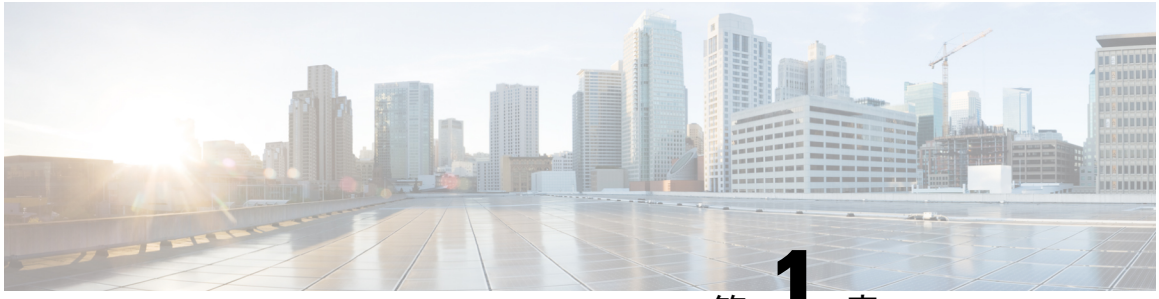
Cisco Business 350 シリーズ スイッチ アドミニストレーション ガイド

初版：2020 年 5 月 7 日

最終更新：2023 年 2 月 6 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

スイッチについて

この章は、次の項で構成されています。

はじめに

Cisco CBS シリーズ スイッチをお買い上げいただき、ありがとうございます。Cisco CBS シリーズスイッチは、強力なネットワークパフォーマンスや信頼性に加えて、強固なビジネスネットワークに必要とされる総合的なネットワーク機能スイートも備えています。これらの拡張可能なギガビット イーサネット スイッチは、ギガビットまたは 10 ギガビットアップリンクを備えており、完全管理型のスイッチよりも低価格でありながら、アンマネージドスイッチやコンシューマ向けスイッチよりもはるかに優れた複数の管理オプション、豊富なセキュリティ機能、レイヤ 3 スタティックルーティング機能などを提供します。

はじめる前に

デバイス設置作業を開始する前に、次の項目を用意していることを確認してください。

- ネットワーク デバイスを接続するための RJ-45 イーサネット ケーブル。10G ポートにはカテゴリ 6a 以上のケーブルが必要です。他のすべてのポートにはカテゴリ 5e 以上のケーブルが必要です。
- ハードウェア設置用の工具。

- スイッチに同梱されているラックマウントキットには、デスクトップ配置用のゴム製の脚4本、およびラックマウント用のブラケット2個とネジ12本が含まれています。
- 付属のネジを紛失した場合は、次のサイズの交換用ネジを使用してください。
  - ネジ頭の直径：6.9 mm
  - ネジ頭の表面からネジ基部までの長さ：5.9 mm
  - 軸径：3.94 mm

警告 通気を妨げないように、通気口の周囲に 3 インチ（7.6 cm）以上のスペースを確保してください。

- コンソールポートまたは Web ベースのインターフェイスを介してデバイスを管理するためのコンピュータ。Web ベースのインターフェイスの場合、このコンピュータは、次のいずれかのブラウザをサポートしている必要があります。
  - Microsoft Edge
  - Firefox（バージョン 82 または 81 以降）
  - Chrome（バージョン 86 または 85 以降）
  - MAC 上の Safari（バージョン 14.0 以降）

警告 米国電気工事規程 645 条および NFPA 75 に従った情報処理機器室への設置に適しています。

ラックへのスイッチのマウント

スイッチは標準規格サイズの19インチ（約48 cm）幅のラックにマウントできます。スイッチを取り付けるには 1 ラック ユニット（RU）のスペース、つまり 1.75 インチ（44.45 mm）の高さが必要です。

注意 安定性を確保するために、重いデバイスから順に下から上へとラックに載せていきます。重いデバイスをラックの一番上に載せると、不安定になり、転倒する可能性があります。

19 インチ標準シャーシにスイッチを設置する手順は次のとおりです。

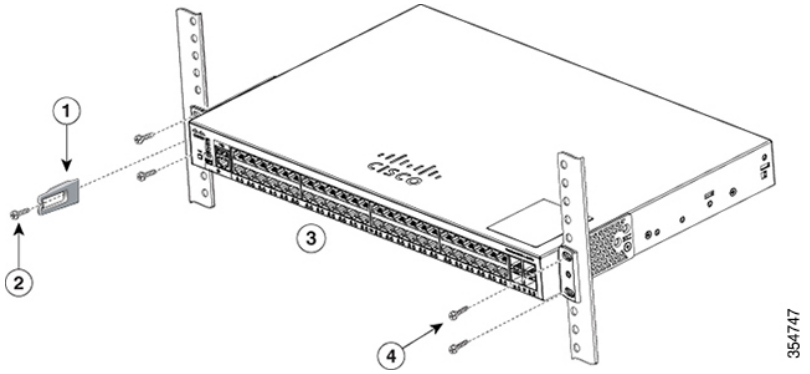
ステップ 1 スイッチの側面に付属のブラケットを 1 つ当て、ブラケットの 4 つの穴をネジ穴に合わせてから、付属のネジ 4 本を使用して固定します。

ステップ 2 前述の手順を繰り返して、もう 1 つのブラケットをスイッチの反対側に固定します。

ステップ 3 ブラケットを完全に固定してから、スイッチを標準 19 インチ ラックに取り付けます。

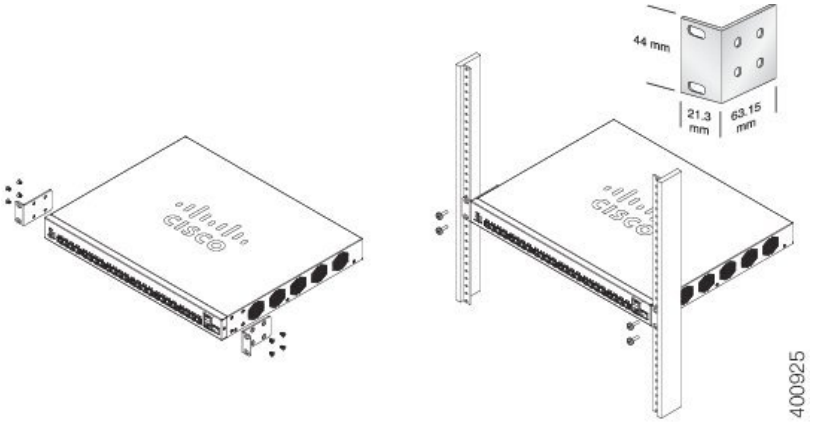
（注） スイッチをラックにマウントするには、付属のブラケットを使用してください。

スイッチモデルに付属のラックマウントブラケットを、前面取り付け位置に合わせます。取り付け金具と前面パネルの位置は、ずれています。



設計の違いにより、一部のマウントブラケットは、取り付けると、スイッチが取り付け面から約 2.5 cm 前に出ます。

スイッチモデルに付属のラックマウントブラケットを、前面取り付け位置に合わせます。取り付け金具と前面パネルの位置にずれはありません。



スイッチの壁面への取り付け

スイッチは、壁面に取り付けることができます。その場合は、壁面の間柱を使用するか、しっかり固定された合板の背板に取り付けます。

注意 取り付けを開始する前に、以下の手順をよく読んでください。適切なハードウェアを使用しなかった場合、または、正しい手順に従わなかった場合は、人体に危険が及んだり、システムが破損したりする可能性があります。

注意 前面パネルを上に向けた状態で、スイッチを壁面に設置しないでください。スイッチを壁面に取り付ける場合は、エアフローを妨げないようにするため、またケーブルを扱いやすくするため、安全上の規定に従ってスイッチの前面パネルを下または横に向けてください。

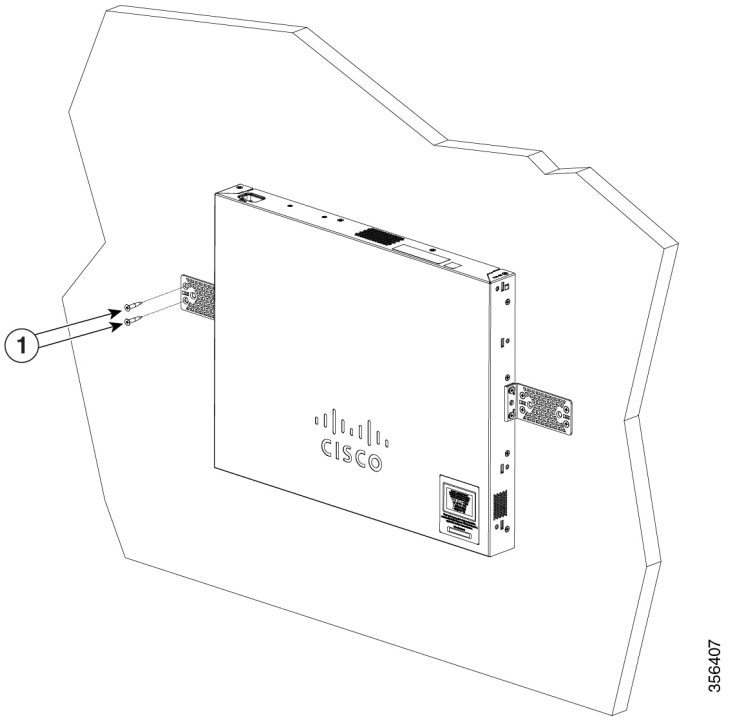
ブラケットを使用して 24 ポートスイッチを壁面に取り付けるには、次の手順を実行します。

ステップ 1 スイッチの片側に 19 インチ ブラケットを取り付けます。

ステップ 2 前述の手順を繰り返して、もう 1 つのブラケットをスイッチの反対側に固定します。

ステップ 3 ブラケットを確実に取り付けたら、前面パネルを下に向けてスイッチを取り付けます。スイッチは、壁面の間柱か、しっかり固定した合板の背板に確実に取り付けてください。24 ポートスイッチの壁面への取り付け

24 ポートスイッチの壁面への取り付け



8 ポートスイッチの壁面への取り付け

取り付けネジを使用して8ポートスイッチを壁面に取り付けるには、次の手順を実行します。

ステップ 1 ネジ用テンプレートを取り出します。このテンプレートは、取り付けネジ穴の位置を決めるために使用します。

ステップ 2 CABLE SIDE ENTRY とマークされたエッジがフロアに向くように、ネジ用テンプレートを置きます。スイッチは、壁面の間柱か、しっかり固定した合板の背板に確実に取り付けてください。

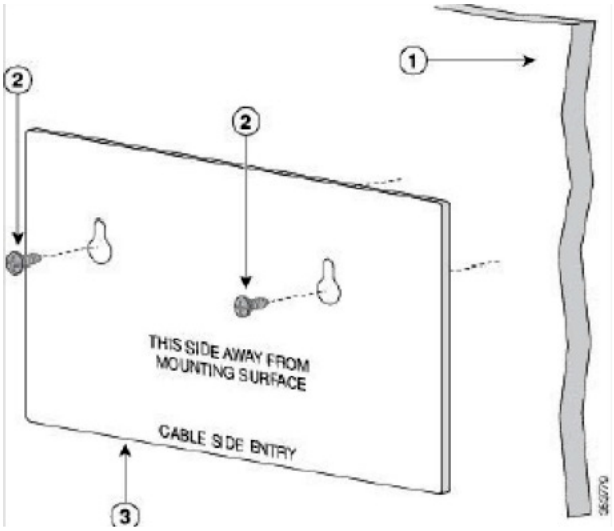
ステップ 3 ネジ用テンプレートの底面から粘着ストリップを剥がします。

ステップ 4 ネジ用テンプレートを壁面に貼り付けます。

ステップ 5 0.144 インチ（3.7 mm）または #27 のドリル ビットを使用し、ネジ用テンプレートの 2 つのスロットに、1/2 インチ（12.7 mm）の穴を開けます。

ステップ 6 ネジ用テンプレートのスロットにネジを 2 本挿入して、ネジ頭がネジ用テンプレートの上面に接触するまで締めます。取り付けネジの壁面への取り付け

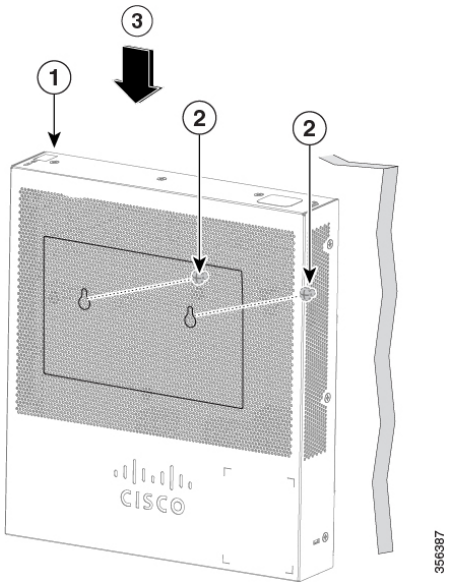
図 3 取り付けネジの壁面への取り付け



ステップ 7 ネジ用テンプレートを壁面から取り外します。

ステップ 8 スイッチを取り付けネジに合わせて、ロックされるまで下方にスライドさせます。8 ポートスイッチの壁面への取り付け

図 4 8 ポートスイッチの壁面への取り付け



アウトオブバンド ポート

CBS350 の「10G ネットワークポート SKU」は、管理ネットワークに使用できるアウトオブバンド（OOB）ポートをサポートしています。アウトオブバンドポートとインバンドポートは、同じ IP ルーティングテーブルを共有します。そのため、インバンドインターフェイスとアウトオブバンド インターフェイスの両方で同じサブネットを使用することはできません。

OOB ポートには、基本 MAC アドレスおよびインバンドポートのアドレスとは異なる MAC アドレスが割り当てられます。この MAC アドレスは、スイッチによって OOB ポートで送信されるすべてのフレームで、送信元 MAC アドレスとして使用されます。

デフォルトでは、VLAN 1 はデフォルトの IP アドレスである 192.168.1.254 で設定されており、任意のインバンドインターフェイスを介してアクセスできます。このデフォルトの IP アドレスは、その他のアドレスが動的または静的に割り当てられていない場合に使用されます。OOB ポートにはデフォルトの IP アドレスはありません。

表 *1: VLAN 1* および *OOB* の工場出荷時のデフォルト *IP* 設定：古い動作と新しい動作

	Cisco Business ファームウェアバージョン 3.1 以前		**Cisco Business ファームウェアバージョン 3.1.1**	
	OOB インターフェース	VLAN 1 インターフェイス	OOB インターフェース	VLAN 1 インターフェイス
IP の設定（IP settings）	デフォルト IP + DHCP		DHCP 有効	デフォルト IP + DHCP

	Cisco Business ファームウェアバージョン 3.1 以前		Cisco Business ファームウェアバージョン 3.1.1	
インターフェイスの CLI 設定	なし	なし	「IP アドレス DHCP」	なし
その他	Bonjour 有効	なし	なし	Bonjour 有効

スイッチのスタック構成

スタックには複数のデバイスを含めることができます。スタック構成には、スイッチの任意の10G ポートを使用できます。

デフォルトでは、スイッチのポートはスタック構成にしない限り、通常のイーサネットポートとして機能します。スイッチ間またはポート間で異なるスタック速度を使用することはできません。

特定のスイッチで2つ以上のポートをスタック構成用に選択する必要があり、これらのポートの速度は 10 ギガビットである必要があります。スタックを形成する 2 つ以上のスイッチは、同じバージョンのファームウェアを実行している必要があります。これが、SG シリーズ スイッチと CBS シリーズ スイッチによるスタック構成が不可能である理由です。CBS250 シリーズ スイッチにはスタック構成機能はありません。

一部のスイッチではスタック LED（LED 番号 1、2、3、および 4）によってアクティブ、スタンバイ、およびメンバーが示されますが、他のスイッチではシステム LED の点滅動作によってそれらが示されます。

（注） スタックポートでは、ポートに接続されるモジュールまたはケーブルの速度性能が同じである必要があります。

スイッチのスタック構成は、メッシュトポロジを含めることはできません。同じスタック内のスイッチは、スタック ポートを介して相互接続されます。スタック ポートのタイプと目的の速度に応じて、Cat6a イーサネット ケーブルやスイッチ用のシスコ認定モジュールまたはケーブルが必要になります。

一部のネットワークスイッチには、他のスイッチに接続して単一のユニットとして連動する機能があります。これらの構成は「スタック」と呼ばれ、ネットワークの容量をすばやく増やすために役立ちます。

スタック管理

Cisco Business スイッチにはいくつかの異なるスタック構成モードがあり、異なるモデルでスタックを構成することができます。

また、異なるスタック構成モード（ネイティブまたはハイブリッド）で使用できる機能とできない機能にも注意する必要があります。

- ネイティブスタック構成：スイッチは、すべてのユニットが同じタイプであるスタックの一部です。
- ハイブリッドスタック構成：スイッチは、異なるタイプの CBS350 デバイスを混在させて構成できるスタックの一部です。

Cisco Business スイッチスタック構成モードセレクタ

このツールを使用すると、指示に従って 10G の Cisco Business 350 シリーズ スイッチの正しいスタック構成設定を選択することができます。ツールにアクセスするには、次のリンクをクリックしてしてください。

https://www.cisco.com/c/en/us/support/docs/smb/switches/Cisco-Business-Switching/kmgmt-2799-switch-stack-selector-cbs.html

（注） レガシースイッチと新しい Cisco Business スタッカブルスイッチをスタック構成にすることはできません。レガシースイッチをスタック構成にしている場合は、次のリンクを参照してください：https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-350x-series-stackable-managed-switches/smb5367-feature-support-comparison-between-the-cisco-stackable-manag.html

ハイブリッドモードでの機能サポート

10G ネットワークポートを備えた CBS350 SKU の機能セットと 10G アップリンクポートを備えた CBS350 SKU の機能セットは、ほぼ同じです。ただし、この 2 つの「サブタイプ」の間には、機能サポートおよびテーブルサイズにいくつかの違いがあります。Cisco Business スイッチのハイブリッドスタックモードは、これらの機能/テーブルの共通する一部がサポートされます。下の表に、2 つのサブタイプの間での機能の違いと、ハイブリッドモードで適用される設定を示します。

ハイブリッドモードは、たとえば、MAC テーブルサイズが小さくなる可能性があり、パフォーマンスが低下しますが、スタック構成の任意の組み合わせで機能します。一方、同じモデル番号（同じ PID）のスイッチであれば、ネイティブスタック構成モードを利用できます。異なる PID を持つ一部のスイッチはネイティブモードでもスタックできますが、その他の組み合わせはハイブリッドモードでしかスタックできません。

一般に、スタック構成をサポートし、PID に指定されたアップリンクポートを持つ CBS350 スイッチはすべて（CBS350-48XT-4X は除く）、それらの間でネイティブにスタックできます。また、アップリンクポートを持たないスイッチ（CBS350-48T-4X を含む）も、それらの間でネイティブモードでスタックできます。ハイブリッドモードのスタック構成は、これら 2 つのブロック（アップリンクをサポートするデバイスと非アップリンクをサポートするデバイス）が混在する場合にのみ、その効果が発揮されます。そのため、特定のスイッチの正確な PID を知ることは、スタック構成モードを決定する上で非常に重要です。CBS350-48T-4X は、PID の最後が、アップリンクをサポートすることを示す 4X ですが、サポートしていません。このスイッ

チにおけるこの4X指定はアップリンクを示しておらず、それらのポートはスイッチの他のポートと同様にネットワークポート（ダウンリンクポート）です。

スタック構成モードをネイティブからハイブリッドに変更すると、スイッチが強制的に再起動され、スタートアップコンフィギュレーションのほとんどの設定がデフォルトにリセットされます。一方、スタック構成モードをハイブリッドからネイティブに変更すると、ユニットは強制的に再起動されますが、設定はデフォルトにリセットされません。

機能	CBS350「10G アップリンクポート SKU」	CBS350「10G ネットワークポート SKU」	ハイブリッドスタック
OOB ポート	未サポート	サポート対象	未サポート
グリーン設定（ショートリーチとエネルギー検出）	SKUおよびポートタイプごとの動作	SKUおよびポートタイプごとの動作	SKUおよびポートタイプごとの動作
MAC テーブル サイズ	16 K	32K または 64K	16 K
マルチキャストグループの数	2 K	4 K	2 K
サポートされる ACE の数	1K - 予約済み	2K - 予約済み	1K - 予約済み
IP エントリの総数	992	7392	992
ARP テーブル サイズ	1K – 予約済み	8K – 予約済み	1K – 予約済み
IPv6インターフェイスの最大数	106	200	106
最大 MAC テーブル エージング	400 秒	630 秒	400 秒
IPv6 手動トンネル/6tp4 トンネル/ISATAP ルーティング トンネル	サポート対象外	対応	サポート対象外
PoE のサポート	特定の SKU でサポート	サポート対象外	SKU タイプごと
VLANマッピングエントリのデフォルト数	0	32	0
デフォルト IP アドレス	VLAN 1 上	VLAN 1 上	VLAN 1 上

Power over Ethernet の考慮事項

スイッチには PoE をサポートしているものとサポートしていないものがあります。PoE をサポートしているスイッチモデルの場合は、モデル番号に P が含まれています（CBSxxx-xxP-xx など）。スイッチが Power over Ethernet（PoE）モデルである場合は、次の電力要件を考慮してください。

警告 スイッチは、外部プラントにルーティングすることなく PoE ネットワークにのみ接続されます。

表 *2 : Power Over Ethernet* モデルのスイッチ

SKU 名	説明	PoE PD チップセットタイプ	PoE PSE サポート
CBS350-8MGP-2X	8 ポート 2.5 G POE マネージドスイッチ	1*69208M	AF/AT
CBS350-8MP-2X	8 ポート 2.5G PoE スタッカブルマネージドスイッチ	1*69208M	AF/AT
CBS350-24MGP-4X	24 ポート 2.5G PoE スタッカブルマネージドスイッチ	1*69208M + 1*69204	AF/AT/60W
CBS350-12NP-4X	12 ポート 5G PoE スタッカブルマネージドスイッチ	3 * TPS2388	AF/AT/60W
CBS350-24NGP-4X	24 ポート 5G PoE スタッカブルマネージドスイッチ	4* TPS2388	AF/AT/60W
CBS350-48NGP-4X	48 ポート 5G PoE スタッカブルマネージドスイッチ	7* TPS2388	AF/AT /60W
CBS350-8P-2G	8 ポートギガビット PoE マネージドスイッチ	TPS2388	AF/AT
CBS350-8P-E-2G	8 ポートギガビット PoE マネージドスイッチ	TPS2388	AF/AT

SKU 名	説明	PoE PD チップセットタイプ	PoE PSE サポート
CBS350-8FP-2G	8 ポートギガビット PoE マネージドスイッチ	TPS2388	AF/AT
CBS350-8FP-E-2G	8 ポートギガビット PoE マネージドスイッチ	TPS2388	AF/AT
CBS350-16P-2G	16 ポート ギガビット PoE 対応マネージドスイッチ	2*TPS2388	AF/AT
CBS350-16P-E-2G	16 ポート ギガビット PoE 対応マネージドスイッチ	2*TPS2388	AF/AT
CBS350-16FP-2G	16 ポート ギガビット PoE 対応マネージドスイッチ	2*TPS2388	AF/AT
CBS350-24P-4G	24 ポート ギガビット PoE 対応マネージドスイッチ	3*TPS2388	AF/AT
CBS350-24FP-4G	24 ポート ギガビット PoE 対応マネージドスイッチ	3*TPS2388	AF/AT
CBS350-48P-4G	24 ポート ギガビット PoE 対応マネージドスイッチ	6*TPS2388	AF/AT
CBS350-48FP-4G	48 ポートギガビット PoE マネージドスイッチ	6*TPS2388	AF/AT
CBS350-24P-4X	24 ポートギガビット PoE スタッカブル マネージド スイッチ（10G アップリンク付き）	3*TPS2388	AF/AT

SKU 名	説明	PoE PD チップセットタイプ	PoE PSE サポート
CBS350-24P-4X	24 ポートギガビット PoE スタッカブル マネージド スイッチ（10Gアップリンク付き）	3*TPS2388	AF/AT
CBS350-24FP-4X	48 ポートギガビット PoE スタッカブル マネージド スイッチ（10Gアップリンク付き）	6*TPS2388	AF/AT
CBS350-48P-4X	48 ポートギガビット PoE スタッカブル マネージド スイッチ（10Gアップリンク付き）	6*TPS2388	AF/AT
CBS350-48FP-4X	48 ポートギガビット PoE スタッカブル マネージド スイッチ（10Gアップリンク付き）	6*TPS2388	AF/AT

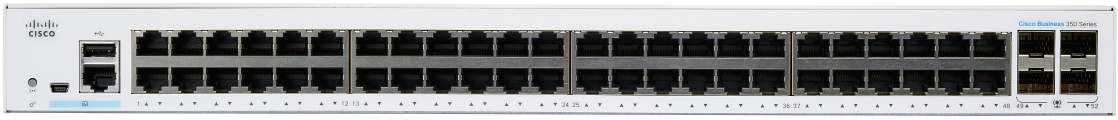
注意 PoE スイッチを接続するときは、次の点を考慮してください。PoE スイッチは、受電デバイス（PD）を接続するための DC 電源を供給できる PSE（給電側機器）です。これらのデバイスには、VoIP 電話、IP カメラ、およびワイヤレス アクセス ポイントが含まれます。PoE スイッチは、先行標準のレガシー PoE PD を検出して給電できます。PoE レガシーサポートが原因で、PSE として動作する PoE スイッチが（他の PoE スイッチを含む）接続先 PSE を誤ってレガシー PD として検出して給電する可能性があります。 PoE スイッチは PSE であり、AC 電源で作動する必要がありますが、誤検出のために別の PSE によってレガシー PD として電源投入される可能性があります。この場合、PoE スイッチが正常に動作せず、接続している PD に正しく電源を供給できない場合があります。

誤検出を防止するには、PSE に接続するために使用されている PoE スイッチのポートで PoE を無効にする必要があります。また、PSE デバイスを PoE スイッチに接続する前に、PSE デバイスの電源を入れる必要があります。デバイスが誤って PD として検出されている場合は、デバイスを PoE ポートから切断し、PoE ポートを再接続する前に AC 電源でデバイスの電源を入れなおす必要があります。

前面パネル

スイッチの前面パネルには、ポート、LED、およびリセットボタンと、次のコンポーネントがあります。

Cisco Business 350 シリーズ モデル



（注） CBS 350 シリーズには異なるモデルがあり、これは単にシリーズに含まれる一つのモデルの例です。

- コンソールインターフェイスが異なる次の 2 つのデバイスタイプがあります。
  - RJ-45 コネクタとミニ USB コネクタを備えたコンソールポート（両方が接続されている場合、RJ-45 よりもミニ USB の方が優先されます）
  - RJ-45 コネクタのみのコンソールタイプ

  コンソールインターフェイスは、シリアルケーブルをコンピュータのシリアルポートに接続するかミニUSBケーブルを使用して（コネクタによって異なります）、端末エミュレーションプログラムで設定できるようにします。
- USB ポート：USB ポートはスイッチと USB デバイスを接続します。これにより、接続した USB デバイスを利用して、コンフィギュレーション ファイル、ファームウェア イメージ、および Syslog ファイルの保存と復元が可能になります。USB ポートは、FAT32 ファイル システムをサポートします。
- RJ-45 イーサネット ポート：RJ-45 イーサネット ポートを使用して、コンピュータ、プリンタ、アクセス ポイントなどのネットワーク デバイスをスイッチに接続します。
- SFP+ ポート（存在する場合）：Small Form-Factor Pluggable Plus（SFP+）は、スイッチを他のスイッチとリンクするためのモジュール用の接続ポイントです。これらのポートは、一般にミニ 10 ギガビット インターフェイス コンバータ ポートとも呼ばれます。このガイドでは SFP+ という用語を使います。
  - SFP+ ポート（存在する場合）は、シスコの SFP 1G 光モジュール（MGBSX1、MGBLX1、MGBLH1、MGBT1）に加えて、他社ブランドのモジュールとも互換性があります。
  - SFP+ ポートは、シスコの SFP 1G 光モジュール（MGBSX1、MGBLX1、MGBLH1、MGBT1）に加えて、他社ブランドのモジュールとも互換性があります。

- シスコのスイッチでサポートされるシスコの SFP+ 銅ケーブルモジュールは、SFP-H10GB-CU1M、SFP-H10GB-CU3M、および SFP-H10GB-CU5M です。
- 対応する RJ-45 ポートの LED は SFP インターフェイス トラフィックに反応して緑色に点滅します。

- Small Form-Factor Pluggable （SFP）ポートは、モジュール用の接続ポイントです。これらのポートを使用して、スイッチを他のスイッチとリンクさせることができます。
- 一部の SFP インターフェイスは、コンボポートと呼ばれる他の 1 つの RJ-45 および SFP+ ポートと共有されます。SFP がアクティブな場合、隣接する RJ-45 ポートは無効になります。
- リセットボタンは、スイッチをリセットまたは再起動するときに使用します。次の表は、スイッチのリセット動作を示しています。

押下の種類	新しい動作（3.2 以降のファームウェア）	古い動作（3.2 より前のファームウェア）
1 ～ 5 秒	システム LED は緑で、ボタンを離してもリロードは発生しません。	リロード
6 ～ 10 秒	システム LED が緑色に点滅し、この間にボタンを離すとデバイスがリロードされますが、システムは工場出荷時のデフォルトに設定されていません。	リロード
11 ～ 15 秒	システム LED は緑、ボタンを離してもリロードは発生しません	工場出荷時
16 ～ 20 秒	システム LED が緑色に点滅し、この間にボタンを離すとデバイスが工場出荷時のデフォルトにリロードされます	工場出荷時
20 秒超	システム LED は緑、ボタンを離してもリロードは発生しません	工場出荷時

（注） スタック動作

リセットボタンの無効設定はスタック内のすべてのユニットに適用されます。つまり、設定されている場合、スタック内のすべてのユニットのリセットボタンが無効になり、設定されていない場合、スタック内のすべてのユニットのリセットボタンが有効になります。これは、既存のスタックに参加するユニットにも適用されます。

- OOB ポート（存在する場合）：OOB（Out of Band）ポートは、管理インターフェイスとしてのみ使用できる CPU のイーサネット ポートです。OOB ポートとインバンド レイヤ 2 インターフェイスの間のブリッジングはサポートされていません。これは 250 デバイスにはありません。
- マルチギガビットイーサネットポート（存在する場合）：青色で強調されたこれらのポートは、Cat5e ケーブルで最大 2.5 Gbps または 5 Gbps のスピードをサポートします。サポートされる最大速度は、ポートの下に青色で網掛けされて印刷されています。CBS350-8MGP-2X のアップリンクポートもマルチギガビット速度をサポートしています。この場合、ポート スピードは 10 Gbps まで可能です。世界中で導入されているケーブルの大半は Cat5e であり、これまでは 100 m で 1 Gbps に制限されていました。Cisco Multigigabit Ethernet により、ケーブルを交換しなくても、同じインフラストラクチャ上で最大 2.5 または 5 Gbps のスピードが可能になります。
- 60 ワット PoE ポート（存在する場合）：60 ワット PoE ポートは、ポートで供給される最大 PoE 電力を 60 W に倍増させます。

前面パネル LED

デバイスには次のグローバル LED が装備されています。

- System：（グリーン）この LED はスイッチの電源がオンになると点灯し、ブート中、セルフテストの実行中、または IP アドレスの取得中は点滅します。LED がオレンジで点滅する場合は、スイッチでハードウェア障害、ファームウェア障害、設定ファイルエラーなどが検出されたことを意味します。

次の LED は、ユニットのスタックステータスを示します。

- *スタック ID LED（グリーン）：スイッチがスタック構成のときに点灯し、対応する数字はスタック ID を示します。
- *アクティブユニット ID LED：このユニットがスタックのアクティブユニットであることを示します。

（注） * これらの 2 つの LED は、特定のモデルでのみ利用できます。

- システム LED：システム LED は、メンバーユニットのユニット ID に対応して 20 秒ごとに点滅します。
  - 点滅 = LED が消灯してから再び点灯します。
  - ユニットのユニット ID に対応します。つまり、次のように動作します。
    - ユニット 1（アクティブユニットではない場合）：システム LED が 1 回点滅します
    - ユニット 2（アクティブユニットではない場合）：システム LED が 2 回点滅します
    - ユニット 3：システム LED が 3 回点滅します
    - ユニット 4：システム LED が 4 回点滅します
  - 各点滅の間隔（LED 消灯時間）は次のとおりです。
    - LED 消灯時間は点滅ごとに約 0.5 秒です。
    - 2 回の LED 消灯間の「一時的」LED 点灯は約 0.5 秒です。
  - メンバーユニットをスタックから削除する場合、そのシステム LED は、上記の定義に従って点滅しつづけます。

ポート LED は以下のとおりです。

- LINK/ACT：（グリーン）各ポートの左側に配置されています。LED は、対応するポートと他のデバイス間のリンクが検出されると点灯し、ポートがトラフィックを渡しているときに点滅します。
- SFP+（存在する場合）：（緑）10G ポートの右側にあります。LED は、共有ポートを介して接続が行われると点灯し、ポートがトラフィックを渡しているときに点滅します。
- XG：（グリーン）10 G ポートの右側に配置されています。LED は、別のデバイスがポートに接続されて電源が投入され、デバイス間で 10 Gbps リンクが確立されたときに点灯します。LED が消灯している場合は、接続速度が 10 Gbps を下回っているか、ポートに何も接続されていません。
- Gigabit：（グリーン）1G ポートの右側に配置されています。この LED は、別のデバイスがポートに接続されていて、電源がオンになっており、かつデバイス間で 1000 Mbps のリンクが確立されているときに点灯します。LED が消灯している場合は、接続速度が 1000 Mbps を下回っているか、ポートに何も接続されていません。（この機能を使用できるのは特定のモデルだけです）。
- PoE（存在する場合）：（オレンジ）ポートの右側に配置されています。LED は、対応するポートに接続されたデバイスに電力が供給されているときに点灯します。（この機能を使用できるのは特定のモデルだけです）。

スイッチの設定

スイッチにアクセスして管理には、IP ネットワーク経由で Web ベースのインターフェイスを使用か、コンソールポートを介してスイッチのコマンドライン インターフェイスを使用します。コンソールポートを使用する方法は、高度なユーザースキルを必要とし、特定のモデルでのみサポートされています。

次の表に、スイッチを最初に設定するときに使用されるデフォルト設定を示します。

パラメータ	デフォルト値
Username	cisco
Password	cisco
LAN IP	192.168.1.254

Web ベースのインターフェイスを使用したスイッチの設定

Webベースのインターフェイスを使用してスイッチにアクセスするには、スイッチが使用しているIPアドレスを知っている必要があります。スイッチは工場出荷時のIPアドレス192.168.1.254（サブネット /24）を使用します。スイッチが工場出荷時の IP アドレスを使用している場合は、システム LED が点滅したままになります。スイッチが DHCP サーバによって割り当てられた IP アドレスを使用している場合、または管理者によって静的 IP アドレスが設定されている場合は、システムLEDが緑色に点灯します（DHCPはデフォルトで有効になっています）。

ネットワーク接続を介してスイッチを管理している場合に、DHCPサーバを介して、または手動でスイッチの IP アドレスを変更すると、スイッチにアクセスできなくなります。スイッチが使用している新しい IP アドレスをブラウザに入力して Web ベースのインターフェイスを使用する必要があります。コンソールポート接続を使用してスイッチを管理している場合には、リンクは保持されます。

Web ベースのインターフェイスを使用してスイッチを設定する手順は次のとおりです。

ステップ 1 コンピュータとスイッチの電源をオンにします。

ステップ 2 コンピュータを任意のネットワーク ポートに接続します。

ステップ 3 コンピュータで IP 設定を行います。

a) スイッチがデフォルトの静的 IP アドレス 192.168.1.254/24 を使用している場合は、192.168.1.2 ～ 192.168.1.253 の範囲でまだ使用されていない IP アドレスをコンピュータ用に選択する必要があります。

b) IP アドレスが DHCP によって割り当てられる場合は、DHCP サーバが動作していて、スイッチおよびコンピュータから DHCP サーバにアクセスできることを確認します。デバイスが DHCP サーバから割り当てられた IP アドレスを検出するために、デバイスの切断と再接続が必要な場合があります。

（注） コンピュータで IP アドレスを変更する方法の詳細については、使用しているアーキテクチャとオペレーティング システムのタイプによって異なります。コンピュータ固有のヘルプとサポート機能を使用して、「IP アドレッシング」を検索してください。

ステップ 4 Web ブラウザ ウィンドウを開きます。

ステップ 5 スイッチの IP アドレスをアドレス バーに入力し、Enter を押します（例：http://192.168.1.254）。

ステップ 6 ログイン ページが表示されたら、Web ベースのインターフェイスで使用する言語を選択し、ユーザ名とパスワードを入力します。

デフォルトのユーザ名は cisco です。デフォルトのパスワードは cisco です。ユーザ名とパスワードは、どちらも大文字と小文字が区別されます。

ステップ 7 [Log In] をクリックします。

ステップ 8 デフォルトのユーザー名とパスワードで初めてログインする場合、[Change username and Password]。新しいユーザー名およびパスワードを入力して確認します。

デフォルトのユーザー名とパスワードで初めてログインする場合、[Change username and Password]

ページが開きます

（注） パスワードを作成する前に、ログイン設定 （308 ページ）のパスワードの複雑さのルールに関するセクションを参照してください。

ステップ 9 [Apply] をクリックします。

注意 Web ベースのインターフェイスを終了する前に[Save] アイコンをクリックして、設定の変更内容を必ず保存してください。設定を保存する前に終了すると、すべての変更内容が失われます。

[はじめに] ページが開きます。これで、スイッチを設定する準備が整いました。詳細については、『Administration Guide』またはヘルプ ページを参照してください。

コンソール ポートを使用したスイッチの設定

特定のモデルでのみサポートされているコンソールポートを使用してスイッチを設定するには、次の手順を実行します。

ステップ 1 シスコのコンソールケーブル（別売）またはミニUSBコネクタ付きケーブルを使用して、コンピュータをスイッチのコンソールポートに接続します。

ステップ 2 コンピュータで Hyper Terminal などのコンソール ポート ユーティリティを起動します。

ステップ 3 次のパラメータを使用してユーティリティを設定します。

- 115200 ビット/秒
- 8 データ ビット
- パリティなし

- 1 ストップ ビット
- フロー制御なし

ステップ 4 ユーザ名とパスワードを入力します。デフォルトのユーザ名は cisco、デフォルトのパスワードは cisco です。ユーザ名とパスワードは、どちらも大文字と小文字が区別されます。

デフォルトのユーザ名とパスワードで初めてログオンすると、次のメッセージが表示されます。

```
Please change your username AND password from the default settings. Change of credentials
 is required for better protection of your network.
Please note that new password must follow password complexity rules
```

ステップ 5 新しい管理者ユーザー名とパスワードを設定します。

注意 終了する前に、必ず設定変更を保存してください。

これで、スイッチを設定する準備が整いました。ご使用のスイッチの『CLI Guide』を参照してください。

（注） ネットワークで DHCP を使用していない場合、スイッチの IP アドレスのタイプをスタティックに設定し、スタティック IP アドレスおよびサブネット マスクを変更してネットワーク トポロジに合わせてください。この変更を実施しないと、複数のスイッチで工場出荷時のデフォルト IP アドレス 192.168.1.254 が共通に使用される可能性があります。

コンソールアクセスは、Web インターフェイス経由では利用できないデバッグアクセス用の追加インターフェイスも提供します。これらのデバッグアクセスインターフェイスは、デバイスの動作をデバッグする必要がある場合に、シスコサポートチームの担当者が使用することを目的としています。これらのインターフェイスはパスワードで保護されています。パスワードは、シスコサポートチームが保持します。デバイスは、次のデバッグ アクセス インターフェイスをサポートしています。

- ブートシーケンス時の U-BOOT アクセスU-BOOT
- ブートシーケンス時の Linux カーネルアクセス
- 実行時デバッグモード：シスコサポートチームがデバイス設定を表示し、プロトコルとレイヤ 1 のデバッグコマンドおよび設定を適用できます。実行時デバッグモードには、コンソールに加えて、Telnet および SSH 端末経由でアクセスできます。

工場出荷時設定の復元

スイッチの工場出荷時設定を復元するには、[Reset] ボタンを使用してスイッチを再起動またはリセットし、次の手順を実行します。

- スイッチを再起動するには、リセット ボタンを 10 秒未満押し続けます。
- スイッチを工場出荷時設定に復元するには、次の手順に従います。

- スイッチをネットワークから接続解除するか、ネットワーク上のすべてのDHCPサーバを無効にします。
- 電源をオンにした状態で**リセット**ボタンを10秒以上押し続けます。

ナビゲーション

各UIページの右上にあるナビゲーションメニューには、デバイスの主な機能のリストが表示されます。一連のカスケードメニューを使用して、各機能のUIページにアクセスできます。個々のUIページにアクセスするには、ナビゲーションメニューの対応する機能タブをクリックしてサブカテゴリのメニューを表示します。サブカテゴリを選択し、目的のページが表示されるまでこのプロセスを繰り返します。ページを選択すると、そのページがメインウィンドウに表示されます。

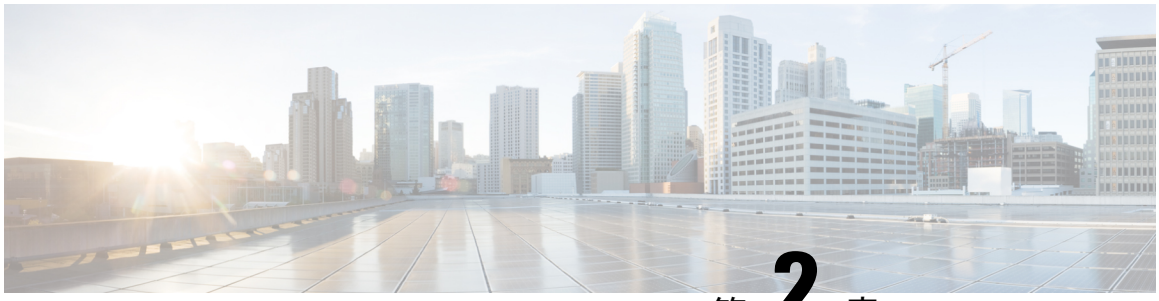
基本および拡張表示モード

この製品は多くの機能をサポートしているため、WEB GUIには数百もの設定ページと表示ページが含まれています。これらのページは、次の表示モードに分けられます。

- 基本：設定オプションの基本的なサブセットを使用できます。必要な設定オプションが表示されない場合は、デバイス ヘッダーで拡張モードを選択します。
- 拡張：すべての設定オプションを使用できます。

ユーザが基本から拡張に切り替えると、ブラウザはページをリロードします。ただし、リロード後は、ユーザーは同じページに留まります。ユーザが拡張から基本に切り替えると、ブラウザはページをリロードします。そのページが基本モードに存在する場合、ユーザは同じページにとどまります。そのページが基本モードに存在しない場合、ブラウザは、ユーザが使用していたフォルダの最初のページをロードします。フォルダが存在しない場合は、[Getting Started]ページが表示されます。

拡張設定が存在し、ページが基本モードでロードされた場合は、ユーザーにページレベルメッセージが表示されます（たとえば、設定されているRADIUSサーバーが2つ存在するが、基本モードで表示できるサーバーは1つだけの場合や、時間範囲が設定されている802.1Xポート認証が存在するが、基本モードでは時間範囲が表示されない場合など）。一方のモードから他方のモードに切り替えると、ページで行われたすべての設定（適用なし）が削除されます。



第 2 章

使用する前に

この章の内容は、次のとおりです。

使用する前に

ここでは、デバイスの設置および管理方法について説明します。

[Getting Started] をクリックすると、さまざまなリンクを使用し、画面の指示に従ってスイッチをすばやく設定できるページに移動します。

基本および拡張表示モード

スイッチの WEB GUI には何百もの設定ページと表示ページが含まれています。これらのページは、次の表示モードに分けられます。

- [Basic]：コンフィギュレーション オプションの基本サブセット。
- [Advanced]：すべてのコンフィギュレーション オプションを利用可能。

一方のモードから他方のモードに切り替えると、ページで行われたすべての設定（適用なし）が削除されます。

初期設定

スタック管理	スタック管理 （69 ページ）
管理アプリケーションおよびサービスの変更	TCP/UDPサービス （333 ページ）
デバイス IP アドレスの変更	IPv4インターフェイス （231 ページ）
VLAN を作成（Create VLAN）	VLAN 設定 （163 ページ）
ポートの設定	ポート設定 （135 ページ）

使用する前に

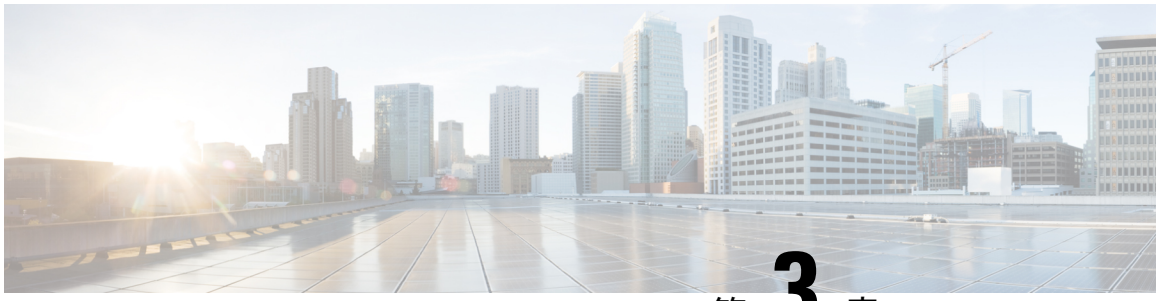
デバイス ステータス

システム概要	システム概要 （39 ページ）
Port 統計	Interface （43 ページ）
RMON 統計	統計情報 （56 ページ）
[ログの表示（View Log）]	RAMメモリ （64 ページ）

クイック アクセス

デバイス パスワードの変更	ユーザ アカウント （70 ページ）
デバイス ソフトウェアのアップグレード	ファームウェア操作 （84 ページ）
デバイス設定のバックアップ	ファイル操作 （87 ページ）
MAC ベースの ACL の作成	MACベースACL （385 ページ）
IP ベースの ACL の作成	IPv4 ベース ACL （387 ページ）
QoS の設定	QoSプロパティ （399 ページ）
SPAN の設定	SPAN および RSPAN （49 ページ）

[Getting Started] ページには、シスコ Web ページの詳細情報にアクセスするための 2 つのホット リンクがあります。[Support] リンクをクリックすると、デバイスの製品サポート ページに移動し、[Forums] リンクをクリックすると、サポート コミュニティ ページに移動します。



第 3 章

ダッシュボード

この章の内容は、次のとおりです。

ダッシュボード

ダッシュボードは8個の四角形の集合で、初めは空ですが、さまざまなタイプの情報を入力できます。使用可能なモジュールから複数のモジュールを選択し、グリッドに配置できます。現在表示されているモジュールの設定をカスタマイズすることもできます。ダッシュボードをロードすると、選択したダッシュボード モジュールがグリッドの所定の場所にロードされます。モジュールのデータは、モジュールのタイプに応じた間隔で更新されます。

ダッシュボードを開くと、グリッドのワイヤフレームビューが表示されます。現在表示されていないモジュールを表示するには、[Customize] をクリックします。モジュールを追加するには、右側にあるモジュールのリストからモジュールを選択し、グリッド内の任意のスペースにドラッグアンドドロップします。

モジュールは次のグループに分類されます。

- スモールモジュールは 1 つの四角形を占有するモジュールです。
- ラージ モジュールは 2 つの四角形を占有するモジュールです。

現在占有されているスペースにモジュールをドラッグすると、新しいモジュールによって古いモジュールが置き換えられます。グリッド内のモジュールの配置を再配置するには、モジュールを占有しているグリッド位置から別の位置にドラッグします。[Done] をクリックした場合にのみ、関連する情報がモジュールに読み込まれます。ダッシュボードの各モジュールのタイトルバーには、モジュールのタイトルと 3 つのボタンが表示されます。

- 鉛筆（）：設定オプション（モジュールによって異なる）を開きます。
- 更新（）：情報を更新します。
- X：モジュールをダッシュボードから削除します。

表 *3:* スモールモジュール

システムの正常性	[System Health] には、デバイスの状態に関する情報が表示されます。
	• Fan Status
	  • 黄色：ファンが故障しているため、冗長ファンによってバックアップされます。
	  • 緑：ファンは動作可能です。
	  • 赤色：ファンは故障しています。
	• [Thermometer Status]
	  • 緑色：正常な温度です。
	  • 黄色：警告が出る温度です。
	  • 赤色：危険な温度です。

リソース使用率	このモジュールには、さまざまなシステムリソースの利用状況が棒グラフでパーセント表示されます。 次のリソースをモニタできます。 • [Multicast Groups]：定義可能な上限数に対する、実際に存在するマルチキャスト グループのパーセンテージ。 • [MAC Address Table]：MAC アドレス テーブルの使用率。 • [TCAM]：QoS エントリと ACL エントリによる TCAM の使用率。 • [CPU]：CPU の使用率。

ID	このモジュールには、デバイスに関する基本情報が表示されます。次のフィールドが表示されます。 • [システムの説明]：デバイスの説明を表示します。 • [Host Name]：システム設定 （67 ページ）で入力した名前、またはデフォルトが使用されます。 • [Firmware Version]：デバイス上で動作している現在のファームウェアのバージョン。 • [MAC Address]：デバイスの MAC アドレス。 • [Serial Number]：デバイスのシリアル番号。 • [システムロケーション]（設定されている場合）：デバイスの物理的な場所を入力します。 • [システムコンタクト先]（設定されている場合）：担当者の名前を入力します。 • [総有効電力]（PoEデバイスの場合のみ）：デバイスに使用可能な電力量。 • [現在の電力消費量]（PoEデバイスの場合のみ）：デバイスで消費されている電力量。

PoE 使用率	このモジュールには、PoE の利用状況がグラフィック形式で表示されます。スタンドアロンユニットの場合、このモジュールには 0 ～ 100 の値の目盛りが付いた計器が表示されます。目盛りのトラップしきい値から 100 までの範囲は赤色です。計器の中央に、実際の PoE 使用率がワット単位で表示されます。 それぞれの横棒は、デバイスの PoE 使用率を 0 ～ 100 の範囲で表します。PoE 使用率がトラップしきい値を超えると、横棒が赤色になります。それ以外の場合、横棒は緑色です。横棒上にカーソルをポイントすると、そのデバイスの実際の PoE 使用率をワット単位で表すツールチップが表示されます。追加のビューを設定オプション（右上隅の鉛筆のアイコン）で選択できます。 • [Refresh Time]：表示されるオプションのいずれかを選択します。 • [PoE Global Properties]：[Port Management] > [PoE] > [Properties] ページへのリンク。 • [PoE Port Settings]：[Port Management] > [PoE] > [Settings] ページへのリンク。 （注） この項は、PoE をサポートするデバイスのみに関係します。

表 *4:* ラージモジュール

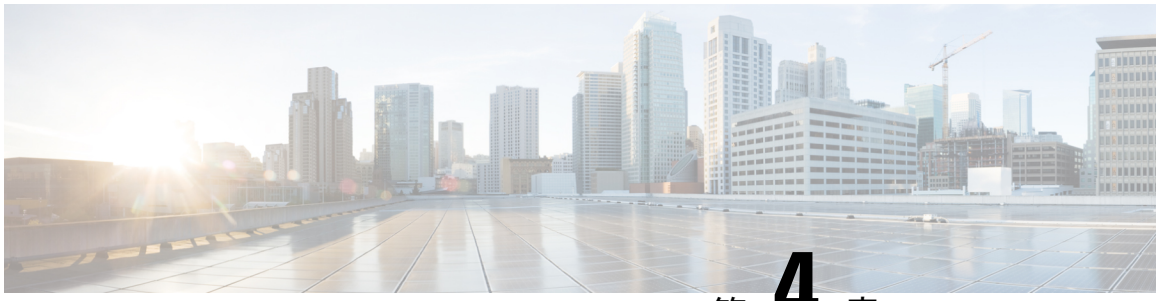
最新のログ	このモジュールには、システムにより SYSLOG としてログに書き込まれた、最新の 5 つのイベントに関する情報が含まれています。次の設定オプション（右上隅）を使用できます。 • [Severity Threshold]：ログ設定 （80 ページ）を参照。 • [Refresh Time]：表示されるオプションのいずれかを選択します。 • [View logs]：クリックするとRAMメモリ （64 ページ）が開きます。

中断されたインターフェイス	このモジュールには、一時停止されたインターフェイスがデバイス ビューまたはテーブル ビューのどちらかで表示されます。ビューは設定オプションの [Display Option]（右上隅にある鉛筆アイコン）で選択します。 • [Device View]：このビューには、デバイスが表示されます。ユニットどうしがスタック内で接続されている場合、ドロップダウン セレクタで、表示するデバイスを選択できます。デバイス内の一時停止されたすべてのポートが赤色で表示されます。 • [Table View]：このビューでは、特定のスタックユニットを選択する必要はありません。情報は、次のように表形式で表示されます。 • [Interface]：一時停止されたポートまたは LAG。 • [Suspension Reason]：インターフェイスが一時停止された理由。 • [Auto-recovery current status]：一時停止の原因となった機能に対して自動修復が有効になっているかどうか。 次の設定オプション（右上隅）を使用できます。 • [Refresh Time]：表示されたオプションのいずれかを選択します。 • [Error Recovery Settings]：クリックするとエラー回復設定（139 ページ）が開きます。
スタックトポロジ	このモジュールには、スタックトポロジがグラフィック形式で表示されます。動作については、[Stack Topology View] と同じです。次のフィールドが表示されます。 • [Stack Topology]：チェーンまたはリングのいずれか。 • [Stack Active Unit]：スタックのアクティブユニットとして機能するユニット数が表示されます。 モジュール内のユニットにマウスカーソルを合わせると、ユニットを識別し、そのユニットのスタッキングポートに関する基本情報を提供するツールチップが表示されます。モジュール内のスタック接続にマウスカーソルを合わせると、接続されているユニットとその接続が行われているスタッキングポートの詳細情報に関するツールチップが表示されます。

