングが失敗します。

ACL 内の ACE はファーストフィット方式で適用されるため、その順序が重要になります。ACE は、最初の ACE から順に処理されます。

ACL は、例えば特定のトラフィックフローを許可または拒否することによりセキュリティを確保する目的で使用できる他、QoS 拡張モードでのトラフィックの分類や優先度設定にも使用できます。

NOTE セキュリティを確保する手段として、ACL および拡張 QoS ポリシーの両方をポートに設定することはできません。

各ポートに設定できる ACL は 1 つのみです。ただし、IP ベースの ACL および IPv6 ベースの ACL の両方を 1 つのポートに関連付けることは可能です。

1 つ以上の ACL をポートに関連付けるには、1 つ以上のクラスマップが割り当てられたポリシーを使用する必要があります。

[ACL 設定ウィザード] ページでは、フレームヘッダのどの部分を調べるかに応じて以下のタイプの ACL を指定できます。

- IPv4 — IP フレームのレイヤ 3 レイヤを調べます。[ACL 設定ウィザード] ページの *[IPv4 ベースの ACL]* ステップで設定します。
- IPv6 — IPv4 フレームのレイヤ 3 レイヤを調べます。[ACL 設定ウィザード] ページの *[Defining IPv6-Based ACL]* ステップで設定します。
- MAC — レイヤ 2 フィールドのみを調べます。[ACL 設定ウィザード] ページの *[Defining MAC-based ACLs]* ステップで設定します。

ACL 内のフィルタに一致したフレームは、その ACL の名前を持つフローとして指定されます。拡張 QoS では、これらのフレームをこのフロー名で参照することができ、これらのフレームに対して QoS を適用できます。

7.1.1 ACL ログ収集

ACE にログ収集オプションを追加できます。このオプションを有効にすると、ACE によってパケットが許可または拒否されると、そのパケットに関連する情報 SYSLOG メッセージが生成されます。

ACL ログ収集は、ACL をインタフェースにバインドすることにより、インタフェースごとに有効にできます。この場合、インタフェースに関連付けられた許可または拒否 ACE に一致したパケットについて SYSLOG が生成されます。

以下のように、フローは同じ特性を持つパケットのストリームとして設定されます。

- **レイヤ 2 のパケット** — 送信元および宛先 MAC アドレスが同一
- **レイヤ 3 のパケット** — 送信元および宛先 IP アドレスが同一
- **レイヤ 4 のパケット** — 送信元および宛先 IP および L4 ポートが同一

すべての新しいフローについて、特定のインタフェースから最初のパケットがトラップされると、情報 SYSLOG メッセージが生成されます。同じフローの以降のパケットは CPU にトラップされますが、このフローに関する SYSLOG メッセージは 5 分ごとに 1 つに制限されます。この SYSLOG により、過去 5 分間で少なくとも 1 つのパケットがトラップされたことが通知されます。

トラップされたパケットの処理後、パケットは、許可の場合は転送され、拒否の場合は破棄されます。

7.1.1.1 SYSLOG

SYSLOG メッセージは、パケットが拒否ルールまたは許可ルールに一致したことを通知する、重大度が情報レベルのメッセージです。

- レイヤ 2 のパケットの場合、SYSLOG には、送信元 / 宛先 MAC、イーサタイプ、VLAN-ID、CoS キューなど、該当する情報が含まれます。
- レイヤ 3 のパケットの場合、SYSLOG には、送信元 / 宛先 IP アドレス、プロトコル、DSCP 値、ICMP タイプ、ICMP コード、IGMP タイプなど、該当する情報が含まれます。
- レイヤ 4 のパケットの場合、SYSLOG には、送信元ポート、宛先ポート、TCP タグなど、該当する情報が含まれます。

以下に SYSLOG の例を示します。

- IP 以外のパケット：
  - 25-Jun-2018 00:12:05 %3SWCOS-I-LOGDENYMAC: ge1/0/5: deny ACE 00:00:00:00:00:01 -> ff:ff:ff:ff:ff:ff, Ethertype-2054, VLAN-10, CoS-4, trapped
- IP パケット（v4 および v6）：
  - 25-Jun-2018 00:12:05 %3SWCOS-I-LOGDENYINET: ge1/0/5: deny ACE IPv4(255) 1.1.1.1 -> 1.1.1.20, protocol-1, DSCP-54, ICMP Type-Echo Reply, ICMP code-5 , trapped
- L4 パケット：
  - 25-Jun-2018 00:12:05 %3SWCOS-I-LOGDENYINETPORTS: ge1/0/5: deny ACE IPv4(TCP) 1.1.1.1(40) -> 1.1.1.20(50), trapped

7.1.2 ACL の設定方法

このセクションでは、ACL を作成し、その ACL にルール（ACE）を追加する方法について説明します。

7.1.2.1 ACL の作成方法

ACL を作成し、その ACL をインタフェースに関連付ける手順の概要は以下のとおりです。

1. 1 つ以上のタイプの ACL を以下のように作成します。
   a. [ACL 設定ウィザード] ページの [MAC ベースの ACL] ステップおよび [MAC- ベース ACE] ステップで MAC ベースの ACL を作成します。
   b. [ACL 設定ウィザード] ページの [IPv4 ベースの ACL] ステップおよび [IPv4 ベース ACE] ステップで IPv4 ベースの ACL を作成します。
   c. [ACL 設定ウィザード] ページの [IPv6 ベースの ACL] ステップおよび [IPv6 ベース ACE] ステップで IPv6 ベースの ACL を作成します。

2. [ACL バインディング（VLAN）] ページまたは [ACL バインディング（ポート）] ページで ACL をインタフェースに関連付けます。

7.1.2.2 ACL の変更方法

使用されていない ACL は変更することができます。ACL を変更するために ACL をバインド解除する手順の概要は以下のとおりです。

1. ACL が QoS 拡張モードのクラスマップに属していないが、インタフェースに関連付けられている場合、[ACL バインディング（VLAN）] ページまたは [ACL バインディング（ポート）] ページを使用してインタフェースからバインド解除します。

2. ACL がクラスマップの一部であり、インタフェースにバインドされていない場合、その ACL を変更できます。

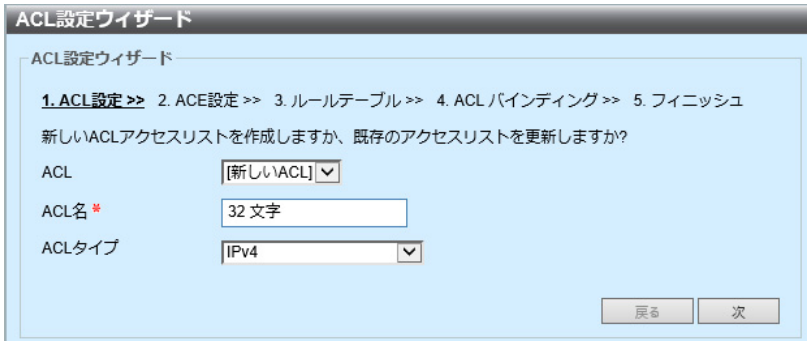
3. ACL がクラスマップの一部であり、そのクラスマップがポリシーに含まれ、そのポリシーがインタフェースにバインドされている場合、以下の一連のバインド解除を実行する必要があります。

- [ACL 設定ウィザード] ページの *[ポリサーバインディング]* ステップで、クラスマップが含まれているポリシーをインタフェースからバインド解除します。
- [ACL 設定ウィザード] ページの *[Configuring a Policy]* ステップで、ACL が含まれているクラスマップをポリシーから削除します。
- [ACL 設定ウィザード] ページの *[Defining Class Mapping]* ステップで、ACL が含まれているクラスマップを削除します。

7.2 ACL 設定ウィザード

新しい ACL を追加 / 変更 / 削除するには：

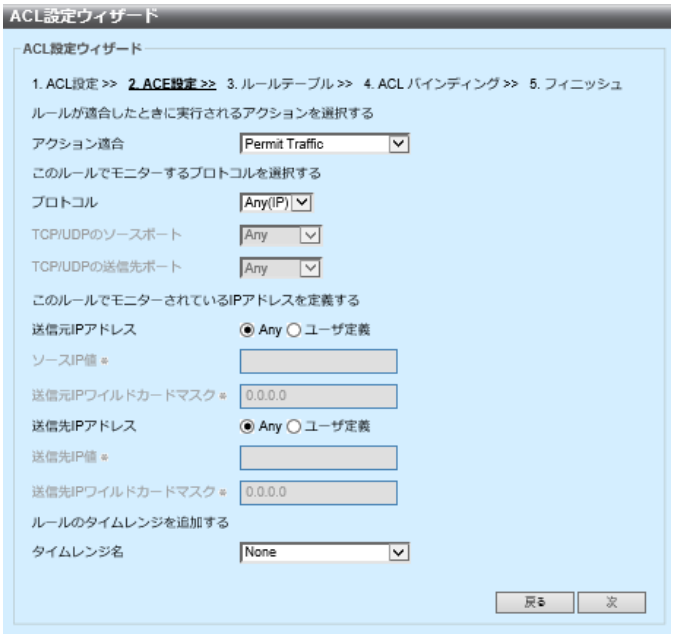
[ACL] > [ACL 設定ウィザード] に進みます。



パラメータ	概要
ACL	この ACL がまだ作成されていない場合は、[新しい ACL] に設定します。
ACL 名	新規 / 既存の ACL の名前を設定します。
ACL タイプ	ACL のタイプとして [IPv4]、[IPv6]、または [MAC] のいずれかを設定します。

[次] を押して 2 番目のステップ **[ACL 設定]** に進みます。

以下のフィールドに入力します。



パラメータ	概要
アクション適合	以下のいずれかのオプションを選択します。 • *[Permit Traffic]* — ACL の基準を満たしているパケットを転送します。 • *[Deny Traffic]* — ACL の基準を満たしているパケットをドロップします。 • *[Shutdown interface]* — ACL の基準を満たしているパケットをドロップし、そのパケットを受信したポートを無効にします。

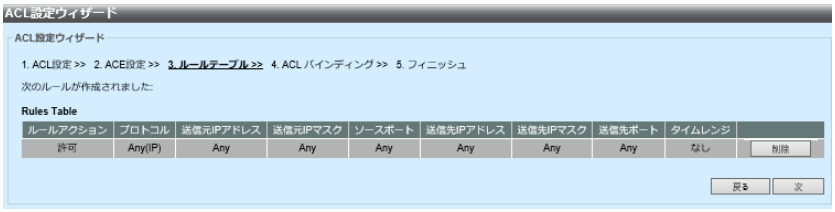
[ACL タイプ] が **[MAC]** の場合、以下のパラメータを入力します。

パラメータ	概要
送信元 MAC アドレス	すべての送信元アドレスを受け入れる場合は [Any] に設定します。送信元アドレスまたは送信元アドレスの範囲を入力する場合は [ユーザ定義] に設定します。
ソース MAC 値	送信元 MAC アドレスと照合する MAC アドレスおよびそのマスク（関連する場合）を入力します。
ソース MAC ワイルドカードマスク	MAC アドレスの範囲を定義するマスクを入力します。
宛先 MAC アドレス	すべての宛先アドレスを受け入れる場合は [任意] に設定します。宛先アドレスまたは宛先アドレスの範囲を入力する場合は [ユーザ定義] に設定します。
送信先 MAC 値	宛先 MAC アドレスと照合する MAC アドレスおよびそのマスク（関連する場合）を入力します。
宛先 MAC ワイルドカードマスク	MAC アドレスの範囲を定義するマスクを入力します。このマスクは、サブネットマスクなど他のマスクとは異なります。ここでは、ビットを 1 に設定した場合は考慮しないことを示し、0 に設定した場合はその値をマスクすることを示します。 注：例えば、0000 0000 0000 0000 0000 0000 1111 1111 というマスクがあるとします。このマスクでは、0 の位置にあるビットでは照合し、1 の位置にあるビットでは照合しないことを意味します。1 のビットは 10 進整数に変換する必要があり、4 つのゼロに対して 0 を記述します。この例では、1111 1111 = 255 であるため、マスクは 0.0.0.255 として記述されます。
タイムレンジ名	**タイムレンジ**を設定する場合、使用するタイムレンジを選択します。タイムレンジは、システムの [時間範囲] ページで指定します。このフィールドは、タイムレンジが作成されている場合にのみ表示されます。

[ACL タイプ] を [IPv4]/[IPv6] に設定した場合、以下のパラメータを入力します。

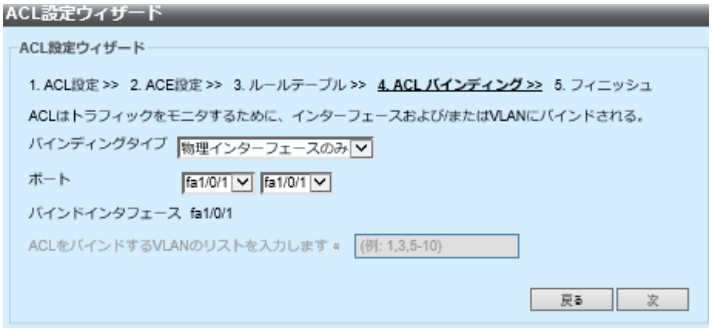
パラメータ	概要
プロトコル	特定のプロトコルに基づいて ACL を作成するには、以下のいずれかのオプションを選択します。 • *[Any(IP)]* — すべての IP プロトコルパケットを受け入れます。 • *[TCP]* — TCP（Transmission Control Protocol）パケットを受け入れます。 • *[UDP]* — UDP（User Datagram Protocol）パケットを受け入れます。 • *[ICMP]* — ICMP プロトコルパケットを受け入れます。 • *[IGMP]* — IGMP プロトコルパケットを受け入れます。
TCP/UDP のソースポート	ドロップダウンリストからポートを設定します。
TCP/UDP の送信先ポート	ドロップダウンリストからポートを設定します。
送信元 IP アドレス	すべての送信元アドレスを受け入れる場合は *[Any]* に設定します。送信元アドレスまたは送信元アドレスの範囲を入力する場合は *[ユーザ定義]* に設定します。
ソース IP 値	送信元 IP アドレスと照合する IP アドレスを入力します。
送信元 IP ワイルドカードマスク	IP アドレスの範囲を定義するマスクを入力します。このマスクは、サブネットマスクなど他のマスクとは異なります。ここでは、ビットを 1 に設定した場合は考慮しないことを示し、0 に設定した場合はその値をマスクすることを示します。
送信先 IP アドレス	すべての送信元アドレスを受け入れる場合は *[Any]* に設定します。送信元アドレスまたは送信元アドレスの範囲を入力する場合は *[ユーザ定義]* に設定します。
送信先 IP 値	送信元 IP アドレスと照合する IP アドレスを入力します。
送信先 IP ワイルドカードマスク	IP アドレスの範囲を定義するマスクを入力します。このマスクは、サブネットマスクなど他のマスクとは異なります。ここでは、ビットを 1 に設定した場合は考慮しないことを示し、0 に設定した場合はその値をマスクすることを示します。
タイムレンジ名	**タイムレンジ**を選択する場合、使用するタイムレンジを選択します。タイムレンジはシステムの [時間範囲] ページで定義します。このフィールドは、タイムレンジが作成されている場合にのみ表示されます。