ポート使用率	このセクションには、デバイスのポート使用率が表示されます。ビューは、設定オプション（右上隅の鉛筆のアイコン）で選択します。
	• [Display Mode] - [Device View]：デバイスが表示されます。ポートにカーソルを置くと、そのポートに関する情報が表示されます。
	• [Display Mode] - [Chart View]：ポートの一覧と各ポート使用状況が表示されます。ポートごとに、次のポート使用率情報を確認できます。
	  • 送信—%（赤色）
	  • 受信—%（青色）
	• [Refresh Time]：表示されるオプションのいずれかを選択します。
	• [Interface Statistics]：[Status and Statistics] > [Interface] ページへのリンク。

トラフィックエラー	このモジュールには、RMON 統計情報に関してカウントされたさまざまなタイプのエラーパケットの数が表示されます。ビューは、設定オプション（右上隅の鉛筆のアイコン）で選択します。 • [Display Mode] - [Device View] デバイス モジュール モードの場合、デバイスのダイアグラムが表示されます。デバイス内の一時停止されたすべてのポートが赤色で表示されます。 一時停止されたポートにマウスカーソルを合わせると、次の情報を含むツールチップが表示されます。 • ポート名。 • ポートが LAG のメンバーである場合は、ポートの LAG アイデンティティ。 • ポート上でログに書き込まれた最新のエラーの詳細情報。 • [Display Mode] - [Table View] • [Interface]：ポートの名前。 • [最後のトラフィックエラー]：ポート上で発生したトラフィックエラーと、エラーが発生した最後の時刻。 • [Refresh Time]：いずれかのリフレッシュレートを選択します。 • [Traffic Error Information]：統計情報 （56 ページ）へのリンクをクリックします。

ダッシュボード



第 4 章

設定ウィザード

この章は、次の項で構成されています。

開始ウィザード

開始ウィザードは、デバイスの初期設定に役立ちます。

ステップ 1 [Configuration Wizards] > [Getting Started Wizard] の順に移動して、[Launch Wizard] をクリックします。

ステップ 2 [Launch Wizard] をクリックして、[Next] をクリックします。

ステップ 3 [General Information] タブのフィールドに入力します。

- [System Location]：デバイスの物理的な場所を入力します。
- [システムコンタクト先]：担当者の名前を入力します。
- [Host Name]：デバイスのホスト名を選択します。これは CLI コマンドのプロンプトで使用されます。
  - [Use Default]：スイッチのデフォルトのホスト名（システム名）は switch 123456 の形式で指定されます。123456 はデバイスの MAC アドレスの最後の 3 バイトを 16 進数で表しています。
  - [ユーザー定義]：ホスト名を入力します。文字、数字、ハイフンだけが使用できます。ホスト名の最初と最後にハイフンを使用することはできません。（RFC1033、1034、1035 で指定されているように）他の記号、区切り文字、または空白スペースは使用できません。

ステップ 4 [Next] をクリックします。

ステップ 5 [IP Settings] タブのフィールドに入力します。

- [Interface]：システムの IP インターフェイスを選択します。
- [IP Interface Source]：次のいずれかのオプションを選択できます。

- [DHCP]：デバイスが自身の IP アドレスを DHCP サーバから受信する場合に選択します。
- [Static]：デバイスの IP アドレスを手動で入力する場合に選択します。

- [IP Interface Source] で [Static] を選択した場合には、次のフィールドを入力します。
  - [IP Address]：インターフェイスの IP アドレス。
  - [Network Mask]：このアドレスの IP マスク。
  - [Administrative Default Gateway]：デフォルトのゲートウェイ IP アドレスを入力します。

- [DNS Server]：DNS サーバーの IP アドレスを入力します。

ステップ 6 [Next] をクリックします。

ステップ 7 [User Account] タブのフィールドに入力します。

- [Username]：新しいユーザ名を 0 ～ 20 文字の範囲で入力します。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）。
- [パスワードの確認]：パスワードを再度入力します。
- [Password Strength]：パスワードの強度が表示されます。
- [Keep current username and password]：現在のユーザ名とパスワードを保持する場合に選択します。

ステップ 8 [Next] をクリックします。

ステップ 9 [Time Settings] タブのフィールドに入力します。

- [Clock Source]：次のいずれかを選択します。
  - [手動設定]：デバイスシステム時刻を入力する場合に選択します。これを選択した場合は、[Date] と [Time] を入力します。
  - [Default SNTP Servers]：デフォルトの SNTP サーバを使用する場合に選択します。

    （注） デフォルト SNTP サーバーは名前で定義されているため、DNS を設定して動作可能にする必要があります。

  - [Manual SNTP Server]：選択した場合は、SNTP サーバの IP アドレスを入力します。

ステップ 10 [Next] をクリックすると、入力した設定の概要が表示されます。

ステップ 11 [Apply] をクリックして、設定データを保存します。

VLAN設定ウィザード

VLAN設定ウィザードは、VLANの設定を支援します。このウィザードを実行するたびに、単一の VLAN 上でポートメンバーシップを設定できます。VLAN 設定ウィザードを使用して VLAN を設定するには、次の手順を実行します。

ステップ 1 [Configuration Wizards] > [VLAN Configuration Wizard] の順に移動して、[Launch Wizard] をクリックします。

ステップ 2 [Launch Wizard] をクリックして、[Next] をクリックします。

ステップ 3 トランク ポートとして設定するポートを選択します（グラフィック表示で必要なポートをマウスでクリックします）。トランク ポートとしてすでに設定されているポートが事前に選択されています。

ステップ 4 [Next] をクリックします。

ステップ 5 [VLAN Configuration] セクションで、次の項目を設定します。

- [VLAN ID]：設定する VLAN を選択します。既存の VLAN または [New VLAN] のいずれかが選択できます。
- [New VLAN ID]：新しい VLAN の VLAN ID を入力します。
- [VLAN Name]：オプションで、VLAN 名を入力します。

ステップ 6 VLAN のタグなしメンバーとして設定するトランク ポートを選択します（グラフィック表示で必要なポートをマウスでクリックします）。このステップで選択されていないトランク ポートは、VLAN のタグ付きメンバーになります。

ステップ 7 [Next] をクリックします。

ステップ 8 VLAN のアクセス ポートに設定するポートを選択します。VLAN のアクセス ポートは、VLAN のタグなしメンバーです（グラフィック表示で必要なポートをマウスでクリックします）。

ステップ 9 [Next] をクリックして、入力した情報の概要を確認します。

ステップ 10 [Apply] をクリックします。

ACL 設定ウィザード

ACL 設定ウィザードは、新しい ACL を作成、または既存の ACL を編集する際に使用します。既存の ACL を追加または変更するには、次の手順を実行します。

ステップ 1 [Configuration Wizards] > [ACL Configuration Wizard] の順に移動して、[Launch Wizard] をクリックします。

ステップ 2 新規 ACL を作成するには、[次へ] をクリックします。既存の ACL を編集するには、[ACL] ドロップダウン リストから編集対象を選択して [次へ] をクリックします。

ステップ 3 次のフィールドに入力します。

- [ACL Name]：新しい ACL の名前を入力します。
- [ACL Type]：ACL の種類を、[IPv4] または [MAC] から選択します。

ステップ 4 ACE 構成では、次のフィールドを設定します。

- [Action on match]：次のいずれかのオプションを選択します。
  - [トラフィックの許可]：ACE 条件に一致するパケットを転送します。
  - [トラフィックの拒否]：ACE 条件に一致するパケットをドロップします。
  - [インターフェイスのシャットダウン]：ACE 条件に一致するパケットをドロップし、パケットが受信されたポートを無効にします。

ステップ 5 MAC ベースの ACL の場合には、次のフィールドに入力します。

Source MAC Address	すべての送信元アドレスを許可する場合は [Any] を選択します。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 [User defined] を選択します。
送信元MACの値	送信元 MAC アドレスが一致する MAC アドレスとマスク（該当する場合）を入力します。
送信元MACワイルドカードマスク	MAC アドレスの範囲を定義するための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許可する場合は [Any] を選択します。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 [User defined] を選択します。
宛先MACの値	宛先 MAC アドレスが一致する MAC アドレスとマスクを入力します（該当する場合）。
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ための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用途とは異なる点に注意してください。ここでビットを 1 と設定すると、その値を気にしないことを意味し、0 はその値をマスクすることを意味します。 （注） 0000 0000 0000 0000 0000 0000 1111 1111 というマスクを例に説明します。この場合、0 になっているビットは照合され、1 になっているビットは照合されません。1 は 10 進数の整数に変換する必要があり、ゼロ 4 つごとに 0 を記述します。この例では 1111 1111 = 255 であるので、マスクは 0.0.0.255 と記述されます。
時間範囲名	[Time Range] を選択した場合、使用する時間範囲を選択します。

ステップ 6 IPv4 ベースの ACL の場合には、次のフィールドに入力します。

プロトコル（Protocol）	特定のプロトコルに基づいてACLを作成するには、次のいずれかのオプションを選択します。 • [任意(IP)]：すべての IP プロトコル パケットを受け入れます。 • [TCP]：伝送制御プロトコル パケットを受け入れます。 • [UDP]：ユーザー データグラム プロトコル 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の送信元ポート	ドロップダウンリストからポートを選択します。
TCP/UDPの宛先ポート	ドロップダウンリストからポートを選択します。
送信元 IP アドレス	すべての送信元アドレスを許可する場合は [Any] を選択します。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 [User defined] を選択します。
送信元IPの値	送信元 IP アドレスの照合に使用する 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ための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用途とは異なる点に注意してください。ここでビットを 1 と設定すると、その値を気にしないことを意味し、0 はその値をマスクすることを意味します。
宛先IPアドレス	すべての IP アドレスを許可する場合は [Any] を選択します。宛先 IP アドレスまたは宛先 IP アドレスの範囲を入力する場合は [User defined] を選択します。
宛先IPの値	宛先 IP の値と一致させる IP の値を入力します。
宛先IPワイルドカードマスク	IPアドレスの範囲を定義するための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用途とは異なる点に注意してください。ここでビットを 1 と設定すると、その値を気にしないことを意味し、0 はその値をマスクすることを意味します。
時間範囲名	[Time Range] を選択した場合、使用する時間範囲を選択します。

ステップ 7 [Next] をクリックします。

ステップ 8 ACL と ACE を作成することを確認します。

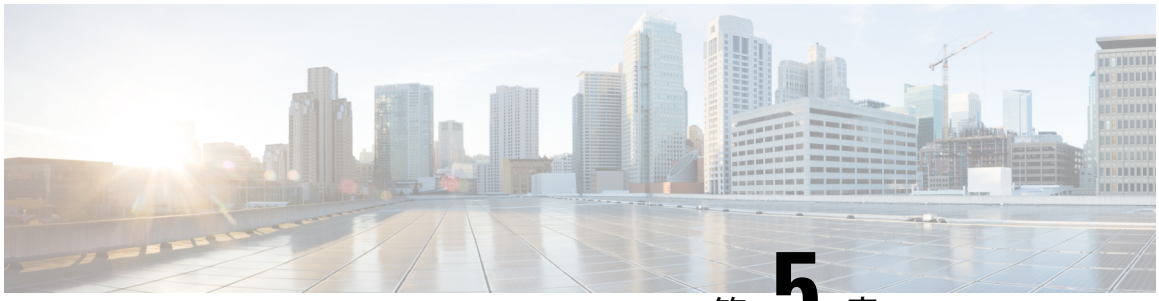
ACL ルールの詳細が表示されます。[Add another rule to this ACL] をクリックして、別のルールを追加することもできます。

ステップ 9 [Next] をクリックして、ACL バインド情報を入力します。

- [Binding Type]：ACL をバインドするためのオプションを次のいずれかから選択します。

- [物理インターフェイスのみ]：ACL をポートにバインドします。ACL をバインドするポートを 1 つまたは複数クリックします。
- [VLANのみ]：ACL を VLAN にバインドします。[Enter the list of VLANs you want to bind the ACL to] 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。

[Apply] をクリックします。



第 5 章

検索

この章の内容は、次のとおりです。

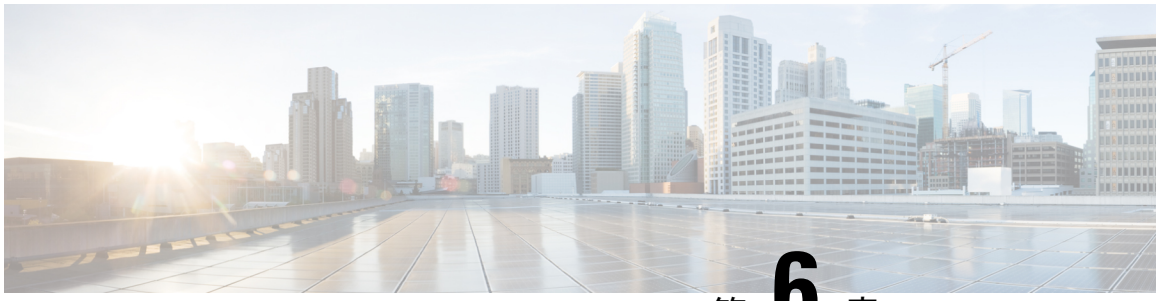
検索

検索機能によって、関連する GUI ページを容易に特定することができます。

キーワードの検索結果には、関連ページへのリンクに加えて、関連ヘルプページへのリンクも含まれます。

検索機能にアクセスするには、キーワードを入力し、虫めがねアイコンをクリックします。

検索



第 6 章

ステータスと統計情報

この章は、次の項で構成されています。

システム概要

[System Summary] には、デバイスの状態、ハードウェア、ファームウェアバージョン、一般的な PoE ステータスなどのシステム情報のプレビューが表示されます。

システム情報を表示するには、[Status and Statistics] > [System Summary] をクリックします。

システム情報

[System Information] セクションでは、デバイスに関する情報を簡単に取得できます。このセクションでは、次の情報を確認できます。

- [システムの説明] : システムの説明。

- システムの場所（System Location）：デバイスの物理的な場所。この値を入力するには、[Edit] をクリックし、システム設定 （67 ページ）に移動します。
- [システムコンタクト先]：担当者の名前。この値を入力するには、[Edit] をクリックし、システム設定 （67 ページ）に移動します。
- [Host Name]：デバイスの名前。この値を入力するには、[Edit] をクリックし、システム設定 （67 ページ）に移動します。デフォルトでは、デバイス ホスト名は、単語「switch」にデバイスの MAC アドレスの 3 最下位バイト（最も右側の16進数の 6 桁）が連結されて構成されます。
- システム オブジェクト ID（System Object ID）：エンティティに含まれるネットワーク管理サブシステムの一意なベンダー ID（SNMP で使用される）。
- [システムアップタイム]：最後のリブートから経過した時間。

（注） システム稼働時間については、スイッチが 21 日 + 20 時間 + 14 分および 58 秒経過すると、時間がリセットされます。スイッチが再起動しない場合、21 日 + 20 時間 + 14 分および 58 秒で稼働時間がリセットされ、最初から開始されます。

- [現在の時刻]：現在のシステム時刻。
- [Base MAC Address]：デバイスの MAC アドレス。
- [ジャンボフレーム]：ジャンボ フレーム サポート ステータス。このサポートは、ポート設定 （135 ページ）で有効または無効にできます。

（注） ジャンボ フレームのサポートは、有効にした後、デバイスがリブートした後でのみ反映されます。

ソフトウェア情報

[Software Information] セクションでは、デバイスで実行されているソフトウェアに関する情報をすばやく取得できます。このセクションでは、次の情報を確認できます。

- ファームウェア バージョン（Firmware Version）（アクティブ イメージ）：アクティブなイメージのファームウェア バージョン番号。
- ファームウェア MD5 チェックサム（Firmware MD5 Checksum）（アクティブ イメージ）：アクティブなイメージの MD5 チェックサム。
- ファームウェア バージョン（非アクティブ）（Firmware Version (Non-active)）：非アクティブなイメージのファームウェア バージョン番号。システムがスタック内に存在する場合、アクテイブユニットのバージョンが表示されます。

- ファームウェア MD5 チェックサム（非アクティブ）（Firmware MD5 Checksum (Non-active)）：非アクティブなイメージの MD5 チェックサム。

TCP/UDPサービスステータス

次のフィールドをリセットするには、[Edit] をクリックします。以下の設定が表示されます。

- HTTP サービス（HTTP Service）：HTTP が有効か無効かを示します。
- HTTPS サービス（HTTPS Service）：HTTPS が有効か無効かを示します。
- SNMP サービス（SNMP Service）：SNMP が有効か無効かを示します。
- Telnet サービス（Telnet Service）：Telnet が有効か無効かを示します。
- SSH サービス（SSH Service）：SSH が有効か無効かを示します。

PoE 対応デバイスの PoE 電源情報

[PoE Power Information on Device Supporting PoE] セクションでは、デバイスの PoE 情報を簡単に取得できます。このセクションでは、次のように表示されます。

- [PoE Power Information]：[Detail] をクリックすると、プロパティ（149 ページ）に直接リンクします。このページには PoE 電源情報が表示されます。
- 最大使用可能な PoE 電力（W）（Maximum Available PoE Power (W)）：スイッチによって供給可能な最大の使用可能電力。
- PoE 電力消費（W）の合計（Total PoE Power Consumption (W)）：接続された PoE デバイスに供給された PoE 電力の合計。
- [PoE 電源モード]：ポート制限またはクラス制限。

ユニットはグラフィカルに表示され、ポートにカーソルを置くとその名前が表示されます。

ユニットごとに、次の情報が表示されます。

- [Unit 1 (Active)]：デバイスモデル ID。
- [シリアル番号]：シリアル番号。

CPU 使用率

デバイス CPU は、管理インターフェイスでのエンドユーザ トラフィック処理に加え、次のタイプのトラフィックを処理します。

- 管理トラフィック
- プロトコル トラフィック

- スヌーピング トラフィック

過剰なトラフィック負荷が CPU にかかると、通常のデバイス操作が妨げられることがあります。デバイスは、セキュアコアテクノロジー（SCT）を使用することにより、管理トラフィックとプロトコルトラフィックの受信および処理を確実に実行できます。SCT はデバイスでデフォルトで有効になっています。無効にすることはできません。

CPU 使用率を表示するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [CPU Utilization] の順にクリックします。

[CPU Input Rate] フィールドに、1 秒あたりの CPU への入力フレームのレートが表示されます。ウィンドウには、デバイスの CPU 使用率を表示するグラフが含まれています。Y 軸が使用率で、X 軸がサンプル番号です。

ステップ 2 [Enable] をオンにして、CPU 使用率を有効にします。

ステップ 3 統計を更新する前に経過させる [Refresh Rate]（秒単位の期間）を選択します。期間ごとに新しいサンプルが作成されます。

デバイスの CPU 使用率を表示するグラフを含むウィンドウが表示されます。

ポート使用率

[ポート使用率]ページには、ポートあたりのブロードバンド（着信と発信の両方）の使用率が表示されます。

ポート使用率を表示するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [Port Utilization] をクリックします。

ステップ 2 インターフェイスのイーサネット統計を更新する前の経過期間として、[Refresh Rate] を入力します。

ポートごとに、次のフィールドが表示されます。

- [Interface]：ポートの名前。
- Tx 使用率（Tx Utilization）：発信パケットによって使用された帯域幅の量。
- Rx 使用率（Rx Utilization）：着信パケットによって使用された帯域幅の量。

ポートの時間の経過に伴う履歴使用率のグラフを表示するには、ポートを選択し、[インターフェイス履歴グラフの表示（View Interface History Graph）] をクリックします。上記に加えて、次のフィールドが表示されます。

- 時間スパン（TimeSpan）：時間の単位を選択します。グラフには、この時間単位のポート使用率が表示されます。

Interface

[インターフェイス]ページには、トラフィック統計情報がポート別に表示されます。このページは、送受信されるトラフィック量とその分散（ユニキャスト、マルチキャスト、ブロードキャスト）を分析するのに便利です。

イーサネット統計情報を表示したり、リフレッシュレートを設定したりするには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [Interface] をクリックします。

ステップ 2 テーブル表示またはグラフィック表示で統計カウンタを表示するには、次の手順を実行します。

- すべてのカウンタをクリアするには、[Clear Interface Counters] をクリックします。
- カウンタを更新するには、[Refresh] をクリックします。
- すべてのポートをテーブル表示で確認するには、[View All Interfaces Statistics] をクリックします。
- これらの結果をグラフィック形式で表示するには、[View Interface History Graph] をクリックします。そのインターフェイスに関する統計を表示するには、[Interface] を選択します。

ステップ 3 パラメータを入力します。

- インターフェイス（Interface）：イーサネット統計を表示するインターフェイスを選択します。
- [リフレッシュレート]：インターフェイスイーサネット統計情報がリフレッシュされるまでの時間を選択します。

ステップ 4 [Receive Statistics] セクションには次の統計が表示されます。

- 合計バイト（オクテット）（Total Bytes (Octets)）：受信オクテット数。不良パケットと FCS オクテットを含むが、フレーミング ビットは除く。
- [ユニキャストパケット]：受信された正常なユニキャスト パケット数。
- [マルチキャストパケット]：受信された正常なマルチキャスト パケット数。
- [ブロードキャストパケット]：受信された正常なブロードキャスト パケット数。
- [エラーがあるパケット]：受信されたエラーのあるパケット数。

ステップ 5 [Transmit Statistics] セクションには次の統計が表示されます。

- 合計バイト（オクテット）（Total Bytes (Octets)）：送信オクテット数。不良パケットと FCS オクテットを含むが、フレーミング ビットは除く。

- [ユニキャストパケット] : 送信された正常なユニキャスト パケット数。
- [マルチキャストパケット] : 送信された正常なマルチキャスト パケット数。
- [ブロードキャストパケット] : 送信された正常なブロードキャスト パケット数。

Etherlike

[Etherlike] ページには、Etherlike MIB 規格定義に従って統計情報がポート別に表示されます。情報のリフレッシュ レートを選択できます。このページは、トラフィックを中断させる可能性がある物理層（レイヤ 1）でのエラーに関するより詳細な情報を提供します。

Etherlike統計情報を表示したり、リフレッシュレートを設定したりするには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [Etherlike] をクリックします。

ステップ 2 パラメータを入力します。

- [Interface]：イーサネット統計情報が表示される特定のインターフェイスを選択します。
- [Refresh Rate]：Etherlike 統計情報が更新されるまでの時間を選択します。

選択したインターフェイスに関する次のフィールドが表示されます。

- [Frame Check Sequence (FCS) Errors]：CRC（Cyclic Redundancy Check）に失敗した受信フレーム数。
- [Single Collision Frames]：シングルコリジョンに含まれるが、正常に送信されたフレーム数。
- [Late Collisions]：データの最初の 512 ビットの後に検出されたコリジョン。
- [Excessive Collisions]：過剰コリジョンが原因で拒否された送信回数。
- [Oversize Packets]：2000 オクテットを超える受信パケット。
- [Internal MAC Receive Errors]：受信側のエラーにより拒否されたフレーム。
- [Pause Frames Received]：受信したフロー制御ポーズフレーム。このフィールドは、XG ポートでのみサポートされます。ポート速度が 1 G の場合は、受信済みポーズフレームカウンタが作動しません。
- [Pause Frames Transmitted]：送信されたフレームが一時停止した数。

（注） 上記のいずれかのフィールドにエラーの数（0 以外）が表示されている場合は、最後のアップタイムが表示されます。

ステップ 3 テーブル表示で統計カウンタを表示するには、テーブル表示ですべてのポートを確認するために、[View All Interfaces Statistics] をクリックします。[Refresh] をクリックして統計情報を更新するか、または [Clear Interface Counters] をクリックしてカウンタをクリアします。

GVRP

[GARP VLAN Registration Protocol (GVRP)] ページには、ポートとの間で送受信された GVRP フレームに関する情報が表示されます。GVRP は、各種の標準規格に準拠したレイヤ 2 ネットワーク プロトコルで、スイッチ上の VLAN 情報を自動設定するためのものです。802.1Q-2005 の 802.1ak 修正で定義されています。ポートの GVRP 統計情報は、GVRP がグローバルに、ポートで有効になっている場合にのみ表示されます。

GVRPの統計情報を表示したり、リフレッシュレートを設定したりするには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [GVRP] をクリックします。

ステップ 2 パラメータを入力します。

Interface	GVRP の統計情報が表示される特定のインターフェイスを選択します。
Refresh Rate	GVRP ページが更新されるまでの経過時間を選択します。[Attribute Counter] ブロックには、インターフェイスごとのさまざまなパケット タイプのカウンタが表示されます。これらは、[Received] および [Transmitted] パケットについて表示されます。

受信済み：送信済み

Join Empty	送受信された GVRP の Join Empty パケット数。
Empty	送受信された GVRP の Empty パケット数。
Leave Empty	送受信された GVRP の Leave Empty パケット数。
Join In	送受信された GVRP の Join In パケット数。
Leave In	送受信された GVRP の Leave In パケット数。
Leave All	送受信された GVRP の Leave All パケット数。[GVRP Error Statistics] セクションには、GVRP エラー カウンタが表示されます。

GVRPエラー統計情報

無効なプロトコルID	無効なプロトコル ID エラー。
無効なアトリビュートタイプ	無効な属性 ID エラー。

無効な属性値	無効な属性値エラー。
無効なアトリビュート長	無効な属性長エラー。
無効なイベント	無効なイベント。

ステップ 3 統計カウンタをクリアするには、[Clear Interface Counters] をクリックします。

ステップ 4 すべてのインターフェイス統計を表示するには、[View All Interfaces Statistics] をクリックして、単一のページですべてのポートを確認してください。

802.1X EAP

[802.1X EAP] ページには、送受信された Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）フレームが表示されます。EAPの統計情報を表示したり、リフレッシュレートを設定したりするには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [802.1x EAP] をクリックします。

ステップ 2 統計をポーリングする [Interface] を選択します。

ステップ 3 EAP 統計を更新する前に経過させる [Refresh Rate]（期間）を選択します。

選択したインターフェイスに関する値が表示されます。

受信済みEAPOL EAPフレーム	ポートで受信した有効な EAPOL フレーム。
受信済みEAPOL開始フレーム	ポートで受信した有効な EAPOL 開始フレーム。
受信済みEAPOLログオフフレーム	ポートで受信した EAPOL ログオフフレーム。
受信済みEAPOL Announcementフレーム	ポートで受診した EAPOL 通知フレーム。
受信済みEAPOL Announcement要求フレーム	ポートで受診した EAPOL 通知要求フレーム。
受信済みEAPOL無効フレーム	ポートで受信した EAPOL 無効フレーム。
受信済みEAPOL EAP長エラーフレーム	このポートで受信したパケット本体の長さが無効な EAPOL フレーム。
受信済みCKN未認識MKPDUフレーム	このポートで受信した未認識 CKN を含む EAP フレーム。
受信済みMKPDU無効フレーム	ポートで受信した MKPDU 無効フレーム。
最終EAPOLフレームバージョン	最後に受信した EAPOL フレームに関連付けられているプロトコルバージョン番号。

最終EAPOLフレーム送信元	最後に受信した EAPOL フレームに関連付けられている送信元 MAC アドレス。
送信済みEAPOL EAPサプリカントフレーム	ポートで送信した EAPOL EAP サプリカントフレーム。
送信済みEAPOL開始フレーム	ポートで送信した EAPOL 開始フレーム。
送信済みEAPOLログオフフレーム	ポートで送信した EAPOL ログオフフレーム。
送信済みEAPOL Announcementフレーム	ポートで送信した EAPOL 通知フレーム。
送信済みEAPOL Announcement要求フレーム	ポートで送信した EAPOL 通知要求フレーム。
送信済みEAPOL認証コードフレーム	ポートで送信した EAP オーセンティケータフレーム。
送信済みCKNなしEAPOL MKAフレーム	ポートで送信した CKN を含まない MKA フレーム。

ステップ 4 統計カウンタをクリアするには、次の手順を実行します。

- [Clear Interface Counters] をクリックして、すべてのインターフェイス カウンタをクリアします。
- カウンタを更新するには、[Refresh] をクリックします。
- [View All Interfaces Statistics] をクリックして、すべてのインターフェイスのカウンタを表示します。

ACL

ACL ロギング機能が有効になっている場合は、ACL 規則に一致するパケットに関する情報 SYSLOG メッセージが生成されます。ACL に基づいてパケットが転送または拒否されたインターフェイスを表示するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [ACL] をクリックします。

ステップ 2 ページを更新する前に経過させる [Refresh Rate]（秒単位の期間）を選択します。期間ごとに新しいインターフェイス グループが作成されます。

次の情報が表示されます。

- グローバル トラップ パケット カウンタ（Global Trapped Packet Counter）：リソース不足のためにグローバルにトラップされたパケット数。
- [Trapped Packets - Port/LAG Based]：ACL ルールに基づいてパケットが転送または拒否されたインターフェイス。
- [Trapped Packets - VLAN Based]：ACL ルールに基づいてパケットが転送または拒否された VLAN。

ステップ3 統計カウンタをクリアするには、[Clear Counters] をクリックするか、[Refresh] をクリックしてカウンタを更新します。

ハードウェアリソース使用率

このページには、アクセスコントロールリスト（ACL）やサービス品質（QoS）など、デバイスが使用するリソースが表示されます。一部のアプリケーションは、それらの開始時に規則を割り当てます。また、システムブート時に初期化されるプロセスは、起動プロセス中にそれらのルールの一部を使用します。

ハードウェアリソース利用率を表示するには、[Status and Statistics] > [Hardware Resource Utilization] をクリックします。

次のフィールドが表示されます。

- ユニット番号（Unit No）：TCAM 使用率を表示する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、これは表示されません。
- IPエントリ
  - [使用中]：IP ルールで使用されている TCAM エントリ数。
  - [最大]：IP ルールで使用可能な TCAM エントリ数。
- IPv4 ポリシーベース ルーティング（IPv4 Policy Based Routing）
  - [In Use]：IPv4 ポリシーベースのルーティングに使用されるルータ TCAM エントリの数。
  - [最大]：IPv4 ポリシーベース ルーティングに使用可能なルータ TCAM エントリの最大数。
- IPv6 ポリシーベース ルーティング（IPv4 Policy Based Routing）
  - [In Use]：IPv6 ポリシーベースのルーティングに使用されるルータ TCAM エントリの数。
  - [最大]：IPv6 ポリシーベース ルーティングに使用可能なルータ TCAM エントリの最大数。
- VLAN Mapping
  - [In Use]：現在 VLAN マッピングに使用されているルータ TCAM エントリの数。
  - [最大]：VLAN マッピングに使用可能なルータ TCAM エントリの最大数。
- ACLとQoSのルール
  - [In Use]：ACL および QoS ルールで使用される TCAM エントリの数。

- [最大]：ACL および QoS ルールで使用可能な TCAM エントリの数。

ハードウェアリソースを表示するには、[Hardware Resources Management] ボタンをクリックします。

次のフィールドが表示されます。

- [Maximum IPv4 Policy-Based Routes]
  - [Use Default]：デフォルト値を使用します。
  - [User Defined]：ユーザー定義値を入力します（範囲 0 ～ 32、デフォルト 12）。
- [Maximum IPv6 Policy-Based Routes]
  - [Use Default]：デフォルト値を使用します。
  - [User Defined]：ユーザー定義値を入力します（範囲 0 ～ 32、デフォルト 12）。
- （範囲 0 ～ 32、デフォルト 12）
- Maximum VLAN-Mapping Entries
  - [Use Default]：デフォルト値を使用します。
  - [User Defined]：ユーザー定義値を入力します（範囲 0 ～ 228、デフォルト 0）。
- [Hardware-Based Routing]：ハードウェアベースのルーティングがアクティブであるか、非アクティブであるかを表示します。

SPAN および RSPAN

SPAN 機能（ポート ミラーリングまたはポート モニタリングとも呼ばれる）は、ネットワーク アナライザによって分析するネットワーク トラフィックを選択します。ネットワークアナライザは、シスコスイッチプローブデバイスまたはその他のリモートモニターリング（RMON）プローブとして使用できます。

ポート ミラーリングは、ネットワーク デバイスが、単一のデバイス ポート、複数のデバイス ポート、またはVLAN全体で検出したネットワーク パケットのコピーを、デバイスの別のポートのネットワーク モニタリング接続に送信するために使用されます。これは、侵入検知システムのように、ネットワーク トラフィックのモニタリングが必要な場合に、一般的に使用されます。モニタリング ポートに接続されているネットワーク アナライザが、データ パケットを処理します。ネットワーク ポートで受信され、ミラーリングの対象となる VLAN に指定されたパケットは、パケットが最終的にトラップまたは廃棄される場合でも、アナライザ ポートにミラーされます。デバイスによって送信されたパケットは、送信（Tx）ミラーリングがアクティブな場合に、ミラーされます。

ミラーリングは、送信元ポートからのすべてのトラフィックがアナライザ（宛先）ポートで受信されることは保証しません。サポート可能な量を超えるデータがアナライザ ポートに送信された場合、一部のデータは失われる可能性があります。

VLAN ミラーリングは、手動で作成されなかった VLAN 上では、アクティブにすることはできません。たとえば、VLAN 23 が GVRP によって作成された場合、ポート ミラーリングは動作しません。

RSPAN

RSPAN は、ネットワーク全体にわたり複数スイッチのモニタリングを可能にし、アナライザ ポートをリモート スイッチ上に定義できるようにすることで、SPAN を拡張します。開始（送信元）および最終（宛先）スイッチに加えて、トラフィックが流れる中間スイッチを定義できます。各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。開始デバイスの送信元インターフェイスからのトラフィックは、リフレクタポートを介して RSPAN VLAN にコピーされ、その後、中間デバイスの全般モードで構成されたトランクポートを経由して、RSPAN VLAN をモニタリングしている最終スイッチの宛先セッションへ転送されます。リフレクタ ポートは、RSPAN VLAN へパケットをコピーするメカニズムです。それは、さまざまなタイプのトラフィックを処理するネットワーク ポートです。RSPAN VLAN は、すべての中間スイッチに設定されている必要があります。

RSPAN VLAN

RSPAN VLAN は、RSPAN 送信元と宛先のセッション間で SPAN トラフィックを伝送します。また、開始デバイス、中間デバイス、最終デバイスで定義する必要があります。

（注） VLAN を RSPAN VLAN として設定するには、VLAN 設定 （163 ページ）画面を使用して VLAN データベースに追加する必要があります。

VLAN を RSPAN VLAN として設定するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > **[SPAN & RSPAN]** > **[RSPAN VLAN]** の順にクリックして、定義済みの RSPAN VLAN を表示します。

ステップ 2 VLAN を RSPAN VLAN として設定するには、VLAN の [RSPAN VLAN] ドロップダウンリストから選択します。

ステップ 3 [Apply] をクリックします。

SPANセッションの宛先

モニターリング セッションは、1 つ以上の送信元ポートと単一の宛先ポートで構成されます。宛先ポートは、開始デバイスと最終デバイスで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 ポートです。最終デバイスでは、アナライザ ポートになります。

宛先ポートを追加するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [SPAN & RSPAN] > [SPAN Session Destinations] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [Session ID]：セッション ID を選択します。これは、送信元ポートのセッション ID に一致している必要があります。
- [Port]：ドロップダウンリストからポートを選択します。
- [Destination Type]：次のいずれかのオプションを選択します。
  - ローカルインターフェイス（Local Interface）：送信元ポートと同じデバイス上の宛先ポートです（SPAN に関係）。
  - リモート VLAN（Remote VLAN）：送信元ポートとは異なるデバイス上の宛先ポートです（RSPAN に関連）。

    [Destination Type] が [Remote VLAN] の場合は、次のフィールドを設定します。
  - リフレクタ ポート（Reflector Port）：最初のデバイスのターゲット ポートとして機能するユニット/ポートを選択します。

    [Destination Type] が [Local Interface] の場合は、次のフィールドを設定します。
- ネットワーク トラフィック（Network Traffic）：選択すると、ポート上で、モニタ対象のトラフィック以外のトラフィックを有効にすることができます。

ステップ 4 [Apply] をクリックします。

SPANセッションの送信元

単一のローカル SPAN または RSPAN セッションの送信元では、受信（Rx）、送信（Tx）、または双方向（両方）のポートトラフィックをモニターできます。スイッチは、任意の数の送信元ポート（スイッチで使用可能なポートの最大数まで）および任意の数の送信元 VLAN をサポートしています。

（注） 1 つまたは複数の SPAN または RSPAN 送信元を開始デバイスと最終デバイスで設定する必要があります。

ミラーする送信元ポートを設定するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [SPAN and RSPAN] > [SPAN Session Sources] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 [セッションID] からセッション番号を選択します。これは、すべての送信元ポートと宛先ポートで同じである必要があります。

ステップ 4 開始スイッチでは SPAN または RSPAN に対して、トラフィックのモニタ元のユニットとポートまたは VLAN（[Source Interface]）を選択します。最終スイッチ上の RSPAN に対して、リモート VLAN を選択します。

ステップ 5 [Monitor Type] フィールドで、ミラーするトラフィックのタイプとして、着信、発信、またはその両方を選択します。

- [Tx and Rx]：着信パケットと発信パケットの両方に対するポートミラーリング。
- [Rx]：着信パケットに対するポートミラーリング。
- [Tx]：発信パケットに対するポートミラーリング。

ステップ 6 [Apply] をクリックします。ミラーリングの送信元インターフェイスが設定されます。

診断

診断を使用して、デバイスがライブネットワークに接続されている間に、システムのハードウェアコンポーネント（シャーシ、スーパーバイザエンジン、モジュール、および ASIC）の機能をテストして検証できます。診断では、ハードウェア コンポーネントをテストして、データ パスおよび制御信号を検証するパケット スイッチング テストが行われます。

カッパーテスト

[カッパーテスト] ページには、カッパー ケーブルに対して Virtual Cable Tester（VCT）によって実行された統合ケーブル テストの結果が表示されます。

VCT は、2 つのタイプのテストを実行します。

- タイム ドメイン反射率計（TDR）技術は、ポートにアタッチされている銅ケーブルの品質と特性をテストします。最長 140m のケーブルをテストすることができます。これらの結果は、[Copper Test] ページの [Test Results] ブロックに表示されます。
- DSP ベースのテストは、ケーブル長を測定するために、アクティブな XG リンク上で実行されます。これらの結果は、[Copper Test] ページの [Advanced Information] ブロックに表示されます。このテストは、リンク速度が 10G のときにのみ実行できます。

カッパーテストを実行するための前提条件

テストを実施する前に、次の手順を実行します。

- （必須）ショートリーチモードの無効化（プロパティ （154 ページ）を参照）。
- （任意）EEE の無効化（プロパティ （154 ページ）を参照）。

VCT を使用してケーブルをテストする場合は、CAT6a データ ケーブルを使用します。

テスト結果の精度は、詳細テストの場合は +/- 10 のエラー範囲、基本テストの場合は +/- 2 のエラー範囲になります。

⚠

注意 ポートをテストする場合、ポートはダウン状態に設定され、通信は中断されます。テスト後に、ポートはアップ状態に戻ります。カッパー ポート テストの実行により、デバイスと通信できなくなるため、Webベースのスイッチ設定ユーティリティの実行に使用しているポートに対してカッパー ポートテストを実行することは推奨できません。

ポートに接続されている銅ケーブルをテストするには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [Diagnostics] > [Copper Test] の順にクリックします。

ステップ 2 テストを実施するユニットとポートを選択します。

ステップ 3 [Copper Test] をクリックします。

ステップ 4 メッセージが表示されたら、[OK] をクリックして、リンクをダウンできることを確認するか、または [キャンセル（Cancel）] をクリックしてテストを中止します。[Test Results] ブロックに次のフィールドが表示されます。

- [Last Update]：ポートに対して最後のテストが実行された時刻。
- [テスト結果]：ケーブル テストの結果。値は次のとおりです。
  - [OK]：ケーブルはテストに合格しました。
  - [ケーブルなし]：ケーブルがポートに接続されていません。
  - [開放ケーブル]：ケーブルが一方側にしか接続されていません。
  - [短絡ケーブル]：ケーブルにショートが発生しています。
  - [テスト結果不明]：エラーが発生しました。
- [障害個所までの距離]：障害が検出されたケーブル位置からポートまでの距離。
- [動作ポートステータス]：ポートの状態（アップまたはダウン）が表示されます。

[Advanced Information] ブロック（一部のポートタイプでサポート）に次の情報が表示されます（情報はページを開くたびに更新されます）。

- ケーブル長（Cable Length）：長さの見積もりを提供します。
- [ペア]：テスト対象のケーブル ワイヤ ペア。
- [ステータス]：ワイヤ ペアの状態。赤色は障害を示し、緑色は状態が良好であることを示します。
- チャネル（Channel）：ワイヤがストレートかクロスオーバーであるかどうかを示すケーブル チャネル。
- [極性]：自動極性検出と修正機能がワイヤ ペアに対して有効になっているかどうかを 示します。

• [ペアスキュー] : ワイヤ ペア間の遅延差。

光モジュールステータス

[Optical Module Status] ページには、SFP（Small Form-factor Pluggable）トランシーバによってレポートされた稼動状況が表示されます。

次の GE SFP（1000Mbps）トランシーバがサポートされています。

- MGBLH1：1000BASE-LH SFP トランシーバ、シングルモード ファイバ用、波長 1310 nm、最大 40 km まで対応
- MGBLX1：1000BASE-LX SFP トランシーバ、シングルモード ファイバ用、波長 1310 nm、最大 10 km まで対応
- MGBSX1：1000BASE-SX SFP トランシーバ、マルチモード ファイバ用、波長 850 nm、最大 550 m まで対応
- MGBT1：1000BASE-T SFP トランシーバ、カテゴリ 5 銅線用、最大 100 m まで対応
- GLC-SX-MMD：1000BASE-SX 短波長、DOM あり
- GLC-LH-SMD：1000BASE-LX/LH 長波長、DOM あり
- GLC-BX-D：1000BASE-BX10-D ダウンストリーム双方向シングルファイバ、DOM あり
- GLC-BX-U：1000BASE-BX10-U アップストリーム双方向シングルファイバ、DOM あり
- GLC-TE：1000BASE-T（標準）

次の XG SFP+（10,000Mbps）トランシーバがサポートされます。

- Cisco SFP-10GBase-T
- Cisco SFP-10G-SR
- Cisco SFP-10G-LR
- Cisco SFP-10G-SR-S
- Cisco SFP-10G-LR-S

次の XG パッシブ ケーブル（Twinax/DAC）がサポートされます。

- Cisco SFP-H10G-CU1M
- Cisco SFP-H10G-CU3M
- Cisco SFP-H10G-CU5M

光テストの結果を表示するには、[Status and Statistics] > [Diagnostics] > [Optical Module Status] の順にクリックします。

このページには、次のフィールドが表示されます。

- [Port]：SFP が接続されているポート番号
- [Description]：光トランシーバの説明
- [Serial Number]：光トランシーバのシリアル番号
- [PID]：トランシーバの製品 ID
- [VID]：トランシーバのバージョン ID
- [Temperature]：SFP の動作温度（摂氏）
- [Voltage]：SFP の動作電圧
- [Current]：SFP の電流消費量
- [Output Power]：送出された光電力
- [Input Power]：受け取った光電力
- [トランスミッタ障害]：リモート SFP から報告される信号損失。値は [TRUE]、[FALSE]、および [N/S]（信号なし）になります。
- [信号消失]：ローカル SFP から報告される信号損失。値は [TRUE] か [FALSE] になります。
- [データレディ]：SFP が稼動しているかどうか。値は [TRUE] か [FALSE] になります。

テクニカルサポート情報

このページは、デバイスの状態の詳細なログを提供します。単一のコマンドで複数の show コマンド（debug コマンドを含む）の出力が得られるため、この情報は、テクニカルサポートがユーザーの問題解決を支援する場合に役立ちます。

デバッグ目的で役立つテクニカル サポート情報を表示するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [Diagnostics] > [Tech-Support Information] の順にクリックします。

ステップ 2 [Generate] をクリックします。

（注） このコマンドの出力を生成するために多少時間がかかる場合があります。情報が生成されたら、[Select tech-support data] をクリックすることで、画面上のテキスト ボックスからそれをコピーできます。

RMON

リモート ネットワーク モニターリング（RMON）を使用すると、デバイスの SNMP エージェントが、トラフィック統計情報の監視をプロアクティブに一定期間行い、トラップを SNMP マネージャに送信できます。ローカルの SNMP エージェントは、実際のリアルタイム カウンタを事前に定義されたしきい値と比較し、アラームを生成します。中央の SNMP 管理プラットフォームによるポーリングは必要ありません。これは、ネットワークのベースラインに応じて正しいしきい値を設定している場合に、プロアクティブな管理の効果的なメカニズムとなります。

RMON では、SNMP マネージャが情報を取得するために頻繁にデバイスをポーリングする必要がないため、マネージャとデバイス間のトラフィックが減少します。さらに、デバイスがイベントの発生時にそれらをレポートするため、マネージャはタイムリーに状態レポートを取得できます。

この機能を使用すると、次のアクションを実行できます。

- 現在の統計を表示する（カウンタ値がクリアされた時点以降）。また、一定期間、これらのカウンタの値を収集して、収集したデータのテーブルを表示できます。収集されたセットがそれぞれ、[History] タブの 1 行になります。
- 「一定数のレイトコリジョンに達した」などのカウンタ値の興味のある変化を定義し（アラームを定義）、このイベントが発生したときにど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）。

統計情報

[統計情報] ページには、パケット サイズについての詳細情報および物理レイヤ エラーについての情報が表示されます。情報は、RMON 標準規格に従って表示されます。オーバーサイズ パケットは、次の条件を満たすイーサネット フレームとして定義されます。

- パケット長が、MRU バイト サイズを超えている。
- コリジョン イベントは検出されていない。
- レイト コリジョン イベントは検出されていない。
- 受信（Rx）エラー イベントは検出されていない。
- パケットは、有効な CRC を保持している。

RMON 統計情報を表示したり、リフレッシュレートを設定したりする場合は、次の手順を実行します。

ステップ 1 [Status and Statistics] > [RMON] > [Statistics] の順にクリックします。
ステップ 2 イーサネット統計を表示する [Interface] を選択します。

ステップ 3 インターフェイスの統計を更新する前の経過期間として、[Refresh Rate] を選択します。

選択インターフェイスに関する次の統計が表示されます。

Bytes Received	受信したオクテット数（不良パケットや FCS オクテットも含まれますが、フレーミングビットは含まれません）。
Drop Events	ドロップされたパケット数。
Packets Received	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む、受信済みの正常なパケット数。
受信済みブロードキャストパケット	受信した良好なブロードキャストパケット数。マルチキャスト パケットは、この数には含まれません。
受信済みマルチキャストパケット	受信した良好なマルチキャストパケット数。
CRC &アラインメントエラー	発生した CRC および配置エラー数。
Undersize Packets	受信したアンダーサイズパケット数（64オクテット未満）。
Oversize Packets	受信したオーバーサイズパケット数（2000 オクテット以上）。
フラグメント	受信したフラグメント（フレーミングビットは含まず、FCS オクテットを含む、64 オクテット未満のパケット）の数。
Jabbers	1632オクテットを超える受信済みパケット数。この数では、フレーム ビットは除外されますが、整数のオクテットを持つ不良 FCS（フレーム チェック シーケンス）（FCS エラー）、または非整数のオクテット（配置エラー）数の不良 FCS のいずれかを伴う FCS オクテットは含まれます。Jabber パケットは、次の条件を満たすイーサネット フレームとして定義されます。
Collisions	受信したコリジョン数。ジャンボ フレームが有効な場合、Jabber フレームのしきい値は、ジャンボ フレームの最大サイズにまで引き上げられます。
64バイトフレーム	送受信された 64 バイトを格納するフレーム数。
65～127バイトフレーム	送受信された 65 ～ 127 バイトを格納するフレーム数。
128～255バイトフレーム	送受信された 128 ～ 255 バイトを格納するフレーム数。
256～511バイトフレーム	送受信された 256 ～ 511 バイトを格納するフレーム数。
512～1023バイトフレーム	送受信された 512 ～ 1023 バイトを格納するフレーム数。
1024 バイト以上のフレーム	送受信された 1024 ～ 2000 バイトを格納するフレーム、およびジャンボフレームの数。

（注） 上記のいずれかのフィールドにエラーの数（0 ではない）が表示されている場合は、最後の更新時間が表示されます。

ステップ 4 テーブル表示またはグラフィック表示でカウンタを表示するには、次の手順を実行します。

- すべてのポートをテーブル表示で確認するには、[View All Interfaces Statistics] をクリックします。
- [Graphic View] をクリックしてグラフィック形式でこれらの結果を表示します。この表示では、結果を表示する [Time Span] と、表示する統計のタイプを選択できます。

履歴

RMON 機能によって、インターフェイスごとに統計をモニタリングできます。

[履歴]ページでは、サンプリング頻度、保存するサンプル数、およびデータ収集元ポートを定義できます。データは、サンプリングおよび保存された後に、[History Table] ページに表示されます。このページは、[History Table] をクリックすると表示できます。

RMON の制御情報を入力するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [RMON] > [History] の順にクリックします。このページに表示されるフィールドは、以下の [Add RMON History] ページで定義されます。このページで、[Add RMON History] ページで定義されない唯一のフィールドが、次のフィールドです。

- [Current Number of Samples]：RMON は、規格により、要求されたすべてのサンプルを許可するのではなく、要求ごとにサンプル数を制限するようになっています。したがって、このフィールドは、要求に対して許可されたサンプル数（要求値以下）を表します。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [New History Entry]：新しい [History] テーブルエントリの番号が表示されます。
- [Source Interface]：履歴サンプルを取得するインターフェイスのタイプを選択します。
- [Max No. of Samples to Keep]：保存されるサンプル数を入力します。
- [Sampling Interval]：ポートからサンプルが収集される秒数を入力します。フィールドの値の範囲は 1 ～ 3600 です。
- [Owner]：RMON 情報を要求した RMON ステーションまたはユーザーを入力します。

ステップ 4 [Apply]をクリックします。エントリが[履歴制御テーブル]ページに追加され、実行コンフィギュレーション ファイルが更新されます。

ステップ 5 [History Table] をクリックして、実際の統計情報を表示します。

イベント

アラームをトリガーする頻度と発生する通知のタイプを制御できます。これは、次のように実行します。

- [Events] ページ：アラームがトリガーされたときにどうするかを設定します。これは、ログとトラップの任意の組み合わせになります。
- [Alarms] ページ：アラームをトリガーする頻度を設定します。

RMON イベントを定義するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [RMON] > [Events] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [Event Entry Number]：新しいエントリのイベント エントリ インデックス番号が表示されます。
- コミュニティ（Community）：トラップが送信されるときに含める SNMP コミュニティ文字列を入力します。
- [Description]：イベントの名前を入力します。この名前は、[Add RMON Alarm] ページで、アラームをイベントにアタッチするために使用されます。
- 通知タイプ（Notification Type）：このイベントの結果生じるアクションのタイプを選択します。値は次のとおりです。
  - なし（None）：アラームが作動したときにアクションを実行しません。
  - ログ（[イベントログ] テーブル）（Log (Event Log Table)）：アラームがトリガーされたときに、[Event Log] 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）（Trap (SNMP Manager and Syslog Server)）：アラームが作動したときに、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（Log and Trap）：[Event Log] テーブルにログ エントリを追加し、アラームが作動したときに、リモート ログ サーバにトラップを送信します。
- 所有者（Owner）：イベントを定義したデバイスまたはユーザを入力します。

ステップ 4 [Apply] をクリックします。RMON イベントが実行コンフィギュレーション ファイルに保存されます。

ステップ 5 発生し、ログに記録されたアラームのログを表示するには、[Event Log Table] をクリックします（以下で説明）。

アラーム

RMON アラームは、エージェントによって維持されるカウンタまたはその他の任意の SNMP オブジェクトカウンタで例外イベントを生成するための、しきい値とサンプリング間隔を設定するメカニズムを提供します。アラームに、上昇しきい値と下限しきい値の両方を設定する必要があります。上昇しきい値を超えた後は、対応する下限しきい値を下回るまで、上昇イベントは生成されません。下限アラームが発行された後は、上昇しきい値を超えたときに、次のアラームが発行されます。

1 つ以上のアラームがイベントにバインドされます。イベントは、アラームが発生したときに実行するアクションを示しています。

アラームカウンタは、絶対値またはカウンタの値の変化（差分）のいずれかによってモニタできます。

RMON アラームを入力するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [RMON] > [Alarms] の順にクリックします。

定義済みのすべてのアラームが表示されます。フィールドについては、以下の [Add RMON Alarm] ページで説明されています。それらのフィールドに加え、次のフィールドが表示されます。

- カウンタ値（Counter Value）：最後のサンプリング期間の統計値が表示されます。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

アラームエントリ	アラームエントリ番号が表示されます。
Interface	RMON 統計情報の表示対象となるインターフェイスのタイプを選択します。
カウンタ名	測定される発生タイプを示す MIB 変数を選択します。
Sample Type	アラームを生成するサンプリング方法を選択します。次のオプションがあります。 • 絶対（Absolute）：しきい値を超える、または下回った場合にアラームが生成されます。 • [Delta]：現在の値から最後にサンプリングされた値を減算します。その値の差がしきい値と比較されます。しきい値を超える、または下回った場合にアラームが生成されます。
Rising Threshold	上昇しきい値アラームをトリガーする値を入力します。
Rising Event	上昇イベントがトリガーされたときに実行するイベントを選択します。イベントはイベント （59 ページ）で設定されます。
Falling Threshold	下降しきい値アラームをトリガーする値を入力します。

Falling Event	下降イベントがトリガーされたときに実行するイベントを選択します。
Startup Alarm	アラームの生成を開始する最初のイベントを選択します。上昇は、低い値のしきい値からより高い値のしきい値へと、その値を超えることとして定義されます。 • 上昇アラーム（Rising Alarm）：上昇値が上昇しきい値アラームをトリガーします。 • 下降アラーム（Falling Alarm）：下降値が下限しきい値アラームをトリガーします。 • 上昇と下降（Rising and Falling）：上昇値と下降値の両方がアラームをトリガーします。
インターバル	アラーム間隔を秒単位で入力します。
Owner	アラームを受信するユーザーまたはネットワーク管理システムの名前を入力します。

ステップ 4 [Apply] をクリックします。RMON アラームが実行コンフィギュレーション ファイルに保存されます。

sFlow

sFlow モニタリング システムは、sFlow エージェント（スイッチまたはルータ、もしくはスタンド アロン プローブに組み込まれている）と、sFlow コレクタと呼ばれる、中央のデータ コレクタで構成されています。sFlow エージェントは、サンプリング技術を使用して、モニタリングしているデバイスからトラフィックと統計をキャプチャします。sFlow データグラムは、分析のために、サンプリングされたトラフィックと統計を sFlow コレクタに転送するために使用されます。

sFlow V5 では、以下が定義されています。

- トラフィックのモニタ方法。
- sFlow エージェントを制御する sFlow MIB。
- 中央のデータ コレクタにデータを転送する際に、sFlow エージェントによって使用されるサンプル データの形式。デバイスは、フロー サンプリングとカウンタ サンプリングの 2 つのタイプの sFlow サンプリングをサポートしています。sFlow V5 に従って、次のカウンタ サンプリングが実行されます（インターフェイスによってサポートされている場合）。
  - 汎用インターフェイス カウンタ（RFC 2233）
  - イーサネット インターフェイス カウンタ（RFC 2358）

sFlowレシーバ

sFlow レシーバは、sFlow エージェントと sFlow コレクタの間の sFlow セッションを維持するために使用される一連のオブジェクトを定義します。sFlow レシーバのパラメータを設定するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [sFlow] > [sFlow Receivers] の順にクリックします。

ステップ 2 次のフィールドに入力します。

- [IPv4 Source Interface]：IPv4 送信元インターフェイスを選択します。

  （注） 自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

- [IPv6 Source Interface]：IPv6 送信元インターフェイスを選択します。

ステップ 3 レシーバ（sFlow アナライザ）を追加するには、[Add] をクリックして、[Receiver Index] で事前に定義されたサンプリング定義インデックスのいずれかを選択します。

ステップ 4 受信者のアドレス フィールドに入力します。

- [レシーバ指定方法]：sflow レシーバを [IPアドレス別] に指定するか、[名前別] に指定するかを選択します。

  [Receiver Definition] が [By IP Address] の場合：

- [IP Version]：サーバーが IPv4 または IPv6 のどちらのアドレスを使用するかを選択します。
- [IPv6 アドレスタイプ]：IPv6 を使用する場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [Link Local]：IPv6 アドレスによって、単一ネットワークリンク上のホストが一意に識別されます。リンク ローカル アドレスのプレフィックスは FE 80 で、ルーティングはできません。また、ローカル ネットワーク上の通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [グローバル]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
- [リンクローカルインターフェイス]：リストからリンク ローカル インターフェイスを選 択します（IPv6 を使用する場合）。

ステップ 5 次のフィールドに入力します。

- 受信者の IP アドレス/名前（Receiver IP Address/Name）：受信者の IP アドレスまたは名前のいずれか関連する方を入力します。
- [Port]：SYSLOG メッセージが送信されるポート。

- 最大データグラム サイズ（Maximum Datagram Size）：単一のサンプル データグラム（フレーム）で、受信者に送信できる最大バイト数。

ステップ 6 [Apply] をクリックします。

sFlowインターフェイス設定

ポートからデータグラムまたはカウンタをサンプリングするには、ポートをレシーバに関連付ける必要があります。sFlow ポートは、[sFlowレシーバ （62 ページ）] ページでレシーバを定義してからしか設定できません。

サンプリングを有効にして、sFlow 情報を収集するポートを設定するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [sFlow] > [sFlow Interface Settings] の順にクリックします。

sFlow インターフェイス設定が表示されます。

ステップ 2 sFlow 受信者をポートに関連付けるには、[Edit] をクリックして、次のフィールドに入力します。

- インターフェイス（Interface）：情報の収集元となるユニット/ポートを選択します。
- （フロー サンプリング）状態（(Flow Sampling) State）：フロー サンプリングを有効/無効にします。
- [Sampling Rate]：x が入力された場合は、フローサンプルが x フレームごとに取得されます。
- [Maximum Header Size (Bytes)]：サンプリングされたパケットからコピーする必要がある最大バイト数。
- [Receiver Index]：[sFlowレシーバ （62 ページ）] ページで定義したインデックスのいずれかを選択します。
- （カウンタ サンプリング）状態（(Counter Sampling) State）：カウンタ サンプリングを有効/無効にします。
- [Sampling Interval (Sec.)]：x が入力されている場合、x 秒ごとにカウンタサンプルが取得されるように指定します。
- [Receiver Index]：これらの [sFlowレシーバ （62 ページ）] ページで定義したインデックスのいずれかを選択します。

ステップ 3 [Apply] をクリックします。

sFlow統計情報

sFlow 統計情報を表示するには、次の手順を実行します。

ステップ 1 [Status and Statistics] > [sFlow] > [sFlow Statistics] の順にクリックします。

ステップ 2 [Refresh Rate] ドロップダウンメニューからリフレッシュレートを選択します。

インターフェイスごとに次の sFlow 統計情報が表示されます。

- [Port]：サンプルが収集されたポート。
- [Packets Sampled]：サンプリングされたパケットの数。
- [Datagrams Sent to Receiver]：送信された sFlow サンプリングパケットの数。

ログの表示

デバイスは、次のログに書き込むことができます。

- RAM 内のログ（リブート時にクリアされる）。
- フラッシュ メモリ内のログ（ユーザ コマンドの実行時にのみクリアされる）。

シビラティ（重大度）別に各ログに書き込まれるメッセージを設定できます。メッセージは、外部 SYSLOG サーバ上に存在するログを含め、複数のログに記録することができます。

RAMメモリ

[RAM Memory] ページには、RAM（キャッシュ）に保存されたすべてのメッセージが時間順に表示されます。すべてのエントリが RAM ログに保存されます。

ポップアップ SYSLOG 通知

新しい SYSLOG メッセージが RAM ログファイルに書き込まれると、Web GUI にその内容に関する通知が表示されます。Web GUI は 10 秒ごとに RAM ログをポーリングします。過去 10 秒間に作成されたすべての SYSLOG に関する SYSLOG 通知ポップアップが画面右下に表示されます。

表示されるポップアップ通知が 8 件以上の場合、サマリーポップアップが表示されます。このポップアップには、表示されていない SYSLOG 通知の数が示されます。また、表示されたすべてのポップアップを閉じるためのボタンも表示されます。

ログエントリを表示するには、[Status and Statistics] > [View Log] > [RAM Memory] の順にクリックします。

ページの上部に、以下が表示されます。

- アラート アイコンの点滅（Alert Icon Blinking）：無効と有効を切り替えます。
- [ポップアップSyslog通知]：前述したようにポップアップ SYSLOG の受信を有効にします。

- 現在のロギングしきい値（Current Logging Threshold）：生成されるロギングのレベルを指定します。これは、フィールドの名前の横にある [Edit] をクリックして、変更できます。

このページには、各ログファイルに関する次のフィールドが含まれます。

- [ログ時刻]：メッセージが生成された時刻。
- [Severity]：イベントのシビラティ（重大度）。
- [Description]：イベントについて説明するメッセージテキスト。

ログ メッセージをクリアするには、[Clear Logs] をクリックします。

フラッシュ メモリ

[フラッシュメモリ]ページには、フラッシュ メモリに保存されたメッセージが時間順に表示されます。ログの最小シビラティ（重大度）はログ設定（80ページ）で設定します。フラッシュのログは、デバイスのリブート時に存続します。ログは手動でクリアすることができます。

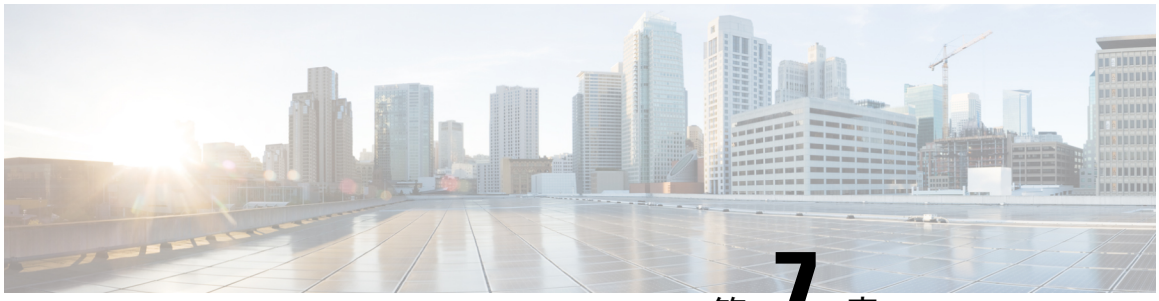
フラッシュのログを表示するには、[Status and Statistics] > [View Log] > [Flash Memory] の順にクリックします。

[Current Logging Threshold] は、生成されるロギングのレベルを指定します。これは、フィールドの名前の横にある [Edit] をクリックして、変更できます。

このページには、各ログファイルに関する次のフィールドが含まれます。

- [Log Index]：ログエントリ番号。
- [ログ時刻]：メッセージが生成された時刻。
- [Severity]：イベントのシビラティ（重大度）。
- [Description]：イベントについて説明するメッセージテキスト。

メッセージをクリアするには、[Clear Logs] をクリックします。メッセージがクリアされます。



第 7 章

管理

この章は、次の項で構成されています。

システム設定

システム設定ページでは、スイッチの設定をカスタマイズできます。次の設定を行えます。

ステップ 1 [Administration] > [System Settings] の順に選択します。

ステップ 2 システム設定を表示または変更します。

- システムの説明（System Description）：デバイスの説明が表示されます。

- [System Location]：デバイスの物理的な場所を入力します。
- [システムコンタクト先] : 担当者の名前を入力します。
- [Host Name]：デバイスのホスト名を選択します。これは CLI コマンドのプロンプトで使用されます。
  - デフォルトを使用（Use Default）：これらのスイッチのデフォルト ホスト名（System Name）は switch123456 であり、123456 はデバイスの MAC アドレスの最後の 3 バイトを 16 進形式で表しています。
  - [ユーザー定義] : ホスト名を入力します。文字、数字、ハイフンだけが使用できます。ホスト名の開始または終了はハイフンにできません。（RFC1033、1034、1035 で指定されているように）他の記号、区切り文字、または空白スペースは使用できません。
- カスタム バナーの設定（Custom Banner Settings）：次のバナーを設定できます。
  - ログイン バナー（Login Banner）：ログイン前のログイン ページに表示するテキストを入力します。[Preview] をクリックして結果を表示します。
  - ウェルカム バナー（Welcome Banner）：ログイン後のログイン ページを表示するテキストを入力します。[Preview] をクリックして結果を表示します。

（注） Web ベースの設定ユーティリティからログイン バナーを定義すると、CLI インターフェイス（コンソール、Telnet、SSH）のバナーも有効化されます。

バナーには最大で 1000 文字を含めることができます。510 文字より後は、<Enter> を押して続行してください。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに値を保存します。

コンソール設定

（注） コンソール設定は、[Advanced Mode] ビューでのみ使用できます。

コンソールポートの速度は、9600、19200、38400、57600、115200 または自動検出に設定できます。[Auto Detection] を選択すると、デバイスがコンソール速度を自動的に検出します。自動検出が有効ではない場合、コンソール ポートの速度は最後に手動で設定された速度（デフォルトは115,200）に自動的に設定されます。自動検出が有効になっているがコンソールのボー レートが検出されていない場合、115,200 の速度が使用されてテキスト（ブートアップ情報など）が表示されます。[Console Settings] ページで自動検出を有効にした後に、コンソールをデバイスに接続して Enter キーを 2 回押すと自動検出が有効化されます。デバイスは、ボー レートを自動的に検出します。

[Auto Detection] を有効にする、またはコンソールのボーレートを手動で設定するには、次のようにします。

ステップ 1 [Administration] > [Console Settings] の順にクリックします。

ステップ 2 [Console Port Baud Rate]フィールドで、次のいずれかのオプションを選択します。

- 自動検出（Auto Detection）：コンソール ボーレートが自動的に検出されます。
- [Static]：使用可能ないずれかの速度を選択します。

ステップ 3 [Apply] をクリックします。

スタック管理

（注） 特定のモデルのみがスタッキング機能を備えています。

スタックを管理するには、次の手順を実行します。

ステップ 1 [Administration] > [Stack Management] をクリックします。

- スタック モード（Stack Mode）：次のオプションのいずれかが表示されます。
  - ネイティブ スタック構成（Native Stacking）：デバイスは、すべてのユニットが同じタイプのスタックの一部です。
  - [Hybrid Stacking]：デバイスは、同じシリーズ内の複数のスイッチで構成できるスタックの一部です。
- スタック トポロジ（Stack Topology）：スタックのトポロジがチェーンまたはリングであるかどうかが表示されます。
- [Stack Active Unit]：スタックのアクティブユニットのユニット ID が表示されます。

スタック トポロジ表示（Stack Topology View）

この表示は、デバイスのグラフィカルビューを提供します。この上にマウスカーソルを移動すると、ユニット番号、スタック内での機能、スタック内で接続されているデバイス、および経由しているスタッキングポートが表示されます。

ユニット表示とスタック ポート設定（Unit View and Stack Port Configuration）

[Stack Topology View] で特定のデバイスをクリックすると、デバイスのグラフィカルビューが表示されます。

ステップ 2 デバイスのスタック ポートを選択するには、次の手順を実行します。

1. [Stack Topology View] でデバイスをクリックします。このデバイスのポートが、[Unit View and Stack Port Configuration] に表示されます。
2. ポートをマウスオーバーすると、ツールヒントにスタック構成ポート番号、接続しているユニット（1つの場合）、ポート速度、および接続ステータスが表示されます。

ステップ 3 スタック内のデバイスのリセット後にユニット ID を設定するには、[Stack Topology View] でデバイスをクリックして、次のフィールドに入力します。

- リセット後のユニット ID（Unit ID After Reset）：ユニット ID を選択するか、システムによってユニット ID が指定されるように [Auto] を選択します。
- ユニット x スタック接続の速度（Unit x Stack Connection Speed）：スタック接続の速度が表示されます。

ステップ 4 [Apply and Reboot] をクリックします。パラメータは実行コンフィギュレーション ファイルにコピーされ、スタックはリブートされます。

ユーザ アカウント

[User Accounts] ページでは、デバイスへのアクセス（読み取り専用または読み取り/書き込み）が許可されている追加ユーザの入力、および既存のユーザのパスワードの変更が可能です。デバイスに初めてアクセスするユーザーは、ユーザー名およびパスワードとして cisco と cisco を使用します。デフォルトのログイン情報を入力すると、デフォルトのレベル 15 のユーザー名およびパスワードを変更するよう求められます。このときに、新しいユーザー名とパスワードを設定する必要があります。新しいパスワードは、パスワードの複雑性ルールを満たす必要があります。

新規ユーザを追加する手順は、次のとおりです。

ステップ 1 [Administration] > [User Accounts] の順にクリックします。

ステップ 2 [Password Recovery Service] で、[Enable] チェックボックスをオンにして、パスワードの復旧を有効にします。

ステップ 3 [Add] をクリックして新しいユーザーを追加するか、[Edit] をクリックしてユーザーおよび/またはパスワードを変更します。

ステップ 4 パラメータを入力します。

- [User Name]：1 ～ 20 文字の新しいユーザー名を入力します。UTF-8 文字は使用できません。
- [Current Password]：これは、既存のユーザーのパスワードを編集する場合に表示されます。
- [Suggest Password]：クリックするとパスワードを自動生成します。
- [Password]：パスワードを入力します（UTF-8 文字は使用できません）。

（注） パスワードを作成する前に、ログイン設定 （308 ページ）のパスワードの複雑さのルールに関するセクションを参照してください。

（注） ユーザーが入力したパスワードは、よくある一般的なパスワードのリストと比較されます。パスワードにこのリストの単語が含まれている場合、パスワードは拒否され、新しいパスワードを入力する必要があります。

- [パスワードの確認] : パスワードを再度入力します。
- [パスワード強度メーター] : パスワードの強度が表示されます。
- [User Level] : ユーザーの権限レベルを選択します。
  - [Read-Only CLI Access (1)] : ユーザーは GUI にアクセスできません。デバイス構成を変更しない CLI コマンドだけにアクセスできます。
  - [Read/Limited Write CLI Access (7)] : ユーザーは GUI にアクセスできません。デバイス構成を変更する一部の CLI コマンドだけにアクセスできます。詳細については、*CLI* のリファレンス ガイドを参照してください。
  - [Read/Write Management Access (15)] : ユーザーは GUI にアクセスしてデバイスを設定できます。

ステップ 5 [Apply] をクリックします。ユーザは、デバイスの実行コンフィギュレーション ファイルに追加されます。

（注） パスワードは、パスワードベースキー派生関数 2（PBKDF2）を使用して、回復不能なハッシュとしてコンフィギュレーション ファイルに保存されます。このとき、ハッシュアルゴリズムとしてセキュア ハッシュ アルゴリズムおよび SHA-512 が使用されます。

アイドルセッションタイムアウト

アイドル セッション タイムアウトは、管理セッションがタイムアウトする前にアイドル状態を維持できる時間間隔を設定します。

さまざまなタイプのセッションのアイドル セッション タイムアウトを設定するには、次の手順を実行します。

ステップ 1 [Administration] > [Idle Session Timeout] の順にクリックします。

ステップ 2 リストから各セッションタイプのタイムアウトを選択します。

- HTTP セッション タイムアウト
- HTTPS セッション タイムアウト
- コンソール 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

デフォルトのタイムアウト値は10分です。選択したセッションのいずれかを再確立するには、もう一度ログインする必要があります。

ステップ3 [Apply] をクリックして、構成時の設定をデバイスに設定します。

時刻設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

ネットワーク上のすべてのデバイスでの基準時間の枠組みが、システムクロックの同期により提供されます。ネットワークの管理、セキュリティ、計画、デバッグといったすべての局面でイベントの発生時刻の判定が行われるため、ネットワーク時間の同期は重要です。クロックを同期しない場合、セキュリティ侵害または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関連付けることが不可能になります。また、ファイルシステムがどこに格納されているかにかかわらず、共有されたファイルシステムでの競合を削減するには変更時間を一定にすることが重要であるため、時刻の同期により競合も削減することができます。これらの理由から、ネットワーク上のすべてのデバイスで、設定された時間が正確であることが重要です。

リアルタイム クロック

一部のデバイスには、デバイスがシャットダウンされて電源に接続されていない場合でも正確な時刻を維持する、自己完結型リアルタイムクロック（RTC）コンポーネントが内蔵されています。この内部クロックは製造中に初期化され、ソフトウェアクロックの設定時に、デバイスの時刻機能によって更新されます。RTCコンポーネントを搭載したデバイスが起動すると、システムクロックはRTCの時刻と日付に設定されます。システムクロックがSimple Network Time Protocol（SNTP）により動的に、または手動で変更されるたびに、RTCコンポーネントは更新されます。

（注） このデバイスはSNTPに対応しています。このプロトコルを有効にすると、デバイスは、SNTPサーバーから取得した時刻でデバイス時刻を動的に同期します。デバイスはSNTPクライアントとしてのみ動作し、他のデバイスに時間に関するサービスを提供することはできません。

システム時刻

システム時刻ページを使用して、システム時刻のソースを選択します。ソースが手動の場合には、ここで時刻を入力できます。

注意 システム時刻を手動で設定し、デバイスをリブートした場合、時刻設定を手動で再入力する必要があります。

システム時刻を定義するには、次の手順を実行します。

ステップ 1 [Administration] > [Time Settings] > [System Time] をクリックします。

次のフィールドが表示されます。

- [Actual Time]：デバイスの実際のシステム時刻。
- [Last Synchronized Server]：最後にシステム時刻が取得されたアドレス、ストラタム、およびSNTP サーバの種類。

ステップ 2 次のパラメータを入力します。

- [クロックソース設定]：システム クロックの設定に使用するソースを選択します。
  - [Main Clock Source (SNTP Servers)]：これが有効な場合、システム時刻が SNTP サーバから取得されます。この機能を使用するには、SNTPマルチキャスト/エニーキャスト （76 ページ）で SNTP サーバーへの接続も設定する必要があります。
  - [Alternate Clock Source (PC via active HTTP/HTTPS sessions)]：HTTP プロトコルを使用した設定コンピュータからの日付と時刻の設定を有効にする場合に、[Enable] にチェックを入れます。

    （注） RIP MD5 認証を機能させるには、[Clock Source Setting] を上記のいずれかに設定する必要があります。

- [手動設定]：日付と時刻を手動で設定します。SNTP サーバーなどの代替時刻ソースがない場合は、現地時間が使用されます。
  - [日付]：システムの日付を入力します。
  - [現地時間]：システムの時刻を入力します。
- [Time Zone Settings]：DHCP サーバまたはタイムゾーン オフセットによるローカル時刻が使用されます。
  - [Get Time Zone from DHCP]：DHCP サーバからのタイムゾーンと DST の動的設定を有効にする場合に選択します。これらのパラメータの一方が設定されるのか両方が設定されるのかは、DHCP パケットに含まれる情報により変わります。このオプションが有効な場合、DHCP クライアントをデバイスで有効にする必要があります。
  - [Time Zone from DHCP]：DHCP サーバから設定されたタイムゾーンの略語が表示されます。この略語は [Actual Time] フィールドに表示されます。

- [時間帯のオフセット]：Greenwich Mean Time （GMT; グリニッジ標準時）と現 地時間との差を選択します。たとえば、パリのタイムゾーン オフセットは GMT +1、ニューヨークのタイムゾーン オフセットは GMT - 5 です。
- [Time Zone Acronym]：このタイムゾーンを表す名前を入力します。この略語は [Actual Time] フィールドに表示されます。

- [夏時間設定]：DST の定義方法を選択します。
  - [Daylight Savings]：サマータイムを有効にする場合に選択します。
  - [Time Set Offset]：GMT からのオフセットの分数を 1 ～ 1440 の範囲で入力します。デフォルトは 60 です。
  - [夏時間タイプ]：次のいずれかをクリックします。

    [米国]：米国で使用されている日付に基づいて DST が設定されます。

    [欧州]：欧州連合およびこの規格を採用しているその他の国で使用されている日付に基づいて DST が設定されます。

    [日付指定]：DST は手動で設定されます。通常は、米国とヨーロッパ諸国以外の国用です。以下のパラメータを入力します。

    [繰り返し]：DST を毎年同じ日付に発生させます。

    [日付指定] を選択すると、DST の開始と終了をカスタマイズできるようになります。

- [開始]：DST が開始する日付と時刻。
- [終了]：DST が終了する日付と時刻。

ステップ 3 [繰り返し] を選択すると、DST の開始と終了を個別にカスタマイズできるようになります。

- [開始]：毎年 DST が開始する日付。
  - [曜日]：毎年 DST が開始する曜日。
  - [週]：毎年 DST が開始する月の週。
  - [月]：毎年 DST が開始する月。
  - [時刻]：毎年 DST が開始する時刻。
- [終了]：毎年 DST が終了する日付。たとえば、当地の DST を毎年 10 月の第 4 週目の金曜日 AM 5:00 に終了するとします。パラメータは次のとおりです。
  - [曜日]：毎年 DST が終了する曜日。
  - [週]：毎年 DST が終了する月の週。
  - [月]：毎年 DST が終了する月。
  - [時刻]：毎年 DST が終了する時刻。

ステップ 4 [Apply] をクリックします。システム時刻値が実行コンフィギュレーション ファイルに書き込まれます。

SNTPユニキャスト

SNTP は、サテライトレシーバやモデムなどの送信元によってすでに同期されているサーバーと、コンピュータのシステム時刻を同期します。SNTP では、ユニキャスト、マルチキャスト、およびエニーキャスト オペレーティング モードがサポートされます。ユニキャストモードでは、クライアントはユニキャストアドレスを参照することで、専用サーバーに要求を送信します。最大 16 台のユニキャスト SNTP サーバーを設定できます。

（注） SNTP クライアントユニキャストを機能させるには、システム時刻 （72 ページ）に記載されているメインクロックソース（SNTP サーバー）を有効にする必要があります。

ユニキャスト SNTP サーバーを追加するには、次の手順を実行します。

ステップ 1 [Administration] > [Time Settings] > [SNTP Unicast] をクリックします。

ステップ 2 次のフィールドを設定します。

SNTPクライアントユニキャスト	これを選択すると、SNTP で事前定義されたユニキャストクライアントをユニキャスト SNTP サーバーとともにデバイスで使用できます。
IPv4送信元インターフェイス	SNTP サーバーとの通信に使用する IPv4 インターフェイスを選択します。
IPv6送信元インターフェイス	SNTP サーバーとの通信に使用する IPv6 インターフェイスを選択します。 （注） 自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

ステップ 3 ユニキャスト SNTP サーバーを追加するには、[Add] をクリックします。

（注） ユーザ定義の SNTP サーバをすべて削除するには、[Restore Default Servers] をクリックします。

ステップ 4 次のパラメータを入力します。

サーバー指定方法	SNTP サーバーを選択します。IP アドレスまたはリスト内の名前で指定します。
IP バージョン	IP アドレスのバージョン（バージョン 6 またはバージョン 4）を選択します。

IPv6 アドレス タイプ	IPv6 アドレスタイプを選択します（IPv6 が使用されている場合）。次のオプションがあります。 • [リンクローカル] : IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンクローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [グローバル] : IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	リストからリンク ローカル インターフェイスを選択します（IPv6 アドレスタイプとしてリンクローカルが選択されている場合）。
SNTPサーバーのIPアドレス/名前	SNTP サーバーの IP アドレスまたは名前を入力します。形式は、選択したアドレス タイプにより異なります。
Poll Interval	選択すると、システムの時刻情報を取得するために SNTP サーバーのポーリングが有効になります。ポーリング対象のすべての NTP サーバーがポーリングされ、クロックは、ストラタムレベルが一番低い、アクセス可能なサーバーから選択されます。最も低いストラタムのサーバはプライマリ サーバと見なされます。次に低いストラタムのサーバはセカンダリ サーバとなり、以下同様です。プライマリ サーバがダウンした場合、デバイスはポーリング設定が有効なすべてのサーバをポーリングし、最も低いストラタムの新しいプライマリ サーバを選択します。
認証	認証を有効にする場合、このチェックボックスをオンにします。
認証キーID	認証が有効な場合、キー ID の値を選択します。

ステップ 5 [Apply] をクリックします。SNTP サーバを追加すると、メインページに戻ります。

SNTPマルチキャスト/エニーキャスト

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

（注） SNTP クライアントユニキャストを機能させるには、システム時刻 （72 ページ）に記載されているメインクロックソース（SNTP サーバー）を有効にする必要があります。

サブネット上のすべてのサーバーから SNTP パケットを受信したり、SNTP サーバーへの時刻要求を送信したりできるようにするには、次の手順を実行します。

ステップ 1 [Administration] > [Time Settings] > [SNTP Multicast/Anycast] をクリックします。

次のオプションから選択します。

オプション	説明
SNTP IPv4マルチキャストクライアントモード(クライアントブロードキャスト受信)	サブネット上の任意の SNTP サーバーから、システム時刻の IPv4 マルチキャスト伝送を受信する場合に選択します。
SNTP IPv6マルチキャストクライアントモード(クライアントブロードキャスト受信)	サブネット上の任意の SNTP サーバーから、システム時刻の IPv6 マルチキャスト伝送を受信する場合に選択します。
SNTP IPv4エニーキャストクライアントモード(クライアントブロードキャスト送信)	システム時刻情報を要求する SNTP IPv4 同期パケットを送信する場合に選択します。パケットは、サブネット上のすべての SNTP サーバに送信されます。
SNTP IPv6エニーキャストクライアントモード(クライアントブロードキャスト送信)	システム時刻情報を要求する SNTP IPv6 同期パケットを送信する場合に選択します。パケットは、サブネット上のすべての SNTP サーバに送信されます。

ステップ 2 [Add] をクリックして、SNTP のインターフェイスを選択します。

インターフェイスを選択し、設定を行います。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

SNTP認証

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

SNTP クライアントは、HMAC-MD5 を使用して応答を認証できます。SNTP サーバーはキーに関連付けられています。このキーは応答自体とともにMD5関数への入力として使用されます。MD5 の結果も応答パケットに組み込まれます。[SNTP Authentication] ページでは、SNTP サーバーとの通信に使用する認証キーを設定できます。

認証キーは、SNTP サーバーのタイプに応じて、独立したプロセスで SNTP サーバーに作成されます。詳細については、SNTP サーバのシステム管理者にお尋ねください。

ステップ 1 [Administration] > [Time Settings] > [SNTP Authentication] をクリックします。

ステップ 2 [SNTP Authentication] を選択し、デバイスと SNTP サーバ間の SNTP セッションの認証をサポートします。

ステップ 3 [Apply] をクリックして、デバイスを更新します。

ステップ 4 [Add] をクリックします。

ステップ 5 次のパラメータを入力します。

- [認証キー ID]：この SNTP 認証キーを内部的に識別するための番号を入力します。
- [Authentication Key (Encrypted)]：認証に使用するキーを暗号化形式で入力します（8 文字以内）。SNTP サーバは、デバイスを自身と同期させるためにこのキーを送信する必要があります。
- [Authentication Key (Plaintext)]：認証に使用するキーをプレーン テキスト形式で入力します（8 文字以内）。SNTP サーバは、デバイスを自身と同期させるためにこのキーを送信する必要があります。
- [Trusted Key]：この認証キーを使用して、デバイスが SNTP サーバからのみ同期情報を受信できるようにする場合に選択します。

ステップ 6 [Apply] をクリックします。SNTP 認証パラメータが、実行コンフィギュレーション ファイルに書き込まれます。

時間範囲

時間範囲を定義し、以下の種類のコマンドと関連付けて、それらのコマンドが定義した時間範囲でのみ適用されるようにできます。

- ポート状態
- 時間ベースの PoE

時間範囲には 2 つの種類があります。

- [Absolute]：このタイプの時間範囲は、特定の日付または即時に開始し、特定の日付で終了するか、無制限に実行されます。これは時間範囲ページで作成されます。定期的な要素をここに追加することができます。
- [Periodic]：このタイプの時間範囲には、絶対範囲に追加される時間範囲要素が含まれており、定期的に開始および終了します。これは、[Periodic Range] ページで定義されます。

時間範囲に絶対範囲と周期範囲の両方が含まれる場合、それに関連したプロセスは、絶対開始時間と周期時間範囲の両方に達した場合にのみアクティブ化されます。このプロセスは、いずれかの時間範囲に達した時点で非アクティブ化されます。デバイスは最大 20 個の絶対時間範囲をサポートします。

時間範囲エントリが目的の時刻に有効になるようにするには、システム時刻を設定する必要があります。時間範囲機能は次の目的で使用できます。

- ネットワークへのコンピュータのアクセスを（たとえば）業務時間内のみに制限し、業務時間後はネットワークポートをロックし、残りのネットワークのアクセスをブロックします（「ポートの設定」および「LAG 情報の設定」を参照してください）。
- 指定した期間に PoE 操作を制限します。

時間範囲の説明を追加

ステップ 1 [Administration] > [Time Settings] > [Time Range] の順にクリックします。

ステップ 2 [Time Range] テーブルで、[Add] をクリックして新しい時間範囲を追加するか、[Edit] または [Delete] をクリックして既存の時間範囲を編集または削除します。

ステップ 3 新しい時間範囲を追加するには、[Add] をクリックし、次のように設定します。

- [Time Range Name]：時間範囲の名前を入力します。
- [Absolute Starting Time]：[Immediate] を選択するか、日付と時刻を入力します。
- [Absolute Ending Time]：[Infinite] を選択するか、日付と時刻を入力します。

ステップ 4 新しい時間範囲設定を適用するには、[Apply] をクリックします。

定期時間範囲

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

定期的な時間要素を絶対時間範囲に追加できます。これにより、絶対範囲内の特定の期間に動作が制限されます。

絶対時間範囲に定期時間範囲要素を追加するには、次の手順を実行します。

ステップ 1 [Administration] > [Time Settings] > [Recurring Range] をクリックします。

既存の定期時間範囲が表示されます（特定の絶対時間範囲ごとにフィルタ処理されます）。

ステップ 2 定期範囲を追加する絶対時間範囲を選択します。

ステップ 3 新しい定期時間範囲を追加するには、[Add] をクリックします。

ステップ 4 次のフィールドに入力します。

- [繰り返し開始時間]：時間範囲の開始点とする曜日と時刻を入力します。
- [繰り返し終了時間]：時間範囲の終了点とする曜日と時刻を入力します。

ステップ 5 [Apply] をクリックします。

システム ログ

ここでは、システム ロギングについて説明します。システム ロギングは、デバイスが複数の独立したログを生成することを可能にします。各ログは、システムイベントが示された一連のメッセージで構成されます。

デバイスでは、次のローカル ログが生成されます。

- コンソール インターフェイスに送信されるログ
- イベントが記録された RAM 内の循環リストに書き込まれるログ。デバイスのリブート時に消去されます。
- フラッシュ メモリに保存される循環ログ ファイルに書き込まれるログ。リブート後も保持されます。

さらに、SNMP トラップ形式および SYSLOG メッセージ形式で、リモートの SYSLOG サーバにメッセージを送信できます。

ログ設定

（注） コンソール設定は、[Advanced Mode] ビューでのみ使用できます）

シビラティ（重大度）レベル別に、ログに記録するイベントを選択できます。各ログ メッセージにはシビラティ（重大度）レベルが設定され、シビラティ（重大度）レベルの最初の文字の両側にダッシュ（-）が付けられてマーキングされています（例外として緊急（Emergency）は文字F で表されます）。たとえば、ログ メッセージ「%INIT-I-InitCompleted: …」のシビラティ（重大度）レベルは I であり、情報（Informational）を意味します。

イベントのシビラティ（重大度）レベルを、最も高いシビラティ（重大度）から最も低いシビラティ（重大度）まで、以下に順に示します。

- 緊急（Emergency）：システムを使用できません。
- アラート（Alert）：処置が必要です。
- 重大（Critical）：システムに重大な問題があります。
- エラー（Error）：システムにエラーがあります。
- 警告（Warning）：システム警告が発生しました。
- 注意（Notice）：システムは正しく機能していますが、システムの注意事項が発生しました。

- 情報（Informational）：デバイス情報です。
- デバッグ（Debug）：イベントに関する詳細応報です。

RAMおよびフラッシュのログに対して、異なるシビラティ（重大度）レベルを選択できます。これらのログはそれぞれRAMメモリ （64 ページ）とフラッシュ メモリ （65 ページ）に表示されます。

ログに保存されるシビラティ（重大度）レベルを選択すると、それより高いシビラティ（重大度）のすべてのイベントが自動的にそのログに保存されます。それより低いシビラティ（重大度）のイベントは、ログに保存されません。たとえば、[Warning] を選択すると、[Warning] およびそれより高いすべてのシビラティ（重大度）レベル（緊急、アラート、重大、エラー、および警告）がログに保存されます。[Warning] より低いシビラティ（重大度）レベル（注意、情報）は保存されません。

グローバルログパラメータを設定するには、次の手順を実行します。

ステップ 1 [Administration] > [System Log] > [Log Settings] の順にクリックします。

ステップ 2 パラメータを入力します。

ログ	これを選択するとメッセージロギングが有効になります。
Syslogアグリゲータ	これを選択すると SYSLOG メッセージとトラップの集約が有効になります。有効な場合、同一および連続した SYSLOG メッセージとトラップが、指定された最大集約時間にわたって集約され、単一のメッセージで送信されます。集約されたメッセージは、その到着順で送信されます。各メッセージには、集約された回数が示されています。
最大集約時間	SYSLOG メッセージが集約される間隔を入力します。
発信元ID	この設定により、SYSLOG メッセージに発信元 ID を追加できます。次のオプションがあります。 • なし（None）：SYSLOG メッセージに発生元識別子を含めません。 • ホスト名（HostName）：SYSLOG メッセージにシステム ホスト名を含めます。 • [IPv4 Address]：送信元インターフェイスの IPv4 アドレスを SYSLOG メッセージに含めます。 • [IPv6 Address]：送信元インターフェイスの IPv6 アドレスを SYSLOG メッセージに含めます。 • ユーザ定義（User Defined）：SYSLOG メッセージに含まれる説明を入力します。
RAMメモリロギング	RAM に記録するメッセージのシビラティ（重大度）を選択します。

フラッシュメモリロギング	フラッシュメモリに記録するメッセージのシビラティ（重大度）を選択します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

リモート ロギングの設定

[Remote Log Servers] ページでは、ログ メッセージの送信先となるリモート SYSLOG サーバを定義できます。各サーバに対して、受信メッセージのシビラティ（重大度）を設定できます。

SYSLOG サーバーを定義するには、次の手順を実行します。

ステップ 1 [Administration] > [System Log] > [Remote Log Servers] をクリックします。

ステップ 2 （注） この設定は、[Advanced Mode] ビューでのみ使用できます）

次のフィールドに入力します。

- IPv4 送信元インターフェイス（IPv4 Source Interface）：送信元インターフェイスを選択します。このインターフェイスの IpV4 アドレスが、SYSLOG サーバに送信される SYSLOG メッセージの送信元 IPv4 アドレスとして使用されます。
- IPv6 送信元インターフェイス（IPv6 Source Interface）：送信元インターフェイスを選択します。このインターフェイスの IpV4 アドレスが、SYSLOG サーバに送信される SYSLOG メッセージの送信元 IPv6 アドレスとして使用されます。

（注） 自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

以前に設定したログサーバーごとに情報が記載されています。フィールドについては、後述の [Add] ページで説明します。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

サーバー指定方法	リモートログサーバーを IP アドレスで識別するか、名前で指定するかを選択します。
IP バージョン	サポートする IP 形式を選択します。

IPv6 アドレス タイプ	IPv6 アドレスタイプを選択します（IPv6 が使用されている場合）。次のオプションがあります。 • [リンクローカル] : IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80::/10 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [グローバル] : IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	リストからリンク ローカル インターフェイスを選択します（IPv6 アドレスタイプとしてリンクローカルが選択されている場合）。
ログサーバーのIPアドレス/名前	ログサーバーの IP アドレスまたはドメイン名を入力します。
UDP Port	ログメッセージの送信先となる UDP ポートを入力します。
ファシリティ	リモートサーバーに送信されるシステムログの出力元のファシリティ値を選択します。サーバに割り当てることができるファシリティ値は 1 つだけです。2 番目のファシリティコードが割り当てられている場合は、最初のファシリティ値がオーバーライドされます。
説明	サーバーの説明を入力します。
シビラティ（重大度）の最小値（Minimum Severity）	サーバーに送信されるシステムログメッセージの最小シビラティ（重大度）を選択します。

ステップ 5 [Apply] をクリックします。[Add Remote Log Server] ページが閉じて、SYSLOG サーバが追加され、実行コンフィギュレーション ファイルが更新されます。

ファイル管理

ファイル管理システムは、デバイス上のファイルを保存、整理、およびアクセスするために使用されるアプリケーションです。システムファイルとは、コンフィギュレーション情報やファームウェアイメージなどの情報を格納したファイルです。一般に、flash://system/ フォルダの下にあるすべてのファイルがシステム ファイルです。これらのファイルを使用してさまざまな処理を実行できます。たとえば、デバイスのブート元となるファームウェアファイルの選択、デバイス内部でのさまざまなタイプのコンフィギュレーションファイルの変更、外部デバイス（外部サーバーなど）との間のファイルのコピーなどです。

次に、デバイスに存在するファイルのタイプの一部を示します。

- 実行コンフィギュレーション：デバイスが動作するために現在使用されているパラメータが含まれています。このファイルは、デバイス上のパラメータ値を変更したときに変更されます。デバイスをリブートすると、実行コンフィギュレーションは失われます。デバイスに加えた変更内容を保持するには、スタートアップ コンフィギュレーション、または別のファイル タイプに実行コンフィギュレーションを保存する必要があります。
- スタートアップ コンフィギュレーション：別の設定（通常は実行コンフィギュレーション）をスタートアップ コンフィギュレーションにコピーすることで保存されるパラメータ値です。スタートアップ コンフィギュレーションはフラッシュに保持され、デバイスがリブートした場合でも保持されます。現時点では、スタートアップ コンフィギュレーションは RAM にコピーされ、実行コンフィギュレーションとして識別されます。
- ミラー コンフィギュレーション：次の条件が存在する場合、デバイスによって作成されるスタートアップ コンフィギュレーションのコピーです。
  - デバイスが継続的に 24 時間にわたって動作している。
  - 過去 24 時間に実行コンフィギュレーションに設定変更が加えられていない。
  - スタートアップ コンフィギュレーションが実行コンフィギュレーションと同一である。

  ミラー コンフィギュレーションにスタートアップ コンフィギュレーションをコピーできるのはシステムだけです。ただし、ユーザはミラー コンフィギュレーションから他のファイル タイプまたは別のデバイスにコピーできます。
- バックアップ ファイル：システム シャットダウンに対する保護のため、または特定の動作状態の保持のために使用されるファイルの手動コピーです。たとえば、ミラー コンフィギュレーション、スタートアップ コンフィギュレーション、または実行コンフィギュレーションをバックアップ ファイルにコピーすることができます。バックアップはフラッシュ、PC または USB ドライブに存在し、デバイスがリブートした場合でも保持されます。
- ファームウェア：デバイスの動作と機能を制御するプログラムです。一般に、イメージと呼ばれています。
- 言語ファイル：選択した言語で Web ベースの設定ユーティリティ ウィンドウを表示できるようにするディクショナリです。
- ログ ファイル：フラッシュ メモリに保存される SYSLOG メッセージです。

ファームウェア操作

[Firmware Operations] ページは、次のために使用できます。

- ファームウェア イメージの更新またはバックアップ
- アクティブイメージのスワップ

スタックの適切な動作を保証するために、スタック内のユニットのソフトウェアイメージは同一である必要があります。スタックのユニットは、次のいずれかの方法でアップグレードできます。

ステップ 1 [Administration] > [File Management] > [Firmware Operations] をクリックします。

次のフィールドが表示されます。

- アクティブなファームウェア ファイル（Active Firmware File）：最新のアクティブなファームウェア ファイルが表示されます。
- アクティブなファームウェア バージョン（Active Firmware Version）：最新のアクティブなファームウェア ファイルのバージョンが表示されます。

ステップ 2 次のオプションから、[Operation Type] を選択します。

- ファームウェアの更新
- ファームウェアのバックアップ
- イメージの切り替え

ステップ 3 次のオプションから、[Copy Method] を選択します。

HTTP/HTTPS	HTTP/HTTPS の場合は、[File Name] フィールドにファイル名を入力するか、[browse] をクリックしてファイルを探して選択します。
USB	USB の場合は、[File Name] フィールドにファイル名を入力するか、[browse] をクリックしてファイルを探して選択します。
TFTP	TFTP については、以下の TFTP の手順に従ってください。
SCP (SSH経由のファイル転送)	SCP については、以下の SCP の手順に従ってください。

TFTP の手順

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

ファームウェア操作のコピー方式として TFTP を選択した場合は、次のように設定します。

サーバー指定方法	次のオプションから選択します。 • IPアドレス別 • 名前別
IP バージョン	次のオプションから選択します。 • IP Version 6 • IP Version 4

IPv6 アドレス タイプ	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [グローバル]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。
サーバーのIPアドレス/名前	サーバーの IP アドレス/名前を入力します。
送信元	送信元の名前を入力します（0 ～ 160 文字を使用）

SCP の手順

（注）　この設定は、[Advanced Mode] ビューでのみ使用できます。

ファームウェア操作のコピー方式として SCP を選択した場合は、次のように設定します。

リモートSSHサーバー認証	SSH サーバー認証（デフォルトでは無効）を有効にするには、[Edit] をクリックします。
SSHクライアント認証	次の中から選択します。 • [Use SSH Client System Credentials] を使用します。 • [SSH Client One-Time Credentials] を使用します。
Username	[SSH Client One-Time Credentials] オプションを使用する場合、ユーザー名を入力します。
パスワード	[SSH Client One-Time Credentials] オプションを使用する場合、パスワードを入力します。
サーバー指定方法	次のオプションから選択します。 • IPアドレス別 • 名前別
IP バージョン	次のオプションから選択します。 • バージョン 6 • バージョン 4

IPv6 アドレス タイプ	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [グローバル]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。
サーバーのIPアドレス/名前	サーバーの IP アドレス/名前を入力します。
送信元	送信元の名前を入力します（0 ～ 160 文字を使用）

ステップ 4 [Apply] をクリックして設定値を保存します。

ファイル操作

ステップ 1 [Administration] > [File Management] > [File Operations] をクリックします。

ステップ 2 次のオプションから、[Operation Type] を選択します。

- 更新ファイル
- バックアップファイル
- 重複

ステップ 3 次のオプションから、[Destination File Type] を選択します。

- 実行コンフィギュレーション
- スタートアップ コンフィギュレーション
- ミラーコンフィギュレーション
- ロギングファイル
- 言語ファイル（Language File）
- ダッシュボード情報ファイル

ステップ 4 次のオプションから、[Copy Method] を選択します。

HTTP/HTTPS	HTTP/HTTPS の場合は、[File Name] フィールドにファイル名を入力するか、[browse] をクリックしてファイルを探して選択します。
USB	USB の場合は、[File Name] フィールドにファイル名を入力するか、[browse] をクリックしてファイルを探して選択します。
内部フラッシュ	内部ファイルの場合は、[File Name] フィールドにファイル名を入力するか、[File Directory] をクリックして参照します。[Sensitive Data Handling]：データの処理方法を選択します。ファイルのバックアップまたは複製にのみ適用されます。 • [Exclude]：機密データを除外します • [Encrypt]：機密データを暗号化します • [Plaintext]：プレーンテキストで機密データを表示します。
TFTP	TFTP については、以下の TFTP の手順に従ってください。
SCP (SSH経由のファイル転送)	SCP については、以下の SCP の手順に従ってください。

TFTP の手順

ファイル操作の更新方式またはバックアップ方式としてTFTPを選択した場合は、次のように設定します。

サーバー指定方法	次のオプションから選択します。 • IPアドレス別 • 名前別
IP バージョン	次のオプションから選択します。 • IP Version 6 • IP Version 4
IPv6 アドレス タイプ	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [グローバル]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。

サーバーのIPアドレス/名前	サーバーの IP アドレス/名前を入力します。
送信元	送信元の名前を入力します（0 ～ 160 文字を使用）。

SCP の手順

ファイル操作のコピー方式として SCP を選択した場合は、次のように設定します。

リモートSSHサーバー認証	SSH サーバー認証（デフォルトでは無効）を有効にするには、[Edit] をクリックします。
SSHクライアント認証	次の中から選択します。 • [Use SSH Client System Credentials] を使用します。 • [SSH Client One-Time Credentials] を使用します。
Username	[SSH Client One-Time Credentials] オプションを使用する場合、ユーザー名を入力します。
パスワード	[SSH Client One-Time Credentials] オプションを使用する場合、パスワードを入力します。
サーバー指定方法	次のオプションから選択します。 • IPアドレス別 • 名前別
IP バージョン	次のオプションから選択します。 • IP Version 6 • IP Version 4
IPv6 アドレス タイプ	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [グローバル]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。
サーバーのIPアドレス/名前	サーバーの IP アドレス/名前を入力します。

送信元	送信元の名前を入力します（0 ～ 160 文字を使用）。

ステップ 5 [File name] セクションで [Browse] ボタンをクリックし、ファイルを探して選択します。

ステップ 6 [Apply] をクリックします。

ファイルディレクトリ

[File Directory] ページには、システムに存在するシステム ファイルが表示されます。

ステップ 1 [Administration] > [File Management] > [File Directory] をクリックします。

ステップ 2 必要な場合、[Auto Mirror Configuration] を有効にします。これにより、ミラー コンフィギュレーション ファイルの自動作成が有効になります。この機能を無効にした場合、ミラーコンフィギュレーションファイルが削除されます（存在する場合）。

ステップ 3 ファイルおよびディレクトリを表示するドライブを選択します。次のオプションを使用できます。

- フラッシュ（Flash）：管理ステーションのルート ディレクトリにあるすべてのファイルを表示します。
- USB：USB ドライブ上のファイルを表示します。

ステップ 4 [Go] をクリックすると、次のフィールドが表示されます。

- ファイル名（File Name）：ファイルタイプに応じてシステム ファイル タイプまたは実際のファイル名。
- 権限（Permissions）：ファイルに対するユーザの読み取り/書き込み権限。
- [Size]：ファイルサイズ。
- 最終更新日時（Last Modified）：ファイルが変更された日付と時刻。
- フル パス（Full Path）：ファイルのパス。

DHCP 自動更新

自動設定/イメージ更新機能は、自動的にネットワーク内のスイッチを設定し、ファームウェアをアップグレードする便利な方法を提供します。管理者はこのプロセスを使用して、ネットワーク内のこれらのデバイスの設定とファームウェアをリモートから最新の状態に保つことができます。

ステップ 1 [Administration] > [File Management] > [DHCP Auto Update] の順にクリックします。

ステップ 2 次を設定します。

DHCP経由の自動コンフィギュレーション	DHCP による自動設定を有効にするには、チェックを付けます。自動設定機能により、ネットワーク内のスイッチの設定と、そのファームウェアのアップグレードを自動で行うことができます。
ダウンロードプロトコル	次のオプションから、ダウンロードプロトコルを選択します。 • [Auto By File Extension]：（デフォルト）この拡張子を持つファイルは SCP を使用して（SSH 経由で）ダウンロードされ、その他の拡張子を持つファイルは TFTP を使用してダウンロードされます。 • TFTP のみ（TFTP Only）：設定ファイル名のファイル拡張子に関係なく、ダウンロードは TFTP で行われます。 • SCP のみ（SCP Only）：設定ファイル名のファイル拡張子に関係なく、ダウンロードは SCP（SSH 経由）で行われます。
DHCP によるイメージ自動更新	チェックを入れると、DHCP によるイメージの自動更新が有効になります。イメージの自動更新機能により、ネットワーク内のスイッチの更新と、そのファームウェアのアップグレードを自動で行うことができます。
ダウンロードプロトコル	次のオプションから、ダウンロードプロトコルを選択します。 • [Auto By File Extension]：（デフォルト）この拡張子を持つファイルは SCP を使用して（SSH 経由で）ダウンロードされ、その他の拡張子を持つファイルは TFTP を使用してダウンロードされます。 • TFTP のみ（TFTP Only）：設定ファイル名のファイル拡張子に関係なく、ダウンロードは TFTP で行われます。 • SCP のみ（SCP Only）：設定ファイル名のファイル拡張子に関係なく、ダウンロードは SCP（SSH 経由）で行われます。

ステップ 3 SCP の SSH 設定を選択します。

リモート SSH サーバー認証	リンクをクリックすると、[SSH Server Authentication] ページに移動します。このページでは、ダウンロードに使用する SSH サーバの認証を有効にし、必要な場合は信頼できる SSH サーバを入力できます。
SSHクライアント認証	• [SSH User Authentication] ページで [System Credentials] をクリックしてユーザーログイン情報を入力します。
バックアップサーバー定義	次のオプションから選択します。 • IPアドレス別 • 名前別

IP バージョン	次のオプションから選択します。 • IP Version 6 • IP Version 4
IPv6 アドレス タイプ	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部はFE80です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [グローバル] : IPv6アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。
バックアップサーバーのIPアドレス/名前	バックアップ設定ファイルの名前を入力します。
バックアップコンフィギュレーションファイル名	バックアップ設定ファイルの名前を入力します（0 ～ 160 文字を使用）。
バックアップ間接イメージファイル名	バックアップ間接イメージファイルの名前を入力します（0 ～ 160 文字を使用）。
最終自動コンフィギュレーション/イメージのサーバーIPアドレス	前回の自動設定/イメージサーバーの IP アドレスのアドレスが表示されます。
最後に自動コンフィギュレーションで使用したファイル名	前回の自動設定ファイルの名前が表示されます。

（注） DHCP自動コンフィギュレーション/イメージは、IPアドレスが動的に設定される場合にのみ機能します。

ステップ 4 [Apply] をクリックして設定値を保存します。

Cisco Business ダッシュボードの設定

Cisco Business ダッシュボードは、Cisco Business ダッシュボードマネージャを使用して、Cisco 100 ー 500 シリーズのネットワークを監視および管理するために役立ちます。Cisco Business ダッシュボードマネージャは、ネットワークを自動的に検出し、シスコのスイッチ、ルータ、ワイヤレスアクセスポイントなど、サポートされているすべての Cisco 100 ～ 500 シリーズのデバイスを設定および監視することを可能にするアドオンです。

Cisco Business ダッシュボードマネージャは、2 つの個別のコンポーネントまたはアプリケーション（Cisco Business ダッシュボードプローブと呼ばれる 1 つ以上のプローブと、Cisco Business ダッシュボードマネージャと呼ばれる 1 つのマネージャ）から構成される分散アプリケーションです。Cisco Business ダッシュボードプローブのインスタンスは、ネットワークの各サイトにインストールされ、ネットワークを検出し各シスコデバイスと直接通信します。

（注） Cisco Business ダッシュボードマネージャおよびプローブのセットアップ方法の詳細については、Cisco Business ダッシュボードのクイックスタートガイドを参照してください。

https://cisco.com/go/cbd-docs

スイッチのグラフィカルユーザーインターフェイス（GUI）で次の手順を実行して、ダッシュボードへのプローブ接続を有効にし、ダッシュボードへの接続を許可するために必要な組織名、ネットワーク名、およびその他の情報を設定します。