[次] を押して 3 番目のステップ **[ルールテーブル]** に進みます。



ACL および ACE の作成を確定します。作成しない場合は、**[削除]** を押します。

[次] を押して 4 番目のステップ **[ACL バインディング]** に進みます。



- **[バインディングタイプ]** — ACL のバインド先として以下のいずれかのオプションを設定します。
  - *[物理インターフェースのみ]* — ACL をポートにバインドします。この場合、ACL のバインド先ポート（1 つまたは複数）を設定します。
  - *[VLAN のみ]* — ACL を VLAN にバインドします。**[ACL をバインドする VLAN のリストを入力します]** フィールドに VLAN のリストを入力します。
  - *[バインディングなし]* — ACL をバインドしません。

[次] を押して最後のステップ [フィニッシュ] に進みます。

[次] または **[ACL Configuration step]** を押してランニングコンフィグレーションファイルを更新し、引き続き別の ACL を設定します。

7.3 ACL バインディング

ACL をインタフェース（ポート、LAG、または VLAN）にバインドすると、ACL の ACE ルールが、そのインタフェースに着信するパケットに適用されます。ACL のどの ACE にも一致しなかったパケットは、デフォルトルールと照合され、このルールに一致しなかったパケットにはドロップアクションが実行されます。

インタフェースにバインドできる ACL は 1 つのみです。ただし、複数の ACL を 1 つのポリシーマップにグループ化し、そのポリシーマップをインタフェースにバインドすることにより、複数の ACL を同じインタフェースにバインドすることも可能です。

インタフェースにバインドした ACL は、ACL のバインド先のすべてのポートまたはその ACL が使用されているすべてのポートからその ACL を削除するまで変更（修正 / 削除）できません。

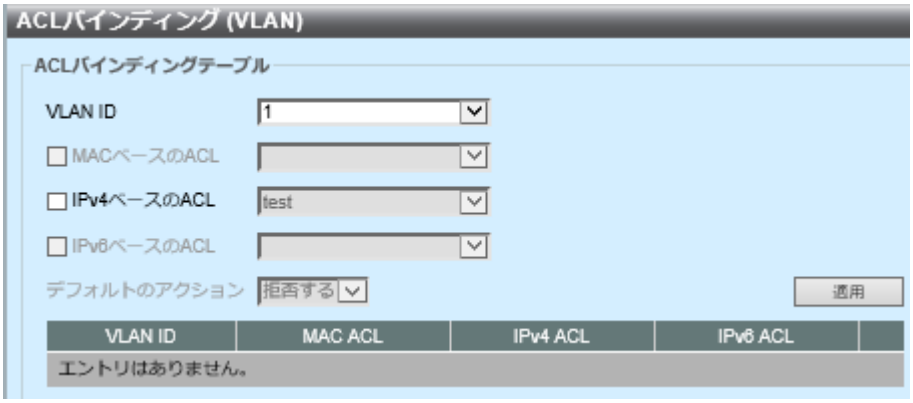
NOTE インタフェース（ポート、LAG、または VLAN）にはポリシーまたは ACL をバインドできますが、ポリシーと ACL の両方をバインドすることはできません。

NOTE 同じクラスマップ内では、MAC ACL と、フィルタリング条件として宛先 IPv6 アドレスを持つ IPv6 ACE とを組み合わせて使用することはできません。

7.3.1 ACL バインディング（VLAN）

ACL を VLAN にバインドするには：

[ACL] > [ACL バインディング (VLAN)] に進みます。



VLAN ID を設定します。

VLAN ID を 1 つの ACL ルールとして設定します。

パラメータ	概要
MAC ベースの ACL	インタフェースにバインドする MAC ベースの ACL を設定します。
IPv4 ベースの ACL	インタフェースにバインドする IPv4 ベースの ACL を設定します。
IPv6 ベースの ACL	インタフェースにバインドする IPv6 ベースの ACL を設定します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

7.3.2 ACL バインディング（ポート）

入力または出力 ACL をポートまたは **LAG** にバインドするには：

[ACL] > [ACL バインディング (ポート)] に進みます。

インタフェースタイプとして **[ポート]/[LAG]** を設定します。

設定したインタフェースのタイプに応じて、そのタイプのすべてのインタフェースと、各インタフェースに現在バインドされている**入力 ACL/ 出力 ACL** のリストが表示されます。

パラメータ	概要
ポート	ACL が定義されているインタフェースの識別子。
MAC ベースの ACL	インタフェースにバインドされている MAC タイプの ACL（存在する場合）。
IPv4 ベースの ACL	インタフェースにバインドされている IPv4 タイプの ACL（存在する場合）。
IPv6 ベースの ACL	インタフェースにバインドされている IPv6 タイプの ACL（存在する場合）。

入力および出力 ACL について以下の情報を入力します。

入力 ACL

パラメータ	概要
MAC ベースの ACL	インタフェースにバインドする MAC ベースの ACL を設定します。
IPv4 ベースの ACL	インタフェースにバインドする IPv4 ベースの ACL を設定します。
IPv6 ベースの ACL	インタフェースにバインドする IPv6 ベースの ACL を設定します。
デフォルトのアクション	以下のいずれかのオプションを設定します。

出力 ACL

パラメータ	概要
MAC ベースの ACL	インタフェースにバインドする MAC ベースの ACL を設定します。
IPv4 ベースの ACL	インタフェースにバインドする IPv4 ベースの ACL を設定します。
IPv6 ベースの ACL	インタフェースにバインドする IPv6 ベースの ACL を設定します。

[適用] を押してランニングコンフィグレーションファイルを更新します。

NOTE ACL を選択しない場合、そのインタフェースにバインドされていた ACL がバインド解除されます。

8 セキュリティ

本章では、デバイスのセキュリティとアクセスコントロールについて説明します。
システムでは、さまざまなタイプのセキュリティを扱っています。

8.1 TACACS+ クライアント

デバイスのセキュリティを一元化するために、TACACS+（*Terminal Access Controller Access Control System*）サーバを設置できます。
このようにして、1 台のサーバで組織内のすべてのデバイスの認証と承認を処理できます。

以下のサービスが、TACACS+ サーバを使用する TACACS+ クライアントとして機能します。

パラメータ	概要
認証	ユーザ名とユーザ定義のパスワードを使用して、ユーザがデバイスにログオンする際の認証を行います。
承認	ログイン時に実行します。認証セッションが完了すると、認証済みユーザ名を用いた承認セッションが開始します。TACACS+ サーバがユーザレベルをチェックします。
Accounting	TACACS+ サーバを使用するログインセッションのアカウンティングを有効にします。システム管理者が、TACACS+ サーバからアカウンティングレポートを生成できます。

認証サービスと承認サービスの提供以外にも、TACACS+ プロトコルによる TACACS ボディメッセージの暗号化を通じて、TACACS メッセージが確実に保護されます。

TACACS+ では、IPv4 のみがサポートされています。

TACACS+ サーバがシングルコネクションをサポートしていない場合、デバイスは多重接続に戻ります。シングルコネクションをサポートしている場合、デバイスはシングルコネクションでのすべての情報を受信できます。

8.1.1 TACACS+ サーバを使用するアカウンティング

ユーザは、RADIUS サーバまたは TACACS+ サーバを使用するログインセッションのアカウンティングを有効にできます。

TACACS+ サーバによるアカウンティングに使用する TCP ポートはユーザが設定可能であり、TACACS+ サーバによる認証および承認に使用される TCP ポートと同じものです。

ユーザがログインまたはログアウトすると、以下の情報が TACACS+ サーバに送信されます。

パラメータ	概要	メッセージ（開始）	メッセージ（停止）
task_id	一意のアカウンティングセッション識別子	Yes	Yes
user	ログイン認証時に入力するユーザ名	Yes	Yes
rem-addr	ユーザの P アドレス	Yes	Yes
elapsed-time	ユーザがログインしていた時間を示します。	Yes	Yes
reason	セッションが終了した理由を報告します。	Yes	Yes

8.1.2 デフォルト設定

- デフォルトとして定義されている TACACS+ サーバはありません。
- TACACS+ サーバが設定されていた場合、アカウンティング機能はデフォルトで無効になります。

8.1.3 その他の機能の競合

RADIUS サーバと TACACS+ サーバの両方でアカウンティングを有効にすることはできません。

8.1.4 TACACS+ サーバの使用方法

TACACS+ サーバを使用するには：

TACACS+ サーバにユーザアカウントを作成します。

[TACACS+ クライアント] ページで、その他のパラメータとともに TACACS+ サーバを設定します。

NOTE 1 つまたは複数の TACACS+ サーバが設定済みの場合、デバイスは利用可能な TACACS+ サーバの設定済み優先度を使用して、デバイスで使用する TACACS+ サーバを選択します。

8.1.5 TACACS+ クライアント

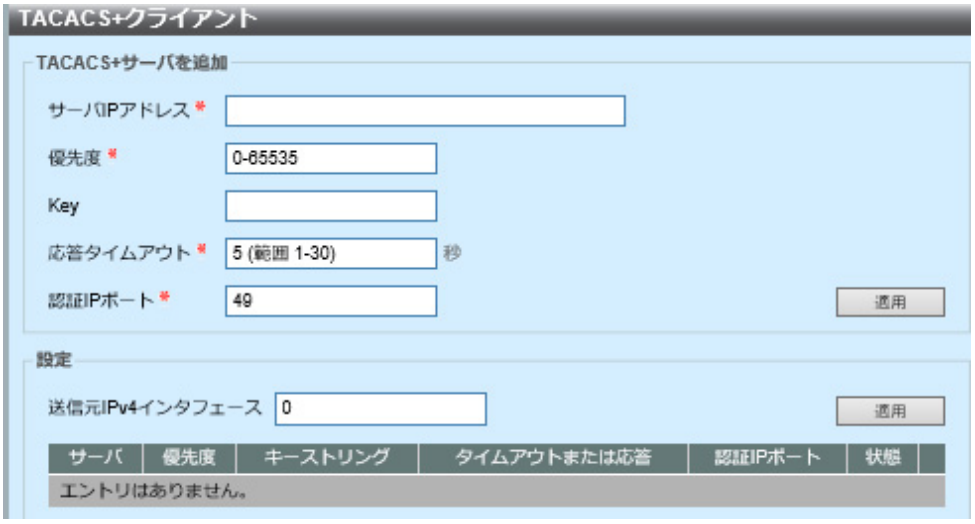
このページで、TACACS+ サーバを設定できます。

デバイスを管理できるのは、TACACS+ サーバに対してユーザレベル 15 を持つユーザだけです。
ユーザレベル 15 は、TACACS+ サーバのユーザまたはユーザグループに付与されます。ユーザ定義 / グループ定義で、以下の文字列を指定します。

```
service = exec {
priv-lvl = 15
}
```

TACACS+ サーバのパラメータを設定するには：

[セキュリティ] > [TACACS+ クライアント] に進みます。



パラメータ	概要
サーバ IP アドレス	TACACS+ サーバの IP アドレスを入力します。
優先度	対象の TACACS+ サーバを使用する順番を入力します。 TACACS+ サーバの最も高い優先度はゼロです。ゼロを指定した TACACS+ サーバが一番に使用されます。優先度の高いサーバとのセッションが確立できない場合、デバイスは次に優先度の高いサーバとのセッションの確立を試みます。

パラメータ	概要
Key	デバイスと TACACS+ サーバ間で認証および暗号化を実行する際に使用する、デフォルトのキー文字列を入力します。このキー文字列は、TACACS+ サーバ上の文字列と同じものとします。 キー文字列は、MD5 を用いた通信の暗号化に使用します。デバイスのデフォルトのキーを選択できます。あるいは、**プレーンテキスト**形式でキーを入力し、**[適用]** をクリックします。暗号化されたキー文字列が生成、表示されます。 ここで入力したキー文字列は、デフォルトのキー文字列よりも優先されます（メインページでデバイスに定義済みの場合）。
応答タイムアウト	デバイスと TACACS+ サーバ間の接続がタイムアウトするまでの時間を入力します。
認証 IP ポート	TACACS+ セッションが発生するポート番号を入力します。

[適用] を押して TACACS+ サーバを追加し、ランニングコンフィグレーションファイルを更新します。

設定を編集するには、**ソース ID** を入力し、**[編集]** をクリックします。

[適用] を押してランニングコンフィグレーションファイルを更新します。

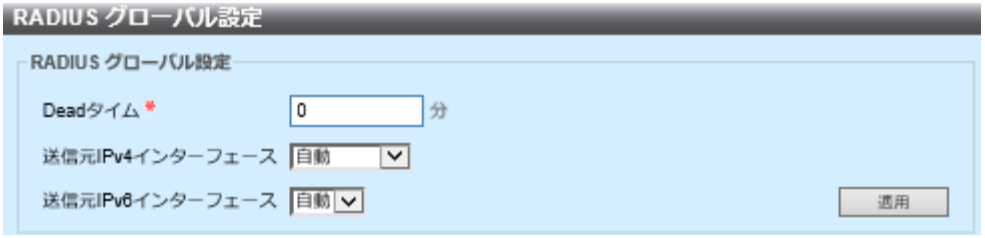
8.2 RADIUS

RADIUS（Remote Authentication Dial-In User Service）サーバが、802.1X または MAC ベースの一元化されたネットワークアクセスコントロールを提供します。

デバイスは、RADIUS サーバを使用して一元化されたセキュリティを提供できる RADIUS クライアントとしても、RADIUS サーバとしても設定できます。

8.2.1 RADIUS グローバル設定

[セキュリティ] > [RADIUS グローバル設定] に進みます。



デフォルトの RADIUS パラメータを入力すると、すべてのサーバに適用されます。

特定のサーバに値が入力されていない場合（[RADIUS サーバを追加する] ページで）、このフィールドの値をデバイスは使用します。

パラメータ	概要
Dead タイム	サービス要求時に無応答の RADIUS サーバがバイパスされるまでの時間を分で入力します（0 を設定した場合、サーバはバイパスされません）。
送信元 IPv4 インターフェース	RADIUS サーバとの通信のメッセージに使用されるデバイスの IPv4 送信元インタフェースを設定します。
送信元 IPv6 インターフェース	RADIUS サーバとの通信のメッセージに使用されるデバイスの IPv6 送信元インタフェースを設定します。 注：[自動] オプションを選択した場合、送信インタフェースで指定されている IP アドレスから送信元 IP アドレスが取得されます。