ステップ 1 [Administration] > [Cisco Business Dashboard Settings] の順にクリックします。

ステップ 2 次を設定します。

[Probe Operation]	Cisco Business ダッシュボードプローブの動作を有効にする場合はチェックを入れます。
[Probe Status]	CBD プローブのステータスが表示されます。可能な値は、[Active]、[Inactive]、または [Fault] です。
[Probe Version]	Cisco Business ダッシュボードプローブのバージョンが表示されます。
Logging Threshold	ドロップダウンリストからオプション（[Information]、[Debug]、[Warning]、または [Error]）を選択して、Cisco Business Dashboard プローブエージェントがログに記録するメッセージのレベルを制限します。指定したレベル以上のメッセージのみがログに記録されます。
[All Module Logging]	有効にする場合はオンにします。これにより、すべてのモジュール間のすべての通信とイベントがログに記録されます。
[Call Home Logging]	有効にする場合はオンにします。これにより、プローブとマネージャの間のすべての通信がログに記録されます。
[Discovery Logging]	有効にする場合はオンにします。これにより、デバイス検出イベントとトポロジ検出がログに記録されます。
[Services Logging]	有効にする場合はオンにします。これにより、ノースバウンドとサウスバウンドの間のメッセージ変換がログに記録されます。
[System Logging]	有効にする場合はオンにします。これにより、他のログの対象になっていないコアシステムプロセスがログに記録されます。

[Northbound Logging]	有効にする場合はオンにします。これにより、マネージャとプローブの間の通信がログに記録されます。
[Southbound Logging]	有効にする場合はオンにします。これにより、プローブとデバイスの間の低レベルの通信がログに記録されます。
[Dashboard Connection]	オンにすると接続が有効になります。
[Dashboard Status]	Cisco Business ダッシュボードマネージャのステータス（[Connected] または [Disconnected]）が表示されます。 ダッシュボードのステータスが [Disconnected] の場合、エラーの理由が表示されます。次に例を示します。 • Certificate-error：未指定の証明書検証エラー • Certificate-error：証明書はまだ有効ではありません • Certificate-error：証明書の有効期限が切れました • Certificate-error：証明書の確認に失敗しました • Connection-error：ホストが見つかりません（権限あり） • Connection-error：ホストへのルートがありません
組織名	デバイスで実行されている Cisco Business ダッシュボードプローブの組織名を入力します。
ネットワーク名（Network Name）	Cisco Business ダッシュボードプローブのサイト名を入力します。
[Dashboard Definition]	Cisco Business ダッシュボードのアドレスを定義します。次のいずれかを選択します。 • [By IP address]：このオプションでは、[IP Address/Name] フィールドに有効な IP アドレスを入力する必要があります。 • [By Name]：このオプションでは、[IP Address/Name] フィールドにホスト名を入力する必要があります。
IPアドレス/名前	Cisco Business ダッシュボードの名前または IP アドレスを入力します。
[Dashboard Port]	ダッシュボードに接続するには、次のいずれかの TCP ポートを指定します。 • デフォルト（443）の使用。 • ユーザー定義（範囲：1 ～ 65535）。このオプションは、[Dashboard Address] フィールドに有効なアドレスが入力されている場合にのみ使用できます。
アクセスキー ID	[Access Key ID] フィールドは、24 桁の 16 進数で構成されています。このフィールドには 16 進数文字以外は入力できないことに注意してください。

アクセスキーシークレット	認証に使用するシークレットを指定します。暗号化またはプレーンテキストのいずれかの形式で指定できます。プレーンテキスト形式は、ホワイトスペースなしで、最大 160 文字の英数字文字列として指定されます。キー ID とシークレットの設定は、同時に設定する必要があります。 （注） 適用時に、[Key ID] フィールドが空で [Secret] フィールドが空でない場合、または [Secret] フィールドが空で [Key ID] フィールドが空でない場合、「Key ID and Secret must be set together」というエラーメッセージが表示されます。

ステップ 3 [適用] をクリックし、実行コンフィギュレーションに設定を保存します。

（注） [Dashboard Connection] 設定が有効になっている場合、フィールドの [Organization Name]、[Network Name]、[Dashboard Address]、[Key ID] は変更できません。これらの設定を変更するには、[Dashboard Connection] チェックボックスをオフにし、[Apply] をクリックして、上記の手順 2 ～ 4 をやり直します。

[Display Sensitive Data as Plaintext]：クリックすると機密データがプレーンテキスト形式で表示されます。

[Reset Connection]：クリックすると、ダッシュボードとの現在の接続を切断し、Cisco Business ダッシュボードプローブのキャッシュデータをフラッシュしてから、ダッシュボードへの再接続を試みます操作の開始前に確認メッセージが表示されます。このコントロールは、[Dashboard Connection] と [Probe Operation] が有効になっている場合にのみ有効になります。

（注） [Reset Connection] は、[Dashboard Connection] チェックボックスと [Probe Operation] チェックボックスがオンになっている場合にのみ有効になります。

[Clear Probe Database]：クリックすると、プローブデータをクリアします。これは、[Probe Operation] チェックボックスがオフになっている（および画面がロードされて以降オフである）場合にのみ有効になります。それ以外の場合、ボタンは無効になり、「Probe Operation must be disabled prior to clearing probe database」というツールチップが表示されます。

（注） スイッチ上の Cisco Business Dashboard プローブが管理できるネットワークデバイスとクライアントの数には、多くの要因が影響します。スイッチ上のプローブでは、15 台以下のネットワークデバイス（スイッチ、ルータ、およびワイヤレスアクセスポイント）と、150 台以下の接続クライアントを管理することを推奨します。ネットワークがより複雑な場合は、Cisco Business Dashboard プローブに他のプラットフォームを使用することをお勧めします。Cisco Business Dashboard の詳細については、https://www.cisco.com/c/en/us/products/cloud-systems-management/business-dashboard/index.html を参照してください。

プラグアンドプレイ（PNP）

新しいネットワーク デバイスの設置やデバイスの交換を手作業で行うと、費用と時間がかかり、誤りが発生しやすくなります。通常、新しいデバイスは最初に中心的な準備施設に送ら

れ、そこでデバイスを開梱し、ステージング ネットワークに接続し、適切なライセンス、設定、イメージを使って更新します。その後、デバイスを梱包して実際の設置場所に運びます。これらの手順が完了した後、専門的な担当者が設置場所まで出向いて設置作業を行う必要があります。デバイスがNOC/データ センター自体に設置される場合でも、デバイスの数が非常に多くて専門家が不足する可能性があります。このすべての問題のために、デプロイが遅れ、運用コストがさらに増えます。

PNP サーバーへの接続

スイッチがPnPサーバーに接続できるように、スイッチがPNPサーバーのアドレス/URLを検出するプロセスが実行されます。検出方法には複数の方法があります。スイッチでは以下に示すシーケンスに従って実行されます。PnPサーバーが特定の方法で検出された場合、検出プロセスは完了し、残りの方法は実行されません。

1. ユーザー設定のアドレス：PnP サーバーの URL または IP アドレスはユーザーが指定します。
2. DHCP 応答オプション 43 から受信したアドレス：PnP サーバーの URL または IP アドレスは、DHCP 応答のオプション 43 の一部として受信されます
3. ホスト名「pnpserver」の DNS 解決：ホスト名「pnpserver」の DNS サーバー解決によって、アドレス指定された PnP サーバー IP が取得されます。
4. Cisco プラグアンドプレイ接続：HTTP を介して実行される完全な PNP サーバー検出を「すぐに使用可能」にするリダイレクションサービス。

スイッチは、FQDN「devicehelper.cisco.com」を使用してリダイレクションサービスに接続します。

Cisco PnP 接続の前提条件

Cisco プラグアンドプレイ接続動作を可能にするには、ユーザーが、プラグアンドプレイ接続でデバイスとコントローラプロファイルを作成する必要があります（https://software.cisco.com に移動し、[Plug and Play Connect] リンクをクリック）。PnP 接続を使用するには Cisco スマートアカウントが必要です。スマートアカウントを作成または更新するには、https://software.cisco.com の [Administration] セクションを参照してください。

さらに、スイッチ自体で次の前提条件が満たされている必要があります。

- PNP サーバーが他の検出方法で検出されていない。
- デバイスが devicehelper.cisco.com という名前を正常に解決できる（静的設定または DNS サーバーを使用）。
- システム時刻が次のいずれかの方式で設定されている。
  - 時刻が SNTP サーバーによって更新されている。
  - クロックがユーザーによって手動で設定されている。
  - リアルタイムクロック（RTC）により、リセット後も時間が保持されている。

CA 署名付き証明書ベースの認証

シスコでは、署名機関によって署名された証明書を .tar ファイル形式で配布し、シスコの認証局（CA）署名を使用してバンドルに署名します。この証明書バンドルは、cisco.com でのパブリックダウンロード向けに Cisco infoSec によって提供されます。

（注） シスコ PnP 接続情報に基づいて PNP サーバーを検出する場合、トラストプールは http://www.cisco.com/security/pki/trs/ios_core.p7b からダウンロードされます。

DHCP オプション 43 に基づいて PNP サーバーを検出する場合は、DHCP オプション 43 の「T<Trust pool CA bundle URL>;」パラメータを使用して、トラストプールをダウンロードするための URL を指定します。このバンドルの証明書は、SSL ハンドシェイク時にサーバー側の検証用シスコデバイスにインストールできます。サーバでは、バンドルで使用可能な CA のいずれかによって署名された証明書を使用するものとします。

PnP エージェントは、組み込み PKI 機能を使用して証明書バンドルを検証します。バンドルはシスコの CA によって署名されるため、エージェントはデバイスに証明書をインストールする前に、改ざんされたバンドルを特定できます。エージェントによってバンドルの整合性が確認されると、デバイスに証明書がインストールされます。証明書がデバイスにインストールされると、サーバから追加手順を実行しなくても PnP エージェントがサーバへの HTTPS 接続を開始します。

（注） デバイスでは、組み込み証明書バンドルをブートアッププロセスの一環としてインストールすることもできます。このバンドルは、PNP サーバーの検証に使用できます。バンドルがシスコ PnP 接続情報に基づいてダウンロードされると、ダウンロードされたバンドルから証明書がインストールされ、組み込みバンドルに基づく証明書はアンインストールされます。

（注） PNP エージェントは、インストールされた CA 証明書に基づいて PNP 証明書を検証するだけでなく、証明書の共通名/サブジェクト代替名（CN/SAN）が PNP サーバーのホスト名/IP アドレスと一致するかも検証します。一致しない場合、証明書の検証は拒否されます。

Cisco PnP DHCP オプション 43 使用上のガイドライン

DHCP オプション 43 はベンダー固有の識別子です。これは、PnP エージェントが PnP サーバーを見つけて接続するために使用できる方法の一つです（詳細については、Cisco プラグアンドプレイを参照）。

DHCP サーバーでの適切な設定を可能にするオプション 43 の設定については、以下を参照してください。

オプション 43 には次のフィールド/パラメータが含まれています。

<DHCP-typecode><feature-opcode><version><debug-option>;<arglist>

<arglist> パラメータでは次の構文を使用する必要があります。

B<IP address type>;I<IP address>;J<Port>;K<Transport protocol>;T<Trust pool CA bundle URL>;Z<SNTP server IP address>

次の表に、オプション 43 のフィールドの説明と使用方法の詳細を示します。

パラメータ	説明
DHCP-typecode	DHCP サブオプションタイプ。PnP の DHCP サブオプションタイプは 5 です。
feature-opcode	機能動作コード：アクティブ（A）またはパッシブ（P）のいずれかにできます。PnP の機能動作コードはアクティブ（A）です。これにより、PnP エージェントが PnP サーバーへの接続を開始します。PnP サーバーに到達できない場合、PnP エージェントは接続を確立するまで再試行します。
バージョン	PnP エージェントが使用するテンプレートのバージョン。1 にする必要があります。
debug-option	DHCP オプション 43 の処理時のデバッグメッセージをオンまたはオフにします。 D：デバッグオプションはオンです。N：デバッグオプションはオフです。
K	PnP エージェントと PnP サーバーの間で使用されるトランスポートプロトコル。 4：HTTP または 5：HTTPS。
B	文字コード「I」で指定される PnP サーバーの IP アドレスの タイプ。 1：ホスト、2：IPv4、3：IPv6
I	PnP サーバーの IP アドレスまたはホスト名。ホスト名を指定する場合は、ホスト名を正常に使用できるように、DHCP サーバーに DNS 関連のオプションが存在している必要があります。

パラメータ	説明
T	トラストプールのCAバンドルのURL。CAバンドルは、Cisco Business ダッシュボードまたは TFTP サーバーから取得できます。 • Cisco Business ダッシュボードを使用する場合は、次の URL 形式を使用します。 http://*CBD IP address or domain name/ca/trustpool/CA_bundle_name* • TFTP サーバーを使用する場合は、次の URL 形式を使用します。tftp://*tftp server IP/CA_bundle_name*
Z	SNTP サーバー IP アドレス。トラストプールを設定する前に、クロックを同期させる必要があります。 （注） スイッチのクロックは、スイッチでサポートされている SNTP サーバーによって更新された場合（デフォルトで、ユーザー設定により、またはZパラメータで）またはユーザーが手動で設定した場合に同期していると見なされます。このパラメータは、スイッチが他の SNTP サーバーに到達できないときにトラストプールセキュリティを使用する場合に必要です。たとえば、初期状態のスイッチで工場出荷時にデフォルト設定が行われているものの、デフォルトの SNTP サーバーに到達するためのインターネット接続がない場合などです。
J	ポート番号 HTTP=80 HTTPS=443

オプション 43 の使用例：

- 次の形式は、HTTP を使用した PnP 接続のセットアップに使用されます。

```
option 43 ascii 5A1N;K4;B2;I10.10.10.3;J80
```

- 次の形式は、トラストプールを直接使用する HTTPS 上での PnP 接続のセットアップに使用されます。HTTPS は、トラストプールの CA バンドルが Cisco Business ダッシュボードからダウンロードされ、Cisco Business ダッシュボードサーバー証明書がサードパーティによって発行されている（自己署名ではない）場合に使用できます。次の例で「10.10.10.3」は Cisco Business ダッシュボードの IP アドレスです。ドメイン名を指定することもできます。

```
option 43 ascii
5A1N;K5;B2;I10.10.10.3;Thttp://10.10.10.3/ca/trustpool/ios.p7b;Z10.75.166.1
```

PNP設定

PNP 設定を行うには、次の手順に従ってください。

ステップ 1 [Administration] > [PNP] > [PNP Settings] の順にクリックします。

ステップ 2 次のフィールドに情報を入力して、PNP を設定します。

PNP状態	有効にする場合はオンにします。
PNP Transport / Settings Definition	使用するトランスポートプロトコル、PNP サーバーアドレス、および使用する TCP ポートに関する設定情報を取得するためのオプションとして、次のいずれかを選択します。 • [デフォルト設定]：このオプションを選択すると、DHCP オプション 43 から PNP 設定が取得されます。DHCP オプション 43 から設定が得られない場合、デフォルト値（デフォルト トランスポート プロトコルの HTTP、PNP サーバーの DNS 名として「pnpserver」、HTTP に関連するポート）が使用されます。「pnpserver」の名前が DNS によって解決されない場合は、DNS 名「devicehelper.cisco.com」を使用して Cisco プラグアンドプレイ接続サービスが使用されます。[デフォルト設定] オプションを選択すると、[PNP トランスポート] セクションのすべてのフィールドがグレー表示になります。デバイス上で PNP エージェントと [DHCP Auto Configuration/Image Update] の両方が有効になっている場合、オプション 43 に加えて、コンフィギュレーションまたはイメージファイル名に関連するオプションが DHCP 応答に含まれていると、デバイスは、受信したオプション 43 を無視します。 • [Manual Settings]：PNP トランスポートに使用する TCP ポートとサーバーを手動で設定します。
Transport Protocol	トランスポートプロトコル（HTTP または HTTPS）を選択します。
TCP Port	TCP ポートの番号。これはシステムによって自動的に入力されます。HTTP の場合は 80 です。
サーバー指定方法	PNP サーバーを IP アドレスで指定するか、名前で指定するかを選択します。
IP バージョン	サポートする IP 形式を選択します。 • [Version 6]：IPv6 • [Version 4]：IPv4

サーバーIPv6アドレスタイプ	IP バージョンタイプが IPv6 である場合は、次のいずれかのオプションを選択します。 • [リンクローカル] : IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [グローバル] : IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	送信元 IPv6 アドレスタイプが [Link Local] である場合は、どこから IPv6 アドレスを受け取るかを選択します。
サーバーのIPアドレス/名前	PNP サーバーの IP アドレスまたはドメイン名を入力します。
PNPユーザー/ユーザー定義	サーバーに送られる PNP パケットに含まれるユーザー情報。次のオプションのいずれかを選択します。 • [デフォルト設定] : このオプションを選択すると、PNP ユーザー名とパスワードの設定が DHCP オプション 43 から取得されます。このオプションを選択すると、ユーザー名とパスワードのフィールドがグレー表示になります。 • [手動設定] : PNP ユーザー名とパスワードを手動で設定するにはこれを選択します。
ユーザー名	PNP パケットに含めるユーザー名。
パスワード	暗号化形式またはプレーンテキスト形式のパスワード。
PNP動作設定/再接続間隔	[User Defined] を選択した場合に、接続が失われてからセッションの再接続が試行されるまでの間隔（秒数）を設定します。
ディスカバリタイムアウト	PNPサーバーの検出に失敗した後、検出を再試行するまでの待機時間（秒数）を指定します。
タイムアウト指数因子	指数を使って検出の試行をトリガーする値。前のタイムアウト値を指数で乗算し、その結果をタイムアウトとして適用します（値がタイムアウト最大値より小さい場合）。
最大ディスカバリタイムアウト	タイムアウトの最大値。[ディスカバリ タイムアウト]値よりも大きくなければなりません。

ウォッチドッグタイムアウト	アクティブなPNPセッション中（ファイルのダウンロード処理中など）にPnPまたはファイルサーバーからの応答を待つ間隔。

ステップ3 [Apply] をクリックします。パラメータが実行コンフィギュレーション ファイルにコピーされます。

暗号化されたパスワードを表示するには、[Display Sensitive Data as Plaintext] をクリックします。

PNPセッション

PNP セッション画面には、現在有効になっている PNP パラメータの値が表示されます。該当する場合、パラメータのソースが括弧で示されます。

PNP パラメータに関する情報を表示するには、次の手順を実行します。

[管理] > [PNP] > [PNP セッション] をクリックします。

次のフィールドが表示されます。

- [管理ステータス]：PNP が有効になっているかどうか。
- [動作ステータス]：PNP が動作中かどうか。
- [PNP Agent State]：アクティブな PNP セッションが存在するかどうかを示します。可能な値は、[ディスカバリ待機]、[ディスカバリ]、[準備未完了]、[無効]、[セッション]、[セッション待機] です。
- [トランスポートプロトコル]：PNP エージェント セッション情報を表示します。
- [TCP ポート]：PNP セッションの TCP ポート。
- [サーバーIPアドレス]：PNP サーバーの IP アドレス。
- [Username]：PNP パケットで送信されるユーザー名。
- [Password MD5]：PNP パケットで送信されるパスワード。
- [Session Interval Timeout]：設定済みのセッション間隔タイムアウト（PNP エージェント状態が「待機中」の場合にのみ表示されます）。
- [残りのタイムアウト]：残っているタイムアウトの値。

（注） [再開] ボタンをクリックすると、ただちにPnPエージェントが次のように待機状態を終了します。

- エージェントがディスカバリ待機中状態の場合は、ディスカバリ状態に設定されます。
- エージェントが PnP セッション待機中状態の場合は、PnP セッション状態に設定されます。

リブート

ジャンボフレームのサポートの有効化などの一部の設定変更では、システムのリブートが必要です。ただし、デバイスをリブートすると、実行コンフィギュレーションが削除されるので、デバイスをリブートする前に、実行コンフィギュレーションをスタートアップ コンフィギュレーションとして保存しておくことが重要です。[Apply] をクリックしても、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されません。

デバイスをリブートするには、次の手順を実行します。

ステップ 1 [Administration] > [Reboot] の順にクリックします。

ステップ 2 [Reboot] をクリックし、デバイスをリブートします。

- [Reboot]：デバイスをリブートします。リブート時に実行コンフィギュレーション内の保存されていない情報は破棄されてしまうので、[Save] をクリックして、ブート中に現在のコンフィギュレーションが保持されるようにする必要があります。[Save] オプションが表示されない場合は、実行コンフィギュレーションがスタートアップ コンフィギュレーションと一致していて、保存する必要がないことを意味しています。

  次のオプションを使用できます。

  - [Immediate]：すぐにリブートします。
  - 日時（Date）：スケジュールリブートの日付（月/日）と時刻（時間と分）を入力します。指定した時刻（24 時間形式を使用）にソフトウェアがリロードされるように、スケジュールが設定されます。

    （注） このオプションは、システム時刻か手動で設定されているか SNTP によって設定されている場合にのみ使用できます。

  - [リブートをキャンセル] をクリックすると、スケジュール済みのリブートがキャンセルされます。
  - [In]：指定された日数、時間数と分数以内にリブートします。指定可能な最大時間は 24 日です。

- 工場出荷時の初期状態に復元（Restore to Factory Defaults）：工場出荷時のデフォルト設定を使用してデバイスをリブートします。このプロセスでアクティブイメージ、非アクティブイメージ、ミラー設定、およびローカリゼーションファイルを除くすべてが消去されます。

- スタートアップ コンフィギュレーション ファイルをクリア（Clear Startup Configuration File）：オンにすると、次回のブート時にデバイスでスタートアップ コンフィギュレーションがクリアされます。

ハードウェアリソース

[Hardware Resources] ページでは、ポリシーベースのルーティング（IPv4 および IPv6）と VLAN マッピングのルールに関してルータ TCAM 割り当てを調整できます。また、ステータスを確認し、ハードウェアベースのルーティングを再アクティブ化できます。

ルータ TCAM 割り当ての変更が正しくない場合、エラーメッセージが表示されます。ルータ TCAM 割り当てが適切な場合、新しい設定で自動リブートが実行されることを知らせるメッセージが表示されます。

ルーティング リソースは、変更が正しく行われない場合があります。次のいずれかの状態が該当します。

- 特定のエントリ タイプに対して割り当てたルータ TCAM エントリ数が、現在使用中のエントリ数より少ない場合。
- 割り当てたルータ TCAM エントリの総数が、使用可能な最大数よりも多い場合。

ルーティングリソースを表示および変更するには、次のようにします。

ステップ 1 [各種管理] > [ハードウェアリソース] の順にクリックします。

次のフィールドが表示されます。

- [Maximum IPv4 Policy-Based Routes]
  - [Use Default]：デフォルト値を使用します。
  - [User Defined]：値を入力します。
- [Maximum IPv6 Policy-Based Routes]
  - [Use Default]：デフォルト値を使用します。
  - [User Defined]：値を入力します。
- [Maximum VLAN-Mapping Entries]：次のいずれかを選択します。
  - [Use Default]：デフォルト値を使用します。
  - [User Defined]：値を入力します。
- [Hardware-Based Routing]：ハードウェアベースのルーティングが有効であるか、一時停止されているかを表示します。

ステップ 2 [Apply] をクリックして新しい設定を保存します。

（注） ハードウェアベースのルーティングがアクティブではない場合には、[Reactivate Hardware Based Routing] ボタンが表示されます。ハードウェア ベースのルーティングを有効にするには、このボタンをクリックします。ハードウェア ベースのルーティングのアクティブ化は、現在のルーティング コンフィギュレーションをサポートするのに使用可能なハードウェア リソースに応じて決まります。デバイス設定をサポートできる十分なルータリソースがない場合は、操作が失敗し、エラーメッセージがユーザーに対して表示されます。

ディスカバリ - Bonjour

Bonjour クライアントとして、デバイスは Bonjour ディスカバリプロトコルのパケットを 直接接続された IP サブネットにブロードキャストします。このデバイスは、ネットワーク管理システムまたはその他のサードパーティ製アプリケーションから検出できます。デフォルトでは、管理 VLAN で Bonjour が有効になっています。

Bonjour 設定を行うには、次の手順に従ってください。

ステップ 1 [Administration] > [Discovery - Bonjour] をクリックします。

ステップ 2 [Enable] を選択し、Bonjour ディスカバリをグローバルに有効にします。

ステップ 3 特定のインターフェイスで Bonjour を有効にするには、[Add] をクリックします。

ステップ 4 設定するインターフェイスを選択します。

ステップ 5 [Apply] をクリックして実行コンフィギュレーション ファイルを更新します。

（注） Bonjour が有効な場合、デバイスは Bonjour ディスカバリ インターフェイス コントロール テーブルで Bonjour に関連付けられている IP アドレスを持つインターフェイスに、Bonjour ディスカバリパケットを送信します。

ステップ 6 [Delete] をクリックして、インターフェイスの Bonjour を無効にします。

（注） Bonjour を無効にすると、デバイスは、Bonjour ディスカバリ アドバタイズメントの送信や、他のデバイスから送信される Bonjour ディスカバリ アドバタイズメントのリスニングを行わなくなります。

ディスカバリ - LLDP

LLDPは、ネットワーク マネージャによるマルチベンダー環境でのネットワーク管理のトラブルシューティングや強化を可能にするプロトコルです。LLDP では、ネットワーク デバイスが、それ自体を他のデバイスにアドバタイズする手法と、検出された情報を保存する手法が標準化されています。LLDPにより、デバイスは、そのID、設定、および機能を近接するデバイスにアドバタイズできます。その後、受信側のデバイスは、それらのデータを管理情報ベース（MIB）に保存します。

LDPはリンク層プロトコルです。デフォルトで、デバイスは、プロトコルの要求に従ってすべての着信 LLDP パケットの終了し、処理します。ここでは、LLDP の設定方法について説明します。内容は次のとおりです。

プロパティ

[プロパティ] ページでは、LLDP の一般パラメータを入力して、機能をグローバルに有効/無効にしたり、タイマーを設定したりすることができます。LLDP のプロパティを入力するには、次の手順を実行します。

ステップ 1 [Administration] > [Discovery - LLDP] > [Properties] をクリックします。

ステップ 2 パラメータを入力します。

LLDPステータス	選択するとデバイス上の LLDP が有効になります（デフォルトで有効）。
LLDPフレーム処理	[LLDP] が有効になっていない場合は、次のいずれかのオプションを選択します。 • [Filtering]：パケットを削除します。 • [Flooding]：VLAN メンバーすべてにパケットを転送します。
TLVアドバタイズ間隔	LLDP アドバタイズメント更新データの送信間隔（単位：秒）を入力するか、デフォルトを使用します。
トポロジ変更SNMP通知間隔	SNMP 通知の最小間隔を入力します。
ホールド係数	LLDP パケットを破棄するまで待機する時間を、[TLV Advertise Interval] の値の倍数で入力します。たとえば、[TLV Advertise Interval] の値が 30 秒であり、[Hold Multiplier] の値が 4 である場合、LLDP パケットは 120 秒後に破棄されます。
再初期化遅延	LLDP 有効/無効サイクルにおいて、LLDP を無効にしてから再初期化するまでの間隔（単位：秒）を入力します。

Transmit Delay	LLDP ローカルシステム MIB の内容が変更されたときに LLDP フレームを送信する間隔（単位：秒）を入力します。
シャーシIDアドバタイズメント	LLDP メッセージのアドバタイズメントに関して、次のオプションのいずれかを選択します。 • [MAC Address]：デバイスの MAC アドレスをアドバタイズします。 • [ホスト名]：デバイスのホスト名をアドバタイズします。

ステップ 3 LED-MED の [Properties] の [Fast Start Repeat Count] フィールドに、LLDP-MED FastStart メカニズムの初期化時に LLDP パケットを送信する回数を入力します。LLDP-MED FastStart メカニズムは、新しいエンドポイント デバイスがデバイスにリンクしたときに初期化されます。LLDP MED の詳細については、「LLDP MED ネットワーク ポリシー」セクションを参照してください。

ステップ 4 [Apply] をクリックします。LLDP プロパティが実行コンフィギュレーション ファイルに追加されます。

ポート設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。）

[LLDP Port Settings] ページで、ポートごとに LLDP と SNMP の通知を有効にできます。LLDP-MED TLV は、LLDP MEDポート設定 （110 ページ）で設定できます。

LLDP ポート設定を定義するには、次の手順を実行します。

ステップ 1 [Administration] > [Discovery - LLDP] > [Port Settings] をクリックします。

このページには、ポートの LLDP 情報が表示されます。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 次のフィールドを設定します。

Interface	編集するポートを選択します。
Administrative Status	このポートの LLDP 発行オプションを選択します。 • [Tx Only]：発行はしますが検出はしません。 • [Rx Only]：検出はしますが発行はしません。 • [Tx および Rx]：送信も検出も行います。 • [無効]：このポート上で LLDP を無効にします。
SNMP Notification	[Enable] を選択すると、SNMP 通知の受信者に通知が送信されます。

使用可能な、または選択されたオプションの TLV	デバイスが発行する情報のオプションを選択します。 • [Port Description]：ポートに関する情報。 • [System Name]：システムに割り当てられた名前。 • [System Description]：ネットワークエンティティの説明。 • [System Capabilities]：デバイスの主な機能、およびそれらの機能がデバイス上で有効になっているかどうか。 • [802.3 MAC-PHY]：送信元デバイスの、設定可能な通信方式（全二重 / 半二重） およびビット レート、ならびに、現在の通信方式およびビット レート。 • [802.3 Power via MDI]：MDI 経由で伝送される最大電力。 • [802.3 リンクアグリゲーション]：LLDP PDU 送信元ポートに関連付けられてい るリンクを集約できるかどうかを示します。 • [802.3 Maximum Frame Size]：MAC/PHY の実装における許容最大フレームサイズ。 • [4-Wire Power via MDI]：（60W PoE をサポートする PoE ポートに関連）60 ワットの電力を可能にする Power over Ethernet をサポートするために定義されたシスコ独自の TLV（標準サポートは最大 30 ワット）。 管理アドレスのオプション TLV
アドバタイズメントモード	デバイスの IP 管理アドレスをアドバタイズする方法を次の中から 1 つ選択します。 • [Auto Advertise]：アドバタイズする管理アドレスをデバイスのすべての IP アドレスからソフトウェアが自動的に選択するように指定します。複数の IP アドレスがある場合、ソフトウェアはダイナミック IP アドレスの中から最下位の 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 アドレスの中から最下位の IP アドレスを選択します。 • [None]：アドバタイズメントモードが不要な場合、このオプションを選択します。 • [手動アドバタイズ]：アドバタイズする管理 IP アドレスを選択します。
IP アドレス	[Manual Advertise] を選択した場合、表示される IP アドレスの中から管理 IP アドレスを選択します。
PVID	TLV で PVID をアドバタイズする場合に選択します。

ポートおよびプロトコルVLAN ID	ポート VLAN プロトコルに基づいてアドバタイズする VLAN ID を設定します。
VLAN ID	アドバタイズする VLAN を選択します。
[Protocol IDs]	アドバタイズするプロトコルを選択します。
選択されたプロトコルID	[Protocols IDs] ボックスで使用するプロトコルを選択して、それらを [Selected Protocols ID] ボックスに移動します。

ステップ 4 関連情報を入力し、[Apply] をクリックします。ポート設定は、実行コンフィギュレーション ファイルに書き込まれます。

[LLDP MED Network Policy]

LLDP-MED ネットワークポリシーは、音声やビデオなどの特定のリアルタイム アプリケーションに関連する設定のセットです。ネットワーク ポリシーが設定されている場合は、接続された LLDP メディア エンドポイント デバイスへの発信 LLDP パケットにそのポリシーを含めることができます。メディア エンドポイント デバイスは、受信したネットワーク ポリシーの指定に従ってトラフィックを送信する必要があります。たとえば、VoIP フォンに対して VoIP トラフィックの次の処理を指示するネットワーク ポリシーを作成できます。

- VLAN 10 の音声トラフィックをタグ付きパケットとして 802.1p プライオリティ 5 で送信する。
- DSCP 46 で音声トラフィックを送信する。

ネットワークポリシーをポートにバインドするには、LLDP MEDポート設定 （110 ページ）を使用します。管理者は、1 つ以上のネットワーク ポリシーと、ポリシーの宛先インターフェイスを手動で設定できます。VLAN を手動で作成することと、ネットワーク ポリシーおよびそれに関連付けられるインターフェイスに従って VLAN のポート メンバーシップを指定することは、管理者が担当します。

また、管理者は、デバイスによって維持されている音声 VLAN に基づいて音声アプリケーションのネットワーク ポリシーを自動的に生成してアドバタイズするようにデバイスを設定することもできます。デバイスが音声 VLAN を維持する方法の詳細については、自動音声 VLAN に関するセクションを参照してください。

LLDP MED ネットワークポリシーを定義するには、次の手順を実行します。

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP MED Network Policy] をクリックします。

このページには、作成済みのネットワーク ポリシーが表示されます。

ステップ 2 デバイスによって維持されている音声 VLAN に基づいて音声アプリケーションのネットワーク ポリシーを自動的に生成してアドバタイズするようにデバイスを設定する場合は、[LLDP-MED Network Policy for Voice Application] で [Auto] を選択します。

（注） このボックスがオンの場合、手動で音声ネットワーク ポリシーを設定できません。

ステップ 3 [Apply] をクリックし、この設定を実行コンフィギュレーション ファイルに追加します。

ステップ 4 新しいポリシーを定義するには、[Add] をクリックします。

ステップ 5 値を入力します。

- [ネットワークポリシー番号]：作成するネットワーク ポリシーの番号を選択します。
- [Application]：定義されるネットワーク ポリシーの対象となるアプリケーションのタイプ（トラフィックのタイプ）を選択します。
- [VLAN ID]：トラフィックの宛先 VLAN ID を入力します。
- [VLAN Type]：トラフィックをタグ付きにするかタグなしにするかを選択します。
- [ユーザープライオリティ]：このネットワーク ポリシーで設定したトラフィックに適 用するプライオリティを選択します。これは CoS 値です。
- [DSCP 値]：ネイバーから送信されるアプリケーション データに割り当てる DSCP 値を選択します。この値により、ネイバーからデバイスに送信するアプリケーション トラフィックにマークする方法をネイバーに通知できます。

ステップ 6 [Apply] をクリックします。ネットワーク ポリシーが定義されます。

（注） [LLDP MED Port Settings] ページを使用して、発信 LLDP パケットに必要な手動定義ネットワーク ポリシーを含めるようにインターフェイスを手動で設定する必要があります。

LLDP MEDポート設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。)

[LLDP MED Port Settings] ページでは、LLDP-MED TLV の設定を有効にします。ネットワーク ポリシーは、[LLDP MED Network Policy] ページを使用して設定します。

（注） [LLDP-MED Network Policy for Voice Application] が [Auto] で、自動音声 VLAN が動作している場合、デバイスは、すべての LLDP ポートについて、音声アプリケーションの LLDP-MED ネットワークポリシーを自動的に生成します。LLDP-MED は有効で、音声 VLAN のメンバーです。

各ポートで LLDP MED を設定するには、次の手順を実行します。

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP MED Port Settings] をクリックします。

このページには、すべてのポートについて次の LLDP MED 設定が表示されます。

- [User-Defined Network Policy]：[LLDP MED Network Policy]（109 ページ）内のトラフィックのタイプに対してポリシーが定義されます。ポート上のポリシーに関する次の情報が表示されます。
  - [Active]：トラフィックのタイプがポートでアクティブになっているかどうか。
  - [アプリケーション]：ポリシーを定義するトラフィックのタイプ。
- [ロケーション]：ロケーション TLV が送信されるかどうか。
- [PoE]：POE-PSE TLV が送信されるかどうか。
- [インベントリ]：インベントリ TLV が送信されるかどうか。

ステップ 2 ページ上部のメッセージは、音声アプリケーションの LLDP MED ネットワークポリシーが自動的に生成されるかどうかを示しています。モードを変更するリンクをクリックします。

ステップ 3 追加の LLDP MED TLV や 1 つ以上のユーザ定義 LLDP MED ネットワーク ポリシーをポートに関連付けるには、目的のものを選択して、[Edit] をクリックします。

ステップ 4 パラメータを入力します。

- [インターフェイス]：設定するインターフェイスを選択します。
- [LLDP MED ステータス]：このポート上で LLDP-MED を有効にするか無効にする かを選択します。
- [SNMP Notification]：MED をサポートするエンドステーションが検出されたときに、ポートごとに SNMP 通知を送信するかどうかを選択します。
- [Selected Optional TLVs]：デバイスが発行できる TLV を選択するには、目的の TLV を [Available Optional TLVs] リストから [Selected Optional TLVs] リストに移動させます。
- [Selected Network Policies]：LLDP が発行する LLDP MED ポリシーを選択するには、目的のポリシーを [Available Network Policies] リストから [Selected Network Policies] リストに移動させます。1 つ以上のユーザー定義のネットワークポリシーをアドバタイズメントに含めるには、[Available Optional TLVs] から [Network Policy] を選択する必要があります。

  （注） 次のフィールドの値は、LLDP-MED 規格（ANSI-TIA-1057_final_for_publication.pdf）で定義されているデータ形式に従い、16 進数で正確に入力する必要があります。

  - [デバイス場所の座標]：LLDP を使用して送信する座標を入力します。
  - [デバイス場所の住所]：LLDP を使用して送信する住所を入力します。
  - [Location ECS ELIN]：LLDP を使用して発行する緊急通報サービス（ECS）の ELIN ロケーションを入力します。

ステップ 5 [Apply] をクリックします。LLDP MED ポート設定は、実行コンフィギュレーション ファイルに書き込まれます。

LLDPポートステータス

[LLDPポートステータス] ページには、各ポートの LLDP グローバル情報が表示されます。

ステップ 1 LLDP ポート ステータスを表示するには、[Administration] > [Discovery - LLDP] > [LLDP Port Status] をクリックします。

すべてのポートの情報が表示されます。

ステップ 2 特定のポートに送信される LLDP および LLDP-MED の TLV の詳細情報を表示するには、ポートを選択して、[LLDP Local Information Detail] をクリックします。

ステップ 3 特定のポートから受信する LLDP および LLDP-MED の TLV の詳細情報を表示するには、ポートを選択して、[LLDP Neighbor Information Detail] をクリックします。

LLDP ポート ステータス グローバル情報

- [シャーシ ID サブタイプ] : シャーシ ID のタイプ（例：MAC アドレス）。
- [シャーシ ID] : シャーシの ID。シャーシ ID サブタイプが MAC アドレスである場合、デバイスの MAC アドレスが表示されます。
- [System Name] : デバイスの名前。
- [System Description] : デバイスの説明（英数字形式）。
- [サポートされているシステム機能] : スイッチでサポートされている主要機能（例：ブリッジ、WLAN AP、ルータ）。
- [有効なシステム機能] : スイッチで有効になっている主要機能。
- [ポート ID サブタイプ] : 表示されるポート ID のタイプ。

LLDP ポート ステータス テーブル

- [インターフェイス] : ポート ID。
- [LLDP ステータス] : 有効または無効。
- [LLDP MED ステータス] : 有効または無効。
- [Local PoE ((Power Type, Power Source, Power Priority, Power Value)] : アドバタイズされるローカル PoE 情報。
- [Remote PoE (Power Type, Power Source, Power Priority, Power Value)] : ネイバーによってアドバタイズされる PoE 情報。
- [ネイバーの数] : 検出されたネイバーの数。

• [Neighbor capability of 1st device]：ネイバーの主要機能（ブリッジ、ルータなど）が表示されます。

LLDPローカル情報

ポートからアドバタイズされているLLDPローカルポートステータスを表示するには、次のようにします。

ステップ1 [Administration] > [Discovery - LLDP] > [LLDP Local Information] をクリックします。

ステップ2 LLDP ローカル情報を表示するインターフェイスとポートを選択します。

[LLDP Local Information] ページには、次のフィールドが含まれています。

Global

• [Chassis ID Subtype]：シャーシ ID のタイプ。（MAC アドレスなど）。

• [シャーシ ID]：シャーシの ID。シャーシ ID サブタイプが MAC アドレスである場合、デバイスの MAC アドレスが表示されます。

• [System Name]：デバイスの名前。

• [System Description]：デバイスの説明（英数字形式）。

• [サポートされているシステム機能]：スイッチでサポートされている主要機能（例：ブリッジ、WLAN AP、ルータ）。

• [有効なシステム機能]：スイッチで有効になっている主要機能。

• [ポート ID サブタイプ]：表示されるポート ID のタイプ。

• [ポート ID]：ポートの ID。

• [ポートの説明]：ポートに関する情報（例：製造元、製品名、ハードウェアバージョン、ソフトウェア バージョン）。

Management Address

• [IPv4 Address]：管理用途に最も適した IPv4 戻りアドレス。

• [IPv6 Global Address]：管理用途に最も適した IPv6 戻りグローバル アドレス。

• [IPv6 Link Local Address]：管理用途に最も適した IPv6 戻りリンク ローカル アドレス。

[MAC/PHY Details]

• [自動ネゴシエーション対応]：ポート速度のオートネゴシエーションがサポートされ ているかどうか。表示される値は [True] または [False] です。

• [自動ネゴシエーション有効]：ポート速度のオートネゴシエーションが有効になっているかどうか。表示される値は [True] または [False] です。

- [自動ネゴシエーションアドバタイズ機能] : オートネゴシエーションが可能なポート 速度のタイプ（例：1000BASE-T 半二重モード、100BASE-TX 全二重モード）。
- [動作 MAU タイプ] : Medium Attachment Unit（MAU）のタイプ。MAU では物理層の機能が実行されます。たとえば、イーサネット インターフェイスのコリジョン検出から入ってきたデータに対するデジタル データ変換、ネットワーク（100BASE-TX 全二重モードなど）へのビット挿入などの処理が実行されます。

[802.3 Details]

- [802.3 Maximum Frame Size] : サポートされている IEEE 802.3 フレームサイズの最大値。

[802.3 Link Aggregation]

- [アグリゲーション機能] : インターフェイスを集約できるかどうか。
- [アグリゲーションステータス] : 現在、インターフェイスが集約されているかどうか。
- [アグリゲーションポート ID] : アドバタイズされている集約インターフェイス ID。

[802.3 Energy Efficient Ethernet (EEE)]

- [Local Tx] : リモートリンクパートナーの Tx 値に対するローカルリンクパートナーのリフレクションを示します。
- [Local Rx] : リモートリンクパートナーの Rx 値に対するローカルリンクパートナーのリフレクションを示します。
- [Remote Tx Echo] : 低電力アイドル（LPI モード）を抜けた後、データの送信を開始するまで、送信リンクパートナーが待機する時間（単位：マイクロ秒）を示します。
- [Remote Rx Echo] : 受信リンクパートナーが要求する、低電力アイドル（LPI モード）後にデータを送信するまでに、送信リンクパートナーが待機する時間（単位：マイクロ秒）を示します。

[802.3 Power via MDI]

- [MDI 電源対応ポートクラス] : アドバタイズされている電力サポート ポート クラス。
- [PSE MDI 電源対応] : ポートで MDI 電力がサポートされているかどうか。
- [PSE MDI 電源状態] : ポートで MDI 電力が有効になっているかどうか。
- [PSE 電源ペア制御機能] : ポートで電力線制御がサポートされているかどうか。
- [PSE 電源ペア] : ポートで電力線制御タイプがサポートされているかどうか。
- [PSE 電力クラス] : アドバタイズされている、ポートの電力クラス。
- 電源タイプ（Power Type） : ポートに接続されたポッド デバイスのタイプ。
- [Power Source] : ポートの電源。
- [Power Priority] : ポートの電力のプライオリティ。
- [PD Requested Power Value] : PSE から PD に割り当てられた電力量。

- [PSE Allocated Power Value]：給電側機器（PSE）に割り当てられた電力量。

[4-Wire Power via MDI]

- [4-Pair PoE Supported]：システムとポートが 4 ペア線の有効化をサポートしていることを示します（この HW 能力を持っている特定のポートにのみ当てはまる）。
- [Spare Pair Detection/Classification Required]：4 ペア線が必要であることを示します。
- [PD Spare Pair Desired State]：POD デバイスが 4 ペア能力を有効にするように要求していることを示します。
- [PD Spare Pair Operational State]：4 ペア能力が有効か無効かを示します。

[MED Details]

- [サポートされている機能]：ポート上で有効になっている MED 機能。
- [現在の機能]：ポートからアドバタイズされている MED TLV。
- [デバイスクラス]：LLDP-MED エンドポイント デバイス クラス。表示されるデバイス クラスは次のとおりです。
  - [Endpoint Class 1]：汎用エンドポイント クラス（基本的な LLDP サービスを提供）を示します。
  - [Endpoint Class 2]：メディア エンドポイント クラス（クラス 1 のすべての機能に加え、メディア ストリーミング機能を提供）を示します。
  - [Endpoint Class 3]：通信デバイス クラス（クラス 1 およびクラス 2 のすべての機能に加え、場所、911、レイヤ 2 スイッチ サポート、およびデバイス情報管理の各機能を提供）を示します。
- [PoE Device Type]：ポートの PoE タイプ（PD/PSE など）。
- [PoE 電源]：ポートの電源。
- [PoE 電力プライオリティ]：ポートの電力のプライオリティ。
- [PoE 電力値]：ポートの電力の値。
- [Hardware Revision]：ハードウェアのバージョン。
- [ファームウェアリビジョン]：ファームウェアのバージョン。
- [ソフトウェアリビジョン]：ソフトウェアのバージョン。
- [Serial Number]：デバイスのシリアル番号。
- [製造業者名]：デバイスの製造元名。
- [モデル名]：デバイスのモデル名。
- [アセット ID]：アセット ID。

[Location Information]

ANSI-TIA-1057 規格の 10.2.4 項に従って、次のデータ構造を 16 進数で入力します。

- [住所]：住所。
- [座標]：位置マップ座標（緯度、経度、および標高）。
- [ECS ELIN]：デバイスの ECS の ELIN。

[Network Policy Table]

- [アプリケーションタイプ]：ネットワーク ポリシーのアプリケーション タイプ（例：
- 音声）。[VLAN ID]：ネットワーク ポリシーがバインドされている VLAN の ID。
- [VLAN タイプ]：ネットワーク ポリシーがバインドされている VLAN のタイプ（タ グ付きまたはタグなし）。
- [ユーザープライオリティ]：ネットワーク ポリシーのユーザー プライオリティ。
- [DSCP]：ネットワーク ポリシーの DSCP。

LLDPネイバー情報

[LLDP Neighbor Information] ページには、ネイバーデバイスから受信した情報が表示されます。タイムアウト（ネイバーから受信した値（ネイバーから LLDP PDU を受信しなかったパケット存続時間 TLV の値）に基づく）後に、情報が削除されます。

LLDP ネイバー情報を表示するには、次の手順を実行します。

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP Neighbor Information] をクリックします。

ステップ 2 LLDP ネイバー情報を表示するインターフェイスを選択します。

このページには、選択したインターフェイスに関する次のフィールドが表示されます。

- [ローカルポート]：ネイバーが接続されているローカル 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：MAC アドレス）。
- [シャーシ ID]：802 LAN 近隣デバイスのシャーシの ID。
- [ポート ID サブタイプ]：表示されるポート ID のタイプ。
- [ポート ID]：ポートの ID。
- [System Name]：発行されたデバイスの名前。
- [存続可能時間]：タイムアウト時間（単位：秒）。この時間内にこのネイバーからLLDP PDU が 1 件も受信されなかった場合、このネイバーの情報は削除されます。

ステップ 3 ローカル ポートを選択し、[Details] をクリックします。

[LLDP Neighbor Information] ページには、次のフィールドが含まれています。

[Port Details]

- [ローカルポート] : ポート番号。
- [MSAP エントリ] : デバイスの Media Service Access Point（MSAP）エントリ 番号。

[Basic Details]

- [シャーシ ID サブタイプ] : シャーシ ID のタイプ（例：MAC アドレス）。
- [シャーシ ID]：802 LAN 近隣デバイスのシャーシの ID。
- [ポート ID サブタイプ] : 表示されるポート ID のタイプ。
- [ポート ID]：ポートの ID。
- [ポートの説明] : ポートに関する情報（例：製造元、製品名、ハードウェアバージョン、ソフトウェア バージョン）。
- [システム名] : 公開されているシステム名。
- [システムの説明] : ネットワーク エンティティの説明（英数字）。これには、システムの名前と、このデバイスでサポートされているハードウェア、オペレーティング システム、およびネットワーキング ソフトウェアのバージョンが含まれます。値は、sysDescr オブジェクトと同一です。
- [サポートされているシステム機能] : このデバイスでサポートされている主要機能。機能は2オクテットで示されます。ビット 0 ～ 7 はそれぞれ、その他、リピータ、ブリッジ、WLAN AP、ルータ、電話、DOCSIS ケーブル デバイス、およびステーションを示します。ビット 8 ～ 15 は予約されています。
- [有効なシステム機能] : スイッチで有効になっている主要機能。

[Management Address Table]

- [Address Subtype]：管理アドレスのサブタイプ（MAC、IPv4 など）。
- [アドレス] : 管理アドレス。
- [インターフェイスサブタイプ] : ポートのサブタイプ。
- [インターフェイス番号] : ポート番号。

[MAC/PHY Details]

- [自動ネゴシエーション対応] : ポート速度のオートネゴシエーションがサポートされ ているかどうか。表示される値は [True] または [False] です。
- [自動ネゴシエーション有効] : ポート速度のオートネゴシエーションが有効になっているかどうか。表示される値は [True] または [False] です。
- [自動ネゴシエーションアドバタイズ機能] : オートネゴシエーションが可能なポート 速度のタイプ（例：1000BASE-T 半二重モード、100BASE-TX 全二重モード）。
- [動作 MAU タイプ] : Medium Attachment Unit（MAU）のタイプ。MAU では物理層の機能が実行されます。たとえば、イーサネット インターフェイスのコリジョン検出から入ってきたデータに対するデ

ジタル データ変換、ネットワーク（100BASE-TX 全二重モードなど）へのビット挿入などの処理が実行されます。

[802.3 Power via MDI]

- [MDI 電源対応ポートクラス] : アドバタイズされている電力サポート ポート クラス。
- [PSE MDI 電源対応] : ポートで MDI 電力がサポートされているかどうか。
- [PSE MDI 電源状態] : ポートで MDI 電力が有効になっているかどうか。
- [PSE 電源ペア制御機能] : ポートで電力線制御がサポートされているかどうか。
- [PSE 電源ペア] : ポートで電力線制御タイプがサポートされているかどうか。
- [PSE 電力クラス] : アドバタイズされている、ポートの電力クラス。
- 電源タイプ（Power Type）：ポートに接続されたポッド デバイスのタイプ。
- [電源] : ポートの電源。
- 電源優先度（Power Priority）：ポートの電源の優先順位。
- [PD Requested Power Value] : POD デバイスから要求された電力量。
- [PSE Allocated Power Value] : PSE から PD に割り当てられた電力量。

[4-Wire Power via MDI]

- [4-Pair PoE Supported] : システムとポートが 4 ペア線の有効化をサポートしていることを示します（この HW 能力を持っている特定のポートにのみ当てはまる）。
- [Spare Pair Detection/Classification Required] : 4 ペア線が必要であることを示します。
- [PD Spare Pair Desired State] : POD デバイスが 4 ペア能力を有効にするように要求していることを示します。
- [PD Spare Pair Operational State] : 4 ペア能力が有効か無効かを示します。

[802.3 Details]

- [802.3 最大フレームサイズ] : アドバタイズされている、ポートの最大フレーム サ イズ。

[802.3 Link Aggregation]

- [アグリゲーション機能] : ポートを集約できるかどうか。
- [アグリゲーションステータス] : 現在、ポートが集約されているかどうか。
- [アグリゲーションポート ID] : アドバタイズされている集約ポート ID。

[802.3 Energy Efficient Ethernet (EEE)]

- [Remote Tx] : 低電力アイドル（LPI モード）を抜けてからデータ送信を開始するまでに送信リンク パートナーが待機する時間（マイクロ秒単位）。

- [Remote Rx]：受信リンク パートナーが要求する、低電力アイドル（LPI モード）を抜けてからデータ送信を開始するまでに送信リンク パートナーが待機する時間（マイクロ秒単位）。
- [Local Tx Echo]：リモート リンク パートナーの Tx 値に対するローカル リンク パートナーのリフレクションを示します。
- [Local Rx Echo]：リモート リンク パートナーの Rx 値に対するローカル リンク パートナーのリフレクションを示します。

[MED Details]

- [サポートされている機能]：ポート上で有効になっている MED 機能。
- [現在の機能]：ポートからアドバタイズされている MED TLV。
- [デバイスクラス]：LLDP-MED エンドポイント デバイス クラス。表示されるデバイス クラスは次のとおりです。
  - [Endpoint Class 1]：汎用エンドポイント クラス（基本的な LLDP サービスを提供）を示します。
  - [Endpoint Class 2]：メディア エンドポイント クラス（クラス 1 のすべての機能に加え、メディア ストリーミング機能を提供）を示します。
  - [Endpoint Class 3]：通信デバイス クラス（クラス 1 およびクラス 2 のすべての機能に加え、場所、911、レイヤ 2 スイッチ サポート、およびデバイス情報管理の各機能を提供）を示します。
- [PoE Device Type]：ポートの PoE タイプ（PD/PSE など）。
- [PoE 電源]：ポートの電源。
- [PoE 電力プライオリティ]：ポートの電力のプライオリティ。
- [PoE 電力値]：ポートの電力の値。
- [Hardware Revision]：ハードウェアのバージョン。
- [ファームウェアリビジョン]：ファームウェアのバージョン。
- [ソフトウェアリビジョン]：ソフトウェアのバージョン。
- [Serial Number]：デバイスのシリアル番号。
- [製造業者名]：デバイスの製造元名。
- [モデル名]：デバイスのモデル名。
- [アセット ID]：アセット ID。

[802.1 VLAN and Protocol]

- [PVID]：アドバタイズされている、ポートの VLAN ID。

[PPVID Table]

- [VID]：プロトコルの VLAN ID。

- [サポート済み] : サポートされている、ポートとプロトコルの VLAN ID。
- [有効] : 有効になっている、ポートとプロトコルの VLAN ID。

[VLAN ID Table]

- [VID] : ポートとプロトコルの VLAN ID。
- [VLAN Name] : アドバタイズされている VLAN 名。

[Protocol ID Table]

- [Protocol ID] : アドバタイズされているプロトコル ID。

[Location Information]

ANSI-TIA-1057 規格の 10.2.4 項に従って、次のデータ構造を 16 進数で入力します。

- [住所] : 住所。
- [座標] : 位置マップ座標（緯度、経度、および標高）。
- [ECS ELIN] : デバイスの ECS の ELIN。
- [不明] : 位置情報不明。

[Network Policy Table]