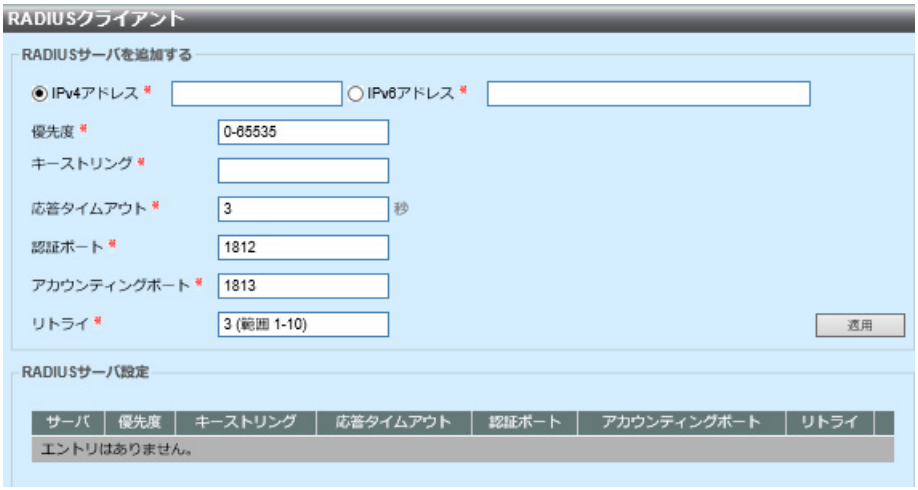
[適用] を押してランニングコンフィグレーションファイルのグローバル設定を更新します。

8.2.2 RADIUS クライアント

RADIUS クライアントとして設定できます。
設定には、下記の GUI ページを使用します。

追加する RADIUS サーバの値を設定するには：

[セキュリティ] > [RADIUS クライアント] に進みます。



パラメータ	概要
IPv4 アドレス	RADIUS サーバの IPv4 アドレスを設定します。
IPv6 アドレス	IPv6 アドレスタイプを設定します（IPv6 使用時）。以下のオプションがあります。 • *リンクローカル* — IPv6 アドレスが単一のネットワークリンク上でホストを一意に識別します。リンクローカルアドレスには **FE80** というプレフィックスが付きます。リンクローカルアドレスはローカルネットワークでの通信にのみ使用できるアドレスであり、このアドレス宛てのパケットはルーティングされません。 • *グローバル* — IPv6 アドレスは、他のネットワークからのアクセスが可能なグローバルユニキャストの IPv6 タイプです。
優先度	サーバの優先度を入力します（0 が最も高い優先度です）。優先度によって、ユーザ認証のためにデバイスがサーバへの接続を試みる順番が決まります。デバイスは、優先度の最も高い RADIUS サーバへの接続を一番に開始します。
キーストリング	デバイスと RADIUS サーバ間で通信の認証および暗号化を実行する際に使用する、キー文字列を入力します。キー文字列には、RADIUS サーバ上の文字列と同じものを使用してください（**プレーンテキスト**形式もサポートします）。

パラメータ	概要
応答タイムアウト	RADIUS サーバからの応答をデバイスが待機する時間を秒で入力します。この時間を経過すると、クエリが再試行されるか、再試行回数が最大数に達した場合には次のサーバに切り替わります。
認証ポート	認証リクエスト用に、RADIUS サーバポートの UDP ポート番号を入力します。
アカウンティングポート	アカウンティングリクエスト用に、RADIUS サーバポートの UDP ポート番号を入力します。
リトライ	失敗が起きたと判断されるまでに RADIUS サーバに送信されるリクエストの数を入力します。

[適用] を押して RADIUS サーバ設定を追加し、ランニングコンフィグレーションファイルを更新します。

8.3 SSL サーバ

以下に、SSL（Secure Socket Layer）機能について説明します。

8.3.1 SSL について

HTTPS セッションを有効にする場合に、SSL サーバを設定できます。HTTPS セッションは、デバイスにあるデフォルトの証明書で開くことができます。

デフォルトの証明書を使用する場合、ブラウザによっては警告が表示されます。これは、この証明書に CA（Certification Authority）の署名がないからです。信頼できる CA の署名入りの証明書を使用することをお勧めします。

ユーザが作成した HTTPS セッションの証明書を開くには：

1. 証明書を生成します。
2. CA の認可を得ます。
3. 署名済みの証明書をデバイスにインポートします。

デバイスにはデフォルトの証明書があり、これを編集することもできます。

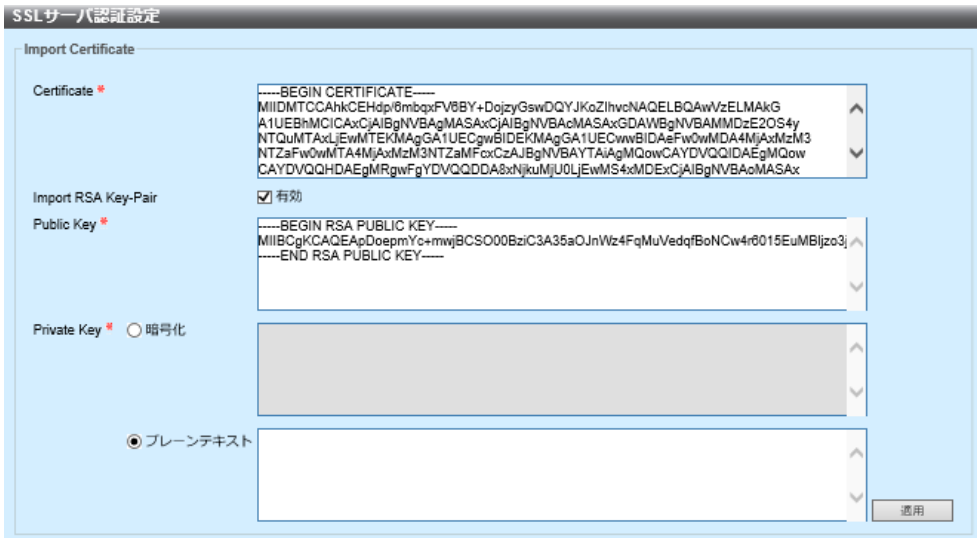
HTTPS はデフォルトで有効です。

8.3.2 SSL サーバ認証設定

デバイスにあるデフォルトの証明書の代わりに、新しい証明書の生成が必要になることがあります。

証明書をインポートするには：

[セキュリティ] > [SSL サーバ] > [SSL サーバ認証設定] に進みます。



[Import Certificate] で、[Certificate] に証明書の情報を入力します。

パラメータ	概要
Import RSA Key-Pair	新しい RSA キーペアでのコピーを有効にするよう設定します。
Public Key	RSA 公開鍵でコピーします。
Private Key	暗号化形式またはプレーンテキスト形式の情報を入力します。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.4 SSH サーバ

このセクションでは、デバイス上で SSH セッションを確立する方法を説明します。

8.4.1 はじめに

この機能を使用すれば、デバイスへの SSH セッションをリモートで確立できます。この機能は TELNET に似ていますが、SSH セッションが保護される点が異なります。

SSH サーバに関して言えば、デバイスはパスワードまたは公開鍵でリモートユーザを認証する SSH ユーザ認証をサポートしています。同時に、このユーザは SSH クライアントであるため、SSH サーバ認証を利用して、デバイスの公開鍵によるデバイス認証を行うこともできます。

SSH サーバで運用可能なモードを以下に示します。

パラメータ	概要
Internal Key (RSA/DSA) (デフォルト設定)	RSA キーおよび DSA キーが生成されます。ユーザは SSH サーバアプリケーションにログオンすると自動的に認証され、デバイスの IP アドレスを入力することによりデバイス上でセッションが開きます。
Public Key	外部の SSH サーバアプリケーション（PuTTY など）で RSA/DSA キーが生成されます。公開鍵がデバイスに入力されます。ユーザは外部の SSH サーバアプリケーションを使用して、デバイス上で SSH セッションを開くことができます。

8.4.2 SSH ユーザ認証

このページでは、公開鍵やパスワードによる SSH ユーザ認証を有効にします。ユーザは公開鍵を使用して SSH サーバを確立する場合、ユーザ名と公開鍵を SSH ユーザ認証テーブルに入力する必要があります。パスワードを使用して SSH セッションを確立する場合は、管理アクセスを持つユーザのユーザ名とパスワードが必要になります。

ユーザを追加するには、外部の SSH キー生成 / クライアントアプリケーション（PuTTY など）を使用して、ユーザの RSA キーまたは DSA キーを事前に生成しておく必要があります。

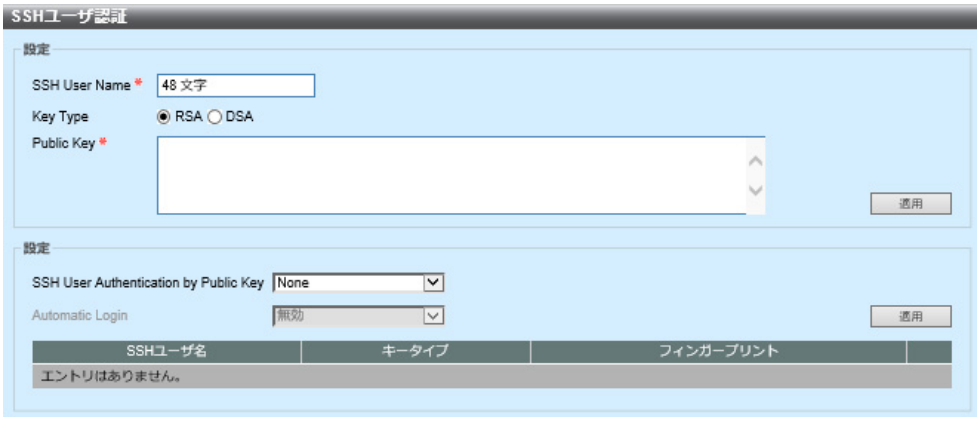
[SSH ユーザ認証] ページを使用して、ローカルユーザデータベースで設定済みのユーザの SSH ユーザ名を作成する場合、自動ログイン機能を設定することによって、追加の認証を回避できます。自動ログイン機能の動作を以下に示します。

パラメータ	概要
有効	ローカルデータベースにユーザが定義されており、このユーザが公開鍵を使って SSH 認証を渡す場合、ローカルデータベースのユーザ名とパスワードによる認証がスキップされます。 注： このような特定の管理方法（コンソール、Telnet、SSH など）に対応する設定済みの認証方式は、ローカル（つまり、*RADIUS*、*TACACS+* 以外）でなければなりません。
無効	SSH 公開鍵による認証が成功した後は、ローカルユーザデータベースにユーザ名が設定されている場合でも、設定済みの認証方式に従ってユーザは再度認証されます。

このページはオプションです。SSH でユーザ認証を処理する必要はありません。

認証を有効にしてユーザを追加するには：

[セキュリティ] > [SSH サーバ > [SSH ユーザ認証] に進みます。



以下のパラメータを設定できます。

パラメータ	概要
SSH User Name	ユーザのユーザ名
Key Type	RSA キーか DSA キーを選択します。
Public Key	公開鍵から生成したフィンガープリント

[適用] を押して新しいユーザを保存します。

[SSH User Authentication by Public Key] フィールドを設定します。

パラメータ	概要
None	認証方式なしで設定します。
パスワード	ローカルデータベースに設定されているユーザ名 / パスワードを使用して SSH クライアントユーザの認証を実行するよう、設定します。
キー	公開鍵を使用して SSH クライアントユーザの認証を実行するよう、設定します。
Automatic Login	**[SSH ユーザ認証]** で **[キー]** を設定した場合に、有効になります。

[Automatic Login] フィールドを設定します。
このフィールドは、**[SSH User Authentication by Public Key]** のパラメータが **[キー]** の時に有効になります。

[適用] を押してランニングコンフィグレーションファイルを更新します。

8.5 (予約)

(将来の追加機能のための予約ページです。)

8.6 ストームコントロール設定

フレームは複製されます。また、ブロードキャスト、マルチキャスト、または未知のユニキャストのフレームが受信されると、使用可能なすべての出口ポートにコピーが送信されます。送信先は、関連する VLAN に属するすべてのポートです。このように、1 つの受信フレームから多数のコピーが送信されることで、トラフィックストームが発生する可能性があります。

ストーム保護によって、デバイスが受信するフレームの数を制限できます。また、この制限値に考慮されるフレームのタイプを指定します。

ブロードキャスト、マルチキャスト、または未知のユニキャストのフレームのレートがユーザ定義の閾値よりも高い場合、その閾値を超えて受信したフレームは破棄されます。

ストームコントロールを設定するには：

[セキュリティ] > [ストームコントロール設定] に進みます。

パラメータ	概要
ポート	ストームコントロールを有効にするポートを設定します。
アクション（ポートでストームが発生した後）	• *なし* — アクションなし • *通知* — トラップを送信 • *破棄* — パッケージを破棄
タイプ	• *ユニキャスト* — ユニキャストパケットに対するストームコントロールを有効に設定します。 • *マルチキャスト* — マルチキャストパケットに対するストームコントロールを有効に設定します。 • *ブロードキャスト* — ブロードキャストパケットに対するストームコントロールを有効に設定します。
レートタイプ	• *By K ビット / 秒* — 閾値を K ビット / 秒で設定します。 • *By パーセンテージ*— 閾値をパーセンテージで設定します。
レート閾値	未知のパケットを転送できる最大レートを入力します。この値は、K ビット / 秒または利用可能な帯域幅の合計のパーセンテージで入力できます。

[適用] を押して、変更したストームコントロールを適用し、ランニングコンフィグレーションファイルを更新します。

8.7 ポートセキュリティ

> **NOTE** 802.1X が有効なポートまたは SPAN 宛先と定義されたポートでは、ポートセキュリティを有効にすることはできません。

ポートへのアクセスを特定の MAC アドレスを持つユーザに限定することによって、ネットワークセキュリティが向上します。MAC アドレスは、スタティックに設定するか、またはダイナミックに学習することが可能です。

ポートセキュリティによって、受信したパケットおよび学習したパケットを監視します。ロックされたポートへのアクセスは、特定の MAC アドレスを持つユーザに限られます。

ポートセキュリティには、以下のように 4 つのモードがあります。

パラメータ	概要
Classic Lock	ポートで学習されたすべての MAC アドレスはロックされ、そのポートで新しい MAC アドレスは学習されません。学習されたアドレスは、エージングまたは再学習の対象にはなりません。
Limited Dynamic Lock	デバイスは、許可されたアドレスに設定されている制限値に達するまで MAC アドレスを学習します。制限値に達した後は、追加のアドレスを学習しません。このモードでは、アドレスがエージングおよび再学習の対象となります。
Secure Permanent	ポートに関連付けられている現在のダイナミック MAC アドレスを維持し、ポートで許可されている最大アドレス数（[最大数] で設定）を上限として学習します。再学習とエージングは無効です。
Secure Delete On Reset	ポートに関連付けられている現在のダイナミック MAC アドレスをリセット後に削除します。新しい MAC アドレスはリセット時に削除する MAC アドレスとして学習できます。学習できる MAC アドレスの上限は、対象のポートで許可される最大アドレス数までです。再学習とエージングは無効です。

承認されていないポートで新しい MAC アドレスからのフレームが検出される場合、デバイス保護が起動し、以下のいずれかのアクションがトリガされます（ポートはクラシックにロックされ、新しい MAC アドレスがある。あるいはポートがダイナミックにロックされ、許可されたアドレスの最大数を超過している）。

- フレームの破棄
- フレームの転送
- ポートのシャットダウン

セキュアな MAC アドレスが別のポートにある場合、フレームは転送されますが、そのポートで MAC アドレスは学習されません。

これらのアクション以外にも、トラップの生成、および頻度と回数の制限により、デバイスのオーバーロードを回避できます。

ポートセキュリティを設定するには：

[セキュリティ] > [ポートセキュリティ] に進みます。

パラメータ	概要
ポート	インタフェースのポートまたは LAG を設定します。
状態	ポートのロックを有効 / 無効に設定します。
学習モード	ポートロックのタイプを設定します。このフィールドを設定するには、[状態] がアンロックである必要があります。[学習モード] フィールドは、[状態] フィールドがロックの場合にのみ有効です。[学習モード] を変更するには、インタフェースのロックをクリアする必要があります。モード変更後、インタフェースのロックは元に戻すことができます。以下のオプションがあります。 • *Classic Lock* — 学習済みのアドレスの数に関係なく、即座にポートをロックします。

パラメータ	概要
	• *Limited Dynamic Lock* — ポートに関連付けられている現在のダイナミック MAC アドレスを削除して、ポートをロックします。ポートは、ポートで許可されている最大アドレス数を上限として学習します。MAC アドレスの再学習とエージングは両方とも有効です。 • *Secure Permanent* — ポートに関連付けられている現在のダイナミック MAC アドレスを維持し、ポートで許可されている最大アドレス数（[最大数] で設定）を上限として学習します。再学習とエージングは有効です。 • *Secure Delete On Reset* — ポートに関連付けられている現在のダイナミック MAC アドレスをリセット後に削除します。新しい MAC アドレスはリセット時に削除する MAC アドレスとして学習できます。学習できる MAC アドレスの上限は、対象のポートで許可される最大アドレス数までです。再学習とエージングは無効です。
最大数	リミテッドダイナミックロックの学習モードを選択した場合は、ポートで学習可能な MAC アドレスの最大数を入力します。0 は、スタティックアドレスのみがインタフェースでサポートされていることを示します。
違反時アクション	以下のように、ロックされたポートに到着するパケットに適用するアクションを設定します。 • *パケット破棄* — 学習されていないソースからのパケットを破棄します。 • *パケット転送* — MAC アドレスを学習せずに、未知のソースからのパケットを転送します。 • *ポートシャットダウン* — 学習されていないソースからのパケットを破棄し、ポートをシャットダウンします。ポートは再アクティブ化するまで、あるいはデバイスを再起動するまで、シャットダウンしたままの状態です。
トラップ	ロックされたポートでパケットを受信するときにトラップを有効にするよう設定します。これは、ロック違反と密接に関連しています。クラシックロックの場合、これは受信済みの新しいアドレスです。リミテッドダイナミックロックの場合、これは許可されたアドレス数を超過する新しいアドレスです。
トラップ周波数	次回のトラップまでに経過する最小時間（秒）を入力します。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.8 AAA

8.8.1 AAA 認証設定

AAA 認証設定を行い、設定内容を表示するには：

[セキュリティ] > [AAA] > [AAA 認証設定] に進みます。

[AAA Web 認証設定]、[AAA MAC 認証設定]、[AAA 802.1X 認証設定] のそれぞれで以下のフィールドを設定し、**[適用]** を押します。

パラメータ	概要
プライマリデータベース	プライマリ認証方式。[RADIUS] か [ローカル] を選択します。
セカンダリデータベース	セカンダリ認証方式。プライマリデータベースが [ローカル] の場合、[RADIUS] か [なし]（認証なし）を選択します。 プライマリデータベースが [RADIOS] の場合、[ローカル] か [なし]（認証なし）を選択します。
認証失敗時動作	プライマリで拒否された場合のセカンダリデータベースを使用した認証アクションを設定します。 プライマリデータベースの RADIUS サーバと通信ができない場合、認証失敗時動作の設定に無関係に、セカンダリデータベースの設定に従った動作となります。
認証失敗ブロックタイム	認証が失敗した場合に該当 MAC アドレスの通信をブロックする期間を指定します。

8.8.2 AAA 認証ユーザ設定

AAA 認証ユーザ設定を行い、設定内容を表示するには：

[セキュリティ] > [AAA] > [AAA 認証ユーザ設定] に進みます。

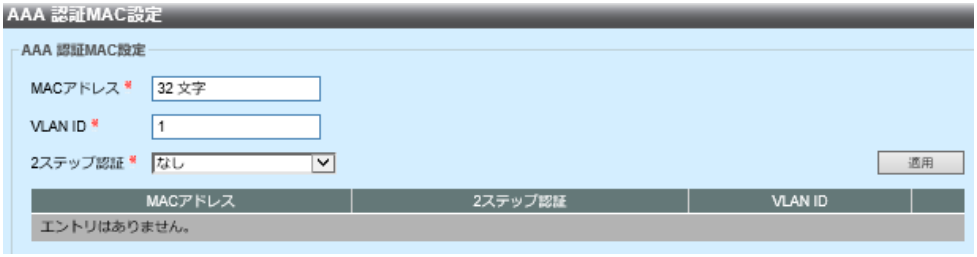
パラメータ	概要
ユーザ名	ローカルユーザアカウントデータベースを設定します。
VLAN ID	VLAN インデックス（1 ～ 4096）
パスワード	ユーザのパスワードをプレーンテキスト形式または暗号化形式で入力します。
認証タイプ	このアカウントを使用するための認証タイプを設定します。 • *両方* — 802.1X 認証と Web 認証の両方を使用 • *802.1x* — 802.1X 認証を使用 • *Web* — Web 認証を使用
2 ステップ認証	2 ステップ認証を有効または無効に設定します。

[適用] を押します。

8.8.3 AAA 認証 MAC 設定

AAA 認証 MAC 設定を行い、設定内容を表示するには：

[セキュリティ] > [AAA] > [AAA 認証 MAC 設定] に進みます。



パラメータ	概要
MAC アドレス	ローカル MAC アドレスデータベースを設定します。
VLAN ID	VLAN インデックス（1 ～ 4096）
2 ステップ認証	2 ステップ認証の次の認証方法を指定します。 **なし** - 次の認証方法を使用しません。 **802.1x** - 次の認証方法として 802.1X 認証を使用します。 **Web** - 次の認証方法として Web 認証を使用します。 **Any** - 次の認証方法として 802.1X と Web による認証を使用します。

[適用] を押します。

8.8.4 認証済みホスト

認証済みホストを表示するには：

[セキュリティ] > [AAA] > [認証済みホスト] に進みます。

パラメータ	概要
ユーザ名	各ポートで認証されたサプリカント名
ポート	ポート番号
時間	サプリカントが認証され、ポートでのアクセスが承認された時間数
認証方式	最後のセッションの認証に使用された方式
MAC アドレス	サプリカントの MAC アドレスを表示します。
VLAN ID	VLAN ID。

8.9 認証

8.9.1 認証ダイナミック VLAN 設定

ダイナミック VLAN 認証設定とゲスト VLAN 設定を行うには：

[認証] > [ダイナミック VLAN 認証設定] に進みます。

[ダイナミック VLAN 許可] で [有効] または [無効] を選択し、
[適用] を押します。

[ポート] を設定します。

[ゲスト VLAN アトリビュート] を [有効] または [無効] に設定します。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

[クリア] を押してゲスト VLAN アトリビュートを無効に戻します。

8.9.2 2 ステップ認証設定

ポートの 2 ステップ認証設定を定義するには：

[認証] > [2 ステップ認証設定] に進みます。

すべてのポートの 2 ステップ認証のパラメータ設定が表示されます。

2 ステップタイムアウト（秒）を入力し、**[適用]** を押します。

[ポート] を設定します。

以下の 2 ステップ方式を有効または無効にします。

パラメータ	概要
MAC-Web	MAC-Web を有効または無効にします。
MAC-802.1X	MAC-802.1X を有効または無効にします。
802.1X-Web	802.1X-Web を有効または無効にします。

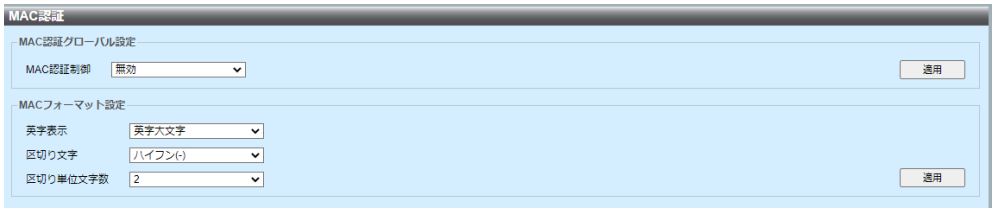
[追加 ...] を押して、ランニングコンフィグレーションファイルを更新します。

[クリア] を押して、ポートの設定をデフォルト値に戻します。

8.10 MAC 認証

MAC 認証設定を行うには：

[セキュリティ] > [MAC 認証] に進みます。



[MAC 認証グローバル設定] で MAC 認証をグローバルに有効または無効にします。
[適用] を押して、ランニングコンフィグレーションファイルを更新します。

[MAC フォーマット設定] で認証するための MAC アドレスの形式について設定を行います。
小文字を使用する場合は [英字表示] を [英字小文字] に設定し、大文字を使用する場合は [英字大文字] に設定します。

[MAC フォーマット設定] で認証するための MAC アドレスの形式について設定を行います。
[英字表示] で MAC アドレスの英字表示を設定します。

パラメータ	概要
英字小文字	小文字を使用します。 たとえば、aa-bb-cc-dd-ee-ff となります。
英字大文字	大文字を使用します。 たとえば、AA-BB-CC-DD-EE-FF となります。

[区切り文字] で MAC アドレス区切り文字の種類を設定します。

パラメータ	概要
ハイフン (-)	区切り文字としてハイフンを使用
コロン (:)	区切り文字としてコロンを使用
ドット (.)	区切り文字としてドットを使用
区切り文字なし	区切り文字を使用しない

[区切り単位文字数] で MAC アドレス区切り文字数を設定します。

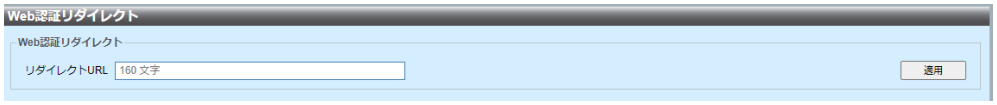
パラメータ	概要
2	MAC アドレスで区切り文字を 5 つ使用します。 たとえば、AA-BB-CC-DD-EE-FF となります。
4	MAC アドレスで区切り文字を 2 つ使用します。 たとえば、AABB-CCDD-EEFF となります。
6	MAC アドレスで区切り文字を 1 つ使用します。 たとえば、AABBCC-DDEEFF となります。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.11 WEB 認証のカスタマイズ

8.11.1 Web 認証リダイレクト

[セキュリティ] > [Web 認証のカスタマイズ] > [Web 認証リダイレクト] に進みます。



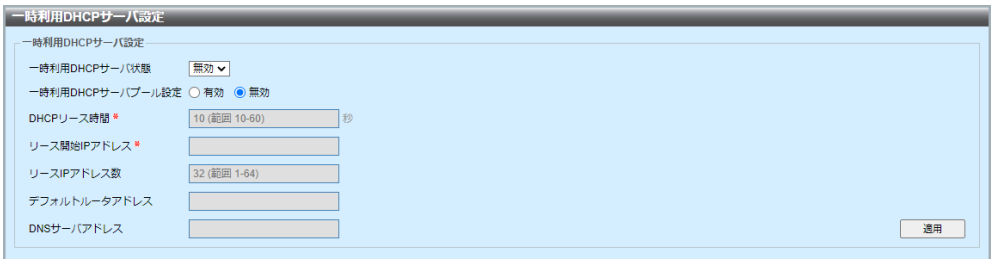
Web 認証のためにリダイレクトする URL を入力します。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.11.2 一時利用 DHCP サーバ設定

一時利用 DHCP サーバ設定を行うには：

[セキュリティ] > [Web 認証のカスタマイズ]>[一時利用 DHCP サーバ設定] に進みます。



一時利用 DHCP サーバを有効にするには [一時利用 DHCP サーバ状態] フィールドで [有効] を選択します。
一時利用 DHCP サーバのプール設定を有効にするには [一時利用 DHCP サーバプール設定] を有効にします。

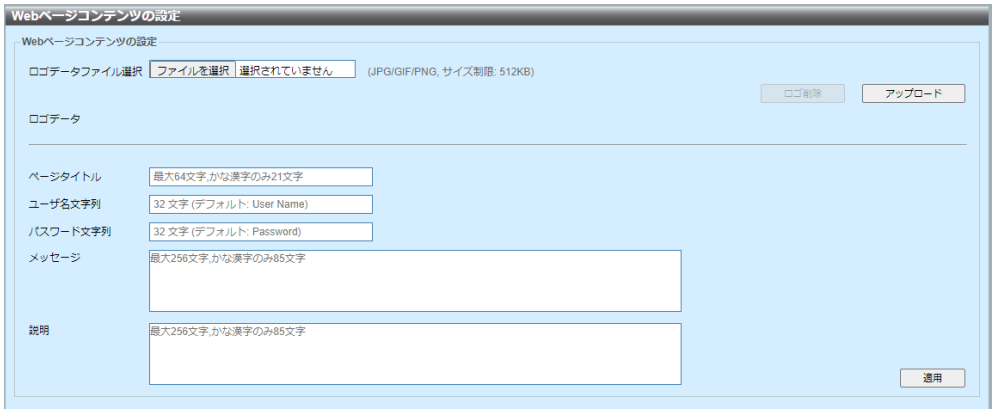
パラメータ	概要
DHCP リース時間	一時利用 DHCP サーバで割り振る IP アドレスのリース時間 (1 ～ 60 秒) を入力します。
リース開始 IP アドレス	リースする IP アドレスの開始アドレスを入力します。
リース IP アドレス数	リースする IP アドレス数 (1 ～ 64) を入力します。
デフォルトルータアドレス	**デフォルトルータアドレスを入力します。**
DNS サーバアドレス	DNS サーバのアドレスを入力します。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.11.3 Web ページコンテンツの設定