- [アプリケーションタイプ] : ネットワーク ポリシーのアプリケーション タイプ（例 :
- 音声）。[VLAN ID] : ネットワーク ポリシーがバインドされている VLAN の ID。
- [VLAN タイプ] : ネットワーク ポリシーがバインドされている VLAN のタイプ（タ グ付きまたはタグなし）。
- [ユーザープライオリティ] : ネットワーク ポリシーのユーザー プライオリティ。
- [DSCP] : ネットワーク ポリシーの DSCP。

LLDP の統計情報

[LLDP統計情報] ページには、ポートごとの LLDP 統計情報が表示されます。

LLDP 統計情報を表示するには、次の手順を実行します。

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP Statistics] をクリックします。

各ポートについて、次のフィールドが表示されます。

- [インターフェイス] : インターフェイス ID。
- [Tx Frames (Total)] : 送信されたフレームの数。

- Rx フレーム
  - [Total]：受信したフレームの合計数。
  - [Discarded]：受信したフレームのうち、廃棄されたフレームの数。
  - [Errors]：受信したフレームのうち、エラーになったフレームの数。
- [Rx TLVs]
  - [Discarded]：受信した TLV のうち、廃棄された TLV の数。
  - [未認識]：受信した TLV のうち、認識されなかった TLV の数。
- [Neighbor's Information Deletion Count]：このインターフェイスでネイバーがエージアウトされた回数。

ステップ 2 最新の統計情報を表示するには、[Refresh] をクリックします。

LLDP過負荷

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。)

LLDP では、情報が LLDP TLV および LLDP-MEDTLV として LLDP パケットに追加されます。LLDP 過負荷は、LLDP パケット内の総情報量がインターフェイスでサポートされている最大 PDU サイズを超えたときに発生します。

[LLDP Overloading] ページには、LLDP/LLDP-MED 情報のバイト数、使用可能なバイト数、および各インターフェイスの過負荷ステータスが表示されます。

LLDP 過負荷情報を表示するには、次の手順に従います。

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP Overloading] をクリックします。

LLDP 過負荷テーブルでは、各ポートについて次の情報が表示されます。

- [インターフェイス]：ポート ID。
- [Total Bytes In-Use]：各パケットの LLDP 情報の合計バイト数。
- [Available Bytes Left]：各パケットで追加の LLDP 情報用に残っている利用可能な合計バイト数。
- [ステータス]：TLV が送信されているか、それとも過負荷状態になっているか。

ステップ 2 特定のポートの過負荷状態を詳細表示するには、そのポートを選択して [Details] をクリックします。

このページには、ポートで送信された各 TLV に関する次の情報が表示されます。

- [LLDP Mandatory TLVs]

- [Size (Bytes)]：必須 TLV の合計バイト数。
- [ステータス]：必須 TLV グループが送信されているか、それとも過負荷状態に なっているか。

- [LLDP MED Capabilities]
  - [Size (Bytes)]：LLDP MED 機能パケットの合計バイト数。
  - [Status]：LLDP MED 機能パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP MED Location]
  - [Size (Bytes)]：LLDP MED 位置パケットの合計バイト数。
  - [Status]：LLDP MED 位置パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP MED Network Policy]
  - [Size (Bytes)]：LLDP MED ネットワーク ポリシー パケットの合計バイト数。
  - [Status]：LLDP MED ネットワーク ポリシー パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP MED Extended Power via MDI]
  - [Size (Bytes)]：LLDP MED 拡張 Power via MDI パケットの合計バイト サイズ。
  - [Status]：LLDP MED 拡張 Power via MDI パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [802.3 TLVs]
  - [Size (Bytes)]：LLDP MED 802.3 TLV パケットの合計バイト サイズ。
  - [Status]：LLDP MED 802.3 TLV パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP Optional TLVs]
  - [Size (Bytes)]：LLDP MED オプション TLV パケットの合計バイト サイズ。
  - [Status]：LLDP MED オプション TLV パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP MED Inventory]
  - [Size (Bytes)]：LLDP MED インベントリ TLV パケットの合計バイト サイズ。
  - [Status]：LLDP MED インベントリ パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- Total

- [Total (Bytes)]：各パケットの LLDP 情報の合計バイト数。
- [使用可能な残りのバイト数]：各パケットで追加のLLDP情報用に未送信のまま残っている利用可能な合計バイト数。

ディスカバリ - CDP

Cisco Discovery Protocol は、メディア独立型かつネットワーク独立型のレイヤ 2 プロトコルであり、ネットワーキングアプリケーションで、直接接続された付近のデバイスに関して学習するために使用されます。Cisco Discovery Protocol はデフォルトでイネーブルになっています。Cisco Discovery Protocol 用に設定された各デバイスは、メッセージを受信できるアドレスを 1 つ以上アドバタイズし、定期的なアドバタイズメント（メッセージ）を既知のマルチキャストアドレス 01:00:0C:CC:CC:CC に送信します。デバイスは、このアドレスをリッスンすることによって相互に検出します。また、メッセージをリッスンすることにより、他のデバイス上のインターフェイスがアップまたはダウン状態になった時期を認識します。

アドバタイズメントには、存続可能時間情報が含まれます。この情報は、受信デバイスがCisco Discovery Protocol情報を廃棄するまでの保持時間の長さを示します。デフォルトで、シスコ ソフトウェアでサポートされている設定済みアドバタイズメントは、サブネットワークアクセスプロトコル（SNAP）ヘッダーをサポートするインターフェイス上で 60 秒ごとに送信されます。シスコ デバイスは、Cisco Discovery Protocol パケットを転送しません。Cisco Discovery Protocol をサポートしているシスコ デバイスは、受信した情報をテーブルに保存します。このテーブル内の情報はアドバタイズメントを受信するたびに更新されます。また、アドバタイズメントの送信に 3 回失敗したデバイスに関する情報は廃棄されます。

ここでは、CDP の設定方法について説明します。

プロパティ

LLDP と同様に、Cisco Discovery Protocol（CDP）は、直接接続されたネイバーが自身とそれぞれの機能を互いにアドバタイズするためのリンク層プロトコルです。LLDP とは異なり、CDP はシスコ独自のプロトコルです。CDPのプロパティを設定するには、次の手順を実行します。

ステップ 1 [Administration] > [Discovery - CDP] > [Properties] をクリックします。

ステップ 2 パラメータを入力します。

CDP Status	選択するとデバイス上の CDP が有効になります。

CDPフレーム処理	CDPが有効でない場合は、選択した基準に一致するパケットを受信したときに実行する処理を次の中から選択します。 • [Bridging]：VLANに基づいてパケットを転送 • [Filtering]：パケットを削除 • [フラッディング]：入力ポートを除くすべてのポートに着信CDPパケットを転送するVLAN非対応のフラッディング。
CDP音声VLANアドバタイズメント	選択すると、CDPが有効で、音声VLANのメンバーであるすべてのポートで、デバイスがCDPを使用して音声VLANをアドバタイズできるようになります。音声VLANの設定については、プロパティ（178ページ）を参照してください。
CDP必須TLVの検証	選択すると、必須TLVを含まない着信CDPパケットは廃棄され、無効エラーカウンタが増加します。
CDPバージョン	使用するCDPのバージョンを選択します。
CDP保留時間	CDPパケットを廃棄するまで待機する時間を、[TLV Advertise Interval]の値の倍数で測定します。たとえば、[TLV Advertise Interval]の値が30秒であり、Hold Multiplier]の値が4である場合、LLDPパケットは120秒後に破棄されます。次のオプションがあります。 • [デフォルトを使用]：デフォルトの時間（180秒）を使用します。 • [ユーザー定義]：時間を入力します（単位：秒）。
CDP転送速度	CDPアドバタイズメント更新データの送信間隔を秒単位で入力します。次のオプションがあります。 • [デフォルトを使用]：デフォルト レート（60秒）を使用します。 • [ユーザー定義]：レートを入力します（単位：秒）。
デバイスID形式	デバイスIDの形式を選択します（MACアドレスまたはシリアル番号）。次のオプションがあります。 • [デフォルトを使用]：デフォルト レート（60秒）を使用します。 • [ユーザー定義]：レートを入力します（単位：秒）。
Source Interface	フレームのTLVで使用されるIPアドレス。次のオプションがあります。 • [デフォルトを使用]：発信インターフェイスのIPアドレスを使用します。 • [ユーザー定義]：アドレスTLV内のインターフェイス（[インターフェイス]フィールド）のIPアドレスを使用します。

Interface	[Source Interface] で [User Defined] が選択された場合は、インターフェイスを選択します。
Syslog音声VLAN不一致	オンにすると、音声 VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内の音声 VLAN 情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。
SyslogネイティブVLAN不一致	オンにすると、ネイティブ VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内のネイティブ VLAN 情報が、ローカルデバイスがアドバタイズしている情報と一致していないことを示しています。
Syslogデュプレックス不一致	オンにすると、デュプレックス情報が一致しないときに SYSLOG メッセージが送信されます。これは、着信フレーム内のデュプレックス情報が、ローカルデバイスがアドバタイズしている情報と一致していないことを示しています。

ステップ 3 [Apply] をクリックします。LLDP のプロパティが定義されます。

インターフェイスの設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

[Interface Settings] ページでは、ポートごとに CDP の有効/無効を設定できます。これらのプロパティ値を設定することにより、LLDP プロトコル対応デバイスに送信する情報のタイプを選択できます。

アドバタイズする LLDP-MED TLV は、LLDP MEDポート設定 （110ページ） で選択できます。

CDP インターフェイス設定を定義するには、次の手順に従います。

ステップ 1 [Administration] > [Discovery - CDP] > [Interface Settings] をクリックします。

このページには、各インターフェイスの次の CDP 情報が表示されます。

- [CDP ステータス]：ポートで CDP を有効または無効にします。
- [Reporting Conflicts with CDP Neighbors]：[Edit] ページで有効/無効になっているレポート オプション（音声 VLAN/ネイティブ VLAN/デュプレックス）のステータス。
- [ネイバー数]：検出されたネイバーの数。

  ページ下部に次の 4 つのボタンがあります。
- [設定のコピー]：選択すると、ポート間でコンフィギュレーションがコピーされます。
- [編集]：フィールドは後述のステップ 2 で説明されています。

- [CDP Local Information Details]：CDPローカル情報 （126 ページ）に移動します。
- [CDP Neighbor Information Details]：CDP ネイバー情報 （128 ページ）に移動します。

ステップ 2 ポートを選択して [Edit] をクリックします。

このページには、次のフィールドがあります。

- [インターフェイス]：定義するインターフェイスを選択します。
- [CDP ステータス]：ポートで CDP を有効または無効にします。

（注） 次の 3 つのフィールドは、デバイスが管理ステーションにトラップを送信するように設定されている場合のオプションです。

- [Syslog Voice VLAN Mismatch]：選択すると、音声 VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内の音声 VLAN 情報が、ローカルデバイスがアドバタイズしている情報と一致していないことを示しています。
- [Syslog Native VLAN Mismatch]：選択すると、ネイティブ VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内のネイティブ VLAN 情報が、ローカルデバイスがアドバタイズしている情報と一致していないことを示しています。
- [Syslog Duplex Mismatch]：選択すると、デュプレックス情報の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内のデュプレックス情報が、ローカルデバイスがアドバタイズしている情報と一致していないことを示しています。

ステップ 3 関連情報を入力し、[Apply] をクリックします。ポート設定は、実行コンフィギュレーションに書き込まれます。

CDPローカル情報

ローカルデバイスに関して CDP プロトコルによってアドバタイズされる情報を表示するには、次の手順に従います。

[Administration] > [Discovery - CDP] > [CDP Local Information] の順にクリックします。次のフィールドが表示されます。

Interface	ローカルポート数。
CDP 状態（CDP State）	CDP が有効かどうかを表示します。
[Device ID TLV]	• [Device ID Type]：デバイス ID TLV でアドバタイズされるデバイス ID のタイプ。 • [Device ID]：デバイス ID TLV でアドバタイズされるデバイス ID。

システム名 TLV	[システム名]：デバイスのシステム名。
アドレス TLV	[Address1-3]：デバイス アドレス TLV でアドバタイズされる IP アドレス。
[Port TLV]	[ポート ID]：ポート TLV でアドバタイズされるポートの ID。
Port ID	ポート TLV でアドバタイズされるポートの ID。
機能 TLV	[Capabilities]：ポート TLV でアドバタイズされる機能。
バージョン TLV	[バージョン]：デバイスが稼動しているソフトウェアのリリースに関する情報。
プラットフォーム TLV	[プラットフォーム]：プラットフォーム TLV でアドバタイズされるプラットフォー ムの ID。
ネイティブ VLAN TLV	[ネイティブ VLAN]：ネイティブ VLAN TLV でアドバタイズされるネイティブVLAN ID。
全二重/半二重 TLV	[Duplex]：全二重 TLV または半二重 TLV でアドバタイズされるポートのデュプレックスが半二重か全二重か。
[Appliance TLV]	• [Appliance ID]：アプライアンス TLV でアドバタイズされる、ポートに接続されたデバイスのタイプ。 • [アプライアンス VLAN ID]：アプライアンスによって使用されるデバイス上の VLAN。たとえば、アプライアンスが IP 電話の場合は、これは音声 VLAN になります。
[Extended Trust TLV]	[Extended Trust]：有効になっている場合、ポートが信頼され、受信されたパケットがマーキングされます。この場合、このようなポートで受信されたパケットは、再度マーキングされることはありません。無効な場合は、ポートが信頼できないことを示しています。この場合、次のフィールドが該当します。
[CoS for Untrusted Ports TLV]	[CoS for Untrusted Ports]：ポートの [Extended Trust] が無効な場合、このフィールドにはレイヤ 2 CoS 値、つまり 802.1D/802.1p プライオリティ値が表示されます。これは、信頼できないポートで受信されたすべてのパケットに、デバイスが再度マーキングする CoS 値です。

[Power Available TLV]	• [要求 ID]：最新の電力要求 ID が、電力要求 TLV で最後に受信した [要求 ID] フィール ドに反映されます。インターフェイスが最後にアップした時点以降に電力要求 TLV を受信しなかった場合は、0 になります。 • [Power Management ID]：次のイベントのいずれかが発生するたびに、値が 1（または、0 を避けるため 2）増加します。 [Available Power] または [Management Power Level] が変化した。 最後に受信した設定値と異なる要求 ID を持つ電力要求 TLV を受信した。 インターフェイスがダウンした。 • [Available Power]：ポートが消費する電力量。 • [Management Power Level]：電力消費量 TLV についての、POD デバイスに対するサプライヤの要求が表示されます。デバイスはこのフィールドに常に [No Preference] と表示します。
[MDI（UPOE）経由の 4 線式電源 TLV（4-Wire Power via MDI (UPOE) TLV）]	この TLV がサポートされているかどうかが表示されます。 • [4-Pair PoE Supported]：PoE がサポートされているかどうかが表示されます。 • [予備ペア検出/分類必要]：この分類が必要かどうかが表示されます。 • [PD Spare Pair Desired State]：PD 予備ペアが必要な状態が表示されます。 • [PD Spare Pair Operational State]：PSE 予備ペアの状態が表示されます。

CDP ネイバー情報

[CDP Neighbors Information] ページには、ネイバー デバイスから受信した CDP 情報が表示されます。

タイムアウトになると、情報は削除されます。タイムアウトは、CDP PDU が 1 件も受信されなかった場合、存続可能時間 TLV から取得した値に基づきます。

CDP ネイバー情報を表示するには、次のようにします。

ステップ 1 [Administration] > [Discovery - CDP] > [CDP Neighbor Information] をクリックします。

ステップ 2 フィルタを選択するには、[Filter] チェックボックスをオンにし、ローカルインターフェイスを選択して、[Go] をクリックします。

リスト上でフィルタが適用されます。[フィルタのクリア] がアクティブになって、フィルタの停止が有効になります。

[CDP Neighbor Information] ページには、リンク パートナー（ネイバー）に関する次のフィールドが表示されます。

Device ID	ネイバーデバイス ID。
システム名	ネイバーシステム名。
Local Interface	ネイバーが接続されているローカルポートの番号。
アドバタイズメントバージョン	CDP プロトコルのバージョン。
Time to Live	このネイバーの情報が削除されるまでの時間間隔（単位：秒）。
Capabilities	ネイバーによってアドバタイズされる機能。
プラットフォーム	ネイバーのプラットフォーム TLV からの情報。
ネイバーインターフェイス	ネイバーの発信インターフェイス。

ステップ 3 デバイスを選択し、[Details] をクリックします。

このページには、ネイバーに関する次のフィールドが含まれています（実際のフィールドの表示は、ネイバーによるアドバタイズの内容によって異なります）。

Device ID	ネイバーデバイス ID。
システム名	ネイバーシステム名。
Local Interface	ネイバーが接続されているローカルポートの番号。
アドバタイズメントバージョン	CDP プロトコルのバージョン。
存続可能時間(秒)	このネイバーの情報が削除されるまでの時間間隔（単位：秒）。
Capabilities	ネイバーによってアドバタイズされる機能。
プラットフォーム	ネイバーのプラットフォーム TLV からの情報。
ネイバーインターフェイス	ネイバーの発信インターフェイス。
ネイティブ VLAN	ネイバーのネイティブ VLAN。
デュプレックス	ネイバーインターフェイスが半二重か全二重か。
Addresses	ネイバーアドレス。
Power Drawn	インターフェイスでネイバーによって消費される電力量。

バージョン	ネイバーのソフトウェアのバージョン。
[Power Request]	ポートに接続された PD によって要求される電力。 • [電力要求リスト]：各 PD は、サポートされる電力レベル（最大 3 つ）からなるリストを送信できます。
[Power Available]	ポートに PSE が接続されている場合に表示されます。

（注） [Clear Table] ボタンをクリックすると、CDP からの場合は、接続されていたデバイスがすべて切断され、Auto Smartport が有効な場合は、すべてのポートタイプがデフォルトに変更されます。

CDP統計情報

[CDP Statistics] ページには、ポートとの間で送受信された CDP フレームに関する情報が表示されます。CDP パケットは、スイッチ インターフェイスに接続されたデバイスから受信され、Smartport 機能用に使用されます。

CDP 統計情報を表示するには、次の手順を実行します。

ステップ 1 [Administration] > [Discovery - CDP] > [CDP Statistics] をクリックします。

各インターフェイスについて、次のフィールドが表示されます。

[受信パケット/送信パケット]

- [Version 1]：受信または送信した CDP バージョン 1 のパケットの数。
- [Version 2]：受信または送信した CDP バージョン 2 のパケットの数。
- [合計]：受信または送信した CDP パケットの合計数。

[CDPエラー統計情報]

- [無効なチェックサム]：無効なチェックサム値とともに受信したパケットの数。
- [その他のエラー]：無効なチェックサム以外のエラーとともに受信したパケットの数。
- [Neighbors Over Maximum]：空き容量がないためパケット情報をキャッシュに格納できなかった回数。

ステップ 2 すべてのインターフェイスのカウンタを完全にクリアするには、[Clear All Interface Counters] をクリックします。インターフェイス上のすべてのカウンタをクリアするには、選択して [Clear Interface Counters] をクリックします。

デバイスの特定

この機能は、ネットワーク内の特定のデバイスのすべてのネットワーク ポート LED を点滅させて、デバイスの物理的な場所を特定できます。この機能は、相互接続された多数のデバイスがある部屋で1つのデバイスを特定する場合に役立ちます。この機能をアクティブにすると、該当するデバイス上のすべてのネットワーク ポート LED が、設定された期間（デフォルトでは 1 分）点滅します。

ステップ 1 **[Administration]** > **[Locate Device]** の順にクリックします。

ステップ 2 次のフィールドに値を入力します。

- [Duration]：ポートの LED を点滅させる時間（秒単位）を入力します。
- 残り時間（Remaining Time）：このフィールドは、この機能が現在アクティブな場合にのみ表示されます。ここには、LED が点滅する残り時間が表示されます。
- ユニット ID（Unit ID）：このフィールドは、デバイスがスタック構成のときにのみ表示されます。ネットワークポート LED を点滅させるユニットを指定するか、すべてのユニットを対象とする場合は [All] を選択します。

ステップ 3 [Start] をクリックして、機能を開始します。

機能が開始されると [Start] ボタンが [Stop] ボタンに置き換わります。このボタンを使用して、定義されたタイマーが終了する前に LED の点滅を停止できます。

ping

Pingユーティリティは、リモートホストに到達できるかどうかをテストし、送信したパケットが往復に要した時間を計測します。

ping は、ICMP（Internet Control Message Protocol）のエコー要求パケットをターゲット ホストに送信して ICMP 応答を待つことによって動作します。ラウンド トリップ時間を計測し、パケット損失がある場合はそれを記録します。

ホストに Ping を実行するには、次の手順を実行します。

ステップ 1 [Administration] > [Ping] の順にクリックします。

ステップ 2 次のフィールドに入力して、ping を設定します。

オプション	説明
ホスト指定方法	送信元インターフェイスをIPアドレスで指定するか、名前で指定するかを選択します。このフィールドは、以下に説明するように [Source IP] フィールドに表示されるインターフェイスに影響します。
IP バージョン	送信元インターフェイスを IP アドレスで識別する場合は、IPv4 または IPv6 を選択し、選択した形式で入力することを示します。
Source IP	宛先との通信用送信元IPv4アドレスとして送信元インターフェイスを選択します。[Host Definition] フィールドに [By Name] を指定した場合、すべてのIPv4 およびIPv6 アドレスが表示されます。[Host Definition] フィールドに [IP Address] を指定した場合、[IP Version] フィールドで指定したタイプの既存のIP アドレスのみが表示されます。 （注） [Auto] オプションを選択すると、システムは宛先アドレスに基づいて送信元アドレスを計算します。
送信先IPv6アドレスタイプ	次のオプションのいずれかを選択します。 • [リンクローカル] : IPv6アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [グローバル] : IPv6アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	IPv6 アドレスタイプが [Link Local] である場合は、どこから IPv6 アドレスを受け取るかを選択します。
宛先IPアドレス/名前	Ping対象デバイスのアドレスまたはホスト名。これがIPアドレスとホスト名のどちらであるかは、ホスト定義によって異なります。
Ping Interval （注） この設定は、[Advanced Mode] ビューでのみ使用できます。	システムがPingパケット間で待機する時間。Pingは、成功したかどうかにかかわらず、[Number of Pings] フィールドで設定した回数繰り返されます。デフォルトの間隔を使用するか、独自の値を指定するかを選択します。
Ping回数	Ping 操作を実行する回数。デフォルトを使用するか、独自の値を指定するかを選択します。

オプション	説明
（注） この設定は、[Advanced Mode] ビューでのみ使用できます。	
Status	Ping が正常に実行されたかどうかが表示されます。

ステップ 3 [Activate Ping] をクリックして、ホストに ping を実行します。ping のステータスが表示され、メッセージのリストにメッセージが追加されて ping 操作の結果が示されます。

ステップ 4 このページの [Ping Counters and Status] セクションに ping の結果が表示されます。

- 送信されたパケットの数（Number of Sent Packets）：ping で送信されたパケットの数
- 受信したパケットの数（Number of Received Packets）：ping で受信されたパケットの数
- [Packet Loss]：Ping プロセス中に損失したパケットの割合
- 最小ラウンド トリップ時間（Minimum Round Trip Time）：パケットが戻った最短の時間
- 最大ラウンド トリップ時間（Maximum Round Trip Time）：パケットが戻った最長の時間
- 平均ラウンド トリップ時間（Average Round Trip Time）：パケットが戻った時間の平均
- [Status]：失敗か成功か

traceroute

トレースルートは、IPパケットをターゲットホストに送信し、デバイスに戻すことにより、転送される IP ルートを検出します。traceroute ページには、デバイスとターゲット ホスト間の各ホップが表示され、このような各ホップへのラウンド トリップ時間が表示されます。

ステップ 1 [Administration] > [Traceroute] の順にクリックします。

ステップ 2 次のフィールドに情報を入力して、トレースルートを設定します。

- ホスト定義（Host Definition）：ホストがその IP アドレスまたは名前で識別されるどうかを選択します。
- IP バージョン（IP Version）：ホストがその IP アドレスで識別される場合、IPv4 または IPv6 のどちらかを選択して、IP アドレスを選択した形式で入力することを示します。
- 送信元 IP（Source IP）：送信元インターフェイスを選択します。このインターフェイスの IPv4 アドレスが、通信メッセージの送信元 Ipv4 アドレスとして使用されます。[Host Definition] フィールドに [By Name] を指定した場合、ドロップダウンフィールドにはすべての IPv4 および IPv6 アドレスが表示さ

れます。[Host Definition] フィールドが [By IP Address] の場合は、[IP Version] フィールドで指定したタイプの既存の IP アドレスのみが表示されます。

- [Host IP Address/Name]：ホストのアドレスまたは名前を入力します。
- TTL（TTL）：traceroute で許容されるホップの最大数を入力します。これは、送信されたフレームが無限ループに陥る状態を防ぐために使用されます。traceroute コマンドは、宛先に到達した場合、またはこの値に到達した場合に終了します。デフォルト値（30）を使用するには、[Use Default] を選択します。

  （注） この設定は、[Advanced Mode] ビューでのみ使用できます。

- [Timeout]：システムがフレームの損失を宣言する前に、フレームが戻るのを待機する時間を入力するか、[Use Default] を選択します。

  （注） この設定は、[Advanced Mode] ビューでのみ使用できます。

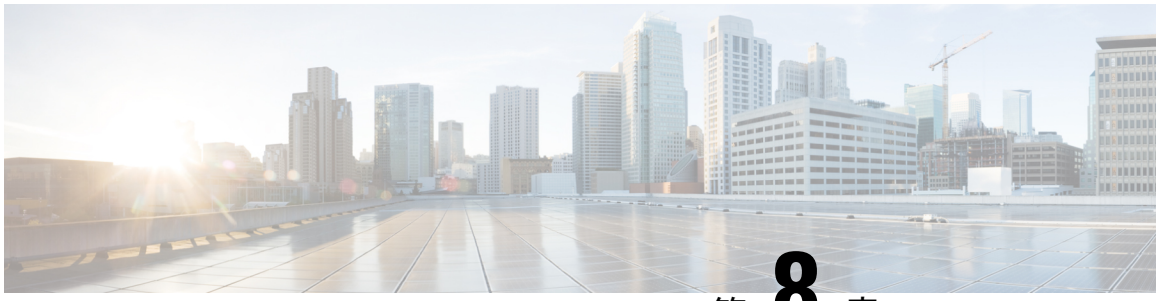
ステップ 3 [Activate Traceroute] をクリックします。操作が実行されます。

（注） トレースルートを停止するかどうかを示すポップアップが表示されます。[Stop Traceroute] をクリックして、プロセスを停止します。

ページが表示され、ラウンドトリップ時間（RTT）、および各トリップのステータスが次のフィールドに表示されます。

- インデックス（Index）：ホップ数が表示されます。
- ホスト（Host）：宛先までのルートに沿ったストップが表示されます。

  [Round Trip Time (1-3)]：ラウンドトリップ時間（ミリ秒）とステータスが表示されます。



第 8 章

ポート管理

この章は、次の項で構成されています。

ポート設定

[Port Settings] ページには、グローバルおよびポートごとにすべてのポートの設定が表示されます。このページでポートを選択し、[Edit Port Settings] ページでそのポートを設定できます。

ポート設定を設定するには、次の手順を実行します。

ステップ 1 [Port Management] > [Port Settings] をクリックします。

すべてのポートのポート設定が表示されます。

ステップ 2 次のフィールドに入力します。

- [Link Flap Prevention]：選択すると、ネットワークの中断を最小限に抑えます。このコマンドを有効にすると、自動的にリンクフラップ イベントが発生したポートを無効化します。
- [Jumbo Frames]：サイズが 9 KB までのパケットをサポートする場合にオンにします。[Jumbo Frames] が有効になっていない場合（デフォルト）、サポートされる最大パケットサイズは2,000バイトです。9 KB を超えるパケットを受信すると、受信ポートがシャットダウンする可能性があることに注意してください。また、10 KB を超えるパケットを送信すると、受信側のポートのシャットダウンが発生する可能性があります。

  ジャンボ フレームを有効にするには、この機能を有効化した後、デバイスをリブートする必要があります。

ステップ 3 [Apply] をクリックして、グローバル設定を更新します。

ジャンボフレーム設定の変更内容は、ファイル操作（87ページ）で実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに明示的に保存し、デバイスを再起動して初めて反映されます。

ステップ 4 ポート設定を更新するには、目的のポートを選択して、[Edit] をクリックします。

ステップ 5 次のパラメータを変更します。

Interface	ポート番号を選択します。
Port Description	ポートのユーザー定義名またはコメントを入力します。 （注） [インターフェイス] と [ポートの説明] は、メイン ページの [ポート] 列に表示されます。
ポート タイプ	ポートタイプと速度が表示されます。オプションは次のいずれかです。 • [Copper Ports]：コンボではなく、通常のポートは、10M、100M、1000M（タイプ：銅）、10G、2.5G、5G、10G の各値をサポートします。 • [Combo Ports]：銅 CAT6a ケーブルまたは SFP ファイバ ギガビット インターフェイスのいずれかで接続されたコンボポート。 • [10G-Fiber Optics]：伝送速度が 1G または 10G のポート。
Administrative Status	デバイスの再起動時にポートを [Up] 状態にするか、[Down] 状態にするかを選択します。
運用ステータス	ポートが現在 [Up] 状態なのか、[Down] 状態なのかが表示されます。ポートがエラーが原因でダウンしている場合、そのエラーの説明が表示されます。
リンクステータスSNMP トラップ	ポートのリンクステータスへの変更を通知する SNMP トラップの生成を有効にする場合に選択します。
時間範囲	ポートを [UP] 状態にする時間範囲を有効にする場合に選択します。時間範囲がアクティブでない場合、ポートはシャットダウン中です。時間範囲が設定されている場合、時間範囲は、ポートが管理上 [Up] の状態である場合にのみ有効です。
時間範囲名	時間範囲を指定するプロファイルを選択します。OOB ポートには関係ありません。時間範囲がまだ定義されていない場合は、[Edit] をクリックします。
動作時間範囲の状態	[Range State]：時間範囲が現在アクティブか非アクティブかが表示されます。
自動ネゴシエーション（Auto Negotiation）	ポートで自動ネゴシエーションを有効にする場合に選択します。自動ネゴシエーションにより、ポート リンク パートナーに対する伝送速度、デュプレックス モード、およびフロー制御機能をアドバタイズするポートが有効になります。

動作自動ネゴシエーション	ポートの現在の自動ネゴシエーションステータスが表示されます。
管理ポート速度	ポートの速度を選択します。ポートのタイプによって使用可能な速度が決まります。ポートの自動ネゴシエーションが無効な場合にのみ、管理速度を指定できます。
動作ポート速度	ネゴシエーションの結果である現在のポート速度が表示されます。
管理デュプレックスモード	ポートのデュプレックスモードを選択します。このフィールドは、自動ネゴシエーションが無効で、ポートの速度が 10 M または 100 M に設定されている場合にのみ設定可能です。ポート速度が 1G の場合、モードは常に全二重です。オプションは次のいずれかです。 • [Half]：インターフェイスは、デバイスとクライアントの間で一度に一方向のみの伝送をサポートします。 • [Full]：インターフェイスは、デバイスとクライアントの間で同時に両方向の伝送をサポートします。
動作デュプレックス モード	ポートの現在のデュプレックスモードが表示されます。
自動アドバタイズメント	自動ネゴシエーションが有効な場合に、アドバタイズされる機能を選択します。 （注） すべてのオプションがすべてのデバイスに関係するわけではありません。 次のオプションがあります。 • [最大機能]：すべてのポート速度と両方のデュプレックス モード。 • [10 Half]：10 Mbps の速度で半二重モード（XG デバイスでは表示されません）。 • [10 Full]：10 Mbps の速度で全二重モード（XG デバイスでは表示されません）。 • [100 Half]：100 Mbps の速度で半二重モード（XG デバイスでは表示されません）。 • [100 Full]：100 Mbps の速度で全二重モード。 • [1000 Full]：1000 Mbps の速度で全二重モード。
動作アドバタイズメント	ポートのネイバーに現在にパブリッシュされている機能が表示されます。[Administrative Advertisement] フィールドで指定されたオプションを使用できます。

プリファレンスモード	自動ネゴシエーションが有効になっている場合のみ使用できます。自動ネゴシエーション操作のための、インターフェイスのアクティブメンバーモードを選択します。次のオプションのいずれかを選択します。 • [Slave]：デバイスポートが自動ネゴシエーションプロセスにおいてメンバーである設定を使用して、ネゴシエーションを開始します。 • [Master]：デバイスポートが自動ネゴシエーションプロセスにおいてアクティブである設定を使用して、ネゴシエーションを開始します。
ネイバーアドバタイズメント	ネイバーデバイスによってアドバタイズされた機能が表示されます。
バックプレッシャ	ポートの [Back Pressure] モード（半二重モードで使用）を選択して、デバイスが輻輳したときのパケット受信速度を遅くします。このオプションを選択すると、信号の妨害によりリモート ポートからのパケットの送信が阻止され、リモート ポートが無効になります。
Flow Control	802.3x フロー制御を有効化または無効化するか、ポートでフロー制御の自動ネゴシエーションを有効にします（全二重モードの場合のみ）。フロー制御の自動ネゴシエーションは、コンボポートでは有効にできません。
[MDI/MDIX]：ポートのMDIX-Media Dependent Interface（MDI）/Media Dependent Interface with Crossover（MDIX）ステータス。	次のオプションがあります。 • [MDIX]：ポートの送受信ペアのスワップを選択します。 • [MDI]：このデバイスをストレート ケーブルを使用してステーションに接続することを選択します。 • [Auto]：他のデバイスとの接続において正しいピン割り当てが自動検出されるようにこのデバイスを設定する場合に選択します。
動作MDI/MDIX	現在の MDI/MDIX 設定が表示されます。

保護ポート	保護ポートにする場合に選択します（保護ポートはプライベート VLAN エッジ（PVE）とも呼ばれます）。保護ポートの機能は次のとおりです。 • 保護ポートは、同じ VLAN を共有するインターフェイス（イーサネットポートと LAG）間のレイヤ 2 分離を提供します。 • 保護ポートから受信されたパケットは、保護されていない出力ポートのみに転送できます。保護ポートのフィルタリング ルールは、スヌーピング アプリケーションなどのソフトウェアによって転送されるパケットにも適用されます。 • ポート保護が VLAN メンバーシップの影響を受けることはありません。保護ポートに接続されているデバイスは、同じ VLAN のメンバーである場合でも、相互に通信することを許可されていません。 • ポートと LAG のいずれも、保護対象または非保護対象として定義できます。保護 LAG については、LAG設定 （142 ページ）を参照してください。
LAGのメンバ	ポートが LAG のメンバーである場合、LAG 番号が表示されます。それ以外の場合、このフィールドは空白のままです。

ステップ 6 [Apply] をクリックします。ポート設定は、実行コンフィギュレーション ファイルに書き込まれます。

エラー回復設定

[Error Recovery Settings] ページを使用すると、自動回復間隔が経過した後に発生したデバイス エラーのためにシャットダウンされたポートを、自動的に再アクティブ化できます。

エラー回復設定を指定するには、次の手順を実行します。

ステップ 1 [Port Management] > [Error Recovery Settings] をクリックします。

ステップ 2 次のフィールドに入力します。

- [Automatic Recovery Interval]：有効にされている場合、ポートがシャットダウンしてから自動エラー回復までの遅延時間を指定します。
- 自動 ErrDisable リカバリ
  - [Port Security]：ポートセキュリティ違反のためにポートがシャットダウンした際に自動エラー回復が有効になるようにするには、このフィールドを選択します。
  - [802.1x Single Host Violation]：802.1x によってポートがシャットダウンした際に自動エラー回復が有効になるようにするには、このフィールドを選択します。
  - [ACL Deny]：選択すると、ACL アクションによる自動エラー リカバリ メカニズムが有効になります。

- [STP BPDU Guard]：STP BPDU ガードによってポートがシャットダウンした際に自動エラー回復機能が有効になるようにするには、このフィールドを選択します。
- [STP Loopback Guard]：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際に自動回復を有効にします。
- [UDLD]：選択すると、UDLD シャットダウン状態に対する自動エラー リカバリ メカニズムが有効になります。
- [Loopback Detection]：選択すると、ループバック検出によつてポートがシャットダウンされた場合のエラー リカバリ メカニズムが有効になります。
- [Storm Control]：選択すると、ストーム制御によってポートがシャットダウンされた場合のエラーリカバリ メカニズムが有効になります。
- [Link Flap Prevention]：選択すると、ネットワークの中断を最小限に抑えます。このコマンドを有効にすると、自動的にリンクフラップ イベントが発生したポートを無効化します。

ステップ 3 [Apply] をクリックして、グローバル設定を更新します。

ポートを手動で再アクティブ化するには、次の手順に従います。

ステップ 4 [Port Management] > [Error Recovery Settings] をクリックします。

無効化されたインターフェイスと中断理由のリストが表示されます。

ステップ 5 [Suspension Reason] をフィルタリングするには、理由を選択して [Go] をクリックします。これにより、選択した理由で中断されたインターフェイスのみがテーブルに表示されます。

ステップ 6 再アクティブ化するインターフェイスを選択します。

ステップ 7 [Reactivate] をクリックします。

ループバック検出設定

ループバック検出は、ループ保護が有効になっているポートからループ プロトコル パケットを送信することにより、ループに対する保護を可能にします。スイッチがループ プロトコル パケットを送信した後、同じパケットを受信した場合、そのパケットを受信したポートをシャットダウンします。

ループバック検出は、STP とは無関係に動作します。ループが検出されると、ループを受信したポートがシャットダウン状態になります。トラップが送信され、イベントがログに記録されます。ネットワーク マネージャは、LBD パケット間の時間間隔を設定する検出間隔を定義できます。

LBD を有効にして設定するには、次の手順を実行します。

ステップ 1 [Port Management] > [Loopback Detection Settings] をクリックします。

ステップ 2 機能を有効にするには、ループバック検出で [Enable] を選択します。

ステップ 3 [Detection Interval] を入力します。これは LBD パケットの伝送間隔です。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

インターフェイスごとに、[Loopback Detection State] に関する次のフィールドが表示されます。

- [Administrative]：ループバック検出が有効になっています。
- [Operational]：ループバック検出が有効になっていますが、インターフェイスでアクティブになっていません。

ステップ 5 フィルタの [Interface Type equals to] フィールドで、ポートまたは LAG で LBD を有効にするかどうかを選択します。

ステップ 6 LBD を有効にするポートまたは LAG を選択して、[Edit] をクリックします。

ステップ 7 選択したインターフェイスの設定を選択します。次に、選択したポートまたは LAG の [Loopback Detection Stat] フィールドで [Enable] を選択します。

ステップ 8 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

リンク集約

リンク集約は、単一の接続で維持可能な範囲を超えてスループットを向上させるために、複数のネットワーク接続を並行して結合するさまざまな方法に適用されます。また、いずれかのリンクで障害が発生した場合に冗長性を提供します。

Link Aggregation Control Protocol（LACP）は IEEE 仕様（802.3ad）の一部であり、複数のポートをバンドルして 1 つの論理チャネル（LAG）を形成できます。LAG を形成すると、2 つのデバイス間での帯域幅を増やし、ポートの柔軟性を高め、リンクの冗長性を提供できます。

次の 2 種類の LAG がサポートされています。

- [Static]：LAG 内のポートは手動で設定されます。LACP が LAG で無効になっている場合、LAG は静的になります。静的 LAG に割り当てられたポートのグループは、常にアクティブなメンバーです。LAG を手動で作成した場合、その LAG を編集してメンバーを削除するまで、LACP オプションの追加や削除はできません（メンバーは適用前に再追加できます）。その後、[LACP] ボタンが編集に使用できるようになります。
- [ダイナミック] : LACP が有効になっている場合、LAG は動的に作成されます。動的 LAG に割り当てられたポートのグループは、メンバー候補のポートです。LACP は、どのメンバー候補のポートがアクティブなメンバーポートであるかを決定します。非アクティブ候補ポートはスタンバイポートになり、アクティブメンバーポートに障害が発生した場合に、アクティブになります。

この項では、LAG の設定方法について説明します。

LAG管理

Link Aggregation Control Protocol（LACP）は IEEE 仕様（802.3ad）の一部であり、複数のポートをバンドルして 1 つの論理チャネル（LAG）を形成できます。LAG を形成すると、2 つのデバイス間での帯域幅を増やし、ポートの柔軟性を高め、リンクの冗長性を提供できます。

LAG のロードバランシング アルゴリズムを選択するには、次の手順を実行します。

ステップ 1 [Port Management] > [Link Aggregation] > [LAG Management] をクリックします。

ステップ 2 次のロード バランス アルゴリズムのいずれかを選択します。

- [MAC アドレス] : すべてのパケットの送信元 MAC アドレスと宛先 MAC アドレスに 基づいて、負荷分散を実行します。
- [IP/MAC Address]：IP パケットの IP アドレス、非 IP パケットの MAC アドレスに基づいて、ロードバランシングを実行します。

ステップ 3 [Apply] をクリックします。ロード バランシング アルゴリズムは、実行コンフィギュレーション ファイルに保存されます。

LAG のメンバーまたはメンバー候補のポートを定義するには、次の手順に従います。

ステップ 4 設定する LAG を選択して、[Edit] をクリックします。

ステップ 5 次のフィールドに値を入力します。

- [LAG]：LAG 番号を選択します。
- [LAG 名] : LAG 名またはコメントを入力します。
- [LACP]：選択した LAG で LACP を有効にする場合に選択します。その結果、LAG は動的 LAG になります。このフィールドは、次のフィールドでポートを LAG に移動した後にのみ有効にすることができます。
- [ユニット]：LAG 情報が定義されているスタック メンバーを表示します。
- [Port List]：[Port List LAGs] に割り当てられているポートを、[LAG Members] に移動します。1 つのスタティック LAG には最大 8 個、 1 つのダイナミック LAG には最大 16 個の候補ポートを追加できます。

ステップ 6 [Apply] をクリックします。LAG のメンバーシップは、実行コンフィギュレーション ファイルに保存されます。

LAG設定

[LAG Settings] ページには、全 LAG の現在の設定に関するテーブルが表示されます。[Edit LAG Settings] ページを起動して、選択した LAG を設定したり、停止中の LAG を再アクティブ化したりすることができます。

LAG を設定したり、停止中の LAG を再アクティブ化したりするには、次の手順を実行します。

ステップ 1 [Port Management] > [Link Aggregation] > [LAG Settings] をクリックします。

システム内の LAG が表示されます。

ステップ 2 LAG を選択して [Edit] をクリックします。

ステップ 3 次のフィールドに値を入力します。

オプション	説明
LAG	LAG ID 番号を選択します。
LAG タイプ	この LAG を構成しているポートのタイプが表示されます。
説明	LAG 名またはコメントを入力します。
Administrative Status	選択した LAG をアクティブ化する場合は [Up]、アクティブ化しない場合は [Down] を選択します。
リンクステータス SNMPトラップ	LAG に含まれるポートのリンクステータスの変化を通知する SNMP トラップの生成を有効にするには、このフィールドを選択します。
時間範囲	ポートを [UP] 状態にする時間範囲を有効にする場合に選択します。時間範囲がアクティブでない場合、ポートがシャットダウンします。時間範囲が設定されている場合、ポートが管理者によって [UP] 状態になっている場合のみ有効です。
時間範囲名	時間範囲を指定するプロファイルを選択します。時間範囲がまだ定義されていない場合は、[Edit] をクリックして時間範囲を設定します。
運用ステータス	LAG が現在アクティブ化されているかどうかが表示されます。
動作時間範囲の状態	時間範囲が現在アクティブか非アクティブかが表示されます。
管理自動ネゴシエーション	LAG での自動ネゴシエーションを有効または無効にします。自動ネゴシエーションは、2 つのリンク パートナー間のプロトコルで、LAG が伝送速度とフロー制御をパートナーにアドバタイズすることを可能にします（デフォルトではフロー制御は無効になっています）。自動ネゴシエーションを集約リンクの両側で有効に保つか、両側で無効に保つことをお勧めします（リンク速度が同一であることを確認します）。
管理速度	LAG 内のポートの速度を選択します。
管理アドバタイズメント	LAGによってアドバタイズされる機能を選択します。次のオプションがあります。 • [最大機能]：すべての LAG 速度と両方のデュプレックス モード。 • [10 全二重]：10 Mbps のスピードのアドバタイズで全二重モード。 • [100 Full]：LAG は 100 Mbps の速度をアドバタイズし、モードは全二重です。

オプション	説明
	• [1000 Full]：LAG は 1000 Mbps の速度をアドバタイズし、モードは全二重です。
管理フロー制御	[Flow Control] を [Enable] または [Disable] に設定するか、LAG で [Flow Control] の [Auto-Negotiation] を有効にします。
動作自動ネゴシエーション	自動ネゴシエーション設定が表示されます。
動作LAG速度	LAG の現在の速度が表示されます。
動作アドバタイズメント	管理アドバタイズメントのステータスが表示されます。LAG は、ネゴシエーションプロセスを開始するネイバーにLAGの機能をアドバタイズします。[Administrative Advertisement] フィールドで指定された値を使用できます。
動作フロー制御	現在のフロー制御の設定が表示されます。
保護LAG	LAG をレイヤ 2 分離の保護ポートにするには、このフィールドを選択します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

LACP

動的LAGではLACPが有効になっており、LACPは、LAGで定義されているすべての候補ポートで実行されます。LACP システムの優先順位と LACP ポートの優先順位はいずれも、8 つを超える候補ポートで設定される動的 LAG で、どの候補ポートがアクティブなメンバー ポートになるかを決定するために使用されます。

[LACP] ページを使用して、LAG の候補ポートを設定し、ポートごとに LACP パラメータを設定します。すべての要因が等しく、アクティブ ポートの許容最大数（8）よりも多くの候補ポートでLAGが設定されている場合、デバイスは、最高の優先順位を持つデバイスの動的LAGからアクティブなポートを選択します。

（注） LACP の設定は、動的 LAG のメンバーではないポートには無関係です。

LACP 設定を定義するには、次の手順を実行します。

ステップ 1 [Port Management] > [Link Aggregation] > [LACP] をクリックします。
ステップ 2 必要に応じて [LACP System Priority] を編集し、[Apply] をクリックします。
ステップ 3 既存のポートを編集するには、ポートを選択し、[編集] をクリックします。
ステップ 4 [LACP設定の編集] ダイアログ ボックスで、次のフィールドに値を入力します。

- [ポート] : タイムアウト値とプライオリティを設定するポートの番号を選択します。
- [LACP ポートプライオリティ] : このポートの LACP プライオリティを入力します。
- [LACP Timeout] : 連続的な LACP PDU の送信と受信の時間間隔。明示的な LACP タイムアウト設定に応じて [Long] または [Short] 伝送速度で実行される、LACP PDU の定期的な伝送を選択します。

ステップ 5 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

UDLD

UDLDは、単方向リンクを有効にするため、光ファイバまたはツイストペアイーサネットケーブルを介して接続されたデバイスを有効にするレイヤ2プロトコルです。隣接するデバイスが送信したトラフィックをローカル デバイスが受信するにもかかわらず、ローカル デバイスから送信されたトラフィックをネイバーが受信しない場合には、常に単一方向リンクが発生します。

UDLD の目的は、ネイバーがローカル デバイスからのトラフィックを受信しないポート（単方向リンク）を検出して、そのようなポートをシャットダウンすることです。

プロトコルが単方向リンクを正しく検出するには、接続されているすべてのデバイスでUDLDをサポートする必要があります。ローカル デバイスのみが UDLD をサポートしている場合、このデバイスがリンクのステータスを検出することはできません。この状況では、リンクのステータスは未定義に設定されます。ユーザーは、[未定]の状態のポートをシャットダウンするかどうかを設定できます。

UDLDグローバル設定

[Fiber Port UDLD Default State] は、光ファイバ ポートのみに適用されます。

[Message Time] フィールドは、銅線ポートと光ファイバ ポートの両方に適用されます。

UDLD をグローバルに設定するには、次の手順を実行します。

ステップ 1 **[Port Management]** > **[UDLD]** > [UDLD Global Settings] の順にクリックします。

ステップ 2 次のフィールドに入力します。

- [Message Time] : UDLD メッセージを送信する間隔を入力します。このフィールドは、光ファイバ ポートと銅線ポートの両方に関係します。
- [Fiber Port UDLD Default State] : このフィールドは、光ファイバ ポートのみに関係します。表示される可能性のある状態は、次のとおりです。
  - [Disabled] : デバイスのすべてのポートで UDLD が無効になっています。
  - [Normal] : リンクが単一方向の場合、デバイスはインターフェイスをシャットダウンします。リンクが未定義の場合、通知が発行されます。

- [Aggressive]：リンクが単一方向の場合、デバイスがインターフェイスをシャットダウンします。リンクが双方向の場合は、UDLD情報がタイムアウトした後、デバイスがシャットダウンします。ポートの状態は未定義としてマーキングされます。

ステップ3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

UDLDインターフェイス設定

特定のポートのUDLD状態を変更するには、[UDLD Interface Settings]ページを使用します。ここでは、銅線ポートまたは光ファイバポートでの状態を設定できます。特定の値のセットを1つ以上のポートにコピーするには、1つのポートの値を設定し、[Copy]ボタンを使用して他のポートにコピーします。

インターフェイスのUDLDを設定するには、次の手順を実行します。

ステップ1 [Port Management] > [UDLD] > [UDLD Interface Settings] の順にクリックします。

UDLDが有効になっているすべてのポートまたは選択したポートグループの情報が表示されます。

- [Port]：ポート識別子。
- [UDLDの状態]：次の状態のいずれかが表示されます。
  - [Default]：ポートは、[Fiber Port UDLD Default State] の値に設定されます。
  - [Disabled]：デバイスのすべてのポートでUDLDが無効になっています。
  - [Normal]：リンクが単一方向であることが検出されると、デバイスはインターフェイスをシャットダウンします。リンクが未定義の場合、通知が発行されます。
  - [Aggressive]：リンクが単一方向の場合、デバイスがインターフェイスをシャットダウンします。リンクが双方向の場合は、UDLD情報がタイムアウトした後、デバイスがシャットダウンします。ポートの状態は未定義としてマーキングされます。
- [Bidirectional State]：次の状態のいずれかが表示されます。
  - [Detection]：ポートの最新のUDLD状態を決定するプロセスが進行中です。最後の検出（もしあれば）から期限切れ時間が経過していないか、UDLDがポートで実行し始めたところで、その状態が未検出である状態。
  - 双方向（Bidirectional）：ローカル デバイスが送信したトラフィックはネイバーが受信し、ネイバーから送信されたトラフィックはローカル デバイスが受信します。
  - [Undetermined]：UDLDメッセージを受信していないか、UDLDメッセージにローカルデバイスIDが含まれていないために、ポートと接続ポートとの間のリンク状態が検出できていない状態。
  - [Disabled]（デフォルト）：このポートのUDLDは無効になっています。

- [Shutdown]：接続デバイスとのリンクがアグレッシブ モードで未定義であるため、ポートがシャットダウンされています。
- [Idle]：ポートはアイドル状態になっています。

- [Number of Neighbors]：検出された接続デバイスのネイバーの数。

ステップ 2 特定のポートにおける UDLD の状態を変更するには、これを選択して [Edit] をクリックします。

ステップ 3 UDLD の状態の値を変更します。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

UDLDネイバー

ローカルデバイスに接続されたすべてのデバイスを表示するには、**[Port Management]** > **[UDLD]** > [UDLD Neighbors] をクリックします。

UDLD が有効なすべてのポートに、次のフィールドが表示されます。

- [Interface Name]：UDLD が有効なローカル ポートの名前。
- ネイバー情報
  - [Device ID]：リモートデバイスの ID。
  - [Device MAC]：リモート デバイスの MAC アドレス。
  - [Device Name]：リモートデバイスの名前。
  - [Port ID]：リモートポートの名前。
- [State]：ローカル ポートにおけるローカルデバイスと隣接デバイス間のリンクの状態。以下の値を指定できます。
  - [Detection]：ポートの最新の UDLD 状態を決定するプロセスが進行中です。最後の決定（あれば）以降、またはUDLDがポートで実行を開始して以降、まだ有効期限は過ぎていないため、状態はまだ決定されていません。
  - 双方向（Bidirectional）：ローカル デバイスが送信したトラフィックはネイバーが受信し、ネイバーから送信されたトラフィックはローカル デバイスが受信します。
  - [Undetermined]：ポートとその接続されたポート間のリンクの状態を決定できません。これは、UDLD メッセージが受信されていないか、UDLD メッセージにローカル デバイス ID が含まれていないことが理由です。
  - [Disabled]：このポートの UDLD は無効になっています。
  - [Shutdown]：接続デバイスとのリンクがアグレッシブ モードで未定義であるため、ポートがシャットダウンされています。

- [Neighbor Expiration Time (Sec.)]：デバイスがポートの UDLD ステータスを判別しようとするまでに経過する時間が表示されます。これは [Message Time] の 3 倍の時間です。
- [Neighbor Message Time (Sec.)]：UDLD メッセージ間の時間が表示されます。

PoE

PoE デバイスは給電機器（PSE）で、ネットワーク トラフィックに干渉したり、物理ネットワークを更新したり、ネットワークインフラストラクチャを変更したりせずに、既存の銅線ケーブルを介して POD デバイス（PD）に電力を供給します。

PoE には次の機能があります。

- 有線 LAN 上のすべてのデバイスに 110/220 V AC 電力を供給する必要がなくなります。
- 企業内に二重ケーブル システムを導入する必要がなくなり、設置コストが大幅に低下します。Power over Ethernet は、イーサネット LAN に接続する比較的低出力のデバイスを導入するエンタープライズ ネットワークで使用できます。これらのデバイスは、IP フォン、ワイヤレスアクセスポイント、IP ゲートウェイ、音声およびビデオ リモート モニターリング デバイスなどです。