Web 認証ログインページのコンテンツの設定を行うには：

[セキュリティ] > [Web 認証のカスタマイズ]>[Web ページコンテンツの設定] に進みます。



ロゴデータファイル選択から Web 認証ログインページで表示するロゴ画像をアップロードまたは削除します。TFTP サーバ経由にて JPG/PNG/GIF 形式の画像データを 512KB まで転送可能です。
WEB ページコンテンツの設定で Web 認証ログインページのコンテンツを設定します。

パラメータ	概要
ページタイトル	WEB 認証ログインページのタイトル文字列を入力します（半角最大 64 文字）。 日本語入力が可能です（最大 21 文字）。
ユーザ名文字列	ユーザ名入力欄の文字列を表示します（工場出荷時設定：User Name）（半角最大 32 文字）。 日本語入力が可能です（最大 10 文字）。
パスワード文字列	パスワード入力欄の文字列を表示します（工場出荷時設定：Password）（半角最大 32 文字）。 日本語入力が可能です（最大 10 文字）。
メッセージ	メッセージ欄の表示テキストを表示します（半角最大 256 文字）。 日本語入力が可能です（最大 85 文字）。
説明	記述欄の表示テキストを表示します（半角最大 256 文字）。 日本語入力が可能です（最大 85 文字）。

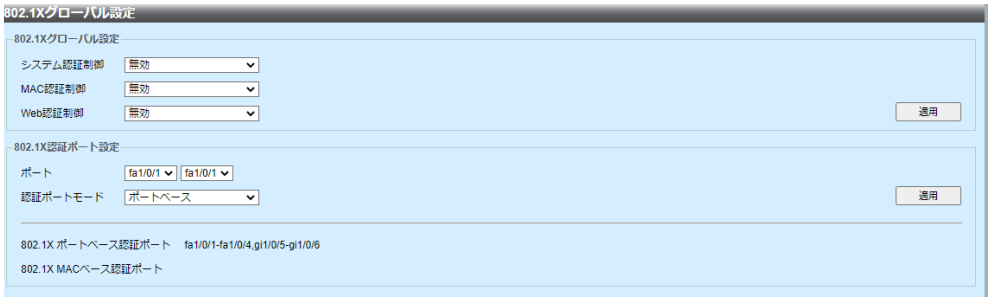
[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.12 802.1X

8.12.1 802.1X グローバル設定

このページでは、802.1X 認証、MAC 認証、WEB 認証のグローバル設定を有効化できます。認証機能は、グローバルにも、各ポート個別にもアクティブ化する必要があります。
また認証ポートのポートモードを変更できます。

[セキュリティ] > [802.1X] > [802.1X グローバル設定] に進みます。



認証機能をグローバルで有効にするためには [システム認証制御] を [有効] に変更し、[適用] を押します。
MAC 認証をグローバルで有効にするためには [MAC 認証制御] を [有効] に変更し、[適用] を押します。
WEB 認証をグローバルで有効にするためには [Web 認証制御] を [有効] に変更し、[適用] を押します。

[ポート] からポートまたはポートの範囲を設定します。

[認証ポートモード] から認証ポートモードを以下のように指定します。

パラメータ	概要
ポートベース	シングルホストモードを有効にします。
MAC ベース	マルチセッションモードを有効にします。

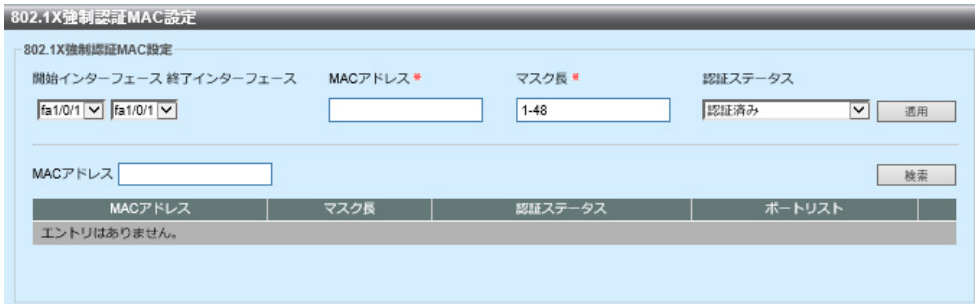
[適用] を押して、ランニングコンフィグレーションファイルを更新します。

NOTE 802.1x とポートセキュリティを同じポートで同時に有効にすることはできません。
インタフェース上でポートセキュリティが有効かつポート制御がオートの場合は、[システム認証制御] の値を [有効] に変更することはできません。

8.12.2 802.1X 強制認証 MAC 設定

インタフェースおよび MAC に 802.1X 強制認証 MAC 設定を指定するには：

[セキュリティ] > [802.1X] > [802.1X 強制認証 MAC 設定] に進みます。



[開始インターフェース] および [終了インターフェース] でインタフェースを選択します。

MAC アドレスとマスク長を設定します。

[認証ステータス] に [認証済み] または [未認証] を指定します。

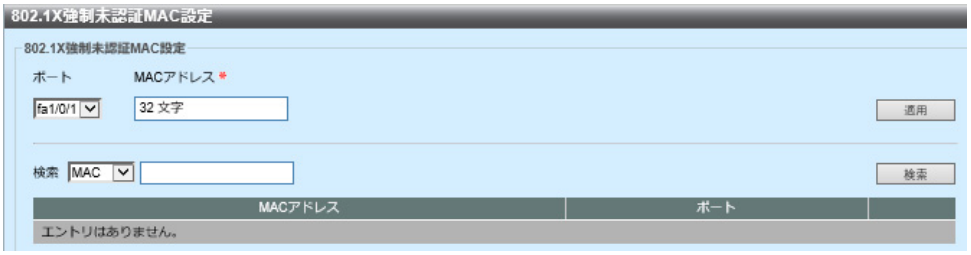
[適用] を押して、ランニングコンフィグレーションファイルを更新します。

MAC アドレスを入力し、次に **[検索]** を押して MAC アドレスによるフィルタリングを行います。

8.12.3 802.1X 未認証 MAC 設定

インタフェースおよび MAC に 802.1X 強制未認証 MAC 設定を指定するには：

[セキュリティ] > [802.1X] > [802.1X 強制未認証 MAC 設定] に進みます。



ポートを選択し、MAC アドレスを指定します。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

MAC アドレスまたはポート番号を入力し、次に **[検索]** を押して MAC アドレスによるフィルタリングを行います。

8.12.4 802.1X ポート設定

各ポートで 802.1X ポート設定を行うことができます。設定変更を行う前にポート制御を強制認証に変える必要があります。これは、ポートが強制認証状態にあるときにしか変更できない設定があるからです（ホスト認証など）。設定が完了したら、ポート制御を前の状態に戻します。

NOTE

802.1x を定義したポートは、LAG のメンバになることはできません。
802.1x とポートセキュリティを同じポートで同時に有効にすることはできません。
インタフェース上でポートセキュリティが有効かつシステム認証制御が有効の場合は、[ポート制御] の値を [オート] に変更することはできません。

802.1X ポート設定を指定するには：

[セキュリティ] > [802.1X] > [802.1X ポート設定] に進みます。

パラメータ	概要
ポート	ポートを設定します。
ホストモード	現在のポート認証状態です。 • *認証済み* – ポートが認証済み、あるいは *[ポート制御]* が *[強制認証]* の状態 • *未認証* – ポートが未認証、あるいは *[ポート制御]* が *[強制未認証]* の状態

パラメータ	概要
ポート制御	管理上のポート認証状態を選択します。以下のオプションがあります。 • *強制未認証* — インタフェースを未認証状態に移行することによって、インタフェースアクセスを拒否します。デバイスは、インタフェースを通じてクライアントに認証サービスを提供しません。 • *オート* — デバイスでのポートベースの認証と承認を有効にします。インタフェースは、デバイスとクライアント間での認証交換に基づき、認証済みと未認証の間で移行します。 • *強制認証* — 認証なしでインタフェースを承認します。
MAC 認証	ポートの MAC 認証機能を有効または無効にします。
Web 認証	ポートの WEB 認証機能を有効または無効にします。
802.1x 手動再認証	サプリカントのポートベースでの手動での再認証を有効に設定します。
802.1X 定期再認証	サプリカントのポートベースでの定期的な再認証を有効に設定します。
MAC ベース手動再認証	サプリカントの MAC アドレスに基づく手動での再認証を有効に設定します。
MAC ベース定期再認証	サプリカントの MAC アドレスに基づく定期的な再認証を有効に設定します。
再認証間隔	選択したポートが再認証されるまでの秒数を入力します。
最大ホスト数	インタフェースで許可されている認証済みホストの最大数を入力します。**[無限]** を選択して制限なしに設定するか、ユーザ定義の制限を設定します。 注： この値を 1 に設定すると、MAC ベース認証のシングルホストモードをマルチセッションモードでシミュレーションできます。
沈黙期間	沈黙期間の長さを入力します。
サプリカントタイムアウト	EAP リクエストがサプリカントに再送信されるまでの秒数を入力します。
サーバタイムアウト	デバイスによるリクエストが認証サーバに再送信されるまでの秒数を入力します。

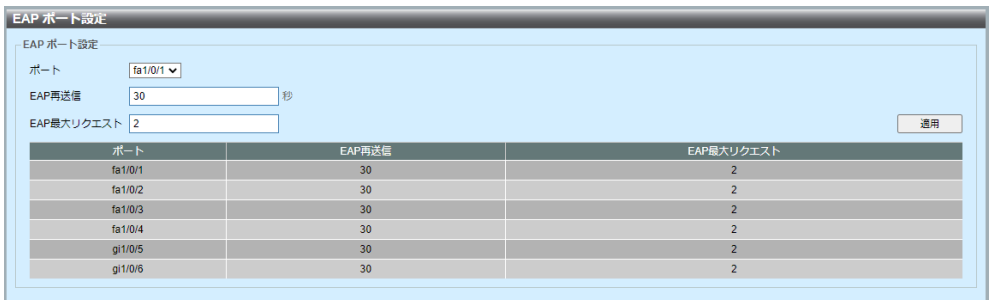
[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.12.5 EAP ポート設定

各ポートで EAP の設定を行うことができます。

ポートの 802.1X EAP 設定を指定するには：

[セキュリティ] > [802.1X] > [EAP ポート設定] に進みます。



パラメータ	概要
ポート	ポート番号を設定します。
EAP 再送信	EAP リクエストを再送する間隔を入力します。
EAP 最大リクエスト	EAP の最大リクエスト数を入力します。

[適用] を押して設定をランニングコンフィグレーションファイルに書き込みます。

8.13 DHCP スヌーピング

8.13.1 はじめに

8.13.1.1 DHCP スヌーピングについて

セキュリティ機構を搭載したデバイスを設定することによって、不正な DHCP 応答パケットの受信を回避し、DHCP アドレスを記録することができます。このため、DHCP スヌーピングでは、デバイスのポートは「信頼できる」か「信頼できない」のいずれかとして扱われます。

信頼できるポートは DHCP サーバに接続され、DHCP アドレスが割り当てられます。信頼できるポートで受信された DHCP メッセージが、デバイスを通過できます。

信頼できないポートには DHCP アドレスを割り当てることができません。デフォルトの設定では、([インタフェース設定] ページで）信頼できると宣言しない限り、すべてのポートが信頼できないものと判断されます。

8.13.1.2 DHCP スヌーピング / リレーとオプション 82 の競合

以下の表に、DHCP スヌーピング / リレーとオプション 82 のさまざまな組み合わせでデバイスがどのように動作するのかを示します。

また、DHCP スヌーピングが有効ではなく、DHCP リレーが有効な場合に、DHCP リクエストパケットがどのように処理されるのかを示します。

	DHCP リレー IP アドレスを設定した VLAN		DHCP リレー IP アドレスを設定していない VLAN	
	オプション 82 のないパケットが到着	オプション 82 が付加されたパケットが到着	オプション 82 のないパケットが到着	オプション 82 が付加されたパケットが到着
オプション 82 挿入無効	オプション 82 のないパケットが送信される	元のオプション 82 でパケットが送信される	リレー – オプション 82 を挿入 ブリッジ – オプション 82 は挿入されない	リレー – パケットを破棄 ブリッジ – 元のオプション 82 でパケットが送信される
オプション 82 挿入有効	リレー – オプション 82 で送信される ブリッジ – オプション 82 は送信されない	元のオプション 82 でパケットが送信される	リレー – オプション 82 で送信される ブリッジ – オプション 82 は送信されない	リレー – パケットを破棄 ブリッジ – 元のオプション 82 でパケットが送信される

DHCP リレーとスヌーピングの両方を有効にする場合に DHCP リクエストパケットがどのように処理されるのかを以下に示します。

	DHCP リレー IP アドレスを設定した VLAN		DHCP リレー IP アドレスを設定していない VLAN	
	オプション 82 のないパケットが到着	オプション 82 が付加されたパケットが到着	オプション 82 のないパケットが到着	オプション 82 が付加されたパケットが到着
オプション 82 挿入無効	オプション 82 のないパケットが送信される	元のオプション 82 でパケットが送信される	リレー – オプション 82 を挿入 ブリッジ – オプション 82 は挿入されない	リレー – パケットを破棄 ブリッジ – 元のオプション 82 でパケットが送信される

	DHCP リレー IP アドレスを設定した VLAN		DHCP リレー IP アドレスを設定していない VLAN	
オプション 82 挿入有効	リレー – オプション 82 で送信される ブリッジ – オプション 82 が追加 (ポートが信頼できる場合は、DHCP スヌーピングが有効でないかのように動作します)	元のオプション 82 でパケットが送信される	リレー – オプション 82 で送信される ブリッジ – オプション 82 が挿入される (ポートが信頼できる場合は、DHCP スヌーピングが有効でないかのように動作します)	リレー – パケットを破棄 ブリッジ – 元のオプション 82 でパケットが送信される