PoE は次の各段階で実装されます。

- 検出：カッパー ケーブルに特殊パルスを送信します。PoEデバイスがもう一方の端にある場合、そのデバイスは前述のパルスに応答します。
- 分類：給電機器（PSE）と POD デバイス（PD）の間のネゴシエーションは、検出段階の後に始まります。ネゴシエーションの間に、PDは、PDの最大消費電力量を示すクラスを指定します。
- 電力消費：分類段階が完了すると、PSE は PD に電力を供給します。PD が PoE をサポートしているものの、分類を実行していない場合、この PD はクラス 0（最大値）と見なされます。PDが標準規格によって許容される範囲を超えて電力を消費しようとすると、PSEは、ポートへの電力供給を停止します。PoE は次の 2 つのモードをサポートします。
  - [Port Limit]：デバイスが供給に同意する最大電力は、分類の結果に関係なく、システム管理者の設定値に制限されます。
  - [Class Power Limit]デバイスが供給に同意する最大電力は、分類段階の結果によって決定されます。これは、クライアントからの要求に従って設定されることを意味します。

警告 PoEユニットは、外部プラントにルーティングすることなくPoEネットワークにのみ接続されます。

プロパティ

（注） この項は、PoE をサポートするデバイスのみに関係します。

[PoE Properties] ページでは、[Port Limit] または [Class Limit] PoE モードのいずれかを選択したり、生成される PoE トラップを指定したりすることができますこれらの設定は事前に入力されます。PD が実際に接続されて電力が消費されるときに、許容される最大電力よりもかなり小さい電力が消費される場合があります。電源投入時のリブート、初期化、およびシステム設定中、出力電力は停止し、PD の損傷が回避されます。

デバイスで PoE を設定したり、現在の電力使用をモニタしたりするには、次の手順に従います。

ステップ 1 [Port Management] > [PoE] > [Properties] の順にクリックします。

ステップ 2 次のフィールドに値を入力します。

- [電力モード]：次のいずれかのオプションを選択します。
  - [Class Limit]：ポートごとの最大電力制限は、分類段階で決まるデバイスのクラスによって決定されます。
  - [Port Limit]：ポートごとの最大電力制限は、ユーザによって設定されます。

    （注） [Port Limit] から [Class Limit] に変更する場合、またはその逆の場合、PoE ポートを無効にし、電源設定を変更した後でポートを有効にします。

- [トラップ]：トラップを有効または無効にします。トラップが有効な場合、SNMP を有効にし、少なくとも 1 つの SNMP 通知の受信者を設定する必要があります。
- [電力トラップしきい値]：消費量しきい値を電力制限割合で入力します。電力がこの値を超えると、アラームが生成されます。

  デバイスについて、次のカウンタが表示されます。
  - [Nominal Power]：接続されているすべての PD にデバイスが供給できる電力量の合計。
  - [消費電力]：PoE ポートが現在消費している電力量。
  - [Available Power]：公称電力から消費電力量を引いた値。
- [Software Version]：PoE チップのソフトウェア バージョンが表示されます。
- [PSEチップセット&ハードウェアリビジョン（PSE Chipset & Hardware Revision]：PoE チップセット番号とハードウェア リビジョン番号。

ステップ 3 [Apply] をクリックして、PoE プロパティを保存します。

PoE の設定

[PoE Settings] には、インターフェイスで PoE を有効にするためのシステム情報が表示されます。PoEモードがポート制限の場合は、ポートごとの電力使用量と最大電力制限が監視されます。ポートでの消費電力がポート制限を超えると、ポートの電力がオフになります。

PoE 設定を指定するには、次の手順を実行します。

ステップ 1 [Port Management] > [PoE] > [PoE Settings] の順にクリックします。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [インターフェイス]：設定するポートを選択します。
- [Administrative Status]：ポートで PoE を有効または無効にします。
- [Time Range]：ポートでの PoE を有効にする場合に選択します。
- [Time Range Name]：[Time Range] が有効な場合、使用する時間範囲を選択します。[Time Range] ページに移動するには、[Edit] をクリックします。
- [Priority Level]：低、高、または重要から、ポートの優先順位を選択します。電力供給が少ない場合に使用します。たとえば、電源が 99% の使用率で実行され、ポート 1 の優先順位付けが高、ポート 3 の優先順位付けが低に設定されている場合、ポート 1 は電力を供給され、ポート 3 は供給を拒否されます。
- [Administrative Power Allocation]：範囲はポートタイプによって異なります。60W PoE をサポートするポートの最大値は 60000 です。それ以外の場合、最大値は 30000 です。値を入力します。（範囲：0 ～ 60000、デフォルト：30000）。
- [4 ペアの強制]：強化された電力を供給するには、この機能を有効にします。
- [Class]：デバイスの最大電力レベルを示す、デバイスのクラスが表示されます。
- [Max Power Allocation]：このフィールドは、[PoE Properties] ページで設定されている電力モードが [Power Limit] である場合にのみ表示されます。このポートで許可されている最大電力量を表示します。
- ネゴシエート済み電力（Negotiated Power）：デバイスに割り当てられた電力。

  （注） CDP または LLDP ネゴシエーションを介してデバイスに電力が割り当てられると、ワット値と一緒に「期限切れ」の警告が表示される場合があります。スイッチが受電デバイスからのネゴシエーションパケットの受信を停止すると、ポートは期限切れ状態になります。この場合、ポートは、このデバイスから受信した最新のネゴシエーションパケットに基づいて電力を供給します。デバイスがネゴシエーションパケットを再送信すると、ポートの期限切れ状態が終了し、新しいパケットの情報に基づいて電力を適用します。

- 電力ネゴシエーション プロトコル（Power Negotiation Protocol）：ネゴシエートされる電力を決定するプロトコル。

- [Power Consumption]：[Settings]（クラス制限）で割り当てられたミリワット単位の電力量を表示します。

ステップ 4 [Apply] をクリックします。ポートの PoE 設定は、実行コンフィギュレーション ファイルに書き込まれます。

PoE 設定 - クラス制限

[PoE Settings (Class Limit)] ページには、システムの PoE 情報が表示され、インターフェイス上で PoE を有効にしたり、現在の電力消費量や最大電力制限をポートごとに監視したりできます。

（注） PoE は、特定の期間、デバイスで設定できます。この機能を使用すると、ポートごとに、PoE が有効になっている曜日と時間を定義できます。時間範囲がアクティブではないと、PoE は無効になります。

このページでは、接続された PD のクラスに基づいてポートあたりの電力を制限します。これらの設定をアクティブにするには、システムが [PoE Class Limit] モードである必要があります。このモードは、PoE のプロパティ（149 ページ）で設定します。ポートでの消費電力がクラス制限を超えると、ポートの電力がオフになります。

PoE のクラス制限を設定するには、次の手順を実行します。

ステップ 1 [Port Management] > [PoE] > [Settings]（クラス制限）をクリックします。

ポートには、PoE の関連情報が表示されます。これらのフィールドは、次のフィールドを除いて [Edit] ページで説明されています。

- [PoE Standard]：60W PoE や 802.3 AT PoE など、サポートされる PoE のタイプが表示されます。
- [Operational Status]：PoE が現在ポート上でアクティブかどうかが表示されます。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [インターフェイス]：設定するポートを選択します。
- [Administrative Status]：有効にするにはチェックボックスをオンにします。
- [Time Range]：ポートで有効になっている PoE を選択します。
- [Time Range Name]：[Time Range] が有効な場合、使用する時間範囲を選択します。[Time Range] ページに移動するには、[Edit] をクリックします。
- [Priority Level]：低、高、または重要から、ポートの優先順位を選択します。電力供給が少ない場合に使用します。たとえば、電源が 99% の使用率で実行され、ポート 1 の優先順位付けが高、ポート 3 の

優先順位付けが低に設定されている場合、ポート 1 は電力を供給され、ポート 3 は供給を拒否されます。

- [Class] : デバイスの最大電力レベルを示す、デバイスのクラスが表示されます。

クラス	デバイス ポートで供給される最大電力
0	15.4 ワットまたは 30.0 ワット
1	4.0 ワット
2	7.0 ワット
3	15.4 ワット
4	30.0 ワット

- [Max Power Allocation]：このフィールドは、[PoE Properties] ページで設定されている電力モードが [Power Limit] である場合にのみ表示されます。このポートで許可されている最大電力量を表示します。
- ネゴシエート済み電力（Negotiated Power）：デバイスに割り当てられた電力。
- [Power Negotiation Protocol]：ネゴシエートされる電力を決定するプロトコル。
- [Power Consumption]：[Settings]（クラス制限）で割り当てられたミリワット単位の電力量を表示します。

ステップ 4 [Apply] をクリックします。ポートの PoE 設定は、実行コンフィギュレーション ファイルに書き込まれます。

PoE 統計情報

PoE 消費量の測定値は、1 分ごとに取得されます。日次統計情報、週次統計情報、および月次統計情報は、リブートしても消えないようにフラッシュメモリに保存されます。サンプルのポート/デバイスごとの平均 PoE 消費量は「一定期間におけるすべての PoE 消費量測定値の合計/サンプリング期間（分単位）」で算出されます。

デバイス上の PoE 消費傾向を表示して、表示用の設定を定義するには、次の手順を実行します。

ステップ 1 [Port Management] > [PoE] > [Statistics] をクリックします。

ステップ 2 ポートを選択します。

ステップ 3 [Refresh Rate] を選択します。

ステップ 4 次のフィールドが選択したインターフェイスに表示されます。

消費履歴

- [Average Consumption over Last Hour]：過去 1 時間の全 PoE 消費量測定値の平均。
- [Average Consumption over Last Day]： 過去 1 日の全 PoE 消費量測定値の平均。
- [Average Consumption over Last Week]過去 1 週間の全 PoE 消費量測定値の平均。

PoE イベント カウンタ

- [Overload Counter]：過負荷状態の検出回数。
- [Short Counter]：不足状態の検出回数。
- [Denied Counter]：拒否状態の検出回数。
- [Absent Counter]：不在状態の検出回数。
- [Invalid Signature Counter]：無効署名状態の検出回数

ステップ 5 [View All Interfaces Statistics] をクリックして、次のタスクを実行します。

- [Clear Event Counters]：表示されたイベント カウンタをクリアします。
- [インターフェイス統計情報の表示]：選択されたインターフェイスに関する上記統計情報を表示します。
- [View Interface History Graph]：選択したインターフェイスのカウンタをグラフ形式で表示します。
- [Refresh]：表示されたカウンタをリフレッシュします。

ステップ 6 [View Interface History Graph] をクリックして、次のタスクを実行します。

- [View Interfaces Statistics]：選択されたインターフェイスに関するグラフ統計情報を表形式で表示します。[Time Span] に期間を時間、日、週、または年単位で入力します。
- [View All Interfaces Statistics]：すべてのインターフェイスの統計情報を表形式で表示します。[Time Span] に期間を時間、日、週、または年単位で入力します。

グリーン イーサネット

グリーンイーサネットは、環境に配慮し、デバイスの電力消費を削減するように設計された一連の機能の通称です。グリーンイーサネットは EEE とは異なり、すべてのデバイスでグリーン イーサネット エネルギー検出が有効になります。EEE ではギガバイトポートのみが有効になります。

グリーン イーサネット機能は、次の方法で全体的な電力使用を削減します。

- エネルギー検出モード：非アクティブリンク上のポートは非アクティブモードに移行します。これにより、ポートの管理ステータスを [Up] にしたまま電力を節約することができます。このモードからフル動作モードへの回復が早く、透過的で、フレームの損失が発生

しません。このモードは、GEポートとFEポートの両方でサポートされます。このモードはデフォルトではディセーブルになっています。

- ショート リーチ モード：短いケーブルで電力が削減されます。ケーブル長が分析された後、さまざまなケーブル長での電力使用が調整されます。10ギガビットポートに接続されるケーブルが 30 m 未満で、他のタイプのポートに接続されるケーブルが 50 m 未満の場合、ケーブルでのフレームの送信にデバイスが使用する電力が減るため、エネルギーを節約できます。このモードは、RJ-45 ポートでのみ使用できます。コンボ ポートでは使用できません。このモードはデフォルトではディセーブルになっています。

前述のグリーン イーサネット機能に加えて、GE ポートをサポートするデバイスでは 802.3az Energy Efficient Ethernet（EEE）を使用できます。EEEは、ポートでトラフィックがないときの電力消費を削減します。EEE はデフォルトでグローバルに有効になっています。

電力削減、現在の電力消費および累積削減エネルギーをモニタすることができます。削減されたエネルギー量の合計は、グリーン イーサネット モードで実行されていなかった場合に物理インターフェイスで消費されたであろう電力に対するパーセンテージと見なすことができます。表示される削減されたエネルギーは、グリーン イーサネットのみに関連付けられます。EEE によって削減された電力量は表示されません。

プロパティ

[Properties] ページでは、デバイスのグリーン イーサネット モードを表示して有効にすることができます。現在の省電力の状態も表示されます。

Green Ethernet および EEE を有効にして電力節約量を表示するには、次のようにします。

ステップ 1 [Port Management] > [Green Ethernet] > [Properties] をクリックします。

ステップ 2 次のフィールドに値を入力します。

- [Energy Detect Mode]：このモードを有効にする場合は、このチェックボックスをオンにします。この設定は一部の XG デバイスではサポートされていません。
- [ショートリーチ]：（非XGデバイスの場合）この機能を有効にする場合はこのチェックボックスをオンにします。
- [Port LEDs]：選択すると、ポートの LED が有効になります。無効になっている場合、リンクステータス、アクティビティなどは表示されません。
- [802.3 Energy Efficient Ethernet (EEE)]：EEE モードをグローバルに有効または無効にします。802.3az EEE は、リンクでトラフィックがない場合に、電力を削減するように設計されています。グリーンイーサネットでは、ポートが停止すると電力が削減されます。802.3Az EEE を使用すると、ポートが稼働状態であるものの、トラフィックがない場合に、電力が削減されます。

（注） Green Ethernet インターフェイスでは、802.3 EEE は 100 Mbps 以上のリンク速度でサポートされています。10Gインターフェイスでは、802.3 EEEは1 Gbps以上のリンク速度でサポートされています。

ステップ 3 [Reset Energy Saving Counter]：累積削減エネルギーの情報をリセットします。

ステップ 4 [Apply] をクリックします。グリーン イーサネット プロパティは、実行コンフィギュレーション ファイルに書き込まれます。

ポート設定

[Port Settings] には、ポートごとの現在のグリーンイーサネットモードおよび EEE モードが表示され、[Edit Port Setting] ページでポート上のグリーンイーサネットを設定できるようにします。ポートでグリーンイーサネットモードを使用するには、プロパティ（154ページ）で対応するモードをグローバルに有効にしておく必要があります。

EEE設定は、GEポートを持つデバイスにのみ表示されます。EEEは、ポートが自動ネゴシエーションに設定されている場合にのみ機能します。例外として、自動ネゴシエーションが無効になっているものの、ポートが 1 GB 以上の場合、EEE は動作を継続します。ショートリーチ機能およびエネルギー検出機能はXGデバイスで常に有効になっており、無効化できません。FEポートまたはGE ポートを持つデバイスでは、これらの機能を有効にしたり無効にしたりできます。

ポートごとにグリーンイーサネットの設定を定義するには、次の手順を実行します。

ステップ 1 [Port Management] > [Green Ethernet] > [Port Settings] をクリックします。

[Port Settings] ページには、以下の項目が表示されます。

- [Global Parameter Status]：次の情報が表示されます。
  - [Energy Detect Mode]：このモードが有効であるかどうか。
  - [Short Reach Mode]：このモードが有効であるかどうか。
  - [802.3 Energy Efficient Ethernet (EEE) Mode]：このモードが有効であるかどうか。

  ポートごとに、次のフィールドが説明されます。

ステップ 2 ポートを選択して [Edit] をクリックします。

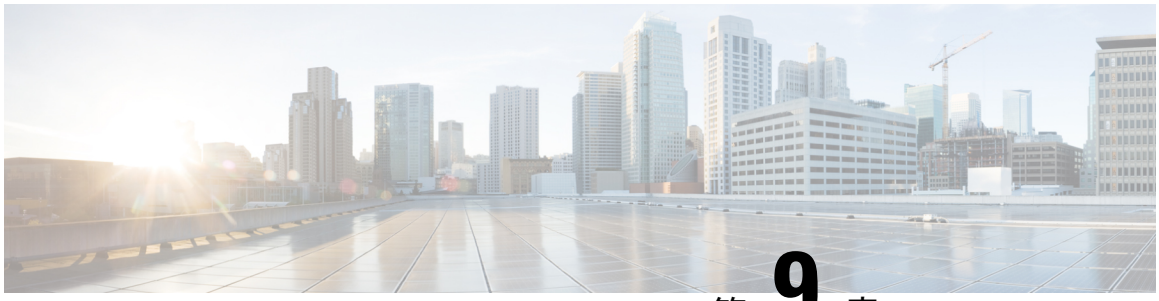
ステップ 3 （XG 以外のデバイスの場合のみ）選択すると、[Energy Detect Mode] モードをポートで有効または無効にできます。

ステップ 4 （XG 以外のデバイスの場合のみ）選択すると、デバイスに GE ポートがある場合、[Short Reach] モードを有効または無効にできます。

ステップ 5 選択すると、[802.3 Energy Efficient Ethernet（EEE] モードをポートで有効または無効にできます。

ステップ 6 選択すると、[802.3 Energy Efficient Ethernet（EEE）LLDP] モードをポートで有効または無効にできます（LLDP を介した EEE 機能のアドバタイズメント）。

ステップ 7 [Apply] をクリックします。グリーン イーサネットのポート設定は、実行コンフィギュレーション ファイルに書き込まれます。



第 9 章

Smartport

この章は、次の項で構成されています。

Smartport プロパティ

Smartport は、組み込み（またはユーザー定義）マクロを適用できるインターフェイス（ポート、VLAN、または LAG）です。この Smartport 機能は、接続しようとしているデバイスのタイプに基づいて、事前設定されたセットアップをスイッチポートに適用します。Auto Smartport を使用すると、スイッチはデバイスを検出すると、これらの設定をインターフェイスに自動的に適用できます。Smartport に接続可能なデバイスのタイプのことを、Smartport タイプと呼びます。

（注） ファームウェアバージョンが 3.0.0.69（またはそれ以前）で、最新（2021 年 3 月）の 3.1 バージョン（または入手可能な場合はそれ以降）にアップグレードすると、デフォルト設定で Smartport 機能が有効になったままになります。

3.1 ファームウェアバージョン（またはそれ以降）のスイッチを購入した場合、ファームウェアの Smartport 機能はデフォルトで**無効**になっています。この変更は、一部のお客様が Smartport 機能を必ずしも使用したくない、またはこれが原因で接続に問題が発生し、お客様が Smartport 機能が有効になっていることを認識していなかったために行われました。

Smartport 機能を設定するには、次の手順を実行します。

ステップ 1 [Smartport] > [Properties] の順にクリックします。

ステップ 2 パラメータを入力します。

- [Administrative Auto Smartport]：Auto Smartport を有効にするか無効にするかを選択します。次のオプションを使用できます。

- [Disable]：デバイスで Auto Smartport を無効にする場合に選択します。これはデフォルト設定です。
- [Enable]：デバイスで Auto Smartport を有効にする場合に選択します。
- [Enable by Auto Voice VLAN]：自動音声 VLAN がオンの場合にのみ、Auto Smartport が有効になります。

- [Operational Auto Smartport]：Auto Smartport ステータスが表示されます。
- [Auto Smartport Device Detection Method]：接続しているデバイスの Smartport タイプを検出する際に使用する着信パケットのタイプ（CDP か LLDP、または両方）を選択します。Auto Smartport でデバイスを識別するには、少なくとも 1 つのタイプを選択する必要があります。
- [Operational CDP Status]：CDP の動作ステータスが表示されます。Auto Smartport が CDP アドバタイズメントに基づいて Smartport タイプを検出する場合は、CDP を有効にします。
- [Operational LLDP Status]：LLDP の動作ステータスが表示されます。Auto Smartport が LLDP/LLDP-MED アドバタイズメントに基づいて Smartport タイプを検出する場合は、LLDP を有効にします。
- [Auto Smartport Device Detection]：Auto Smartport で Smartport タイプをインターフェイスに割り当て可能にするデバイスのタイプを選択します。未選択の場合、Auto Smartport では、その Smartport タイプはどのインターフェイスにも割り当てられません。

ステップ 3 [Apply] をクリックします。これは、デバイスのグローバル Smartport パラメータを設定します。

Smartportタイプ設定

Smartportタイプ設定を編集し、マクロのソースを表示するには、Smartportタイプ設定（Smartport Type Settings）ページを使用します。Auto Smartport によって適用された Smartport タイプのパラメータを編集することで、各パラメータのデフォルト値を設定します。

（注） Auto Smartport タイプを変更すると、Auto Smartport によってそのタイプに割り当てられているインターフェイスに新しい設定が適用されます。この場合、無効なマクロをバインドしたり無効なデフォルト パラメータ値を設定したりすると、この Smartport タイプのすべてのポートが不明になる場合があります。

ステップ 1 [Smartport] > [Smartport Type Settings] の順にクリックします。

ステップ 2 Smartport タイプに関連付けられている Smartport マクロを表示するには、Smartport タイプを選択して、[View Macro Source...] をクリックします.

ステップ 3 マクロのパラメータを変更するには、Smartport タイプを選択して、[Edit] をクリックします。

ステップ 4 フィールドに入力します。

- [ポートタイプ]：Smartport タイプを選択します。
- [マクロ名]：現在、Smartport タイプに関連付けられている Smartport マクロ名が 表示されます。
- [Macro Type]：この Smartport タイプに関連付けられているマクロとアンチマクロのペアが、[Built-in Macro] か [User-Defined Macro] かを選択します。
- [User Defined Macro]：必要に応じて、Smartport タイプと関連付けられるユーザー定義マクロを選択します。2 つのマクロのペアリングは名前によって実行されます。詳細は「Smartport マクロ」セクションで説明されています。
- マクロ パラメータ（Macro Parameters）：マクロの 3 つのパラメータ向けに、次のフィールドが表示されます。
  - [Parameter Name]：マクロ内にあるパラメータの名前。
  - [Parameter Value]：マクロ内にあるパラメータの現在の値。
  - [Parameter Description]：パラメータの説明。

ステップ 5 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。Smartport マクロや、Smartport タイプに関連付けられているパラメータ値を変更すると、現在 Auto Smartport によって Smartport タイプが割り当てられているインターフェイスに、Auto Smartport がマクロを自動的に再適用します。Auto Smartport は、Smartport タイプが静的に割り当てられているインターフェイスに変更を適用しません。

[Restore Defaults] をクリックすると、選択されている Smartport タイプのデフォルト値に戻ります。

（注） タイプとの関連付けが設定されていないので、マクロパラメータを検証する方法はありません。したがって、この時点ではあらゆるエントリは有効になります。ただし、Smartport タイプがインターフェイスに割り当てられて、関連付けられているマクロが適用されたときに、パラメータが無効な場合、エラーの原因になる可能性があります。

Smartport インターフェイス設定

[Interface Settings] ページでは、次の作業を実行します。

- マクロ パラメータのインターフェイス固有の値を持つインターフェイスに、特定の Smartport タイプを静的に適用します。
- インターフェイスで Auto Smartport をイネーブル化します。
- 適用時に失敗し、Smartport タイプが不明になる原因となった Smartport マクロを診断します。
- インターフェイスに Smartport マクロを再適用します。いくつかの状況では、インターフェイスの設定が最新となるように、Smartport マクロを再適用することができます。たとえ

ば、デバイスインターフェイスでスイッチSmartportマクロを再適用すると、インターフェイスは最後のマクロ適用以降に作成された VLAN のメンバーになります。

- 不明なインターフェイスをリセットして、[Default] に設定します。

Smartport マクロを適用するには、次の手順を実行します。

ステップ 1 **[Smartport]** > **[Interface Settings]** の順にクリックします。

インターフェイスのグループに関連付けられたSmartportマクロを再適用するには、次のオプションのいずれかを選択して [Apply] をクリックします。

- [All Switches, Routers, and Wireless Access Points]：すべてのインターフェイスにマクロを再適用します。
- すべてのスイッチ（All Switches）：スイッチとして定義されているすべてのインターフェイスにマクロを再適用します。
- [All Routers]：ルータとして定義されたすべてのインターフェイスにマクロを再適用します。
- すべてのワイヤレス アクセス ポイント（All Wireless Access Points）：アクセス ポイントとして定義されているすべてのインターフェイスにマクロを再適用します。

  インターフェイスに関連付けられたSmartportマクロを再適用するには、そのインターフェイスを選択して [Reapply] をクリックします。

  [Reapply]アクションにより、新たに作成したすべてのVLANにもインターフェイスが追加されます。

ステップ 2 Smartport 診断。

Smartport マクロが失敗すると、インターフェイスの Smartport タイプは不明となります。不明なタイプのインターフェイスを選択し、[Show Diagnostic] をクリックします。すると、マクロの適用が失敗したコマンドが表示されます。

ステップ 3 不明なインターフェイスすべてをデフォルトのタイプにリセットします。

- [Smartportタイプが次に等しい] チェックボックスを選択します。
- [不明] を選択します。
- [Go] をクリックします。
- [Reset All Unknown Smartports] をクリックします。前述の方法でマクロを再適用します。これにより、タイプが不明なすべてのインターフェイスでリセットが実行されます。つまり、すべてのインターフェイスがデフォルトのタイプに返されることを意味します。

ステップ 4 インターフェイスを選択して、[Edit] をクリックします。

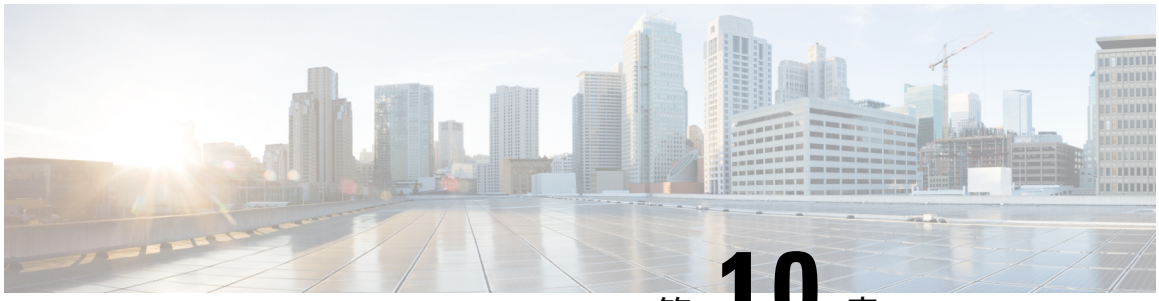
ステップ 5 フィールドに入力します。

- [インターフェイス]：ポートまたは LAG を選択します。
- [Smartport タイプ]：現在、ポート /LAG に割り当てられている Smartport タイプ が表示されます。

- [Smartport の適用] : [Smartport の適用] プルダウンから Smartport タイプを選択 します。
- [Smartport Application Method] : Auto Smartport を選択した場合、Auto Smartport によって、接続しているデバイスから受信した CDP および LLDP アドバタイズメントに基づいて、Smartport タイプが自動的に割り当てられ、対応する Smartport マクロが適用されます。Smartport タイプを静的に割り当て、対応する Smartport マクロをそのインターフェイスに適用するには、目的の Smartport タイプを選択します。
- [永続性ステータス] : 永続性ステータスを有効にする場合、これを選択します。有効にすると、インターフェイスがダウンしたりデバイスが再起動したりした場合でも、インターフェイスへの Smartport タイプの関連付けが維持されます。永続化は、インターフェイスの Smartport アプリケーションが Auto Smartport である場合のみ適用されます。インターフェイスで永続化を有効にすると、それ以外の場合に発生するデバイスの検出遅延がなくなります。
- マクロ パラメータ（Macro Parameters）：マクロの最大 3 つのパラメータ向けに、次のフィールドが表示されます。
  - [Parameter Name] : マクロ内にあるパラメータの名前。
  - [Parameter Value] : マクロ内にあるパラメータの現在の値。この値は、ここで変更できます。
  - [Parameter Description] : パラメータの説明。

ステップ 6 （マクロ適用が失敗した結果）インターフェイスのステータスが不明となっている場合、[Reset] をクリックしてインターフェイスをデフォルトに設定します。マクロはメインページ上で再適用できます。

ステップ 7 [Apply] をクリックして変更内容を更新し、Smartport タイプをインターフェイスに割り当てます。



第 10 章

VLAN管理

この章は、次の項で構成されています。

VLAN 設定

仮想ローカルエリアネットワーク（VLAN）を作成することで、スイッチ上で個別のブロードキャストドメインを設定できます。ブロードキャストドメインは、ルータなどのレイヤ3デバイスを使用して、互いに関連付けることができます。VLANは、ホストの物理的な配置場所に関係なく、ホスト間でグループを形成するために主に使用されます。したがって、VLANはホスト間にグループを形成することでセキュリティを向上させます。VLANを作成しても、そのVLANが少なくとも1つのポートに手動で、または動的に接続されるまでは何の効果もありません。VLAN を設定する最も一般的な理由の 1 つは、音声用の VLAN と、データ用の VLAN を個別に設定するためです。そうすることで、同じネットワークを使用していても、両方のタイプのデータのパケットが送信されます。

VLAN を作成するには、次の手順を実行します。

ステップ 1 [VLAN Management] > [VLAN Settings] をクリックします。

ステップ 2 [Add] をクリックして、1 つ以上の新しい VLAN を追加します。

このページでは、単一の VLAN または特定範囲の複数 VLAN が作成できます。

ステップ 3 単一の VLAN を作成するには、[VLAN] オプション ボタンを選択して [VLAN ID] を入力し、必要に応じて [VLAN Name] を入力します。

ステップ 4 新しい VLAN に次のフィールドを追加します。

- [VLAN Interface State]：VLAN を有効にする場合に選択します。
- [Link Status SNMP Traps]：SNMP トラップのリンクステータス生成を有効にする場合に選択します。

ステップ 5 VLAN の範囲を追加するには、[Range] チェックボックスをオンにし、[VLAN range] フィールドに VLAN 範囲（2 ～ 4094）を入力します。

ステップ 6 [Apply] をクリックして、VLAN を作成します。

VLANインターフェイス設定

[VLAN Interface Settings] ページには、VLAN 関連のパラメータが表示され、設定が可能になります。

VLAN 設定を行うには、次の手順を実行します。

ステップ 1 [VLAN Management] > [Interface Settings] をクリックします。

ステップ 2 S-VLAN タグに [Global Ethertype Tagging] 方式を選択します。

- Dot1q-8100
- Dot1ad-88a8
- 9100
- 9200

ステップ 3 インターフェイス タイプ（ポートまたは LAG）を選択し、[Go] をクリックします。ポートまたは LAG とその VLAN パラメータが表示されます。

ステップ 4 ポートまたは LAG を設定するには、それらを選択して [Edit] をクリックします。

ステップ 5 次のフィールドに値を入力します。

Interface	ポートまたは LAG を選択します。
スイッチポートモード	レイヤ 2 またはレイヤ 3 を選択します。

インターフェイスVLANモード	VLANのインターフェイスモードを選択します。次のオプションがあります。 • [アクセス] : インターフェイスは、1 つの VAN のタグなしメンバになります。このモードで設定されているポートは、アクセス ポートと呼ばれます。 • [トランク] : インターフェイスは、最大 1 つの VLAN のタグなしメンバと、0以上のVLANのタグ付きメンバになります。このモードで設定されているポートは、トランク ポートと呼ばれます。 • [General] : インターフェイスは IEEE 802.1q の規格で定義されているすべての機能をサポートできます。インターフェイスは、1 つまたは複数の VLAN のタグ付きまたはタグなしメンバーになれます。 • [カスタマー] : このオプションを選択すると、インターフェイスが Q-in-Q モー ドになります。これにより、プロバイダー ネットワーク全体で独自のVLAN配置（PVID）が使用できます。デバイスは、1つ以上の顧客ポートがある場合には Q-in-Q モードです。 • [Private VLAN—Host] : インターフェイスを隔離またはコミュニティとして設定する場合に選択します。この後、[Secondary VLAN - Host] フィールドで、隔離 VLAN またはコミュニティ VLAN のいずれかを選択します。 • [Private VLAN—Promiscuous] : インターフェイスを混合として設定する場合に選択します。 • [VLAN Mapping—Tunnel] : インターフェイスを VLAN トンネルエッジポートとして設定する場合に選択します。 • [VLAN Mapping—One to One] : インターフェイスを VLAN マッピング ワンツーワン エッジ ポートとして使用するように設定する場合に選択します。
EtherTypeタギング	S-VLAN タグの EtherType タギング方式を選択します（前述の [Global Ethertype Tagging] フィールドを参照）。
フレーム タイプ（Frame Type）	（一般モードでのみ使用可能）インターフェイスで受信可能なフレームのタイプを選択します。設定されたフレームタイプではないフレームは、入力時に廃棄されます。値は次のとおりです。 • [Admit All] : インターフェイスは、タグなしフレーム、タグ付きフレーム、優先順位タグ付きフレームのすべての種類のフレームを受信します。 • [タグ付きのみ通過] : インターフェイスはタグ付きフレームのみを受け入れます。 • [タグなしのみ通過] : インターフェイスはタグなしおよびプライオリティタグ付 きフレームのみ受け入れます。

入力フィルタング	（一般モードでのみ使用可能）入力フィルタリングを有効にする場合に選択します。入力フィルタリングが有効になると、インターフェイスは、そのインターフェイスがメンバーになっていない VLAN に分類されるすべての着信フレームを破棄します。入力のフィルタリングは全般ポートで無効または有効にできます。アクセスポートとトランクポートでは常に有効になっています。
Primary VLAN	プライベート VLAN のプライマリ VLAN を選択します。プライマリ VLAN は、無差別ポートから隔離ポートおよびコミュニティ ポートにレイヤ 2 で接続できるようにするために使用します。[None] が選択された場合、インターフェイスはプライベート VLAN モードになりません。
セカンダリ VLAN ホスト	単一のセカンダリ VLAN のみを必要とするホストの隔離 VLAN またはコミュニティ VLAN を選択します。
選択されたセカンダリ VLAN に使用可能なセカンダリ VLAN	混合ポートの場合は、通常のパケット転送に必要となるセカンダリ VLAN すべてを、[Available Secondary VLANs] から移動します。混合ポートとトランクポートは複数の VLAN のメンバーにすることができます。

ステップ 6 [Apply] をクリックします。

VLANへのポート

[Port to VLAN] セクションには、ポートの VLAN メンバーシップがさまざまな表現で表示されます。これらを使用して、VLAN にメンバーシップを追加、または VLAN からメンバーシップを削除することができます。

ポートに、禁止されているデフォルト VLAN メンバーシップが設定されている場合、そのポートには他の VLAN のメンバーシップは設定できません。内部 VID として 4095 がそのポートに割り当てられます。

パケットを転送するには、エンドノード間のパスで VLAN トラフィックを伝達する VLAN 対応デバイスを手動で設定するか、VLAN とそのポートメンバーシップを Generic VLAN Registration Protocol（GVRP）から動的に学習する必要があります。

VLAN 認識型デバイスが介入しない 2 つの VLAN 認識型デバイス間のタグなしポートのメンバーシップは、同じ VLAN である必要があります。2 つのデバイス間にあるポートの PVID は、そのポートと VLAN 間でタグなしパケットの送受信を行う場合、同じである必要があります。そうでない場合、トラフィックは VLAN の外に漏えいします。

VLAN タグ付きのフレームは、VLAN 認識型または VLAN 非認識型の他のネットワーク デバイスを通過できます。宛先エンドノードが VLAN 未対応なのに、VLAN からのトラフィックを受信する場合、最後の VLAN 対応デバイスが、宛先 VLAN のフレームをタグなしのエンドノードに送信する必要があります。

[Port to VLAN] ページを使用して、特定 VLAN 内のポートを表示および設定できます。

ポートや LAG をVLAN にマッピングするには、次の手順を実行します。

ステップ 1 [VLAN Management] > [Port to VLAN] をクリックします。

ステップ 2 VLAN とインターフェイスの種類（ポートまたはLAG）を選択し、[Go] をクリックして、VLAN に関するポートの特性を表示または変更します。

各ポートまたはLAG のポートモードは、VLANインターフェイス設定 （164 ページ）で設定されている現在のポートモードとともに表示されます。

各ポートまたは LAG には、VLAN への現在の登録が表示されます。

次のフィールドが表示されます。

- [VLAN Mode]：VLAN のポートの種類が表示されます。
- [Membership Type]：次のいずれかのオプションを選択できます。
  - [Forbidden]：このインターフェイスは、GVRP 登録からであってもVLANに参加できません。ポートが他の VLAN のメンバーではない場合、ポートでこのオプションを有効にすると、内部 VLAN 4095 のポート部分（予約済み VID）になります。
  - [Excluded]：インターフェイスは現在 VLAN のメンバーではありません。VLAN の新規作成時には、すべてのポートおよびLAG でこれがデフォルトで設定されます。
  - [タグ付き]：インターフェイスは、VLAN のタグ付きメンバになります。
  - [タグなし]：インターフェイスは、VLAN のタグなしメンバになります。VLAN のフレームはタグなしでインターフェイス VLAN に送信されます。
  - [Multicast MTV VLAN]：マルチキャスト IP を使用してデジタル TV に使用されるインターフェイス。ポートは、マルチキャスト TV VLAN の VLAN タグを使用して VLAN に参加します。
- [PVID]：インターフェイスの PVID を VLAN の VID に設定します。PVID はポート単位の設定です。

ステップ 3 [Apply] をクリックします。インターフェイスはVLANに割り当てられ、同時に実行コンフィギュレーション ファイルに書き込まれます。

別の VLAN ID を選択すれば、続けて別の VLAN のポート メンバーシップを表示または設定できます。

ポートVLANメンバシップ

[Port VLAN Membership] ページは、デバイスのすべてのポートと、各ポートが属する VLAN のリストを表示します。インターフェイスのポート ベースの認証方式は 802.1x であり、ポートの管理制御は自動です。この場合、次のように動作します。

- ポートは、認証されるまで、ゲスト VLAN および未認証 VLAN を除くすべての VLAN から除外されます。[VLAN to Port] ページでは、ポートは大文字の P でマーク付けされます。

- ポートが認証されると、そのポートが設定されている VLAN でメンバーシップを受信します。

（注） VLAN IS モードをサポートします。したがって、さまざまな VLAN モードを適用するまえにポートの VLAN メンバーシップを設定することができます。ポートに特定の VLAN モードが適用されると、設定がアクティブになります。

1 つまたは複数の VLAN にポートを割り当てるには、次の手順を実行します。

ステップ 1 [VLAN Management] > [Port VLAN Membership] をクリックします。

ステップ 2 インターフェイスの種類（ポートまたはLAG）を選択し、[Go] をクリックします。選択した種類のすべてのインターフェイスに対して、次のフィールドが表示されます。

- [インターフェイス]：ポート /LAG ID。
- [Mode]：VLANインターフェイス設定 （164 ページ）で選択されたインターフェイス VLAN モード。
- [管理 VLAN]：インターフェイスがメンバになる可能性のあるすべての VLAN が表 示されるドロップダウン リスト。
- [動作 VLAN]：インターフェイスが現在メンバになっているすべての VLAN が表示 されるドロップダウン リスト。
- [LAG]：選択したインターフェイスが [Port] の場合、このインターフェイスがメンバーになっている LAG が表示されます。

ステップ 3 ポートを選択し、[Join VLAN] をクリックします。

ステップ 4 次のフィールドに値を入力します。

- [インターフェイス]：ポートまたは LAG を選択します。
- [Current VLAN Mode]：VLANインターフェイス設定 （164 ページ）で選択したポート VLAN モードが表示されます。
- [Access Mode Membership (Active)]
  - [Access VLAN ID]：ドロップダウンリストから、VLAN を選択します。
  - [Multicast TV VLAN]：ドロップダウンリストからマルチキャスト TV VLAN を選択します。
- [Trunk Mode Membership]
  - [Native VLAN ID]：ポートがトランクモードになっている場合は、この VLAN のメンバーになります。
  - [Tagged VLANs]：ポートがトランクモードになっている場合は、これらの VLAN のメンバーになります。次のオプションがあります。

[All VLANs]：ポートがトランクモードになっている場合は、すべての VLAN のメンバーになります。

[User Defined]：ポートがトランクモードになっている場合は、ここに入力された VLAN のメンバーになります。

- [General Mode Membership]
  - [Untagged VLANs]：ポートが一般モードになっている場合は、この VLAN のタグなしメンバーになります。
  - [Tagged VLANs]：ポートが一般モードになっている場合は、これらの VLAN のタグ付きメンバーになります。
  - [Forbidden VLANs]：ポートが一般モードになっている場合は、インターフェイスが GVRP 登録からであっても VLAN に参加できません。ポートが他の VLAN のメンバーではない場合、ポートでこのオプションを有効にすると、内部 VLAN 4095 のポート部分（予約済み VID）になります。
  - [General PVID]：ポートが一般モードになっている場合は、これらの VLAN のメンバーになります。
- [Customer Mode Membership]
  - [Customer VLAN ID]：ポートがカスタマーモードになっている場合は、この VLAN のメンバーになります。
  - [Customer Multicast VLANs]：ポートがカスタマーモードになっている場合は、このマルチキャスト TV VLAN のメンバーになります。

ステップ 5 ポートを選択して、[Details] をクリックすると、次のフィールドが表示されます。

- [Administrative VLANs]：ポートはこれらの VLAN に対して設定されています。
- [Operational VLANs]：ポートは現在これらの VLAN のメンバーです。

[Apply] をクリックします（VLAN に参加します）。設定が変更され、実行コンフィギュレーションファイルに書き込まれます。

VLAN 変換

VLAN 変換は、同じ転送ドメインに複数の異なる VLAN が含まれている場合に参照されることがあります。したがって、特定の VLAN ID を持つ入力インターフェイスのフレームは、別の VLAN ID を使用して別のポートに転送できます。

VLAN Mapping

VLAN マッピングを設定するには、次の手順を実行します。

ステップ 1 [VLAN Management] > **[VLAN Translation]** > **[VLAN Mapping]** の順にクリックします。

定義済みの VLAN マッピング設定のテーブルが表示されます。

ステップ 2 次のいずれかのマッピングタイプを選択します。

- [One to One]：1 対 1 VLAN マッピング モードに設定されたインターフェイスの設定を表示および編集するには、このオプションを選択します。
- [Tunnel Mapping]：トンネル VLAN マッピング モードに設定されたインターフェイスの設定を表示および編集するには、このオプションを選択します。

ステップ 3 [Add] をクリックして、次のフィールドに入力します。

- [Interface]：ポートを選択します。
- [Interface VLAN Mode]：現在のインターフェイス モードが表示されます。
- [Mapping Type]：次のいずれかを選択します。
  - [One to One]：1 対 1 VLAN マッピング設定を定義する場合には、このオプションを選択します。
  - [トンネルマッピング]：このオプションは、トンネル VLAN マッピング設定を定義する場合に選択します。
- [ワンツーワン変換]：このオプションは、[マッピングタイプ] の選択時に [ワンツーワン] オプションが選択された場合に表示されます。次のいずれかを選択します。
  - [Source VLAN]：S-VLAN（変換後の VLAN）に変換される顧客 VLAN（C-VLAN）の ID を設定します。
  - [Translated VLAN]：指定された C-VLAN を置き換える S-VLAN を設定します。
- [トンネルマッピング]：このオプションは、[マッピングタイプ] の選択時に [トンネルマッピング] オプションが選択された場合に表示されます。次のいずれかを選択します。
  - [Customer VLAN]：指定されていない C-VLAN に必要なアクションを定義する場合は [Default] を選択します。または、一覧表示された VLAN の VLAN トンネル動作を明示的に定義する場合は [VLAN List] を選択します。
  - [Tunneling]：[Drop] を選択するか、または外部 VLAN ID が選択されている場合は [Outer VLAN ID] を選択して、VLAN を入力します。

ステップ 4 [Apply] をクリックします。パラメータが、実行コンフィギュレーション ファイルに書き込まれます。

プロトコル処理

（注） インターフェイスごとのプロトコル処理動作を設定するには、ハードウェアリソース（104ページ）を VLAN マッピング機能に割り当てる必要があります。

VLAN 変換トンネルエッジポートで受信される L2CP PDU の処理を設定するには、次の手順を実行します。

ステップ 1 [VLAN Management] > [VLAN Translation] > [Protocol Handling] の順にクリックします。

（注） インターフェイスごとにプロトコル処理動作を設定するには、ハードウェアリソースを VLAN マッピング機能に割り当てる必要があります。

ステップ 2 任意で、[Default Tunneling CoS] を設定します。0 ～ 7 の値（デフォルト = 5）を入力して、VLAN トンネリングエッジポートで転送およびカプセル化される L2CP PDU に適用するグローバル CoS 値を定義します。この値は、特定のユーザー CoS 設定を持たないすべてのインターフェイスに使用されます。

ステップ 3 リスト内のいずれかのエントリを選択して [Copy Settings] をクリックすると、選択したエントリの設定が、1 つ以上のエントリにコピーされます。選択したエントリを編集するには [Edit] をクリックします。

ステップ 4 次のフィールドに入力します。

- [Interface]：ポートを選択します。
- [Interface VLAN Mode]：現在のインターフェイス VLAN モードが表示されます。
- [BPDU VLAN ID]：次のいずれかを選択します。
  - [なし]：L2CP BPDU トンネリングのために選択されている VLAN はありません。このオプションは、L2CP PDU のトンネリングを無効にする場合に使用します。
  - [vlan-id]：デバイス上で設定されている、いずれかの VLAN ID：このインターフェイスで L2CP PDU をトンネリングする際に使用する VLAN ID として、利用可能な VLAN ID の中から 1 つ選びます。
- [CoS]：次のいずれかを選択します。
  - [Use Default]：グローバルなデフォルト値を使用する場合に選択します。
  - [User defined]：このオプションを選択し、0 ～ 7 の範囲で値を設定します。
- [Drop threshold]：次のいずれかを選択します。
  - [None]：ドロップしきい値を無効にする場合にこれを選択します。
  - [User Defined]：ドロップしきい値を設定するには、このオプションを選択します。有効な値は 8 ～ 256 Kbps（デフォルトは 32 Kbps）です。
- [Protocol Forwarding]：デバイスで転送およびカプセル化するプロトコルを選択します。

- [CDP]：このプロトコルの転送およびカプセル化を有効にする場合に選択します。
- [LLDP]：このプロトコルの転送およびカプセル化を有効にする場合に選択します。
- [STP]：このプロトコルの転送およびカプセル化を有効にする場合に選択します。
- [VTP]：このプロトコルの転送およびカプセル化を有効にする場合に選択します。

ステップ5 [Apply] をクリックします。パラメータが、実行コンフィギュレーション ファイルに書き込まれます。

プライベートVLAN設定

プライベートVLAN機能は、ポート間でのレイヤ2の分離を提供します。つまり、IPルーティングとは異なり、ブリッジング トラフィックのレベルで、同じブロードキャスト ドメインを共有するポートが相互に通信することはできません。プライベート VLAN 内のポートはレイヤ2ネットワークの任意の場所に配置できます。よって、これらのポートは同じスイッチ上にある必要はありません。プライベートVLANは、タグなしまたは優先順位タグ付きトラフィックを受信し、タグなしトラフィックを送信するように設計されています。

（注） プライベートVLANのインターフェイス メンバーシップをVLANインターフェイス設定（164ページ）で設定します。コミュニティ VLAN および隔離 VLAN にはプライベート VLAN - ホスト インターフェイス モードを使用し、プライマリ VLAN にはプライベート VLAN - プロミスキャス インターフェイス モードを使用します。

新しいプライベート VLAN を作成するには、次の手順を実行します。

ステップ1 [VLAN Management] > [Private VLAN Settings] をクリックします。

ステップ2 [Add] をクリックします。

ステップ3 次のフィールドに値を入力します。

- [Primary VLAN ID]：プライベート VLAN でプライマリ VLAN として定義する VLAN を選択します。プライマリ VLAN は、無差別ポートから隔離ポートおよびコミュニティ ポートにレイヤ 2 で接続できるようにするために使用します。
- [Isolated VLAN ID]：隔離 VLAN は、隔離ポートがプライマリ VLAN にトラフィックを送信する場合に使用します。
- [Available Community VLANs]：コミュニティ VLAN にする VLAN を [Selected Community VLANs] リストに移動します。コミュニティ VLAN により、コミュニティポートからプロミスキャスポートや同じコミュニティのコミュニティポートへのレイヤ 2 接続が可能になります。これはメイン ページでは [Community VLAN Range] と表示されます。

ステップ 4 [Apply] をクリックします。設定が変更され、実行コンフィギュレーション ファイルに書き込まれます。

GVRP設定

隣接する VLAN 認識型デバイスは、Generic VLAN Registration Protocol（GVRP）を使用して相互に VLAN 情報を交換できます。GVRP はGeneric Attribute Registration Protocol（GARP）に基づいており、ブリッジ型ネットワーク全体に VLAN 情報を伝播させます。

GVRPは、グローバルに、かつ各ポートでアクティブにする必要があります。アクティブにすると、GVRP によって GARP パケットデータ単位（GPDU）が送受信されます。定義済みでもアクティブではないGVRP されません。VLAN を伝播するには、少なくとも 1 つのポートで有効化する必要があります。デフォルトでは、GVRP はグローバルおよびポートで無効です。

インターフェイスの GVRP 設定を定義するには、次の手順を実行します。

ステップ 1 [VLAN Management] > [GVRP Settings] をクリックします。

ステップ 2 [GVRP Global Status] を選択して、GVRP をグローバルで有効にします。

ステップ 3 [Apply] をクリックして、グローバル GVRP ステータスを設定します。

ステップ 4 インターフェイスの種類（ポートまたは LAG）を選択して [Go] をクリックし、その種類のすべてのインターフェイスを表示します。

ステップ 5 ポートの GVRP 設定を定義するには、ポートを選択して [Edit] をクリックします。

ステップ 6 次のフィールドに値を入力します。

- [インターフェイス]：編集するインターフェイス（ポートまたは LAG）を選択します。
- [GVRP State]：インターフェイスで GVRP を有効にする場合に選択します。
- [Dynamic VLAN Creation]：このインターフェイスで動的な VLAN の作成を有効にする場合に選択します。
- [GVRP Registration]：このインターフェイスで GVRP を使用した VLAN の登録を有効にする場合に選択します。

ステップ 7 [Apply]をクリックします。GVRP設定が変更され、実行コンフィギュレーションファイルに書き込まれます。

VLAN グループ

VLAN グループは、レイヤ 2 ネットワークでのトラフィックのロード バランシングに使用されます。パケットは、さまざまな分類に従って VLAN に割り当てられます。

分類スキームを複数定義した場合は、次の順序で VLAN にパケットが割り当てられます。

- タグ：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 ベースの VLAN：MAC ベースの VLAN が定義されている場合、VLAN は入力インターフェイスの送信元 MAC から VLAN へのマッピングにより取得されます。
- サブネットベースの VLAN：サブネットベースの VLAN が定義されている場合、VLAN は入力インターフェイスの送信元 IP から VLAN へのマッピングにより取得されます。
- プロトコルベースの VLAN：プロトコルベースの VLAN が定義されている場合、VLAN は入力インターフェイスの（イーサネットの種類）プロトコルから VLAN へのマッピングにより取得されます。
- PVID：VLAN は、ポートのデフォルト VLAN ID から取得されます。

MACベースグループ

MAC ベースの VLAN 分類を使用すると、パケットを送信元 MAC アドレスによって分類できます。その後、インターフェイスごとに MAC から VLAN へのマッピングを定義することができます。複数の異なる MAC アドレスを含む MAC ベース VLAN グループが複数定義できます。これらの MAC ベース グループは、特定のポートまたは LAG に割り当てることができます。MAC ベース VLAN グループには、同じポート上の重複する範囲の MAC アドレスを含めることはできません。

VLAN グループに MAC アドレスを割り当てるには、次の手順を実行します。

ステップ 1 [VLAN Management] > [VLAN Groups] > [MAC-Based Groups] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [MAC Address]：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 MAC アドレスを他の VLAN グループに割り当てることはできません。

- [Prefix Mask]：次のいずれかを入力します。
  - [Host(48)]：プレフィックス マスク（48 ビット）に MAC アドレスのすべてのビットを含める場合
  - [Length]：MAC アドレスのプレフィックス
- [Group ID]：ユーザ作成の VLAN グループ ID 番号を入力します。

ステップ 4 [Apply] をクリックします。MAC アドレスが VLAN グループに割り当てられます。

VLANに対するMACベースグループ

インターフェイス上の VLAN に MAC ベース VLAN グループを割り当てるには、次の手順を実行します。

ステップ 1 [VLAN Management] > [VLAN Groups] > [MAC-Based Groups to VLAN] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [Group Type]：グループが MAC ベースであることが表示されます。
- [Interface]：トラフィックを受信する全般インターフェイス（ポートまたは LAG）を入力します。
- [Group ID]：VLAN グループを選択します。
- [VLAN ID]：VLAN グループからのトラフィックを転送する VLAN を選択します。

ステップ 4 [Apply] をクリックして、VLAN グループから VLAN へのマッピングを設定します。このマッピングはインターフェイスを VLAN に動的にバインドしないため、インターフェイスを VLAN に手動で追加する必要があります。

サブネットベースグループ

サブネットベース グループの VLAN 分類により、サブネットに基づいてパケットを分類することができます。その後、インターフェイスごとにサブネットから VLAN へのマッピングを定義することができます。複数の異なるサブネットを含むサブネットベース VLAN グループが複数定義できます。

これらのグループは、特定のポートまたはLAGに割り当てることができます。サブネットベース VLAN グループ間では、同一ポートでサブネット範囲を重複させることはできません。

サブネットベースのグループを追加するには、次の手順を実行します。

ステップ 1 [VLAN Management] > [VLAN Groups] > [Subnet-Based Groups] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [IP Address]：サブグループの元になる IP アドレスを入力します。
- [Prefix Mask]：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。
- [Group ID]：グループ ID を入力します。

ステップ 4 [Apply] をクリックします。グループが追加され、実行コンフィギュレーション ファイルに書き込まれます。

VLANに対するサブネットベースグループ

サブネット グループをポートにマッピングするには、ポート上で DVA を設定しないようにする必要があります（VLANインターフェイス設定 （164 ページ）を参照）。複数のグループを単一ポートに結合でき、各ポートがそれぞれ独自の VLAN に関連付けられています。複数のグループを単一の 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、次の手順を実行します。

ステップ 1 [VLAN Management] > [VLAN Groups] > [Subnet-Based Groups to VLAN] の順にクリックします。

ステップ 2 インターフェイスをプロトコルベース グループと VLAN に関連付けるには、[Add] をクリックします。

[Group Type] フィールドには、マッピングされているグループの種類が表示されます。

ステップ 3 次のフィールドに入力します。

- [Interface]：プロトコルベース グループに従って VLAN に割り当てられるポートまたは LAG 番号。
- [Group ID]：プロトコルグループ ID。
- [VLAN ID]：このインターフェイスに指定したグループを、ユーザ定義の VLAN ID に結びつけます。

ステップ 4 [Apply]をクリックします。サブネットベース グループのポートがVLANにマッピングされ、実行コンフィギュレーション ファイルに書き込まれます。

プロトコルベースグループ

プロトコルのグループを定義し、ポートにバインドできます。プロトコル グループをポートにバインド後、グループ内のプロトコルに基づいて生成されたすべてのパケットが、プロトコルベース グループ ページで設定された VLAN に割り当てられます。一連のプロトコルを定義するには、次の手順を実行します。

ステップ 1 [VLAN Management] > [VLAN Groups] > [Protocol-Based Groups] をクリックします。

ステップ 2 [Add] をクリックして、プロトコルベース VLAN グループを追加します。

ステップ 3 次のフィールドを入力します。

- [Encapsulation]：プロトコルパケットタイプ。次のオプションを使用できます。
  - [Ethernet V2]：これを選択した場合には、[Ethernet Type] を選択します。
  - [LLC-SNAP（rfc1042]：これを選択した場合には、[Protocol Value] を入力します。

- [LLC]：これを選択した場合には、[DSAP-SSAP Values] を選択します。

- [Ethernet Type]：イーサネット V2 カプセル化のイーサネットの種類を選択します。これは、VLAN グループのイーサネットパケットのペイロード内にカプセル化されているプロトコルを示すために使用される、イーサネットフレーム内の 2 オクテットのフィールドです。
- [Protocol Value]：LLC-SNAP（rfc 1042）カプセル化のプロトコルを入力します。
- [Group ID]：プロトコル グループ ID を入力します。

ステップ 4 [Apply] をクリックします。プロトコル グループが追加され、実行コンフィギュレーション ファイルに書き込まれます。

VLANに対するプロトコルベースグループ

プロトコルベースの VLAN は、物理ネットワークを各プロトコルの論理 VLAN グループに分割します。フレームがポートで受信されると、その VLAN メンバーシップはプロトコルタイプに基づいて決定されます。複数のグループを単一ポートに結合でき、各ポートがそれぞれ独自の VLAN に関連付けられています。いくつかのグループを単一のポート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、次の手順を実行します。

ステップ 1 [VLAN Management] > [VLAN Groups] > [Protocol-Based Groups to VLAN] をクリックします。

ステップ 2 インターフェイスをプロトコルベース グループと VLAN に関連付けるには、[Add] をクリックします。

[Group Type] フィールドには、マッピングされているグループの種類が表示されます。

ステップ 3 次のフィールドに入力します。

- [Interface]：プロトコルベース グループに従って VLAN に割り当てられるポートまたは LAG 番号。
- [Group ID]：プロトコルグループ ID。
- [VLAN ID]：インターフェイスを、ユーザ定義の VLAN ID に結びつけます。

ステップ 4 [Apply] をクリックします。プロトコル ポートが VLAN にマッピングされ、実行コンフィギュレーション ファイルに書き込まれます。

Voice VLAN

音声 VLAN 機能を使用すると、アクセス ポートで IP Phone からの IP 音声トラフィックを伝送できます。スイッチが IP フォンに接続されると、その IP フォンはレイヤ 3 IP プレシデンス値およびレイヤ 2 サービスクラス（CoS）値を使用して、音声トラフィックを送信します。どち

らの値もデフォルトでは 5 に設定されます。データ送信が均質性に欠ける場合、IP Phone の音質が低下することがあります。そのため、このスイッチでは、IEEE 802.1p CoS に基づく Quality of Service（QoS）をサポートしています。QoS は、分類およびスケジューリングを使用して、スイッチからのネットワーク トラフィックを予測可能な方法で送信します。

音声 VLAN は、LLDP-MED ネットワーク ポリシーを使用して、CoS/802.1p と DSCP 設定を伝播させることができます。LLDP-MED はデフォルトでは、アプライアンスが LLDP-MED パケットを送信する場合に音声 QoS 設定で応答するよう設定されます。MED をサポートするデバイスは、LLDP-MED 応答で受け取った CoS/802.1p 値および DSCP 値と同じ値を使用して音声トラフィックを送信します。ユーザーは、音声 VLAN と LLDP-MED の間の自動更新を無効にしたり、独自のネットワークポリシーを使用したりできます。OUI モードで動作する場合、デバイスはさらに、OUI に基づく音声トラフィックのマッピングと検知（CoS/802.1p）を設定できます。

デフォルトでは、すべてのインターフェイスは CoS/802.1p で信用されます。デバイスは、音声ストリームで検出された CoS/802.1p 値に基づいて QoS を適用します。テレフォニー OUI 音声ストリームでは、QoS をオーバーライドでき、必要に応じて、必要な CoS/802.1p 値を指定し、テレフォニー OUI の検知オプションを使用することで、音声ストリームの 802.1p を検知できます。

プロパティ

音声 VLAN のプロパティ ページを使用して、次が行えます。

- 音声 VLAN の現在の設定内容を表示します。
- 音声 VLAN の VLAN ID を設定します。
- 音声 VLAN の QoS を設定します。
- 音声 VLAN のモード（テレフォニー OUI または自動音声 VLAN）を設定します。
- 自動音声 VLAN のトリガー方法を設定します。

音声 VLAN のプロパティを表示および設定するには、次の手順を実行します。

ステップ 1 [VLAN Management] > [Voice VLAN] > [Properties] をクリックします。

- デバイスに設定されている音声 VLAN の設定が、[Voice VLAN Settings (Administrative Status)] ブロックに表示されます。
- 音声 VLAN の導入に対して実際に適用されている音声 VLAN 設定が、[Voice VLAN Settings (Operational Status)] ブロックに表示されます。

ステップ 2 次の [管理ステータス] フィールドに値を入力します。

- [音声 VLAN ID]：音声 VLAN にする VLAN を入力します。

（注） 音声 VLAN ID、CoS/802.1p、DSCP を変更すると、デバイスは、管理音声 VLAN をスタティック音声 VLAN としてアドバタイズします。外部音声 VLAN によってトリガーされる [自動音声VLANアクティブ化] オプションを選択した場合は、デフォルト値のままにしておく必要があります。

- [CoS/802.1p]：音声ネットワークポリシーとして LLDP-MED の CoS/802.1p 値を選択します。詳細については、[Administration] > [Discovery] > [LLDP] > [LLDP MED Network Policy] を参照してください。
- [DSCP]：音声ネットワークポリシーとして LLDP-MED の DSCP 値を選択します。詳細については、[Administration] > [Discovery] > [LLDP] > [LLDP MED Network Policy] を参照してください。

次の [Operational Status] フィールドが表示されます。

- [Voice VLAN ID]：音声 VLAN。
- [CoS/802.1p]：LLDP-MED により音声ネットワーク ポリシーとして使用されている値。詳細については、[Administration] > [Discovery] > [LLDP] > [LLDP MED Network Policy] を参照してください。
- [DSCP]：音声ネットワーク ポリシーとして LLDP-MED で使用される値。

次の [Dynamic Voice VLAN Settings] フィールドが表示されます。

- [ダイナミック音声 VLAN]：次のいずれかの方法で音声 VLAN 機能を無効または有 効にするにはこのフィールドを選択します。
  - [自動音声VLANの有効化]：ダイナミック音声 VLAN を自動音声 VLAN モードで有効にします。
  - [テレフォニー OUI の有効化（Enable Telephony OUI）]：テレフォニー OUI モードでダイナミック音声 VLAN を有効化します。
  - [Disable]：自動音声 VLAN またはテレフォニー OUI を無効にします
- [自動音声 VLAN のアクティブ化]：自動音声 VLAN が有効な場合は、自動音声VLAN をアクティブ化するために、次のいずれかのオプションを選択します。
  - [即時]：有効にすると、デバイスでただちに自動音声 VLAN がアクティブになり、動作状態になります。
  - [外部音声VLANトリガーを使用]：音声 VLAN をアドバタイズするデバイスをデバイスが検出した場合にのみ、デバイス上の自動音声 VLAN がアクティブになり、動作状態になります。

（注） 音声 VLAN ID、CoS/802.1p、DSCP のすべて、またはいずれかを手動でデフォルト値から再設定すると、自動音声 VLAN よりもプライオリティが高いスタティック音声 VLAN になります。

ステップ 3 [Apply] をクリックします。VLAN のプロパティが実行コンフィギュレーション ファイルに書き込まれます。

自動音声 VLAN

自動音声 VLAN モードが有効になっている場合は、自動音声 VLAN ページを使用して、関連するグローバルおよびインターフェイスのパラメータを表示します。

また、このページを使用して、[Restart Auto Voice VLAN] をクリックして自動音声 VLAN を手動で再起動することができます。これにより、短い遅延の後、音声 VLAN がデフォルトの音声 VLAN にリセットされ、自動音声 VLAN 検出が再起動されて、自動音声 VLAN が有効な LAN 内のすべてのスイッチで同期プロセスが再実行されます。

（注） [ソースタイプ] が [非アクティブ] の状態の場合、音声 VLAN をデフォルトの音声 VLAN にリセットする処理のみが実行されます。

自動音声 VLAN パラメータを表示するには、次の手順を実行します。

ステップ 1 [VLAN Management] > [音声 VLAN（Voice VLAN] > [Auto Voice VLAN] をクリックします。

このページの [動作ステータス] ブロックに、現在の音声 VLAN およびそのソースに関する情報が表示されます。

- [自動音声 VLAN ステータス]：自動音声 VLAN が有効かどうかを表示します。
- [音声 VLAN ID]：現在の音声 VLAN の ID。
- [Source Type]：ルート デバイスで音声 VLAN を検出する送信元の種類が表示されます。
- [CoS/802.1p]：LLDP-MED により音声ネットワーク ポリシーとして使用される CoS/802.1p 値を表示します。
- [DSCP]：LLDP-MED により音声ネットワーク ポリシーとして使用される DSCP 値を表示します。
- [ルートスイッチ MAC アドレス]：自動音声 VLAN ルート デバイスの MAC アドレ ス。ルート デバイスは、この音声 VLAN の学習元となった音声 VLAN によって検出 または設定されたものです。
- [Switch MAC Address]：デバイスの基本 MAC アドレス。デバイスのスイッチ MAC アドレスがルートスイッチ MAC アドレスの場合、デバイスは自動音声 VLAN のルート デバイスです。
- [音声 VLAN ID 変更時刻]：音声 VLAN が更新された最後の時刻。

ステップ 2 [Restart Auto Voice VLAN] をクリックすると、音声 VLAN がデフォルトの音声 VLAN にリセットされ、自動音声 VLAN が有効な、LAN 内のすべてのスイッチの自動音声 VLAN 検出が再起動されます。

[Voice VLAN Local Source Table] には、デバイスで設定されている音声 VLAN、および直接接続されたネイバーデバイスによってアドバタイズされた音声 VLAN の設定が表示されます。ファイルには、次のフィールドがあります。

- [Interface]：音声 VLAN 設定を受信または設定されたインターフェイスが表示されます。[N/A] が表示された場合には、デバイス自身に設定が行われています。インターフェイスが表示された場合には、ネイバーから受信した音声設定が使用されています。

- [Source MAC Address]：音声設定の受信元 UC の MAC アドレス。
- [Source Type]：音声設定の受信元 UC のタイプ。次のオプションを使用できます。
  - [Default]：デバイスのデフォルトの音声 VLAN 設定
  - [Static]：デバイス上に定義されているユーザー定義の音声 VLAN 設定。
  - [CDP]：音声 VLAN 設定が CDP を実行していることをアドバタイズした UC。
  - [LLDP]：音声 VLAN 設定が LLDP を実行していることをアドバタイズした UC。
  - [Voice VLAN ID]：アドバタイズまたは設定された音声 VLAN の識別子
- [Voice VLAN ID]：現在の音声 VLAN の識別子。
- [CoS/802.1p]：LLDP-MED により音声ネットワーク ポリシーとして使用される、アドバタイズまたは設定された CoS/802.1p 値。
- [DSCP]：LLDP-MED により音声ネットワーク ポリシーとして使用される、アドバタイズまたは設定された DSCP 値。
- [Best Local Source]：この音声 VLAN がデバイスにより使用されたかどうかが表示されます。次のオプションを使用できます。
  - [Yes]：デバイスはこの音声 VLAN を使用して、自動音声 VLAN が有効な他のスイッチと同期します。より優先順位の高い送信元からの音声 VLAN が検出されない限り、この音声 VLAN がネットワークの音声 VLAN です。最適なローカル送信元はただ 1 つだけです。
  - [No]：この音声 VLAN は最適なローカルソースではありません。

ステップ 3 ページ上の情報を更新するには、[Refresh] をクリックします。

テレフォニー OUI

OUI は電気電子学会（IEEE）の登録局により割り当てられます。IP フォン製造者の数は有限であり、また広く知られているため、既知の OUI 値により関連フレームとポートから製造者が判定され、音声 VLAN に自動的に割り当てられます。テレフォニー OUI ページを使用して、テレフォニー OUI の QoS プロパティを設定します。さらに、自動メンバーシップ エージングタイムを設定できます。テレフォニーのアクティビティなしに指定した期間が経過した場合、ポートは音声 VLAN から削除されます。

テレフォニー OUI の設定や新しい音声 VLAN OUI の追加を行うには、次の手順を実行します。

ステップ 1 [VLAN Management] > [Voice VLAN] > [Telephony OUI] をクリックします。

テレフォニー OUI ページには次のフィールドがあります。

- [テレフォニー OUI 動作ステータス] : OUI が音声トラフィックの識別に使用されて いるかどうかを表示します。
- [CoS/802.1p] : 音声トラフィックに割り当てる CoS キューを選択します。
- [CoS/802.1p のリマーク] : 出トラフィックをリマークするかどうかを選択します。
- [自動メンバシップエージングタイム] : ポートで検出された電話の MAC アドレスす べてが期限切れになった後、音声 VLAN からそのポートを削除するまでの遅延時間 を入力します。

ステップ 2 [Apply] をクリックして、デバイスの実行コンフィギュレーションをこれらの値で更新します。

テレフォニー OUI テーブルには次が表示されます。

- [テレフォニー OUI] : OUI 用に予約されている MAC アドレスの最初の 6 桁。
- [説明] : ユーザーが割り当てた OUI の説明。

ステップ 3 [Restore Default OUIs] をクリックすると、ユーザーが作成した OUI はすべて削除され、デフォルトの OUI のみがテーブルに残ります。OUI の情報は、復元が完了するまでは不正確な可能性があります。これには数秒かかることがあります。数秒が経過した後、このページを閉じて再度表示させると、ページが更新されます。

すべての OUI を削除するには、上部のチェックボックスをオンにします。すべての OUI が選択され、[Delete] をクリックすることで削除できます。その後、[Restore Default OUIs] をクリックすると、既知の OUI が復元されます。

ステップ 4 新しい OUI を追加する場合には、[Add] をクリックします。

ステップ 5 次のフィールドに値を入力します。

- [テレフォニー OUI] : 新しい OUI を入力します。
- [説明] : OUI 名を入力します。

ステップ 6 [Apply] をクリックします。OUI がテレフォニー OUI テーブルに追加されます。

電話機 OUI インターフェイス

QoS 属性は、次のいずれかのモードで、ポートごとに音声パケットに割り当てることができます。

- [すべて] : そのインターフェイスで受信され、音声 VLAN に分類されるすべての着 信フレームに、その音声 VLAN に設定されている Quality of Service（QoS）値が 適用されます。
- [Telephony Source MAC Address (SRC)] : 音声 VLAN に設定された QoS 値は、音声 VLAN へと分類されるすべての受信フレームに適用され、設定したテレフォニー OUI と一致する送信元 MAC アドレスの OUI が含まれます。

テレフォニー OUI インターフェイス ページを使用して、OUI 識別子に基づいて音声 VLAN にインターフェイスを追加し、音声 VLAN の OUI QoS モードを設定します。

インターフェイスでテレフォニー OUI を設定するには、次の手順を実行します。

ステップ 1 [VLAN Management] > [Voice VLAN] > [Telephony OUI Interface] をクリックします。

テレフォニー OUI インターフェイス ページには、すべてのインターフェイスの音声 VLAN OUI パラメータが表示されます。

ステップ 2 インターフェイスをテレフォニー OUI ベース音声 VLAN の候補ポートに設定するには、[Edit] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [インターフェイス] : インターフェイスを選択します。
- [テレフォニー OUI VLAN メンバシップ] : 有効にすると、インターフェイスは、テ レフォニー OUI ベースの音声 VLAN の候補ポートになります。設定されているテレフォニー OUI のいずれかと一致するパケットを受信すると、ポートは音声 VLAN に追加されます。
- [Voice VLAN QoS Mode]（メイン ページでは [Telephone OUI QoS Mode]）：次のオプションのいずれかを選択します。
  - [All] : QoS 属性は音声 VLAN へと分類されるすべてのパケットに適用されます。
  - [テレフォニー送信元 MAC アドレス] : IP 電話からのパケットのみに QoS 属性が 適用されます。

ステップ 4 [Apply] をクリックします。OUI が追加されます。

アクセスポートマルチキャストTV VLAN

マルチキャスト TV VLAN では、同じデータ VLAN（レイヤ 2 隔離）ではないサブスクライバに対して、サブスクライバ VLAN ごとにマルチキャスト伝送フレームを複製せずに、マルチキャスト伝送が行えます。

同じデータ VLAN（レイヤ 2 隔離）ではなく、異なる VLAN ID メンバーシップでデバイスに接続しているサブスクライバは、同じマルチキャスト VLAN ID へのポートに参加することで、同じマルチキャスト ストリームを共有できます。

マルチキャスト サーバに接続しているネットワーク ポートは、マルチキャスト VLAN ID のメンバーとして静的に設定されます。

サブスクライバが（IGMP メッセージの送信による）マルチキャスト サーバとの通信に使用するネットワーク ポートは、マルチキャスト パケット ヘッダーにマルチキャスト TV VLAN を含んだマルチキャスト ストリームを、マルチキャスト サーバから受信します。このため、ネットワーク ポートは静的に次のように設定する必要があります。

- ポートの種類はトランクまたは全般（「VLANインターフェイス設定 （164 ページ）」を参照）
- マルチキャスト TV VLAN のメンバー

アクセス ポートとして定義されている場合にのみ、サブスクライバの受信者ポートはマルチキャスト TV VLAN と関連付けることができます。

1 つまたは複数の IP マルチキャスト アドレスのグループを、同じマルチキャスト TV VLAN に関連付けることができます。

すべての VLAN がマルチキャスト TV VLAN として設定できます。マルチキャスト TV VLAN に割り当てられたポートは、次のようになります。

- マルチキャスト TV VLAN に参加します。
- マルチキャスト TV VLAN の出力ポートを通過するパケットは、タグなしです。
- ポートのフレームタイプパラメータは [Admit All] に設定され、タグなしパケットが許可されます（VLANインターフェイス設定 （164 ページ）を参照）。

マルチキャスト TV VLAN の設定は、ポートごとに定義されます。顧客ポートは、[Port Multicast VLAN Membership] ページを使用してマルチキャスト TV VLAN のメンバーに設定されます。

VLANに対するマルチキャストグループ

最大 256 組の IPv4 アドレス範囲がマルチキャスト TV VLAN にマッピングできます。範囲ごとに、マルチキャストアドレスの全範囲を設定できます。

（注） *は、関連するマルチキャストTV VLANが存在しなくなったため、対応するマルチキャストグループが非アクティブであることを示します。VLAN 設定 （163 ページ）に進んで、VLAN を作成します。

マルチキャスト TV VLAN 設定を定義するには、次の手順を実行します。

ステップ 1 [VLAN Management] > [Access Port Multicast TV VLAN] > [Multicast Group to VLAN] の順にクリックします。

ステップ 2 [Add] をクリックして、マルチ キャスト グループを VLAN に関連付けます。任意の VLAN が選択できます。

次のフィールドに入力します。

- [Multicast TV VLAN]：マルチキャストパケットの割り当て先 VLAN。ここで選択した VLAN がマルチキャスト TV VLAN になります。
- [Multicast Group Start]：マルチキャストグループ範囲の最初の IPv4 アドレス。
- [Group Definition]：次の範囲オプションのいずれかを選択します。

- [By group size]：グループ範囲に含まれるマルチキャストアドレスの数を指定します。
- [By range]：[Multicast Group Start] フィールド内のアドレスより大きい IPv4 マルチキャストアドレスを指定します。これが範囲内の最後のアドレスです。

ステップ 3 [Apply] をクリックします。マルチキャスト TV VLAN 設定が変更され、実行コンフィギュレーション ファイルに書き込まれます。

ポートマルチキャスト TV VLAN メンバーシップ

マルチキャスト TV VLAN の設定を定義するには、次の手順を実行します。

ステップ 1 **[VLAN Management]** > **[Access Port Multicast TV VLAN]** > **[Port Multicast VLAN Membership]** の順にクリックします。

ステップ 2 [マルチキャストTV VLAN] から VLAN を選択します。

ステップ 3 [Interface Type] からインターフェイスを選択します。

ステップ 4 [Candidate Access Ports] リストには、デバイスに設定されているすべてのアクセス ポートが含まれています。必要なポートを、[Member Access Ports] フィールドに移動します。

ステップ 5 [Apply] をクリックします。マルチキャスト TV VLAN 設定が変更され、実行コンフィギュレーション ファイルに書き込まれます。

カスタマーポートマルチキャストTV VLAN

トリプル プレイ サービスでは、1 つのブロードバンド接続で次の 3 つのブロード バンド サービスをプロビジョニングします。

- 高速なインターネット アクセス
- ビデオ
- 音声

トリプル プレイ サービスはサービス プロバイダーのサブスクライバに対してプロビジョニングされ、サブスクライバはレイヤ 2 での分離が維持されます。

各サブスクライバには、CPE MUX ボックスがあります。MUX には、サブスクライバのデバイス（PC、電話機など）に接続されている複数のアクセス ポートと、アクセス デバイスに接続されている 1 つのネットワーク ポートがあります。

ボックスは、パケットの VLAN タグに基づいて、パケットをネットワーク ポートからサブスクライバのデバイスに転送します。各 VLAN は MUX アクセス ポートのいずれかにマッピングされています。

サブスクライバからサービス プロバイダー ネットワークへのパケットは、サービスの種類を区別するために、VLANタグ付きフレームとして転送されます。つまり、各サービスの種類に対して一意の VLAN ID が CPE ボックスにあります。

サブスクライバからサービスプロバイダーネットワークへのすべてのパケットは、顧客VLANとして設定されているサブスクライバの VLAN を使用してアクセス デバイスによりカプセル化されます（外部タグまたは S-VID）。ただし、マルチキャスト TV VLAN に関連付けられている TV 受信者からの IGMP スヌーピング メッセージは除きます。TV 受信者からも送信される VOD 情報は、その他の種類のトラフィックと同様にして送信されます。

ネットワーク ポートでパケットを受信したサービス プロバイダー ネットワークからサブスクライバへのパケットは、サービス プロバイダー ネットワークで二重タグ パケットとして送信されます。外部タグ（サービス タグまたは S タグ）は、次のようにして、2 種類の VLAN の 1 つを置き換えます。

- サブスクライバの VLAN（インターネットと IP フォンを含む）
- マルチキャスト TV VLAN

内部 VLAN（C タグ）は、サブスクライバのネットワークでの宛先を決定するために（CPE MUX により）使用されるタグです。

VLANへのCPE VLAN

サブスクライバの VLAN を使用して CPE MUX をサポートする場合に、複数のビデオ プロバイダーが必要になることがあります。各プロバイダーには異なる外部 VLAN が割り当てられます。

CPE（内部）マルチキャスト VLAN は、マルチキャスト プロバイダー（外部）VLAN にマッピングする必要があります。

CPE VLAN をマルチキャスト VLAN にマッピングすると、IGMP スヌーピングに参加できます。

CPE VLAN をマッピングするには、次の手順を実行します。

ステップ 1 [VLAN Management] > **[Customer Port Multicast TV VLAN]** > **[CPE VLAN to VLAN]** をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [CPE VLAN]：CPE ボックスで定義した VLAN を入力します。
- [Multicast TV VLAN]：CPE VLAN にマッピングするマルチキャスト TV VLAN を選択します。

ステップ 4 [Apply] をクリックします。CPE VLAN マッピングが変更され、実行コンフィギュレーション ファイルに書き込まれます。

ポートマルチキャストVLANメンバシップ

マルチキャスト VLAN が関連付けられているポートは、顧客ポートとして設定する必要があります（「VLANインターフェイス設定 （164 ページ）」を参照）。

ポートをマルチキャスト TV VLAN にマッピングするには、次の手順を実行します。

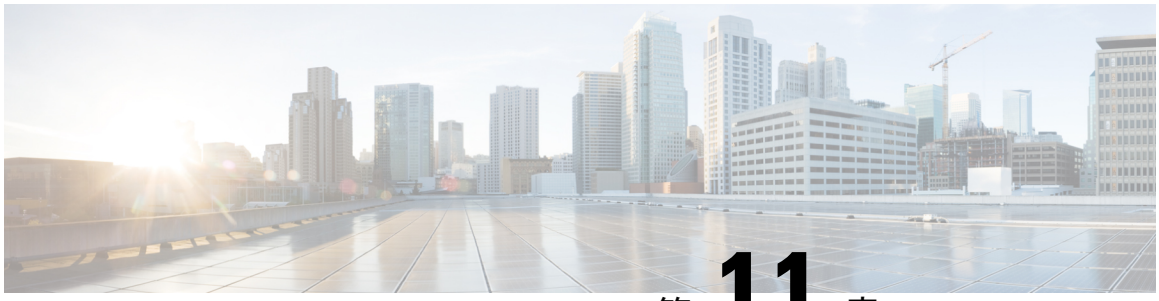
ステップ 1 [VLAN Management] > **[Customer Port Multicast TV VLAN]** > **[Port Multicast VLAN Membership]** の順にクリックします。

ステップ 2 [マルチキャストTV VLAN] から VLAN を選択します。

ステップ 3 [Interface Type] からインターフェイスを選択します。

ステップ 4 [Candidate Customer Ports] リストには、デバイスに設定されているすべてのアクセス ポートが含まれています。必要なポートを、[Member Customer Ports] フィールドに移動します。

ステップ 5 [Apply] をクリックします。新しい設定が変更され、実行コンフィギュレーション ファイルに書き込まれます.



第 11 章

スパニングツリー

この章は、次の項で構成されています。

STP 状態およびグローバル設定

スパニングツリープロトコル（STP）は、リンクを選択的にスタンバイモードに設定してループを回避することで、レイヤ2のブロードキャストドメインをブロードキャストストームから保護します。スタンバイ モードでは、これらのリンクがユーザ データの転送を一時的に停止します。データ転送が可能になるようにトポロジが変更された後、リンクが自動的に再度有効化されます。

STPは、ネットワーク上のエンドステーション間に一意のパスを作成し、それによってループをなくすことで、スイッチと相互接続リンクの配置においてツリー トポロジを提供します。

[STPステータス&グローバル設定]ページには、必要なSTPモードを有効にするためのパラメータが含まれています。それぞれ、[STP Interface Settings] ページ、[RSTP Interface Settings] ページ、[MSTP Properties] ページを使用します。STP のステータスとグローバル設定を設定するには、次の手順を実行します。

ステップ 1 [Spanning Tree] > [STP Status & Global Settings] をクリックします。

ステップ 2 パラメータを入力します。

グローバル設定（Global Settings）：

スパニングツリー状態	選択すると、デバイスで有効になります。
STPループバックガード	選択すると、デバイスでループバックガードが有効になります。

STP動作モード	STP モードを選択します。
BPDU の処理	STPが無効になっている場合のブリッジプロトコルデータユニット（BPDU）パケットの管理方法を選択します。BPDUは、スパニングツリー情報を送信するために使用されます。 • [Filtering]：インターフェイスでスパニングツリーが無効になっている場合に BPDU パケットをフィルタ処理します。 • [Flooding]：インターフェイスでスパニングツリーが無効になっている場合に BPDU パケットをフラッディングします。
パスコストデフォルト値	STPポートにデフォルトパスコストを割り当てる際に使用する方法を選択します。インターフェイスに指定されるデフォルトのパスコストは、選択した方法に応じて異なります。 • [Short]：ポートのパスコストとして 1 ～ 65,535 の範囲の値を入力します。 • [Long]：ポートのパスコストとして 1 ～ 200,000,000 の範囲の値を入力します。 ブリッジ設定（Bridge Settings）：

ブリッジ設定（Bridge Settings）：

Priority	ブリッジプライオリティ値を入力します。BPDUを交換した後、最低優先順位のデバイスがルートブリッジになります。すべてブリッジが同じ優先順位を使用している場合は、ルートブリッジを決定するために、それらのMACアドレスが使用されます。ブリッジの優先順位値は、4096 の増分単位で提供されます。たとえば、4096、8192、12288 などとなります。
Hello タイム	ルートブリッジが設定メッセージを待機する時間間隔を秒数で入力します。
最大経過時間	このデバイスが設定メッセージを待機する時間を秒数で入力します。この時間内に設定メッセージが届かない場合、デバイス自体の設定情報が再定義されます。
転送遅延	ブリッジがラーニングステートを維持する時間を秒数で入力します。この時間を過ぎると、ブリッジからパケットが転送されます。詳細については、STPインターフェイス設定 （191 ページ） を参照してください。
代表ルート/ブリッジ ID	このデバイスのブリッジプライオリティ値と MAC アドレスを結合した値。
ルートブリッジID	ルートブリッジのプライオリティ値と MAC アドレスを結合した値。
Root Port	このブリッジからルートブリッジへの最小のコストパスを提供するポート。
Root Path Cost	このブリッジからルートまでのパスのコスト。
トポロジ変更回数	STP トポロジが今までに変更された回数。

最後のトポロジ変更からの経過時間	最後にトポロジが変更されてからの経過時間。時間は、日/時間/分/秒の形式で表示されます。

ステップ 3 [Apply] をクリックします。STP グローバル設定は、実行コンフィギュレーション ファイルに書き込まれます。

STP インターフェイス設定

[STP Interface Settings] ページでは、ポート単位で STP を設定したり、代表ブリッジなどのプロトコルによって学習された情報を表示したりすることができます。

入力された定義済みの設定は、STP プロトコルのすべての派生版で有効です。

インターフェイスで STP を設定するには、次の手順を実行します。

ステップ 1 [Spanning Tree] > [STP Interface Settings] をクリックします。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ステップ 3 パラメータを入力します。

Interface	スパニングツリーを設定するポートまたは LAG を選択します。
STP	このポートに対して STP を有効または無効にします。
エッジ ポート	このポートに対してファストリンクを有効または無効にします。ポートで高速リンク モードが有効な場合、ポート リンクがアップすると、ポートは自動的にフォワーディング ステートに設定されます。高速リンクは、STP プロトコルのコンバージェンスを最適化します。次のオプションがあります。 • [Enable]：ファストリンクをすぐに有効にします。 • 自動（Auto）：インターフェイスがアクティブになった数秒後に、高速リンクを有効にします。この場合、ファストリンクが有効になる前にループが解消されます。 • [Disable]：ファストリンクを無効にします。 （注） 値を [Auto] に設定することを推奨します。このようにすると、このデバイスにホストが接続されたときにポートがファストリンクモードに設定され、別のデバイスに接続されたときには通常の STP ポートとして設定されます。これによって、ループを回避できます。エッジポートは MSTP モードでは動作しません。

ルート ガード	ルート ガード（Root Guard）：デバイス上のルート ガードを有効または無効にします。ルートガードオプションにより、ネットワークのルートブリッジの配置を適用できるようになります。 ルート ガードは、この機能が有効なポートが指定ポートになるように保証します。通常、ルートブリッジの2個以上のポートが接続されていない限り、すべてのルート ブリッジが指定ポートです。ブリッジが、ルート ガードが有効なポートで上位 BPDU を受信すると、ルート ガードはこのポートをルート不整合 STP 状態に移行します。このルート不整合状態は、実質的にはリスニング ステートと同じです。トラフィックはこのポートを介して転送されません。このようにして、ルート ガードはルート ブリッジを強制的に配置します。
BPDU ガード	BPDU ガード（BPDU Guard）：ポートの Bridge protocol data unit（BPDU）Guard を有効または無効にします。 BPDU Guard を使用すると、STP ドメインの境界を強化し、アクティブなトポロジを予測可能な状態に保つことができます。BPDU ガードが有効になっているポートの背後にあるデバイスは、STP トポロジに影響を与えることはありません。BPDU を受信すると、BPDU Guard の動作によって BPDU が設定されたポートは無効になります。この場合、BPDU メッセージが受信され、適切な SNMP トラップが生成されます。
BPDU の処理	ポート上またはデバイス上で STP が無効になっている場合の BPDU パケットの処理方法を選択します。BPDU は、スパニング ツリー情報を送信するために使用されます。 • [Use Global Settings]：STP 状態およびグローバル設定 （189 ページ）で定義した設定を使用する場合に選択します。 • フィルタリング（Filtering）：インターフェイスでスパニング ツリーが無効な場合、BPDU パケットをフィルタ処理します。 • フラッディング（Flooding）：インターフェイスでスパニング ツリーが無効な場合、BPDU パケットをフラッドします。
Path Cost	ルートパスコストにおけるこのポートのコストを入力するか、または、このシステムによって生成されたデフォルトのコストを使用します。
Priority	このポートのプライオリティ値を設定します。優先順位値は、ブリッジにループ内で接続された2個のポートがある場合に、ポートの選択に影響します。プライオリティ値は 0 ～ 240 で 16 の倍数である必要があります。

Port State	このポートの現在の STP 状態が表示されます。 • [無効]：このポートに対して STP は現在無効になっています。ポートは、MAC アドレスを学習しながら、トラフィックを転送します。 • [Blocking]：このポートは現在ブロックされており、BPDUデータ以外のトラフィックを転送したり、MAC アドレスを学習したりすることはできません。 • [リスニング]：このポートはリスニングモードになっています。ポートはトラフィックを転送できず、MAC アドレスを学習できません。 • [ラーニング]：このポートは学習モードになっています。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]：このポートはフォワーディングモードになっています。ポートはトラフィックを転送でき、新しい MAC アドレスを学習することもできます。
Designated Bridge ID	代表ブリッジのブリッジプライオリティ値と MAC アドレスが表示されます。
指定ポートID	選択したポートのプライオリティ値とインターフェイスが表示されます。
Designated Cost	STP トポロジに属しているポートのコストが表示されます。STP がループを検出した場合、低コストのポートがブロックされることはほとんどありません。
フォワーディングへの移行	このポートがブロッキング状態からフォワーディング状態に移行した回数が表示されます。
Speed	このポートの速度が表示されます。
LAG	このポートが所属している LAG が表示されます。ポートが LAG のメンバーである場合、LAG 設定はポート設定をオーバーライドします。

ステップ 4 [Apply] をクリックします。インターフェイス設定は、実行コンフィギュレーション ファイルに書き込まれます。

RSTPインターフェイス設定

Rapid Spanning Tree Protocol（RSTP）では、転送ループを作成することなく、より高速な STP コンバージェンスが可能となります。

[RSTP Interface Settings] ページでは、ポートごとに RSTP を設定できます。このページで設定した情報は、グローバル STP モードが RSTP に設定されている場合に有効になります。

RSTP 設定を入力するには、次の手順を実行します。

ステップ 1 [Spanning Tree] > [STP Status and Global Settings] をクリックします。

ステップ 2 [RSTP] を有効にします。

ステップ 3 [Spanning Tree] > [RSTP Interface Settings] をクリックします。[RSTP Interface Settings] ページが表示されます。

ステップ 4 ポートを選択します。

（注） [Activate Protocol Migration] は、テストされているブリッジ パートナーに接続されたポートを選択した後にのみ使用可能となります。

ステップ 5 STP を使用して、リンク パートナーが検出されたら、[Activate Protocol Migration] をクリックして、プロトコル移行テストを実行します。これは、STP を使用しているリンク パートナーが引き続き存在しているかどうか、存在する場合に、それが RSTP または MSTP へ移行したかどうかを検出します。引き続き STP リンクが存在している場合、デバイスは STP を使用して通信を継続します。STP リンクが存在せず、RSTP または MSTP に移行している場合は、デバイスはそれぞれ RSTP または MSTP を使用して通信します。

ステップ 6 インターフェイスを選択して、[Edit] をクリックします。

ステップ 7 パラメータを入力します。

Interface	インターフェイスを設定し、RSTP を設定するポートまたは LAG を指定します。
ポイントツーポイント管理ステータス	ポイントツーポイントリンクのステータスを定義します。全二重として定義されているポートは、ポイントツーポイント ポート リンクと見なされます。 • [Enabled]：RSTP が有効になっている場合、このポートは RSTP エッジポートになり、通常 2 秒以内にフォワーディングモードに移行します。 • [Disabled]：このポートは、RSTP のためのポイントツーポイントとは見なされません。つまり、このポート上では、STP は高速ではなく通常速度で動作します。 • [Auto]：RSTP BPDU を使用して、デバイスのステータスを自動的に決定します。
ポイントツーポイント動作ステータス	[Point to Point Administrative Status] フィールドで [Auto] を選択した場合、ポイントツーポイントリンクの動作ステータスが表示されます。

ロール	STP パスを構成するために、STP によってこのポートに割り当てられているロールが表示されます。ロールには次のものがあります。 • [Root]：パケットをルートブリッジに転送するためのコストパスが最も低いロール。 • [Designated]：このブリッジを LAN に接続するためのインターフェイス。LAN からルートブリッジまでのコストパスが最小です。 • [Alternate]：ルートポートからルートブリッジへの代替パスに使用されます。 • [Backup]：スパニングツリーのリーフへの指定ポートパスに対するバックアップパスに使用されます。これは、ポイントツーポイントリンクによって、ループ内で2個のポートが接続されている構成を提供します。バックアップ ポートは、LAN に共有セグメントへの 2 つ以上の確立された接続がある場合にも使用されます。 • [Disabled]：このポートはスパニングツリーに属していません。
モード	現在のスパニングツリーモード（従来の STP または RSTP）が表示されます。
ファストリンク動作ステータス	このインターフェイスに対するファストリンク（エッジポート）のステータス（有効、無効、または自動）が表示されます。値は次のとおりです。 • [Enabled]：ファストリンクが有効になっています。 • [Disabled]：ファストリンクが無効になっています。 • [Auto]：このインターフェイスがアクティブになってから数秒後に、ファストリンクモードが有効になります。
Port Status	特定のポートの RSTP ステータスが表示されます。 • [Disabled]：このポートに対して STP は現在無効になっています。 • [Discarding]：このポートは現在廃棄/ブロックされており、トラフィックを転送したり、MAC アドレスを学習したりすることはできません。 • [Listening]：このポートはリスニングモードになっています。ポートはトラフィックを転送できず、MAC アドレスを学習することもできません。 • [Learning]：このポートは学習モードになっています。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。 • [Forwarding]：このポートはフォワーディングモードになっています。ポートはトラフィックを転送でき、新しい MAC アドレスを学習することもできます。

ステップ 8 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

MSTP

Multiple Spanning Tree Protocol（MSTP）は、複数の異なる VLAN 上のさまざまなドメインの間のスパニングツリープロトコル（STP）ポートの状態を分離するために使用されます。たとえば、ポート A を VLAN A のループのために 1 つの STP インスタンス内でブロックする一方、同じポートを別の STP インスタンスでフォワーディング ステートにすることができます。[MSTP Properties] ページでは、グローバル MSTP 設定を定義できます。

多重 STP（MSTP）：MSTP は RSTP に基づきます。レイヤ 2 ループを検出し、それに関与するポートがトラフィックを伝送するのを防ぐことで、軽減を試みます。ループはレイヤ2 ドメイン単位で存在するため、STP ループをなくすためにポートがブロックされると、その状況が発生することがあります。トラフィックはブロックされていないポートに転送され、ブロックされているポートにはトラフィックは転送されません。これは、ブロックされたポートが常に未使用となるため、帯域幅の効率的な使用方法ではありません。MSTP は、各 STP インスタンスで個別にループを検出し、軽減できるように、いくつかの STP インスタンスを有効化することで、この問題を解決します。これにより、1 個のポートを 1 つまたは複数の STP インスタンスに対してブロックし、その他の STP インスタンスに対してはブロックしないように指定できます。異なる VLAN が異なる STP インスタンスに関連付けられている場合、それらのトラフィックは関連付けられた MST インスタンスの STP ポートの状態に基づいてリレーされます。結果として、帯域幅利用が改善されます。

MSTPプロパティ

グローバル MSTP は、VLAN グループごとに個別のスパニング ツリーを設定し、各スパニング ツリー インスタンス内で候補となる代替パスの 1 つを除き、すべての代替パスをブロックします。MSTP では、複数の MST インスタンス（MSTI）を実行できる MST リージョンを形成できます。複数のリージョンとその他の STP ブリッジは、単一の Common Spanning Tree（CST）を使用して相互接続されます。

MSTP は RSTP ブリッジと互換性があり、RSTP ブリッジにより MSTP BPDU は RSTP BPDU として解釈されます。これにより、設定を変更することなく、RSTP ブリッジとの互換性が有効となるだけでなく、リージョン自体の内部の MSTP ブリッジの数に関係なく、MSTP リージョン外部の RSTP ブリッジは、リージョンを単一の RSTP ブリッジとして見なすようになります。複数のスイッチを同じ MST リージョンに配置するには、それらのスイッチで VLAN から MST インスタンスへのマッピング、設定リビジョン番号、およびリージョン名が同じである必要があります。同じ MST リージョン内に配置するスイッチは、別の MST リージョンのスイッチによって分離されることはありません。それらが分離されている場合、リージョンは 2 つの個別のリージョンになります。

このマッピングは、MSTPインスタンス設定 （197 ページ）で実行できます。このページは、システムが MSTP モードで動作している場合に使用します。

MSTP を定義するには、次の手順を実行します。

ステップ 1 [Spanning Tree] > [MSTP] > [MSTP Properties] の順にクリックします。

ステップ 2 パラメータを入力します。

- リージョン名（Region Name）：MSTP リージョン名を定義します。
- リビジョン（Revision）：現在の MST 設定のリビジョンを表す、符号なし 16 ビット数を定義します。このフィールド値の範囲は 0 ～ 65535 です。
- 最大ホップ（Max Hops）：BPDU を破棄する前に、特定のリージョンで発生するホップの合計数を設定します。BPDU を破棄すると、ポート情報は陳腐化します。このフィールド値の範囲は 0 ～ 40 です。
- [IST Active]：アクティブリージョンが表示されます。

ステップ 3 [Apply] をクリックします。MSTP プロパティが定義され、実行コンフィギュレーション ファイルが更新されます。

MSTPインスタンス設定

[MSTPインスタンス設定] ページでは、MST インスタンスごとにパラメータを設定して表示できます。これは、インスタンス単位で [STP Status and Global Settings] を設定するのと同じです。

MSTP インスタンスの設定を入力するには、次の手順を実行します。

ステップ 1 [Spanning Tree] > [MSTP] > [MSTP Instance Settings] の順にクリックします。

ステップ 2 パラメータを入力します。

- [Instance ID]：表示および定義する MST インスタンスを選択します。
- [Included VLAN]：選択したインスタンスにマッピングされた VLAN が表示されます。デフォルト マッピングでは、すべての VLAN が Common and Internal Spanning-Tree（CIST）インスタンス 0 にマッピングされます。
- [Bridge Priority]：選択された MST インスタンスに対するこのブリッジの優先順位を設定します。
- [Designated Root Bridge ID]：MST インスタンスに対するルートブリッジの優先順位と MAC アドレスが表示されます。
- [Root Port]：選択したインスタンスのルートポートが表示されます。
- [Root Path Cost]：選択したインスタンスのルートパスコストが表示されます。
- [Bridge ID]：選択されたインスタンスにおけるこのデバイスのブリッジ優先順位と MAC アドレスが表示されます。
- [Remaining Hops]：次の宛先までの残りのホップ数が表示されます。

ステップ 3 [Apply] をクリックします。MST インスタンスの設定が定義され、実行コンフィギュレーション ファイルが更新されます。

MSTPインターフェイス設定

[MSTPインターフェイス設定]ページでは、すべてのMSTインスタンスに対してポートのMSTP設定を行い、MST インスタンス単位の代表ブリッジなど、プロトコルによって現在学習されている情報を表示できます。

MST インスタンスでポートを設定するには、次の手順を実行します。

ステップ 1 [Spanning Tree] > [MSTP] > [MSTP Interface Settings] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インスタンスが次に等しい]：設定する MSTP インスタンスを選択します。
- 次に等しいインターフェイス タイプ（Interface Type equals to）：ポートまたは LAG のいずれのリストを表示するかどうかを選択します。

ステップ 3 [Go] をクリックします。インスタンス上のインターフェイスの MSTP パラメータが表示されます。

ステップ 4 インターフェイスを選択して、[Edit] をクリックします。

ステップ 5 パラメータを入力します。

オプション	説明
インスタンス ID（Instance ID）	設定する MST インスタンスを選択します。
Interface	MSTI 設定を定義するインターフェイスを選択します。
インターフェイス プライオリティ（Interface Priority）	指定されたインターフェイスと MST インスタンスのポートの優先順位を設定します。
Path Cost	[User Defined] テキストボックスのルートパスコストにポートのコントリビューションを入力するか、[Use Default] を選択してデフォルト値を使用します。
Port State	特定の MST インスタンス上の特定のポートの MSTP ステータスが表示されます。パラメータは次のように定義されます。 • [Disabled]：STP は現在無効です。 • [廃棄]：このインスタンスのポートは現在廃棄/ブロックされており、BPDU データ以外のトラフィックを転送したり、MAC アドレスを学習したりすることはできません。

オプション	説明
	• リスニング（Listening）：このインスタンスのポートはリスニングモードになります。ポートはトラフィックを転送できず、MAC アドレスを学習することもできません。 • 学習（Learning）：このインスタンスのポートは学習モードになります。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。 • 転送（Forwarding）：このインスタンスのポートは転送モードになります。ポートはトラフィックを転送でき、新しい MAC アドレスを学習することもできます。 • [境界]：このインスタンスのポートは境界ポートになっています。このポートは、インスタンス 0 から状態を継承し、STP インターフェイス設定 （191 ページ）で確認できます。
ポート ロール（Port Role）	STP パスを提供するために MSTP アルゴリズムによって割り当てられた、ポートまたは LAG 単位のインスタンスごとのポートまたは LAG のロールが表示されます。 • ルート（Root）：このインターフェイスを介したパケット転送は、ルートデバイスへのパケットの転送の中で最も低コストなパスとなります。 • 指定ポート（Designated Port）：ブリッジが LAN に接続される際に経由するインターフェイス。LAN から MST インスタンスのルート ブリッジへの最も低コストのルート パスを提供します。 • 代替（Alternate）：インターフェイスは、ルート ポートからルート ブリッジへの代替パスを提供します。 • バックアップ（Backup）：インターフェイスは、スパニング ツリーのリーフに向かう指定ポート パスへのバックアップ パスを提供します。バックアップ ポートは、ポイントツーポイント リンクによって、ループ内で 2 つのポートが接続されているときに発生します。バックアップ ポートは、LAN に共有セグメントへの 2 つ以上の確立された接続がある場合にも発生します。 • 無効（Disable）：インターフェイスは、スパニング ツリーに参加しません。 • [境界]：このインスタンスのポートは境界ポートになっています。このポートは、インスタンス 0 から状態を継承し、STP インターフェイス設定 （191 ページ）で確認できます。
モード	現在のインターフェイス スパニング ツリー モードが表示されます。 • リンク パートナーが MSTP または RSTP を使用している場合、表示されるポート モードは RSTP です。 • リンク パートナーが STP を使用している場合、表示されるポート モードは STP です。

オプション	説明
Type	ポートの MST タイプが表示されます。 • 境界（Boundary）：境界ポートがリモート リージョン内の LAN に MST ブリッジを接続します。ポートが境界ポートである場合は、リンクの他端のデバイスが RSTP または STP のどちらのモードで動作しているかも示されます。 • 内部（Internal）：ポートは内部ポートです。
Designated Bridge ID	リンクまたは共有 LAN をルートに接続するブリッジの ID 番号が表示されます。
指定ポートID	リンクまたは共有 LAN をルートに接続する代表ブリッジのポート ID 番号が表示されます。
Designated Cost	STP トポロジに属しているポートのコストが表示されます。STP がループを検出した場合、低コストのポートがブロックされることはほとんどありません。
残存ホップ	次の宛先までの残りのホップ数が表示されます。
フォワーディングへの移行	このポートがフォワーディングステートから廃棄ステートに変更された回数が表示されます。

ステップ 6 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

MSTP インスタンスへの VLAN

[VLAN to MSTP Instance] ページでは、各 VLAN をマルチ スパニング ツリー インスタンス（MSTI）にマッピングできます。同じリージョン内に存在するデバイスの場合は、VLAN と MSTI 間のマッピングを同一にする必要があります。

（注） 同じ MSTI を複数の VLAN にマップできますが、各 VLAN には 1 つの MST インスタンスしかアタッチできません。このページ（およびすべての MSTP ページ）の設定は、システム STP モードが MSTP の場合に適用されます。インスタンス 0 に加え、最大 16 の MST インスタンスを定義できます。MST インスタンスの 1 つに明示的にマッピングされていない VLAN では、デバイスが CIST（Core and Internal Spanning Tree）インスタンスに自動的にマッピングされます。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には、次の手順を実行します。

ステップ 1 [Spanning Tree] > [MSTP] > [VLAN to MSTP Instance] の順にクリックします。

[VLAN to MSTP Instance] ページには、次のフィールドが表示されます。

- [MSTP Instance ID]：すべての MST インスタンスが表示されます。
- [VLAN]：MST インスタンスに属するすべての VLAN が表示されます。

ステップ 2 MSTP インスタンスに VLAN を追加するには、MST インスタンスを選択し、[Edit] をクリックします。

ステップ 3 パラメータを入力します。

- [MSTP Instance 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 を定義します。
- [Action]：VLAN を MST インスタンスに追加（マッピング）するか、削除するかを定義します。

ステップ 4 [Apply] をクリックします。MSTP VLAN マッピングが定義され、実行コンフィギュレーション ファイルが更新されます。

PVST

Per VLAN Spanning Tree（PVST）は、デバイス上で設定された VLAN ごとに 802.1Q STP 標準プロトコルの個別インスタンスを実行するプロトコルです。デバイス上で設定された VLAN ごとの RSTP 標準プロトコルです。PVST プロトコルは、STP/RSTP 標準ベースの実装に存在する問題への対応策として設計されたプロトコルです。つまり、（複数の VLAN に対して）ブロッキングモードになっているポートはトラフィック転送に一切使用できないため、場合によっては帯域幅を効率的に使用できないことがあるという問題です。

PVST は、デバイス上で設定された各 VLAN 向けに個別のスパニング ツリー インスタンスを割り当てることによって、この問題に対処します。サポートされる PVST インスタンスの数は最大で 126 です。したがって、デバイス上で設定される VLAN の数が 126 を超えた場合、PVST を有効にすることはできません。同様に、PVST を有効にする場合は、126 を超える VLAN を設定することはできません。

デバイスは、プロトコルの PVST/RPVST Plus フレーバをサポートします。この項で PVST と述べた場合、PVST+ と RPVST+ の両方の機能動作を意味しています。

PVST VLANの設定

PVST VLAN 設定を定義するには、次の手順を実行します。

ステップ 1 [Spanning Tree] > [PVST] > [PVST VLAN Settings] の順にクリックします。

[PVST VLANの設定] ページでは、デバイス上で設定されている各 VLAN ID の PVST の設定を構成することができます（ただし VLAN ID 1 は除きます）。

インターフェイスの PVST パラメータを設定するには、次のようにします。

ステップ 2 表内の行を選択し、[設定のコピー]をクリックして、選択した行に基づく新規PVST VLANを作成します。あるいは、[編集] をクリックして、選択した行を修正します。

（注） VLAN エントリ 1 は編集できません。必要に応じて PVST VLAN の値を編集します。

- [VLAN ID]：PVST インスタンスの VLAN ID。
- [プライオリティ]：PVST VLAN STP のプライオリティ値。
- [Address]：VLAN のアドレス
- [ハロータイム]：ルート ブリッジが設定メッセージを待機する時間間隔（秒単位）。
- [最大経過時間]：この VLAN STP インスタンスが設定メッセージを待機する時間間隔（秒単位）。この時間内に設定メッセージが届かない場合、インスタンス自体の設定情報が再定義されます。
- [転送遅延]：この VLAN STP インスタンスがラーニング ステートを維持する時間間隔（秒単位）。この時間を過ぎると、インスタンスからパケットが転送されます。

ステップ 3 [Details] をクリックすると、PVST VLAN の詳細が表示されます。

- [VLAN ID]：PVST インスタンスの VLAN ID。
- [Root Priority]：PVST VLAN STP の優先順位値。
- [Root Hello Time]：ルートブリッジが設定メッセージを待機する時間間隔（秒単位）。
- [Root Max Age]：この VLAN STP インスタンスが設定メッセージを待機する時間間隔（秒単位）。この時間内に設定メッセージが届かない場合、インスタンス自体の設定情報が再定義されます。
- [Root Forward Delay]：この VLAN STP インスタンスがラーニングステートを維持する時間間隔（秒単位）。この時間を過ぎると、インスタンスからパケットが転送されます。
- [Root Port]：このブリッジからルートへの最小のコストパスを提供するポート。
- [Root Path Cost]：このブリッジからルートまでの VLAN におけるパスコスト。
- [Root Bridge ID]：この VLAN のルートブリッジの ID。
- [Bridge ID]：このデバイスと VLAN のブリッジ ID。
- [Topology Change Count]：この VLAN のトポロジが最後に変更されるまでの間に、STP トポロジが変更された回数。
- [Last Topology Change]：トポロジが最後に変更された日時の詳細。

ステップ 4 [Apply] をクリックします。新規/修正済み PVST VLAN が追加/更新されます。

PVSTインターフェイスの設定

[PVSTインターフェイス設定] ページでは、PVST をポート単位および VLAN ベースで設定したり、代表ブリッジなどのプロトコルによって学習された情報を表示したりできます。

インターフェイスで PVST パラメータを設定するには、次の手順を実行します。

ステップ 1 [Spanning Tree] > [PVST] > [PVST Interface Settings] の順にクリックします。

ステップ 2 フィルタを使用して、ドロップダウンリストから [VLAN ID] と [Interface Type]（[Port] または [LAG]）を選択し、[Go] をクリックします。各 VLAN PVST に関する次の PVST インターフェイス情報が表示されます。

オプション	説明
Interface	インターフェイス名。
Priority	この VLAN インスタンスのポートの優先順位値。優先順位値は、ブリッジにループ内で接続された 2 個のポートがある場合に、ポートの選択に影響します。プライオリティ値は 0 ～ 240 で 16 の倍数である必要があります。
ポート コスト	ルートパスコストにおける VLAN インスタンスごとのポートコントリビューションを入力するか、またはシステムによって生成されたデフォルトのコストを使用します。
状態	ポートの現在の STP 状態が VLAN インスタンスごとに表示されます。 • [Disabled]：ポートの PVST は現在無効になっています。ポートは、MAC アドレスを学習しながら、トラフィックを転送します。 • [Blocking]：この VLAN インスタンスのポートはブロックされていて、BPDU データ以外のトラフィックを転送したり、MAC アドレスを学習したりできません。 • [リスニング]：この VLAN インスタンスでは、ポートはリスニング モードになっています。ポートはトラフィックを転送できず、MAC アドレスを学習できません。 • [ラーニング]：この VLAN インスタンスでは、ポートは学習モードになっています。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。 • [転送]：この VLAN インスタンスでは、ポートは転送状態になっています。ポートはトラフィックを転送でき、新しい MAC アドレスを学習することもできます。
ロール	STP パスを提供するために PVST アルゴリズムによって割り当てられた、PVST インスタンスごとの PVST ロールが表示されます。 • ルート（Root）：このインターフェイスを介したパケット転送は、ルートデバイスへのパケットの転送の中で最も低コストなパスとなります。 • [指定]：このブリッジを LAN に接続するためのインターフェイス。PVST インスタンスに対する LAN からルート ブリッジまでのルート コスト パスが最小です。

オプション	説明
	• 代替（Alternate）：インターフェイスは、ルートインターフェイスからルートデバイスへの代替パスを提供します。 • バックアップ（Backup）：インターフェイスは、スパニングツリーのリーフに向かう指定ポート パスへのバックアップ パスを提供します。バックアップ ポートは、ポイントツーポイントリンクによって、ループ内で2つのポートが接続されているときに発生します。バックアップ ポートは、LAN に共有セグメントへの 2 つ以上の確立された接続がある場合にも発生します。 • [Disabled]：インターフェイスはスパニングツリーに属していません。
モード	PVST モードが表示されます。 • [RPVST]：ポートで RPVST+ フレーバの PVST が実行されています。 • [PVST]：ポートで PVST+ フレーバの PVST が実行されています。
不整合	不一致が表示されます。
Designated Bridge ID	現在の VLAN インスタンスのブリッジ優先順位と代表ブリッジの MAC アドレスが表示されます。
指定ポートID	現在のVLANインスタンスについて、選択したポートの優先順位とインターフェイスが表示されます。
Designated Cost	現在のVLANインスタンスについて、STPトポロジに属しているポートのコストが表示されます。コストが小さいポートは、STP でループが検出されたときにブロックされる可能性が低くなります。
フォワーディングへの移行	現在の VLAN インスタンスについて、ポートがブロッキングステートからフォワーディングステートに変更された回数が表示されます。

ステップ 3 インターフェイスを選択し、[編集] をクリックして、選択した VLAN の [インターフェイスタイプ]、[プライオリティ]、または [パスコスト] を編集します。

選択したポートのコンフィギュレーション設定を、現在のVLAN内の別ポートにコピーするには、[設定をポートにコピー...] をクリックします。

ポートのコンフィギュレーション設定を、他の一連の VLAN 内の同一ポートにコピーするには、[Copy Settings to VLANs...] をクリックします。.