DHCP スヌーピングを無効にする場合に DHCP 応答パケットがどのように処理されるのかを以下に示します。

	DHCP リレー IP アドレスを設定した VLAN		DHCP リレー IP アドレスを設定していない VLAN	
	オプション 82 のないパケットが到着	オプション 82 が付加されたパケットが到着	オプション 82 のないパケットが到着	オプション 82 が付加されたパケットが到着
オプション 82 挿入無効	オプション 82 のないパケットが送信される	元のオプション 82 でパケットが送信される	リレー – オプション 82 を破棄 ブリッジ – オプション 82 のないパケットが送信される	リレー – 1. 応答がデバイスから発生する場合、オプション 82 のないパケットが送信される 2. 応答がデバイスから発生しない場合、パケットは破棄される ブリッジ – 元のオプション 82 でパケットが送信される
オプション 82 挿入有効	リレー – オプション 82 で送信される	リレー – オプション 82 のないパケットが送信される ブリッジ – オプション 82 でパケットが送信される	リレー – オプション 82 を破棄 ブリッジ – オプション 82 のないパケットが送信される	リレー – オプション 82 のないパケットが送信される ブリッジ – オプション 82 でパケットが送信される

DHCP スヌーピングとリレーの両方を有効にする場合に DHCP 応答パケットがどのように処理されるのかを以下に示します。

	DHCP リレー IP アドレスを設定した VLAN		DHCP リレー IP アドレスを設定していない VLAN	
	オプション 82 のないパケットが到着	オプション 82 が付加されたパケットが到着	オプション 82 のないパケットが到着	オプション 82 が付加されたパケットが到着
オプション 82 挿入無効	オプション 82 のないパケットが送信される	元のオプション 82 でパケットが送信される	リレー – オプション 82 を破棄 ブリッジ – オプション 82 のないパケットが送信される	リレー – 1. 応答がデバイスで発生する場合、オプション 82 のないパケットが送信される 2. 応答がデバイスで発生しない場合、パケットは破棄される ブリッジ – 元のオプション 82 でパケットが送信される
オプション 82 挿入有効	オプション 82 のないパケットが送信される	オプション 82 のないパケットが送信される	リレー – オプション 82 を破棄 ブリッジ – オプション 82 のないパケットが送信される	オプション 82 のないパケットが送信される

8.13.1.3 DHCP スヌーピングバインディングデータベース

DHCP スヌーピングによって、データベース（DHCP スヌーピングバインディングデータベース）が構築されます。このデータベースは、信頼できるポートを通じてデバイスに入ってきた DHCP パケットから取得された情報を基にしています。

DHCP スヌーピングバインディングデータベースには、入力ポート、入力 VLAN、クライアントの MAC アドレス、クライアントの IP アドレス（存在する場合）が含まれます。

DHCP スヌーピングバインディングデータベースは、IP ソースガードおよびダイナミック ARP でも使用されます。

8.13.1.4 DHCP スヌーピングの信頼できるポート

ポートは、DHCP trusted か DHCP untrusted のいずれかに設定できます。デフォルトの設定では、すべてのポートが「信頼できない」状態です。信頼できるものとしてポートを作成するには、[インタフェース設定] ページを使用します。これらのポートからのパケットは自動的に転送されます。信頼できるポートからのパケットはバインディングデータベースの作成に使用され、下記の説明に従って処理されます。

DHCP スヌーピングが有効でない場合は、デフォルトですべてのポートが信頼されます。

以下のアクションが実行されます。

デバイスは DHCPDISCOVER を送信して IP アドレスをリクエストするか、DHCPREQUEST を送信して IP アドレスを受け入れ、リースします。

デバイスはパケットをスヌーピングし、IP アドレスと MAC アドレスの情報を DHCP スヌーピングバインディングデータベースに追加します。

デバイスは DHCPDISCOVER パケットまたは DHCPREQUEST パケットを転送します。

DHCP サーバは DHCPOFFER パケットを送信して IP アドレスを提案するか、DHCPACK を送信して IP アドレスを割り当てます。あるいは、DHCPNAK を送信してアドレスリクエストを拒否します。

デバイスはパケットをスヌーピングします。DHCP スヌーピングバインディングデータベースにそのパケットと一致するエントリが存在する場合、デバイスは DHCPACK を受信するとそのエントリを IP-MAC バインディングに置き換えます。

デバイスは DHCPOFFER、DHCPACK、DHCPNAK のいずれかを転送します。

以下に、信頼できるポートからの DHCP パケットと信頼できないポートからの DHCP パケットがどのように処理されるのかをまとめます。DHCP スヌーピングバインディングデータベースは、不揮発性メモリに保存されます。

DHCP スヌーピングパケットの処理

パケットのタイプ	信頼できない入口インタフェースから受信したパケット	信頼できる入口インタフェースから受信したパケット
DHCPDISCOVER	信頼できるインタフェースにのみ転送します。	信頼できるインタフェースにのみ転送します。
DHCPOFFER	フィルタリングします。	DHCP 情報に従ってパケットを転送します。ディスティネーションアドレスが未知の場合、パケットはフィルタリングされます。
DHCPREQUEST	信頼できるインタフェースにのみ転送します。	信頼できるインタフェースにのみ転送します。
DHCPACK	フィルタリングします。	DHCPOFFER と同じです。DHCP スヌーピングバインディングデータベースにエントリが追加されます。
DHCPNAK	フィルタリングします。	DHCPOFFER と同じです。エントリが存在する場合は削除します。
DHCPDECLINE	データベース内に情報があるかどうかをチェックします。情報が存在し、メッセージが受信されたインタフェースに一致しない場合、パケットはフィルタリングされます。 それ以外の場合、パケットは信頼できるインタフェースにのみ転送され、エントリはデータベースから削除されます。	信頼できるインタフェースにのみ転送します。
DHCPRELEASE	DHCPDECLINE と同じです。	DHCPDECLINE と同じです。
DHCPINFORM	信頼できるインタフェースにのみ転送します。	信頼できるインタフェースにのみ転送します。
DHCPLEASEQUERY	フィルタリングされます。	転送します。

8.13.1.5 DHCP スヌーピングと DHCP リレー

DHCP リレーと DHCP スヌーピングの両方をグローバルに有効にし、さらに DHCP スヌーピングがクライアントの VLAN で有効な場合、DHCP スヌーピングバインディングテーブルに含まれる DHCP スヌーピングルールが適用されます。また、中継されるパケットについては、DHCP スヌーピングバインディングテーブルがクライアントの VLAN および DHCP サーバの VLAN で更新されます。

8.13.1.6 デフォルトの DHCP 設定

以下に、DHCP スヌーピングとリレーのデフォルトオプションを示します。

オプション	デフォルトの状態
DHCP スヌーピング	無効
Option 82 Insertion	無効
Option 82 Passthrough	無効
Verify MAC Address	有効
Backup DHCP Snooping Binding Database	無効
DHCP リレー	無効

8.13.1.7 DHCP の設定

DHCP リレーおよびスヌーピングを設定するには：

DHCP スヌーピングおよび / またはリレーを有効にします（プロパティページを参照）。

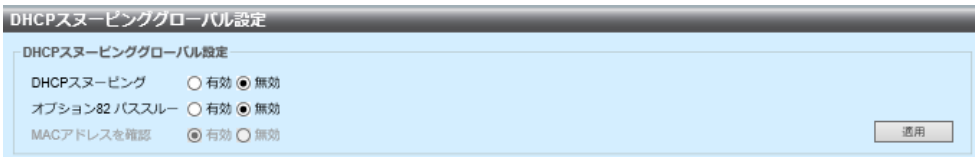
インタフェースを trusted または untrusted に設定します（*[DHCP スヌーピングポート設定]* ページを参照）。

必要に応じて、DHCP スヌーピングバインディングテーブルにエントリを追加します（*[DHCP スヌーピングバインディングエントリ]* ページを参照）。

8.13.1.8 プロパティ

DHCP リレー、スヌーピング、オプション 82 を設定するには：

[セキュリティ] > [IMPB] > [DHCP スヌーピング] > [プロパティ] に進みます。



パラメータ	概要
DHCP スヌーピング	DHCP スヌーピングを有効に設定します。
オプション 82 パススルー	パケット転送時に信頼できない情報を許可できるように設定します。
MAC アドレスを確認	DHCP untrusted ポートでレイヤの送信元 MAC アドレスが DHCP ヘッダ（ペイロードの一部）に表示されていることを確認するよう設定します。

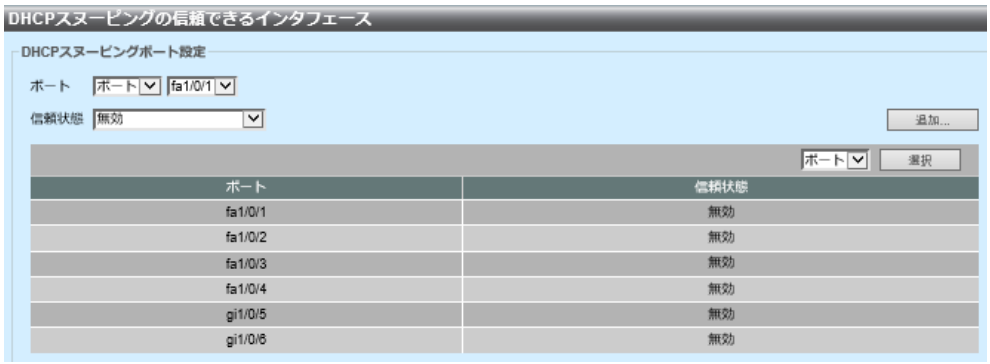
[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.13.2 DHCP スヌーピングポート設定

ポートまたは LAG で DHCP スヌーピングを有効にできます。

特定のインタフェースで DHCP スヌーピングを有効にするには：

[セキュリティ] > [IMPB] > [DHCP スヌーピング] > [DHCP スヌーピングの信頼できるインタフェース] に進みます。



ポート /LAG インタフェースの [信頼状態] を [無効] または [有効] に設定し、**[追加 ...]** を押します。

[選択] を押してポートまたは LAG をフィルタリングします。

8.13.3 DHCP スヌーピングバインディングエントリ

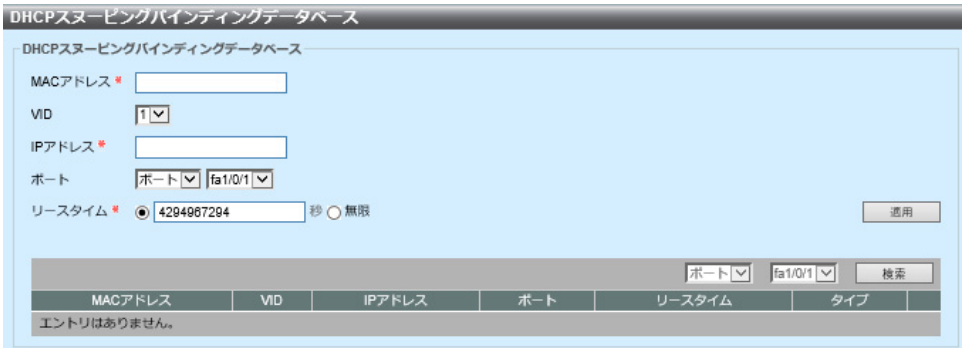
DHCP スヌーピングバインディングデータベースの構築方法が分かれば、データベースにダイナミックエントリを追加できます。

以下に、データベースのメンテナンスに関する説明を示します。

- 本デバイスでは、ステーションが別のインタフェースに移行するときに DHCP スヌーピングバインディングデータベースは更新されません。
- ポートがダウンしている場合、ポートのエントリは削除されません。
- VLAN の DHCP スヌーピングを無効にすると、その VLAN 用に収集されたバインディングエントリが削除されます。
- データベースがフルの場合、DHCP スヌーピングによるパケットの転送は継続されますが、新しいエントリは作成されません。IP ソースガードおよび / または ARP 検査の機能がアクティブな場合、DHCP スヌーピングバインディングデータベースに書き込まれないクライアントはネットワークに接続できないため、注意してください。

DHCP スヌーピングバインディングデータベースにエントリを追加するには：

[セキュリティ] > [IMPB] > [DHCP スヌーピング / リレー] > [DHCP スヌーピングバインディングデータベース] に進みます。



パラメータ	概要
MAC アドレス	パケットの MAC アドレス
VID	パケットが予想される VLAN
IP アドレス	パケットの IP アドレス
ポート	パケットが予想されるユニット / スロット / インタフェース
タイプ	以下のフィールド値があります。 • *ダイナミック* — エントリのリース期間が制限されています。 • *スタティック* — エントリがスタティックに設定されました。

パラメータ	概要
リースタイム	エントリがダイナミックな場合は、DHCP データベース内でエントリがアクティブになる時間数を入力します。リース期間がない場合は、[無限] をオンにします。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.14 IP ソースガード

IP ソースガードは、一種のセキュリティ機能です。この機能によって、ホストがネイバーの IP アドレスを使用しようとする場合に発生するトラフィック攻撃を防止することができます。

IP ソースガードを有効にすると、クライアントの IP トラフィックのみが、DHCP スヌーピングバインディングデータベース内の IP アドレスに送信されます。これには、DHCP スヌーピングによって追加されたアドレスと手動で追加したエントリの両方が含まれます。

パケットが DHCP スヌーピングバインディングデータベース内のエントリに一致する場合、デバイスはそのパケットを転送します。それ以外の場合は破棄されます。

8.14.1 はじめに

以下に、IP ソースガードに関連する情報を示します。

- IP ソースガードをインタフェースで有効にするために、DHCP スヌーピングをグローバルに有効にする必要があります。
- IP ソースガードは、以下の場合にのみインタフェースでアクティブにできます。
  - DHCP スヌーピングは、ポートの VLAN のいずれか 1 つ以上で有効になります。
  - インタフェースは DHCP untrusted です。信頼できるポートのすべてのパケットが転送されます。
- ポートが DHCP trusted として設定されている場合は、その状態で IP ソースガードがアクティブでなくても、ポートで IP ソースガードを有効にすることによってスタティック IP アドレスのフィルタリングを設定できます。
- ポート状態が DHCP untrusted から DHCP trusted に変わると、スタティック IP アドレスフィルタリングのエントリがバインディングデータベースに残りますが、インアクティブになります。
- ソース IP および MAC アドレスフィルタリングがポートで設定されている場合、ポートセキュリティを有効にすることはできません。
- IP ソースガードは TCAM リソースを使用しており、IP ソースガードのアドレスエントリごとに単一の TCAM ルールが必要です。IP ソースガードのエントリ数が利用可能な TCAM ルールの数を超える場合、追加のアドレスはインアクティブになります。

ポートでの IP ソースガードを有効にした後は：

- DHCP スヌーピングで許可される DHCP パケットが許可されます。
- 送信元 IP アドレスのフィルタリングも有効にする場合：
  - IPv4 トラフィック：ポートに関連付けられている送信元 IP アドレスを設定したトラフィックのみが許可されます。
  - IPv4 以外のトラフィック：許可されます（ARP パケットを含む）。

8.14.2 IP ソースガードの操作

IP ソースガードを設定するには：

DHCP スヌーピングのプロパティページで有効にします。

[DHCP スヌーピングポート設定] ページで、DHCP スヌーピングが有効になる VLAN を定義します。

[DHCP スヌーピングポート設定] ページで、インタフェースを trusted または untrusted に設定します。

IP ソースガードの [プロパティ] ページで、IP ソースガードを有効にします。

IP ソースガードの [インタフェース設定] ページで、IP ソースガード状態を [No]/[Yes] に設定します。

IP ソースガードの [バインディングデータベース] ページで、バインディングデータベースをテーブルに表示します。

8.14.3 プロパティ

IP ソースガードをグローバルに有効化するには：

[セキュリティ] > [IMPB] > [IP ソースガード] > [プロパティ] に進みます。

IP ソースガード状態を有効または無効に設定します。

[適用] を押して、IP ソースガード状態を有効または無効にします。

8.14.4 インタフェース設定

信頼できないポート /LAG で IP ソースガードを有効にすると、DHCP パケット（DHCP スヌーピングで許可される）が送信されます。送信元 IP アドレスのフィルタリングを有効にすると、以下のようにパケット送信が許可されます。

パラメータ	概要
IPv4 traffic	特定のポートに関連付けられている送信元 IP アドレスを設定した IPv4 のみが許可されます。
Non IPv4 traffic	非 IPv4 トラフィックがすべて許可されます。

IP ソースガードポート設定 /LAG 設定を行うには：

[セキュリティ] > [IMPB] > [IP ソースガード] > [インタフェース設定] に進みます。

パラメータ	概要
ポート	これが DHCP trusted インタフェースであるかどうかを示します。
ステータス	ポートで IP ソースガードが有効になっているかどうかを示します。

ポート /LAG を設定してテーブルの表示をフィルタリングし、**[選択]** を押します。

8.14.5 バインディングデータベース

IP ソースガードは、DHCP スヌーピングバインディングデータベースを使用して、信頼できないポートからのパケットをチェックします。デバイスから DHCP スヌーピングバインディングデータベースに書き込もうとするエントリが多すぎると、余分なエントリはインアクティブ状態に維持されます。リース期間が期限切れになったエントリが削除されるため、インアクティブなエントリがアクティブになる可能性があります。

「DHCP スヌーピングについて」、「DHCP リレーについて」を参照。

NOTE [バインディングデータベース] ページに表示されるのは、IP ソースガードの有効ポートに定義されている DHCP スヌーピングバインディングデータベース内のエントリだけです。

IP ソースガードの有効ポートに定義されている DHCP スヌーピングバインディングデータベースを表示するには：

[セキュリティ] > [IMPB] > [IP ソースガード] > [バインディングデータベース] に進みます。

パラメータ	概要
VLAN ID	パケットが予想される VLAN
MAC アドレス	照合する MAC アドレス
IP アドレス	照合する IP アドレス
インタフェース	パケットが予想されるインタフェース
状態	インタフェースがアクティブかどうかが表示されます。
タイプ	エントリがダイナミックとスタティックのどちらなのかが表示されます。
理由	インタフェースがアクティブでない場合は、その理由が表示されます。表示される可能性があるのは、以下の理由です。 • *問題ありません* — インタフェースはアクティブです。 • *スヌープ VLAN なし* — VLAN で DHCP スヌーピングが有効ではありません。 • *Trusted Port* — ポートが信頼できるものになりました。 • *Resource Problem* — TCAM リソースが使い尽くされました。

[選択] を押すと、これらのエントリのサブセットがポート /LAG でフィルタリングされます。

8.15 ARP 検査

IP アドレスを MAC アドレスにマッピングすることによって、ARP ではレイヤ 2 ブロードキャストドメイン内での IP 通信が可能です。

悪意のあるユーザは、サブネットに接続するシステムの ARP キャッシュを無効化し、サブネット上の他のホストへ向けたトラフィックを遮断することによって、レイヤ 2 ネットワークに接続するスイッチ、ホスト、ルータを攻撃できます。このような攻撃が発生するのは、ARP リクエストが受信されなかった場合でもホストからの不必要な応答が ARP によって許可されることが原因だと考えられます。攻撃後は、攻撃を受けたデバイスのすべてのトラフィックが攻撃者のコンピュータを通り、ルータ、スイッチ、ホストに到達します。

ホスト A、B、C は同じサブネットの同じスイッチ（ポート A、B、C）に接続されています。各ホストの IP アドレス、MAC アドレスは括弧内に表示されます（例：ホスト A は IP アドレスとして IPX、MAC アドレスとして MAXX を使用）。ホスト A はホスト B と IP 層で通信する場合、IP アドレス IPB に関連付けられている MAC アドレスの ARP リクエストをブロードキャストします。ホスト B は ARP リプライで応答します。スイッチとホスト A は、自身の ARP キャッシュをホスト B の MAC アドレスおよび IP アドレスで更新します。

ホスト C は偽の ARP 応答をブロードキャストすることによって、スイッチ、ホスト A、ホスト B の ARP キャッシュを無効化できます。また、IP アドレスとして IPA（または IPB）、MAC アドレスとして MACC を設定したホストをバインディングします。無効化された ARP キャッシュを持つホストは、IPA または IPB へ向けたトラフィックの宛先 MAC アドレスとして MAC アドレス MACC を使用します。これにより、そのトラフィックをホスト C が遮断します。ホスト C は IA および IB に関連付けられている実際の MAC アドレスを把握しています。そのため、正確な MAC アドレスを宛先として使用することによって、遮断されたトラフィックを対象のホストに転送できます。ホスト C はホスト A からホスト B へのトラフィックストリームに自身を挿入しています。つまり、典型的な中間者攻撃です。

8.15.1 ARP によるキャッシュ無効化の防止

ARP 検査は、trusted または untrusted のいずれかとしてインタフェースに関連付けられます（[インタフェース設定] ページを参照）。

ユーザは、インタフェースを信頼できるものと信頼できないものに分類できます。

パラメータ	概要
信頼できる	パケットは検査されません。
信頼できない	パケットは前述のように検査されます。

ARP 検査は信頼できないインタフェースに対してのみ実行されます。信頼できるインタフェースで受信された ARP パケットは転送されます。

信頼できないインタフェースにパケットが到着すると、以下の論理が実装されます。

- ARP アクセスコントロールルールにパケットの IP アドレス /MAC アドレスがないか検索します。IP アドレスが見つかり、リスト内の MAC アドレスがパケットの MAC アドレスに一致する場合、パケットは有効です。それ以外の場合は無効です。
- パケットの IP アドレスが見つからず、パケットの VLAN で DHCP スヌーピングが有効な場合は、DHCP スヌーピングバインディングデータベースにパケットの <VLAN - IP アドレス > のペアがないか検索します。<VLAN - IP アドレス > のペアが見つかり、MAC アドレスがパケットの MAC アドレスに、データベース内のインタフェースが入口インタフェースに一致する場合、パケットは有効です。
- ARP アクセスコントロールルールまたは DHCP スヌーピングバインディングデータベースにパケットの IP アドレスが見つからない場合、パケットは無効になり、破棄されます。SYSLOG メッセージが生成されます。
- 有効なパケットが転送され、ARP キャッシュが更新されます。

[ARP パケット検証] オプションが設定されている場合（[プロパティ] ページを参照）は、以下に示す追加の有効性確認が実施されます。

パラメータ	概要
ソース **MAC**	Ethernet ヘッダにあるパケットの送信元 MAC アドレスを、ARP 要求の送信元 MAC アドレスと比較します。この確認は、ARP 要求と応答の両方に対して実施されます。
ディスティネーション **MAC**	Ethernet ヘッダにあるパケットの宛先 MAC アドレスを、ディスティネーションインタフェースの MAC アドレスと比較します。この確認は、ARP 応答に対して実施されます。
IP Addresses	ARP ボディで無効な IP アドレスと予期しない IP アドレスを比較します。アドレスには、0.0.0.0、255.255.255.255、およびすべての IP マルチキャストアドレスが含まれます。

無効な ARP 検査バインディングを持つパケットはログに記録され、破棄されます。

ARP アクセスコントロールテーブルには最大で 1024 エントリを登録できます。

8.15.2 ARP 検査と DHCP スヌーピングの競合

DHCP スヌーピングを有効にすると、ARP 検査では ARP アクセスコントロールルールに加えて DHCP スヌーピングバインディングデータベースが使用されます。DHCP スヌーピングを無効にすると、ARP アクセスコントロールルールのみが使用されます。

8.15.3 ARP のデフォルト値

以下に、オプションとデフォルトの状態の関係を示します。

オプション	デフォルトの状態
ダイナミック ARP 検査	無効
ARP パケット検証	無効
ARP Inspection Enabled on VLAN	無効
ログバッファ間隔	破棄されたパケットの SYSLOG メッセージ生成が 5 秒間隔で有効になります。

8.15.4 ARP 検査の操作

ARP 検査を設定するには：

プロパティページで ARP 検査を有効にし、各種オプションを設定します。

[インタフェース設定] ページで、インタフェースを ARP trusted または ARP untrusted に設定します。

[ARP アクセスコントロール] ページでルールを追加します。

[VLAN ARP 検査設定] ページで、ARP 検査が有効な VLAN および各 VLAN のアクセスコントロールルールを定義します。

8.15.5 プロパティ

ARP 検査のプロパティを設定するには：

[セキュリティ] > [IMPB] > [ARP 検査] > [プロパティ] に進みます。

パラメータ	概要
ARP 検査状態	ARP 検査を有効または無効に設定します。
ARP パケット検証	有効性確認を有効または無効に設定します。
ログバッファ間隔	破棄されたパケットの SYSLOG メッセージ送信間隔を入力します。メッセージが送信される頻度を設定します。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.15.6 インタフェース設定

DHCP スヌーピングが有効な場合、信頼できないポート /LAG からのパケットは、ARP アクセスルールテーブルおよび DHCP スヌーピングバインディングデータベースに照合されます（[DHCP スヌーピングバインディングデータベース] ページを参照)。

ポート /LAG のデフォルトの設定は、「信頼できない」状態の ARP 検査です。

ポート /LAG の信頼できる状態に ARP を設定するには：

[セキュリティ] > [IMPB] > [ARP 検査] > [インタフェース設定] に進みます。

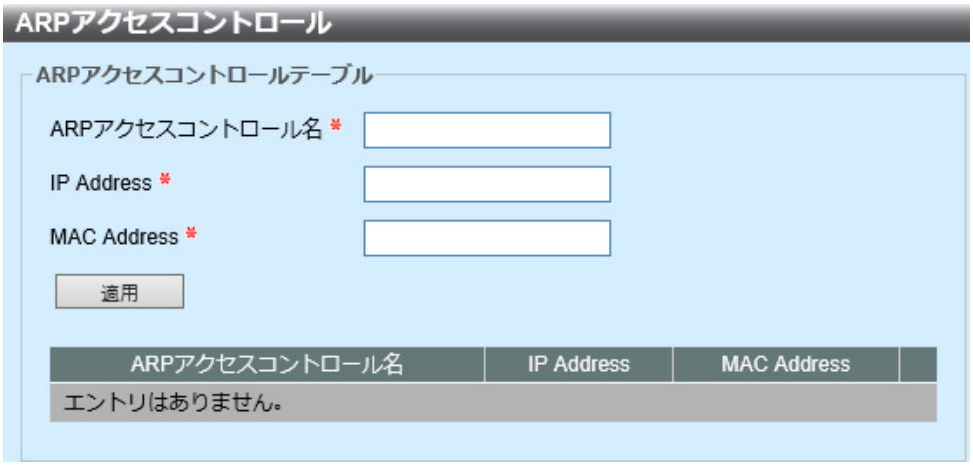
ポート /LAG の信頼状態を「有効」または「無効」に設定し、**[適用]** を押します。

テーブル内でポート /LAG をフィルタリングするには、**[適用]** を押します。

8.15.7 ARP アクセスコントロール

ARP 検査テーブルにエントリを追加するには：

[セキュリティ] > [IMPB] > [ARP 検査] > [ARP アクセスコントロール] に進みます。



パラメータ	概要
ARP アクセスコントロール名	ユーザが作成した名前を入力します。
IP Addres	パケットの IP アドレス
MAC Address	パケットの MAC アドレス

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

8.15.8 VLAN ARP 検査設定

VLAN の ARP 検査を有効にし、アクセスコントロールグループを VLAN に関連付けるには：

[セキュリティ] > [IMPB] > [ARP 検査] > [VLAN 設定] に進みます。

パラメータ	概要
VLAN ID	VLAN のリストから ID を設定します。
状態	VLAN の ARP 検査を有効または無効に設定します。
ARP アクセスコントロール名	ユーザが作成した名前を入力します。

[適用] を押して、ランニングコンフィグレーションファイルを更新します。

9 QAM

9.1 診断

診断を使用することによって、ケーブルテストの実行、デバイス操作情報の表示が可能です。

9.1.1 カッパーケーブルテスト

このページには、VCT（Virtual Cable Tester）によるカッパーケーブルに対する統合ケーブルテストの結果が表示されます。

このケーブルテストには 2 つのタイプがあります。

- TDR（時間分域反射率測定）法では、ポートに接続するカッパーケーブルの品質と特性をテストします。最長 140 メートルのケーブルをテストできます。このテストの結果は、[カッパーテスト] ページの [テスト結果] ブロックに表示されます。

9.1.1.1 カッパーポートテストを実行するための前提条件

テストを実行する前に、以下を実施してください。

基本的なテストの場合が +/-2 という誤差範囲に収まります。

> **注意** ポートはテスト時にダウン状態に設定され、通信が遮断されます。テストの後、ポートはアップ状態に戻ります。Web ベースのスイッチ設定ユーティリティを実行しているポートでは、銅ポートテストを実行しないでください。デバイスとの通信に混乱が生じます。

カッパーケーブルをテストするには：

[QAM] > [診断] > [ケーブル診断] に進みます。

テストするポートを設定します。

[テスト] を押します。

[テスト結果] テーブルに以下の値が表示されます。

パラメータ	概要
最終アップデート	最後のポートのテストが実行された時間
テスト結果	• *OK* — ケーブルのテストは合格です。 • *ケーブルなし* — ポートにケーブルが接続されていません。 • *オープンケーブル* — ケーブルの片側だけがポートに接続されています。 • *ショートケーブル* — ケーブルがショートしています。 • *未知のテスト結果* — エラーが発生しました。
障害までの距離	ポートからケーブルの障害発見箇所までの距離
オペレーションポート状態	ポートがアップ状態かダウン状態かが表示されます。

9.1.2 DDM 設定

DDM 設定を表示するには：

[QAM] > [診断] > [DDM Settings] に進みます。

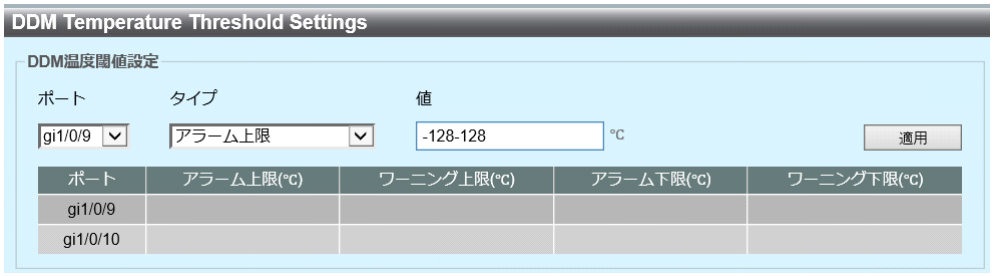
パラメータ	概要
ポート	SFP の接続先ポート番号
状態	有効または無効に設定します。
シャットダウン	[なし]、[ワーニング]、[アラーム] のいずれかを設定します。

[適用] を押します。

9.1.3 DDM 温度閾値設定

DDM 温度閾値設定を表示します。

[QAM] > [診断] > [DDM Temperature Threshold Settings] に進みます。



パラメータ	概要
ポート	SFP の接続先ポート番号
タイプ	[アラーム上限]、[ワーニング上限]、[アラーム下限]、[ワーニング下限] のいずれかを設定します。
値	摂氏で値 (-128 ～ 128) を入力します。

[適用] を押します。

9.1.4 DDM 電圧閾値設定

DDM 電圧閾値設定を表示するには：

[QAM] > [診断] > [DDM Voltage Threshold Settings] に進みます。

パラメータ	概要
ポート	SFP の接続先ポート番号
タイプ	[アラーム上限]、[ワーニング上限]、[アラーム下限]、[ワーニング下限] のいずれかを設定します。
値	mV で値 (0-6554) を入力します。

[適用] を押します。

9.1.5 DDM バイアス電流閾値設定

DDM バイアス電流閾値設定を表示するには：

[QAM] > [診断] > [DDM Bias Current Threshold Settings] に進みます。

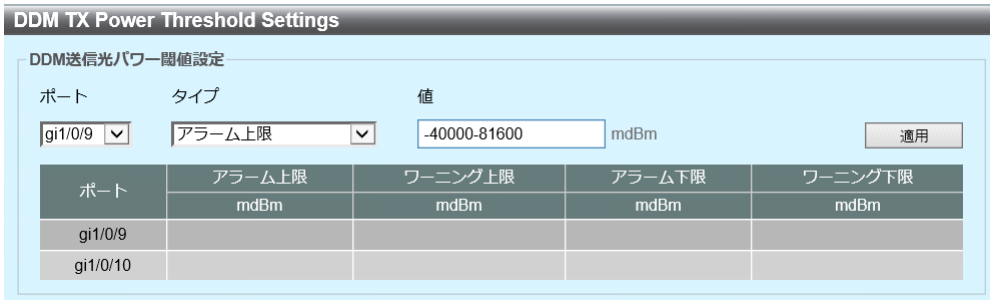
パラメータ	概要
ポート	SFP の接続先ポート番号
タイプ	[アラーム上限]、[ワーニング上限]、[アラーム下限]、[ワーニング下限] のいずれかを設定します。
値	mA で値 (0-131) を入力します。

[適用] を押します。

9.1.6 DDM 送信光パワー閾値設定

DDM 送信光パワー閾値を表示するには：

[QAM] > [診断] > [DDM TX Power Threshold Settings] に進みます。



パラメータ	概要
ポート	SFP の接続先ポート番号
タイプ	[アラーム上限]、[ワーニング上限]、[アラーム下限]、[ワーニング下限] のいずれかを設定します。
電力単位	mdBm を設定します。
値	値 (mdBm: -40000-81600) を入力します。

[適用] を押します。

9.1.7 DDM 受信光パワー閾値設定

DDM 受信光パワー閾値を表示するには：

[QAM] > [診断] > [DDM RX Power Threshold Settings] に進みます。

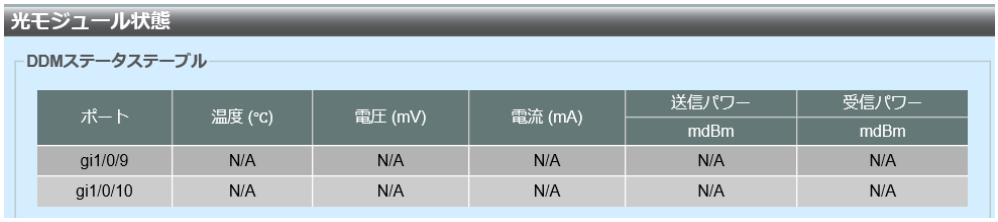
パラメータ	概要
ポート	SFP の接続先ポート番号
タイプ	[アラーム上限]、[ワーニング上限]、[アラーム下限]、[ワーニング下限] のいずれかを設定します。
電力単位	mdBm を設定します。
値	値 (mdBm: -40000-81600) を入力します。

[適用] を押します。

9.1.8 DDM 状態テーブル

光学テストを表示するには：

[QAM] > [診断] > [光モジュール状態] に進みます。



パラメータ	概要
ポート	SFP の接続先ポート番号
温度	SFP が動作している温度（℃）
電圧	SFP が動作している電圧 (mV)
電流	SFP バイアス電流消費量 (mA)
送信パワー	送信された光パワー (mdBm)
受信パワー	受信された光パワー (mdBm)

10 モニタリング

10.1 統計

10.1.1 インタフェース

[インターフェース] ページで、ポートごとのトラフィック統計を確認できます。情報のリフレッシュレートを設定できます。
この機能により、送受信されているトラフィックの量とその分散（ユニキャスト、マルチキャスト、ブロードキャスト）を分析できます。
Ethernet 統計情報を表示、および / またはリフレッシュレートを設定するには：

[モニタリング] > [統計] > [インタフェース] に進みます。

[リフレッシュ] を押して、受信統計情報および送信統計情報を表示します。

受信パケット：

パラメータ	概要
受信バイト総計	受信したオクテット数。不良パケットと FCS オクテットを含みますが、フレーミングビットは除きます。
受信パケット総計	受信したパケットの総計

送信パケット：

パラメータ	概要
送信バイト総計	送信したオクテット数。不良パケットと FCS オクテットを含みますが、フレーミングビットは除きます。
送信パケット総計	送信したパケットの総計

10.1.2 ポート使用率

このページには、ポートあたりの使用率が表示されます（送信と受信の両方）。

ポート使用率を表示するには：

[モニタリング] > [統計] > [ポート使用率] に進みます。

インタフェースの Ethernet 統計情報を検索するには **[検索]** を押し、リフレッシュするには **[リフレッシュ]** を押します。

パラメータ	概要
ポート	ポートの名前
送信 (パケット / 秒)	送信パケットで使用される帯域幅の量
受信 (パケット / 秒)	受信パケットで使用される帯域幅の量
使用率	使用率パケットで使用される帯域幅の量

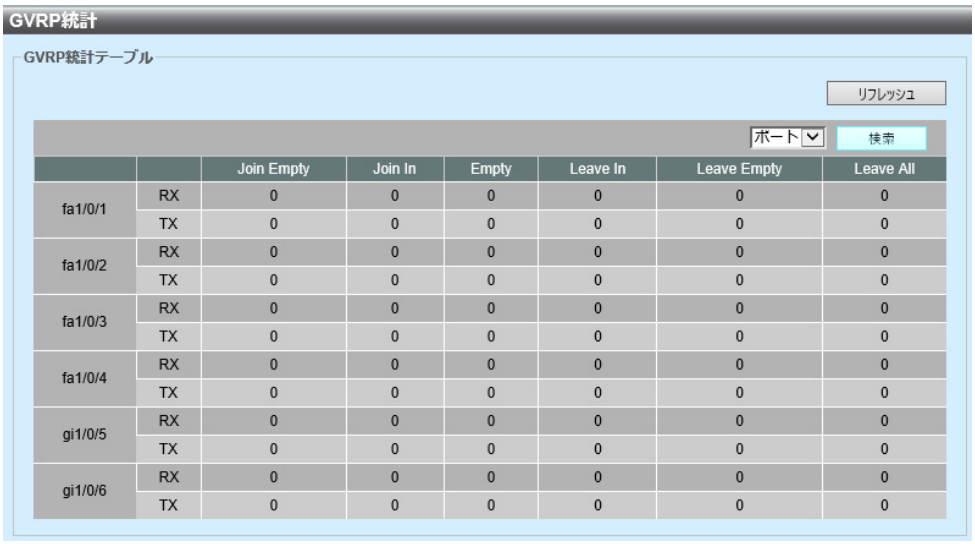
10.1.3 GVRP 統計

GVRP は標準ベースのレイヤ 2 ネットワークプロトコル（802.1Q-2005 の 802.1ak 修正）であり、スイッチでの VLAN 情報の自動設定に対応しています。このページには、あるポートから送受信された GVRP（GARP VLAN Registration Protocol）フレームが表示されます。

あるポートの GVRP 統計は、GVRP がグローバルに有効な場合およびそのポートで有効な場合にのみ表示されます。

GVRP 統計を表示するには：

[モニタリング] > [統計] > [GVRP 統計] に進みます。



受信パケットおよび送信パケットを表示するには、**[リフレッシュ]** を押します。

パラメータ	概要
Join Empty	受信 / 送信された GVRP Join Empty パケット
Join In	受信 / 送信された GVRP Join In パケット
Empty	受信 / 送信された GVRP empty パケット
Leave In	受信 / 送信された GVRP Leave In パケット
Leave Empty	受信 / 送信された GVRP Leave Empty パケット
Leave All	受信 / 送信された GVRP Leave All パケット

テーブル内でテーブル情報をフィルタリングするには、**[検索]** を押します。

10.1.4 デバイス

デバイス環境を表示するには：

[モニタリング] > [統計] > [ヘルスと電源] を押します。

パラメータ	概要
ユニット	どのデバイスかを示すスタック内のユニット。デバイスがスタックの一部でない場合、このパラメータは表示されません。
センサーステータス	デバイスのセンサーステータス
温度 (℃)	デバイスの温度
ワーニングアラーム温度 (℃)	デバイスのワーニングアラーム温度
クリティカルアラーム温度 (℃)	デバイスのクリティカルアラーム温度

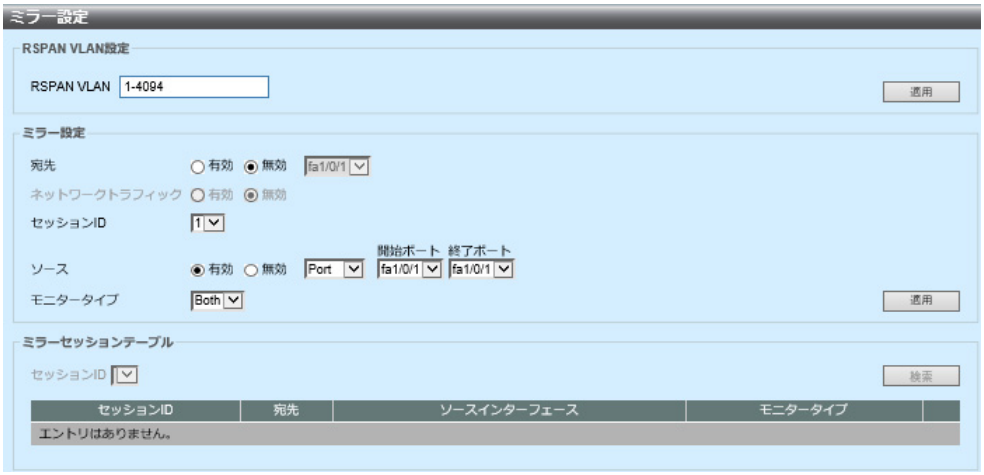
10.2 ミラー設定

RSPAN VLAN を定義する必要があります。

また、開始デバイスと最終デバイスでディスティネーションポートを設定する必要があります。

開始デバイスでは、これはリフレクタポートになります。最終デバイスでは、アナライザポートです。

[モニタリング] > [ミラー設定] > [ミラー設定] に進みます。



[RSPAN VLANs 設定] ブロックで RSPAN VLAN として VLAN を設定するには、VLAN の **[RSPAN VLAN]** ドロップダウンリストから VLAN を選択し、**[適用]** を押します。

[ミラー設定] ブロックで以下のパラメータを設定します。

パラメータ	概要
宛先	宛先の有効 / 無効およびインタフェースを設定します。
ネットワークトラフィック	ポートでのモニタリングされていないトラフィックの受け入れを有効または無効に設定します。
セッション ID	ソースポートのセッション ID に一致するように、セッション ID を設定します。
ソース	ソースのインタフェースを有効または無効に設定します。

パラメータ	概要
モニタータイプ	送信、受信、またはその両方のどのタイプのトラフィックをミラーリングするのかを以下の値で設定します。 • *両方* — 受信パケットと送信パケットの両方に対するポートミラーリング • *受信* — 受信パケットに対するポートミラーリング • *送信* — 送信パケットに対するポートミラーリング

[適用] を押してミラーセッションを追加し、ランニングコンフィグレーションファイルを更新します。

テーブル内でセッション ID をフィルタリングするには、設定を行った後に **[検索]** を押し、次に **[編集]** を押してセッションを編集します。

11 ECO モード

11.1 ECO モード

11.1.1 ポート設定

この機能は、デバイスの省電力化を実現するためのものです。

[ポート設定] ページでは、ポートごとの現在の ECO モードが表示され、使用中のポートに ECO モードを設定できます。

[ECO モード] > [ポート設定] に進みます。

特定のポートまたはポート範囲の EEE ステータスを有効または無効に設定し、**[適用]** を押します。以下の情報がポートインタフェース設定単位でテーブルに表示されます。

パラメータ	概要
EEE ステータス	EEE ステータスは、有効または無効です。
EEE LLDP ステータス	EEE LLDP 機能に関連するポートの状態： • *設定* — LLDP を通じた EEE カウンタのアドバタイズが有効だったかどうかが表示されます。 • *オペレーショナル* — LLDP を通じた EEE カウンタのアドバタイズが現在稼働中であるかどうかが表示されます。

パナソニックEWネットワークス株式会社

〒105-0021　東京都港区東新橋 2 丁目 12 番 7 号　住友東新橋ビル 2 号館 4 階
TEL 03-6402-5301 / FAX 03-6402-5304
URL: https://panasonic.co.jp/ew/pewnw/

P0519-15092