ステップ 4 パラメータを入力します。

ステップ 5 [Apply] をクリックします。インターフェイス設定は、実行コンフィギュレーション ファイルに書き込まれます。

ステップ 6 [Apply to all existing VLANs] をクリックして、スイッチに作成されたすべての VLAN に設定を適用します。

PVST不整合ポート

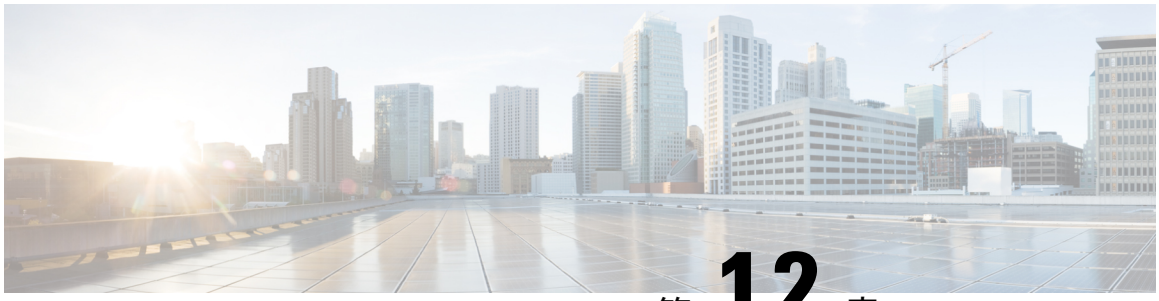
[PVST不整合ポート] ページには、不整合の PVST ポートが表示されます。

不整合の PVST ポートを表示するには、次の手順を実行します。

[Spanning Tree] > [PVST] > [PVST Inconsistent Ports] の順にクリックします。

このページには、PVST 不整合状態にあるポートの詳細が表示されます。

- [VLAN ID]：PVST インスタンスの VLAN ID。
- [Interface Name]：インターフェイスの ID。
- [不整合]：不整合状態が表示されます。



第 12 章

MAC アドレス テーブル

この章は、次の項で構成されています。

スタティック アドレス

スタティック MAC アドレスは、デバイスの特定の物理インターフェイスと VLAN に割り当てられます。スタティック MAC アドレスが別のインターフェイスで検出された場合、そのアドレスは無視され、アドレステーブルには書き込まれません。

スタティックアドレスを定義するには、次の手順を実行します。

ステップ 1 [MAC Address Tables] > [Static Addresses] の順にクリックします。

[スタティックアドレス] ページには、現在定義されているスタティック アドレスが含まれます。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [VLAN ID]：ポートに対して VLAN ID を選択します。
- [MAC アドレス]：インターフェイス MAC アドレスを入力します。
- [Interface]：エントリのインターフェイスを選択します。
- [ステータス]：エントリの処理方法を選択します。次のオプションがあります。
  - 永続的（Permanent）：システムはこの MAC アドレスを削除しません。スタティック MAC アドレスは、スタートアップ コンフィギュレーションに保存されている場合、再起動後も保持されます。

- リセット時に削除（Delete on reset）：デバイスをリセットすると、スタティック MAC アドレスが削除されます。
- [タイムアウト時に削除] : 期限が切れると、アドレスは削除されます。
- [セキュア] : インターフェイスが従来のロック モードであれば MAC アドレスは セキュリティで保護されます。

ステップ 4 [Apply] をクリックします。新しいエントリがテーブルに表示されます。

ステップ 5 静的アドレスを削除するには、[Delete] アイコンをクリックし、[Apply] をクリックして新しい設定を保存します。

ダイナミックアドレス設定

ダイナミックアドレステーブル（ブリッジングテーブル）には、デバイスに送信されたフレームの送信元アドレスを監視することによって取得された MAC アドレスが含まれています。このテーブルのオーバーフローを防止し、新しい MAC アドレスの格納場所を確保するために、対応するトラフィックが特定の期間（エージングタイムという）にわたって受信されなかった場合、アドレスが削除されます。

ダイナミックアドレスのエージングタイムを設定するには、次の手順を実行します。

ステップ 1 [MAC Address Tables] > [Dynamic Address Settings] の順にクリックします。

ステップ 2 [Aging Time] に値を入力します。エージング タイムは、ユーザが設定する値と、その値の 2 倍 - 1 の間の値です。たとえば、300 秒を入力した場合、エージング タイムは 300 ～ 599 秒です。

ステップ 3 [Apply] をクリックします。エージング タイムが更新されます。

ダイナミック アドレス

ダイナミックアドレスを照会するには、次の手順を実行します。

ステップ 1 **[MAC Address Tables]** > **[Dynamic Addresses]** の順にクリックします。

ステップ 2 [Filter] ブロックで、次のクエリ条件を入力できます。

- [VLAN ID] : テーブルに対して照会する VLAN ID を入力します。
- [MAC アドレス] : テーブルに対して照会する MAC アドレスを入力します。
- [インターフェイス] : テーブルに対して照会するインターフェイスを選択します。照会によって、特定のポートまたは LAG を検索できます。

ステップ 3 [Go] をクリックします。ダイナミック MAC アドレス テーブルに対してクエリが実行され、結果が表示されます。

ステップ 4 すべてのダイナミック MAC アドレスを削除するには、[Clear Table] をクリックします。

予約済みMACアドレス

デバイスが（IEEE規格に基づく）予約済み範囲に属する宛先MACアドレスを持つフレームを受信すると、そのフレームを破棄またはブリッジできます。予約済み MAC アドレス テーブルのエントリでは、予約済み MAC アドレスか、または予約済み MAC アドレスとフレーム タイプのいずれかを指定できます。

予約済みの MAC アドレスのエントリを追加するには、次の手順を実行します。

ステップ 1 **[MAC Address Tables]** > **[Reserved MAC Addresses]** の順にクリックします。

予約済み MAC アドレスが表示されます。フィールドについては、次のフィールドを除いて [Add] ページで説明されています。

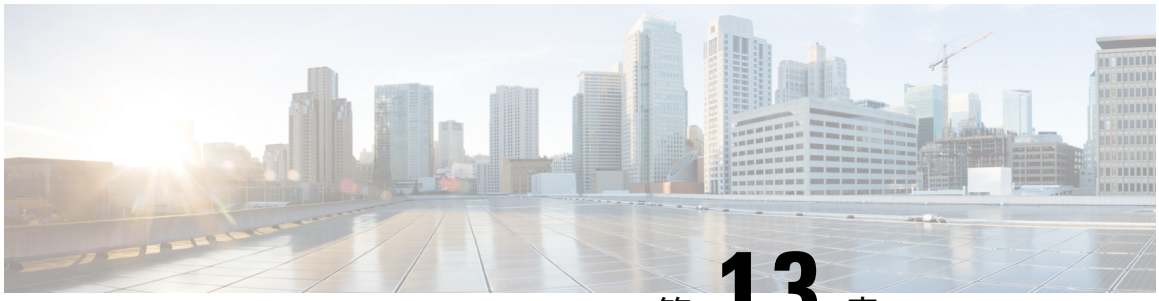
プロトコル（Protocol）：デバイスでサポートされているプロトコルを表示します。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [MAC Address]：予約する MAC アドレスを選択します。
- フレーム タイプ（Frame Type）：次の条件に基づいてフレーム タイプを選択します。
  - [Ethernet V2]：特定の MAC アドレスが指定された Ethernet V2 パケットに適用されます。
  - [LLC]：特定の MAC アドレスが指定された論理リンク制御（LLC）パケットに適用されます。
  - [LLC-SNAP]：特定の MAC アドレスが指定された論理リンク制御/サブネットワーク アクセス プロトコル（LLC-SNAP）パケットに適用されます。
  - [すべて]：特定の MAC アドレスが指定されたすべてのパケットに適用されます。
- アクション（Action）：選択した条件に一致するパケットの受信時に実行するアクションを次の中から 1 つ選択します。
  - [Bridge]：すべての VLAN メンバーにパケットを転送します。
  - [破棄]：パケットを削除します。

ステップ 4 [Apply] をクリックします。新しい MAC アドレスが予約されます。



第 13 章

マルチキャスト

この章は、次の項で構成されています。

マルチキャストのプロパティ

マルチキャスト転送により、1 対複数の情報伝達が可能になります。マルチキャスト アプリケーションは、クライアントがコンテンツ全体の受信を必要としないときに、複数のクライアントに情報伝達する場合に役立ちます。通常のアプリケーションは、クライアントが伝送の途中でチャネルに参加し、伝送が終了する前にチャネルから離れる、ケーブル TV のようなサービスです。

データは関連するポートのみに送信されます。関連するポートのみにデータを転送することにより、リンクの帯域幅とホスト リソースが節約されます。デフォルトでは、すべてのマルチキャスト フレームは、VLAN のすべてのポートにフラッディングされます。このセクションでブリッジ 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と、対象ポートにのみマルチキャストフレームを選択的に転送し、それ以外のポートへのマルチキャストはフィルタ処理（ドロップ）できます。

マルチキャスト アドレスには次のプロパティがあります。

- 各 IPv4 マルチキャスト アドレスのアドレスの範囲は、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 グする方法は次のとおりです。

IPv4 の場合、IPv4 アドレスから下位 23 ビットを取得して、01:00:5e プレフィックスに追加することにより、マッピングします。標準規格では、IP アドレスの上位 9 ビットは無視され、これら上位ビットの値のみが異なる 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（使用される下位 23 ビットが同一であるため）。たとえば、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 個の IP マルチキャスト グループ 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。

IPv6 の場合、マルチキャスト アドレスから下位 32 ビットを取得して、33:33 のプレフィックスに追加することにより、マッピングします。たとえば、IPv6 マルチキャストアドレス FF00:1122:3344 はレイヤ 2 マルチキャストアドレス 33:33:11:22:33:44 にマッピングされます。

マルチキャスト フィルタリングを有効にし、転送方法を選択するには、次の手順を実行します。

ステップ 1 [Multicast] > [Properties] の順にクリックします。

ステップ 2 パラメータを入力します。

ブリッジマルチキャスト フィルタリングステータス	フィルタリングを有効にする場合に選択します。
VLAN ID	転送方式を設定する VLAN ID を選択します。
IPv6用フォワーディング方式	IPv6 アドレスには次のいずれかの転送方式を設定します。 • [MAC Group Address]：MAC マルチキャスト グループ アドレスに基づいてパケットを転送します。 • [IP Group Address]：IPv6 マルチキャスト グループ アドレスに基づいてパケットを転送します。 • [Source-Specific IP Group Address]：送信元 IPv6 アドレスおよび IPv6 マルチキャスト グループ アドレスに従ってパケットを転送します。VLAN 上に IPv6 アドレスが設定されている場合、IPv6 マルチキャストの動作転送方式は IP グループアドレスになります。 （注） IPv6 IP グループアドレスおよび送信元固有 IP グループアドレスモードの場合、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の一致のみをチェックします。宛先のマルチキャスト アドレスでは、グループ ID の最後の 4 バイトが一致します。発信元アドレスでは、最後の 3 バイトと、最後のバイトから 5 番目のバイトが一致します。

IPv4用フォワーディング方式	IPv4 アドレスには次のいずれかの転送方式を設定します。 • [MAC Group Address]：MAC マルチキャスト グループ アドレスに基づいてパケットを転送します。 • [IP Group Address]：IPv4 マルチキャスト グループ アドレスに基づいてパケットを転送します。 • [Source-Specific IP Group Address]：送信元 IPv4 アドレスおよび IPv4 マルチキャスト グループ アドレスに従ってパケットを転送します。VLAN 上に IPv4 アドレスが設定されている場合、IPv4 マルチキャストの動作転送方式は IP グループアドレスになります。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

MACグループアドレス

[MAC Group Address] ページは次の機能を備えています。

- 特定の VLAN ID または特定の MAC アドレスグループに関連する、マルチキャスト フォワーディング データベース（MFDB）からの情報をクエリおよび表示する。このデータは、IGMP/MLDのスヌーピングによって動的に、または手動入力によって静的に取得されます。
- 宛先 MACアドレスに基づいて、静的転送情報を提供する MFDB に静的エントリを追加または削除します。
- 各 VLAN ID と MAC アドレスグループのメンバーであるすべてのポートまたは LAG を表示する。

MAC マルチキャストグループを定義して表示するには、次の手順を実行します。

ステップ 1 **[Multicast]** > **[MAC Group Address]** の順にクリックします。

ステップ 2 フィルタのパラメータを入力します。

- [VLAN IDが次に等しい]：表示するグループの VLAN ID を設定します。
- [MACグループアドレスが次に等しい]：表示するマルチキャスト 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 からのすべての MAC グループ アドレスが含められます。

ステップ 3 [Go] をクリックすると、MAC マルチキャスト グループ アドレスが下方のブロックに表示されます。

ステップ 4 [Add] をクリックして、静的 MAC グループ アドレスを追加します。

ステップ 5 パラメータを入力します。

- [VLAN ID]：新規に作成するマルチキャスト グループの VLAN ID を指定します。
- [MAC グループアドレス]：新規に作成するマルチキャスト グループの MAC アドレ スを指定します。

ステップ 6 [Apply] をクリックすると、MAC マルチキャスト グループが実行コンフィギュレーション ファイルに保存されます。

グループ内のインターフェイスの登録を設定および表示するには、アドレスを選択して、[Details] をクリックします。

ページには次の項目が表示されます。

- [VLAN ID]：マルチキャスト グループの VLAN ID。
- [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。

ステップ 7 [Filter: Interface Type] メニューからポートと LAG のいずれかを選択します。

ステップ 8 [Go] をクリックして、VLAN のポートまたは LAG のメンバーシップを表示します。

ステップ 9 各インターフェイスをマルチキャスト グループに関連付ける方法を選択します。

- [スタティック]：このインターフェイスは、スタティック メンバとしてマルチキャス ト グループに関連付けられています。
- [ダイナミック]：このインターフェイスは、IGMP/MLD スヌーピングの結果、マル チキャスト グループに追加されました。
- [Forbidden]：ポートが VLAN 上のマルチキャストグループに参加できないことを指定します。
- [None]：ポートが現在、VLAN 上のマルチキャストグループのメンバーでないことを指定します。

ステップ 10 [Apply] をクリックすると、実行コンフィギュレーション ファイルが更新されます。

IPマルチキャストグループアドレス

[IP Multicast Group Address] ページは、マルチキャスト グループが IP アドレスで識別される点を除いて、[MAC Group Address] ページとよく似ています。[IP Multicast Group Address] ページを使用して、IP マルチキャスト グループのクエリと追加を有効にすることができます。

IP マルチキャストグループを定義して表示するには、次の手順を実行します。

ステップ 1 **[Multicast]** > **[IP Multicast Group Address]** の順にクリックします。

このページには、スヌーピングで学習されたすべての IP マルチキャスト グループ アドレスが含まれます。

ステップ 2 フィルタリングに必要なパラメータを入力します。

- [VLAN ID が次に等しい]：表示するマルチキャスト グループの VLAN ID を選択し ます。

- [IP バージョンが次に等しい]：IPv6 または IPv4 を選択します。
- [IP マルチキャストグループアドレスが次に等しい]：表示するマルチキャスト グループの IP アドレスを指定します。これは転送モードが（S,G）の場合にのみ該当します。
- [送信元 IP アドレスが次に等しい]：送信元デバイスの IP アドレスを指定します。モードが（S,G）の場合、送信者 S を入力します。この送信者と IP グループ アドレスは、表示対象となるマルチキャスト グループ ID（S,G）です。モードが（*.G）の場合、マルチキャスト グループが宛先のみで定義されていることを示す * を入力します。

ステップ 3 [Go] をクリックします。下方のブロックに結果が表示されます。

ステップ 4 [Add] をクリックして、静的 IP マルチキャスト グループ アドレスを追加します。

ステップ 5 パラメータを入力します。

- [VLAN ID]：追加するグループの VLAN ID を指定します。
- [IP バージョン]：IP アドレスのバージョンを選択します。
- [IP マルチキャストグループアドレス]：新規に作成するマルチキャスト グループのIP アドレスを指定します。
- [送信元固有]：このフィールドを選択した場合、このエントリに特定の送信元 IP アドレスを設定すること、および、その送信元 IP アドレスを [送信元 IP アドレス] フィールドで指定することを意味します。このパラメータを指定しない場合、エントリは（*, G）エントリ、つまり任意の IP 送信元からの IP グループアドレスとして追加されます。
- [Source IP Address]：含められる発信元アドレスを定義します。

ステップ 6 [Apply] をクリックします。IP マルチキャスト グループが追加され、デバイスが更新されます。

ステップ 7 IP グループ アドレスの登録を設定および表示するには、アドレスを選択して [Details] をクリックします。

VLAN ID、IP バージョン、IP マルチキャスト グループ アドレス、および発信元 IP アドレスが、読み取り専用としてウィンドウ上部に表示されます。次のフィルタ タイプのいずれかを選択できます。

- [インターフェイスタイプが次に等しい]：インターフェイス タイプ（ポートまたはLAG）を選択します。

ステップ 8 インターフェイスごとに、関連付けのタイプを選択します。オプションは次のとおりです。

- [スタティック]：このインターフェイスは、スタティック メンバとしてマルチキャスト グループに関連付けられています。
- [Dynamic]：動的メンバーとしてのマルチキャスト グループにインターフェイスを接続します。
- [禁止]：このポートは、この VLAN 上のこのグループに参加することを禁じられて います。
- [None]：ポートが現在、VLAN 上のマルチキャストグループのメンバーではないことを示します。デフォルトでは、[Static] または [Forbidden] が選択されるまでは、これが選択されます。

ステップ 9 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

IPv4マルチキャストコンフィギュレーション

マルチキャストアドレスは、ネットワークホストグループを表す単一のIPデータパケットセットです。マルチキャストアドレスは、指定されたネットワークサービスにマルチキャストすることを目的としたデータグラムまたはフレームを処理するために使用できます。マルチキャストアドレッシングは、IP バージョン 4（IPv4）および 6（IPv6）のリンクレイヤ（OSI モデルのレイヤ 2）とインターネットレイヤ（OSI モデルのレイヤ 3）に適用されます。

IPV4 のマルチキャストアドレスは、このアドレスグループが Class D として指定された初期インターネットのクラスフルネットワーク設計から発信される、1110 の先頭アドレスビットを使用して定義されます。

IPv4 マルチキャストパケットは、イーサネット MAC アドレス範囲（01:00:5e:00:00:00 ～ 01:00:5e:7f:ff:ff）を使用して配信されます。この範囲には、23 ビットの使用可能なアドレス空間があります。最初のオクテット（01）には、ブロードキャスト/マルチキャストビットが含まれています。28 ビットのマルチキャスト IP アドレスの下位 23 ビットは、使用可能なイーサネットアドレス空間の 23 ビットにマッピングされます。これは、パケットの配信にあいまいさがあることを意味します。同じサブネット上の2つのホストがそれぞれ異なるマルチキャストグループに登録し、それぞれのアドレスが最初の5ビットのみ異なっている場合、両方のマルチキャストグループのイーサネットパケットが両方のホストに配信されるため、ホスト内のネットワークソフトウェアが不要なパケットを破棄する必要があります。

このセクションでは、IPv4 マルチキャストの設定方法について説明します。

IGMP スヌーピング

選択的な IPv4 マルチキャスト転送を可能にするには、（マルチキャストのプロパティ （211 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。IGMP スヌーピングは、[IGMP Snooping] ページで、グローバルに、または関連する各 VLAN に対して有効にする必要があります。

IGMP スヌーピングを有効にし、このデバイスを VLAN での IGMP スヌーピングクエリアとして指定するには、次の手順を実行します。

ステップ 1 [Multicast] > [IPv4 Multicast Configuration] > [IGMP Snooping] の順にクリックします。

- [IGMP Snooping Status]：選択すると、IGMP スヌーピングがすべてのインターフェイスでグローバルに有効になります。
- [IGMP Querier Status]：選択すると、IGMP クエリアがすべてのインターフェイスでグローバルに有効になります。

ステップ 2 IGMP スヌーピングは、ブリッジ マルチキャスト フィルタリングが有効になっている場合にのみ機能します。これはマルチキャストのプロパティ （211 ページ）で有効にできます。

ステップ 3 インターフェイスでIGMPを設定するには、静的VLANを選択して、[Edit]をクリックします。次のフィールドに入力します。

オプション	説明
VLAN ID	ドロップダウンリストから VLAN ID を選択します。
IGMPスヌーピングステータス	これを選択すると、VLAN で IGMP スヌーピングが有効になります。デバイスは、ネットワーク トラフィックを監視して、どのホストがマルチキャスト トラフィックの送信を求められたかを判断します。
マルチキャストルータポート自動学習	これを選択すると、マルチキャストルータの自動学習が有効になります。
即時脱退	これを選択すると、スイッチは、脱退メッセージを送信してきたインターフェイスを転送テーブルから削除する際、まず最初に MAC に基づく一般クエリーをそのインターフェイスに送らなくても削除できるようになります。IGMP グループ脱退（IGMP Leave Group）メッセージをホストから受信すると、システムは、テーブル エントリからホスト ポートを削除します。マルチキャストルータからの IGMP クエリーを中継した後、マルチキャストクライアントから IGMP メンバーシップ報告を受け取らなければ、エントリを定期的に削除します。有効にすると、この機能は、デバイス ポートに送信される不必要なIGMP トラフィックのブロックにかかる時間を短縮します。
最終メンバクエリーカウンタ	このデバイスがクエリアとして選出されている場合に、グループメンバーがこれ以上存在しないとデバイスが判断する基準となる、MLD グループ固有のクエリーの送信回数。この値に達すると、デバイスはグループメンバーがこれ以上存在しないと見なします。 • [Use Query Robustness (x)]：括弧内の数字は現在のクエリーロバストネス値です。 • [User Defined]：ユーザー定義値を入力します。
IGMPクエリアステータス	これを選択すると、この機能が有効になります。マルチキャストルータが存在しない場合には、この機能が必要です。
IGMPクエリアバージョン	[GMP Querier Election]：IGMP クエリア選択が有効または無効かを示します。IGMP クエリア選定メカニズムが有効になっている場合、IGMP スヌーピング クエリアは、RFC3810 で指定された標準の IGMP クエリア選定メカニズムをサポートします。 IGMP クエリア選出メカニズムが無効になっている場合、IGMP スヌーピングクエリアは、有効化された後に一般クエリーメッセージの送信を 60 秒間遅らせ、他のクエリアがなければ一般クエリーメッセージを送信し始めます。別のクエリアが検出されると、一般的なクエリ メッセージの送信を停止します。IGMP スヌーピング クエリアは、クエリ パッシブ間隔の間に、別のクエリアが検出され

オプション	説明
	なかった場合、一般的なクエリ メッセージの送信を再開します。クエリ パッシブ間隔は、堅牢性 *（クエリ間隔）+0.5 * クエリの応答間隔に相当します。
IGMPクエリアバージョン	デバイスがクエリアとして選出された場合に使用する IGMP バージョンを選択します。送信元固有のIPマルチキャスト転送を行うスイッチやマルチキャストルータが VLAN 内に存在する場合は、IGMPv3 を選択してください。存在しない場合には、IGMPv2 を選択します。
クエリアソースIPアドレス	送信されるメッセージで使われるデバイス送信元インターフェイスの IP アドレス。MLD では、このアドレスはシステムによって自動的に選択されます。 • [自動]：システムは、発信インターフェイスで定義された IP アドレスからソース IP アドレスを取得します。 • [ユーザー定義]：ユーザー定義の IP アドレスを入力します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

（注） クエリの堅牢性、クエリ間隔など、IGMP スヌーピングタイマーの設定を変更しても、すでに作成済みのタイマーには影響を及ぼしません。

IGMP インターフェイス設定

マルチキャストルータポートとして定義されたインターフェイスは、すべてのIGMPパケット（レポートとクエリー）およびすべてのマルチキャストデータを受信します。

インターフェイス上で IGMP を定義するには、次の手順を実行します。

ステップ 1 [Multicast] > [IPv4 Multicast Configuration] > [IGMP Interface Settings] の順にクリックします。

IGMP が有効になっている各インターフェイスには、次のフィールドが表示されます。

- [インターフェイス名]：IGMP スヌーピングが定義されるインターフェイス。
- [ルータIGMPバージョン]：IGMP バージョン。
- [Query Robustness]：リンクで予想されるパケット損失の数を入力します。
- [Query Interval (sec)]：このデバイスが選択したクエリアである場合に使用される一般的なクエリ間隔。
- Query Max Response Interval (sec)]：定期的な一般的クエリに挿入される最大応答コードを計算するために使用される遅延。

- [Last Member Query Interval (msec)]：選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延。
- [Multicast TTL Threshold]：インターフェイスで転送されるパケットの存続可能時間（TTL）のしきい値を入力します。

  しきい値より小さいTTL値を持つマルチキャストパケットは、インターフェイスで転送されません。

  デフォルト値は0で、すべてのマルチキャストパケットがインターフェイスで転送されることを意味します。

  256の値は、インターフェイスでマルチキャスト パケットが転送されないことを意味します。

  TTLしきい値は、ボーダルータだけで設定します。逆に、ルータTTLしきい値を設定するルータは、自動的にボーダ ルータになります。

ステップ2 インターフェイスを選択して、[Edit] をクリックします。上記のフィールドの値を入力します。

ステップ3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

IGMP VLAN 設定

特定の VLAN における IGMP を設定するには、次の手順を実行します。

ステップ1 [Multicast] > **[IPv4 Multicast Configuration]** > **[IGMP VLAN Settings]** をクリックします。

IGMP が有効になっている各 VLAN には、次のフィールドが表示されます。

- [インターフェイス名]：IGMP スヌーピングが定義される VLAN。
- [ルータIGMPバージョン]：IGMP スヌーピングのバージョン。
- [Query Robustness]：リンクで予想されるパケット損失の数を入力します。
- [Query Interval (sec)]：このデバイスが選択したクエリアである場合に使用される一般的なクエリ間隔。
- Query Max Response Interval (sec)]：定期的な一般的クエリに挿入される最大応答コードを計算するために使用される遅延。
- [Last Member Query Interval (msec)]：選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延を入力します。
- [Multicast TTL Threshold]：インターフェイスで転送されるパケットの存続可能時間（TTL）のしきい値を入力します。

  しきい値より小さいTTL値を持つマルチキャストパケットは、インターフェイスで転送されません。

  デフォルト値は0で、すべてのマルチキャストパケットがインターフェイスで転送されることを意味します。

  256の値は、インターフェイスでマルチキャスト パケットが転送されないことを意味します。

TTL しきい値は、ボーダ ルータだけで設定します。逆に、ルータ TTL しきい値を設定するルータは、自動的にボーダ ルータになります。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。上記のフィールドの値を入力します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

IGMP プロキシ

（注） IGMP プロキシは、IPv4インターフェイス （231 ページ）で IPv4 ルーティングが有効になっている場合にのみ動作します。

IGMP プロキシを設定するには、次の手順を実行します。

ステップ 1 [Multicast] > [IPv4 Multicast Configuration] > [IGMP Proxy] の順にクリックします。

ステップ 2 次のグローバル フィールドに入力します。

IGMPマルチキャストルーティング	IPv4 マルチキャストルーティングを有効にする場合に選択します。
ダウンストリーム保護	デバイスに不要なダウンストリームパケットを廃棄する場合に選択します。
Source Specific Multicast	次のフィールドで定義された特定の送信元アドレスから発信されるマルチキャストパケットを配信する場合に選択します。
SSM IPv4アクセスリスト	マルチキャストパケットの配信元の送信元アドレスを含むリストを定義します。 • [デフォルトリスト]：SSM 範囲アクセス リストを 232.0.0.0/8 に定義します。 • [User-defined access list]：SSM 範囲を定義する標準の IPv4 アクセスリスト名を選択します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ステップ 4 VLAN に保護を追加するには、[Add] をクリックして次のフィールドに入力します。

アップストリームインターフェイス	アップストリームインターフェイスを選択します。アップストリームインターフェイスは1つだけであるため、すでに選択済みの場合、このフィールドはグレー表示されます。
ダウンストリームインターフェイス	ダウンストリーム インターフェイスを選択します。複数のダウンストリームインターフェイスを指定できます。

ダウンストリーム保護	次のオプションのいずれかを選択します。 • [グローバルの使用]：グローバルブロックで設定されたステータスを使用します。 • [無効]：ダウンストリーム インターフェイスからの IPv4 マルチキャスト トラフィックの転送が可能になります。 • [有効]：ダウンストリーム インターフェイスからの転送が不可になります。

ステップ 5 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

各 IPv4 マルチキャスト ルートには、次のフィールドが表示されます。

送信元アドレス	ユニキャスト送信元 IPv4 アドレス。
Group Address	マルチキャスト宛先 IPv4 アドレス。
Incoming Interface	送信元からのマルチキャストパケット用のインターフェイスです。このインターフェイス以外で受信したパケットは、破棄されます。
出力インターフェイス	パケットが転送される際に通過したインターフェイス。
Uptime	エントリが IP マルチキャスト ルーティング テーブルに保存されている時間の長さ（時間、分、秒）。
Expiry Time	エントリが IP マルチキャスト ルーティング テーブルから削除されるまでの時間の長さ（時間、分、秒）。

IPv6マルチキャストコンフィギュレーション

IP マルチキャストは、インターネットプロトコル（IP）データグラムを対象の受信者のグループに 1 回の伝送で送信する方式です。これは IP 固有のマルチキャスト形式であり、ストリーミングメディアやその他のネットワーク アプリケーションに使用されます。この方式では、IPv4 および IPv6 で特別に予約されたマルチキャスト アドレス ブロックが使用されます。

ユニキャストパケットは、イーサネット パケット アドレスに特定のレイヤ 2 MAC アドレスを設定することにより、イーサネットまたは IEEE 802.3 サブネット上の特定の受信者に配信されます。ブロードキャストパケットは、ブロードキャスト MAC アドレス（FF:FF:FF:FF:FF:FF）を使用します。IPv6 マルチキャストアドレスの場合、イーサネット MAC は、下位 4 オクテットと MAC アドレス 33:33:00:00:00:00 の OR 演算によって導出されます。たとえば、IPv6 アドレス FF02:DEAD:BEEF::1:3 はイーサネット MAC アドレス 33:33:00:01:00:03 にマッピングされます。

このセクションでは、IPv6 マルチキャストの設定方法について説明します。

MLD スヌーピング

選択的な IPv6 マルチキャスト転送を可能にするには、（マルチキャストのプロパティ （211 ページ）で）ブリッジ マルチキャスト フィルタリング機能を有効にするとともに、MLD スヌーピングページでグローバルおよび該当する VLAN ごとに MLD スヌーピングを有効にする必要があります。

MLD スヌーピングを有効にして VLAN でそれを設定するには、次の手順を実行します。

ステップ 1 [Multicast] > **[IPv6 Multicast Configuration]** > **[MLD Snooping]** の順にクリックします。

（注） MLD スヌーピングは、ブリッジ マルチキャスト フィルタリングが有効になっている場合にのみ機能し、マルチキャストのプロパティ （211 ページ）で有効にできます。

ステップ 2 次の機能をイネーブルまたはディセーブルにします。

- [MLD Snooping Status]：選択すると、MLD スヌーピングがすべてのインターフェイスでグローバルに有効になります。
- [MLD Querier Status]：選択すると、MLD クエリアがすべてのインターフェイスでグローバルに有効になります。

ステップ 3 インターフェイスで MLD プロキシを設定するには、静的 VLAN を選択して、[Edit] をクリックします。次のフィールドに入力します。

オプション	説明
MLDスヌーピング ステータス	これを選択すると、VLAN で MLD スヌーピングが有効になります。デバイスは、ネットワーク トラフィックを監視して、どのホストがマルチキャスト トラフィックの送信を求められたかを判断します。デバイスは、MLD スヌーピングおよびブリッジ マルチキャスト フィルタリングの両方が有効になっている場合にのみ、MLD スヌーピングを実行します。
マルチキャスト ルータポート自動学習	これを選択すると、マルチキャストルータの自動学習が有効になります。
即時脱退	これを選択すると、スイッチは、脱退メッセージを送信してきたインターフェイスを転送テーブルから削除する際、まず最初に MAC に基づく一般クエリーをそのインターフェイスに送らなくても削除できるようになります。MLD 脱退グループ メッセージをホストから受信すると、システムはテーブル エントリからホスト ポートを削除します。マルチキャスト ルータからの IGMP クエリーを中継後は、マルチキャスト クライアントから MLD メンバーシップ レポートを受信しない限り、定期的にエントリを削除します。有効にすると、この機能は、デバイス ポートに送信される不必要な MLD トラフィックをブロックする所要時間を削減します。
最終メンバクエリーカウンタ	このデバイスがクエリアとして選出されている場合に、グループメンバーがこれ以上存在しないとデバイスが判断する基準となる、MLD グループ固有のクエリーの送

オプション	説明
	信回数。この値に達すると、デバイスはグループメンバーがこれ以上存在しないと見なします。 • [Use Query Robustness (x)]：括弧内の数字は現在のクエリーロバストネス値です。 • [User Defined]：ユーザー定義値を入力します。
MLDクエリアステータス	これを選択すると、この機能が有効になります。この機能は、マルチキャスト ルータがない場合に必要です。
MLDクエリア選出	MLDクエリアの選出を有効にするか、無効にするか。MLDクエリア選定メカニズムが有効になっている場合、MLD スヌーピング クエリアは RFC3810 で指定した標準 MLD クエリア選定メカニズムをサポートします。 MLD クエリア選定メカニズムが無効な場合、MLD スヌーピング クエリアは、有効化された後で一般的なクエリ メッセージの送信を 60 秒間遅らせ、他にクエリアがなければ、一般的なクエリ 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と、一般的なクエリ メッセージの送信を停止します。MLD スヌーピング クエリアは、クエリ パッシブ間隔の間に、別のクエリアが検出されなかった場合、一般的なクエリ メッセージの送信を再開します。クエリ パッシブ間隔は、堅牢性 * （クエリ間隔） + 0.5 * クエリの応答間隔に相当します。
MLDクエリアバージョン	デバイスがクエリアとして選出された場合に使用する MLD バージョンを選択します。送信元固有の IP マルチキャスト転送を行うスイッチやマルチキャストルータが VLAN 内に存在する場合は、MLDv2 を選択してください。存在しない場合には、MLDv1 を選択します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

（注） クエリの堅牢性、クエリ間隔など、MLD スヌーピング タイマーの設定を変更しても、すでに作成済みのタイマーには影響を及ぼしません。

MLDインターフェイス設定

マルチキャストルータポートとして定義されたインターフェイスは、すべての MLD パケット（レポートとクエリー）およびすべてのマルチキャストデータを受信します。

インターフェイスをマルチキャスト ルータ インターフェイスとして設定するには、次の手順を実行します。

ステップ 1 [Multicast] > **[IPv6 Multicast Configuration]** > **[MLD Interface Settings]** の順にクリックします。

MLD が有効になっている各インターフェイスには、次のフィールドが表示されます。

- [Router MLD Version]：マルチキャスト ルータの MLD バージョン。
- [Query Robustness]：リンクで予想されるパケット損失の数を入力します。
- [Query Interval (sec)]：このデバイスが選択したクエリアである場合に使用される一般的なクエリ間隔。
- [Query Max Response Interval (sec)]：定期的な一般的クエリに挿入される最大応答コードを計算するために使用される遅延。
- [Last Member Query Interval (msec)]：選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延。
- [Multicast TTL Threshold]：インターフェイスで転送されるパケットの存続可能時間（TTL）のしきい値を入力します。

  しきい値より小さい TTL 値を持つマルチキャストパケットは、インターフェイスで転送されません。

  デフォルト値は 0 で、すべてのマルチキャストパケットがインターフェイスで転送されることを意味します。

  256 の値は、インターフェイスでマルチキャスト パケットが転送されないことを意味します。

  TTL しきい値は、ボーダ ルータだけで設定します。逆に、ルータ TTL しきい値を設定するルータは、自動的にボーダ ルータになります。

ステップ 2 インターフェイスを設定するには、インターフェイスを選択して [Edit] をクリックします。前述のフィールドに入力します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

MLD VLAN設定

特定の VLAN における MLD を設定するには、次の手順を実行します。

ステップ 1 [Multicast] > **[IPv6 Multicast Configuration]** > **[MLD VLAN Settings]** をクリックします。

MLD が有効になっている各 VLAN には、次のフィールドが表示されます。

- [Interface Name]：MLD 情報が表示される VLAN。
- [ルータMLDバージョン]：MLD ルータのバージョン。
- [Query Robustness]：リンクで予想されるパケット損失の数を入力します。
- [Query Interval (sec)]：このデバイスが選択したクエリアである場合に使用される一般的なクエリ間隔。
- Query Max Response Interval (sec)]：定期的な一般的クエリに挿入される最大応答コードを計算するために使用される遅延。

- [Last Member Query Interval (msec)]：選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延を入力します。
- [Multicast TTL Threshold]：インターフェイスで転送されるパケットの存続可能時間（TTL）のしきい値を入力します。

  しきい値より小さい TTL 値を持つマルチキャストパケットは、インターフェイスで転送されません。

  デフォルト値は 0 で、すべてのマルチキャストパケットがインターフェイスで転送されることを意味します。

  256 の値は、インターフェイスでマルチキャスト パケットが転送されないことを意味します。

  TTL しきい値は、ボーダ ルータだけで設定します。逆に、ルータ TTL しきい値を設定するルータは、自動的にボーダ ルータになります。

ステップ 2 VLAN を設定するには、VLAN を選択して [Edit] をクリックします。前述のフィールドに入力します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

MLD プロキシ

（注） MLD プロキシは、IPv6グローバルコンフィギュレーション （267 ページ）で IPv6 ルーティングが有効になっている場合にのみ動作します。

MLD プロキシを設定するには、次の手順を実行します。

ステップ 1 [Multicast] > [IPv6 Multicast Configuration] > [MLD Proxy] の順にクリックします。

ステップ 2 次のフィールドに入力します。

- [IGMP Multicast Routing]：選択すると、IPv6 マルチキャスト ルーティングが有効になります。
- [Downstream Protection]：選択すると、デバイスに必要のないダウンストリームのパケットを破棄します。
- [Source Specific Multicast]：選択すると、次のフィールドに定義された特定の発信元アドレスから発信されたマルチキャスト パケットの配信が有効になります。
- [SSM IPv6 Access List]：マルチキャスト パケットを配信する発信元アドレスを含むリストを定義します。
  - [Default List]：SSM 範囲 FF3E::/32 のアクセス リストを定義します。
  - [User-defined access list]：SSM 範囲を定義する標準の IPv6 アクセスリスト名を選択します。これらのアクセス リストはIPv6 アクセス リスト （281 ページ） で定義されています。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ステップ 4 VLAN に保護を追加するには、[Add] をクリックして次のフィールドに入力します。

- [Upstream Interface]：発信インターフェイスを選択します。
- [Downstream Interface]：着信インターフェイスを選択します。
- ダウン ストリームの保護（Downstream Protection）：次のいずれかのオプションを選択できます。
  - [グローバルの使用]：グローバル ブロックで設定されたステータスを使用します。
  - [無効]：ダウンストリーム インターフェイスからの IPv6 マルチキャスト トラフィックの転送が可能になります。
  - [有効]：ダウンストリーム インターフェイスからの転送が不可になります。

ステップ 5 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

各 IPv6 マルチキャスト ルートには、次のフィールドが表示されます。

- [Source Address]：ユニキャスト送信元 IPv4 アドレス。
- [Group Address]：マルチキャスト宛先 Ipv4 アドレス。
- 着信インターフェイス（Incoming interface）：送信元からのマルチキャスト パケットが着信する予定のインターフェイス。このインターフェイス以外で受信したパケットは、破棄されます。
- 発信インターフェイス（Outgoing interface）：パケット転送時に使用されるインターフェイス。
- 稼働時間（Uptime）：IP マルチキャスト ルーティング テーブル内にエントリが存在する時間（時間、分、秒）です。
- 期限（Expiry Time）：IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの時間（時間、分、秒）です。

IGMP/MLDスヌーピングIPマルチキャストグループ

[IGMP/MLD Snooping IP Multicast Group] ページには、IGMP/MLD メッセージから学習された 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 Group Address] ページの情報は異なっている場合があります。たとえば、システムが MAC ベースのグループに従ってフィルタ処理され、マルチキャストグループ 224.1.1.1 と 225.1.1.1 に参加するように要求されたポートがあるとします。どちらも、同じ MAC マルチキャストアドレス 01:00: 5e:01:01:01 にマッピングされます。この場合、[MAC Multicast] ページにはエントリが 1 つありますが、このページにはエントリが 2 つあります。

IP マルチキャストグループをクエリするには、次の手順を実行します。

ステップ 1 [Multicast] > [IGMP/MLD Snooping IP Multicast Group] をクリックします。

ステップ 2 検索対象となるスヌーピング グループのタイプを IGMP または MLD のいずれかに設定します。

ステップ 3 次のクエリ フィルタ条件の一部またはすべてに入力します。

- [グループアドレスが次に等しい] : 照会するマルチキャスト グループの MAC アドレ スまたは IP アドレスを指定します。
- [送信元アドレスが次に等しい] : 照会する送信元アドレスを指定します。
- [VLAN ID が次に等しい] : 照会する VLAN ID を指定します。

ステップ 4 [Go] をクリックします。各マルチキャスト グループには、次のフィールドが表示されます。

- [VLAN] : VLAN ID。
- [グループアドレス] : マルチキャスト グループの MAC アドレスまたは IP アドレス。
- [送信元アドレス] : 指定したすべてのグループ ポートに対する送信元アドレス。
- [含まれるポート] : マルチキャスト ストリームの宛先ポートのリスト。
- [除外ポート] : このグループに含まれないポートのリスト。
- [Compatibility Mode] : デバイスが IP グループ アドレスで受信する、ホストからの登録の最も古い IGMP/MLD バージョン。

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 ルータに接続されたポートです。マルチキャストストリームおよび IGMP/MLD 登録メッセージを転送するときに、デバイスは 1つ以上のマルチキャストルータポート番号を含めます。マルチキャストルータが、マルチキャストストリームを転送し、登録メッセージを他のサブネットに伝達するには、マルチキャストルータポートを設定する必要があります。

マルチキャストルータに接続されるポートを静的に設定したり、動的に検出されるそれらのポートを確認するには、次の手順を実行します。

ステップ 1 [Multicast] > [Multicast Router Port] をクリックします。

ステップ 2 次のクエリ フィルタ条件の一部またはすべてに入力します。

- [VLAN ID が次に等しい] : ルータ ポートの VLAN ID を選択します。
- [IP バージョンが次に等しい] : マルチキャスト ルータでサポートされている IP バー ジョンを選択します。

- [インターフェイスタイプが次に等しい]：インターフェイス タイプ（ポートまたはLAG）を選択します。

ステップ 3 [Go] をクリックします。クエリ条件に一致するインターフェイスが表示されます。

ステップ 4 ポートまたは LAG ごとに、関連付けのタイプを選択します。オプションは次のとおりです。

- [スタティック]：このポートをマルチキャスト ルータ ポートとして静的に設定します。
- [ダイナミック]：（表示のみ）このポートは、IGMP/MLD クエリー メッセージによって、マルチキャスト ルータ ポートとして動的に設定されています。マルチキャストルータポートの動的学習を有効にするには、IGMP/MLDスヌーピングIPマルチキャストグループ（226 ページ）を使用します。
- [Forbidden]：このポートで IGMP/MLD クエリーが受信された場合でも、このポートをマルチキャストルータポートとして設定しません。ポートで [Forbidden] が有効になっている場合、このポートでのマルチキャストルータの学習は行われません（つまり、このポートでのマルチキャストルータポート自動学習が無効になります）。
- [None]：このポートは現在、マルチキャストルータポートではありません。

ステップ 5 [Apply] をクリックして、デバイスを更新します。

不在転送

ブリッジ マルチキャスト フィルタリングが有効になっている場合、登録されたマルチキャストパケットは、IGMP および MLD の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 フィルタリングが無効になっている場合、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。

[Forward All] ページでは、特定の VLAN からのマルチキャストストリームを受信するポートや LAG を設定します。この機能を利用するには、マルチキャストのプロパティ（211 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。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。ポートに接続されているデバイスで IGMP または MLD がサポートされていない場合、そのポートに対して [Forward All] を静的に（手動で）設定できます。IGMP および MLD メッセージを除くマルチキャスト パケットは、常時、[Forward All] に設定されているポートに転送されます。この設定は、選択した VLAN のメンバーであるポートのみに影響します。

[Forward All Multicast] を定義するには、次の手順を実行します。

ステップ 1 [Multicast] > [Forward All] をクリックします。

ステップ 2 次のパラメータを定義します。

- [VLAN ID が次に等しい]：表示するポート /LAG がメンバになっている VLAN の ID。

- [インターフェイスタイプが次に等しい]：インターフェイス タイプ（ポートまたはLAG）を選択します。

ステップ 3 [Go] をクリックします。すべてのポート/LAG のステータスが表示されます。

ステップ 4 次の方法を使用して、[Forward All] に設定するポート/LAG を選択します。

- [スタティック]：このポートではすべてのマルチキャスト ストリームが受信されます。
- [Forbidden]：IGMP/MLD スヌーピングにより、マルチキャストグループに参加するポートとして指定されている場合でも、このポートはマルチキャストストリームを受信できません。
- [None]：このポートは現在、[Forward All] ポートとして設定されていません。

ステップ 5 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

登録解除済みマルチキャスト

この機能は、要求された（登録済み）マルチキャストグループのみをお客様が受信できるようにするために使用します。

未登録マルチキャストフレームは、VLAN 上のすべてのポートに転送されます。未登録マルチキャストストリームをフィルタ処理するポートを選択できます。この設定は、ポートがメンバーであるすべての VLAN に対して有効です。

未登録マルチキャスト設定を定義するには、次の手順を実行します。

ステップ 1 [Multicast] > [Unregistered Multicast] をクリックします。

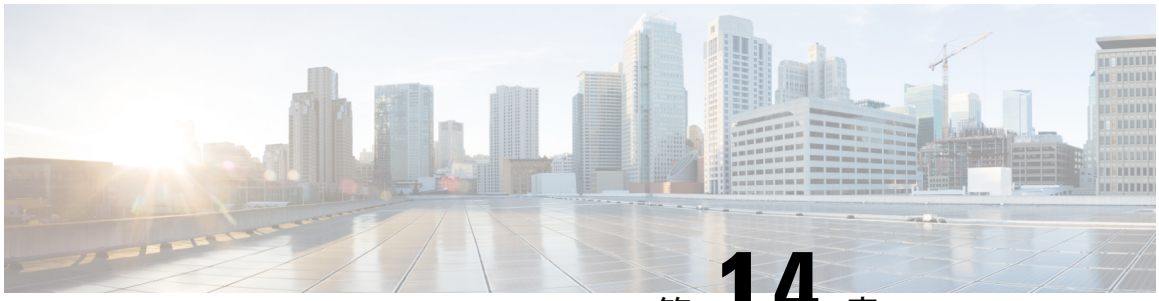
ステップ 2 [Interface Type equals to]：ポートと LAG のいずれかを表示します。

ステップ 3 [Go] をクリックします。

ステップ 4 次のパラメータを定義します。

- [ポート]/[LAG]：ポート ID または LAG ID を表示します。
- 選択したインターフェイスの転送のステータスを表示します。次の値が可能です。
  - [フォワーディング]：選択したインターフェイスで、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]：選択したインターフェイスで、未登録マルチキャスト フレームのフィルタリング（拒否）を有効にします。

ステップ 5 [Apply] をクリックします。設定が保存され、実行コンフィギュレーション ファイルが更新されます。



第 14 章

IPv4 の設定

この章は、次の項で構成されています。

IPv4インターフェイス

IPv4 インターフェイスのアドレスは、ユーザーが手動で割り当てるか、または、DHCP サーバーから自動的に割り当てられます。このセクションでは、デバイスの IPv4 アドレスを手動で、またはデバイスを DHCP クライアントにして定義することについて説明します。デバイス管理用の IP アドレスを設定するには、[IPv4 Interface] ページを使用します。この IP アドレスは、ポート、LAG、VLAN、ループバック インターフェイス、またはアウトオブバンド インターフェイスに設定できます。デバイスに複数の IP アドレス（インターフェイス）を設定できます。これにより、さまざまなインターフェイス間のトラフィック ルーティングと、リモート ネットワークへのトラフィック ルーティングがサポートされます。一般に（デフォルトでは）ルーティング機能はハードウェアにより実行されます。ハードウェアリソースを使い尽くした場合、またはハードウェアでルーティングテーブルのオーバーフローが発生した場合は、IP ルーティングはソフトウェアにより実行されます。

（注） 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 1 つの VLAN ID（VID）を使用します。4094 以降で未使用の VID のうち最初のものが採用されます。

IPv4 アドレスを設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [IPv4 Interface] をクリックします。

次のフィールドに入力します。

- [IP v 4ルーティング]： IPv4 ルーティングを有効にするには、[有効] ボックスをオンにします（デフォルトで有効になっています）。

ステップ 2 [Apply] をクリックします。パラメータが実行コンフィギュレーション ファイルに保存されます。

次のフィールドが IPv4 インターフェイス テーブルに表示されます。

- [Interface]：IPアドレスが定義されているインターフェイス。これは、アウトオブバンドポートにすることもできます。
- [IP Address Type]：使用可能なオプションを以下に示します。
  - [DHCP]：DHCP サーバーから受信したもの。
  - [Static]：手動で入力したもの。スタティック インターフェイスは、ユーザが作成した DHCP 以外のインターフェイスです。
  - デフォルト（Default）：設定が行われる前にデフォルトでデバイスに存在するデフォルトのアドレス。
- [IP Address]：インターフェイスに設定されている IP アドレス。
- マスク（Mask）：設定された IP アドレス マスク。
- 状態（Status）：IP アドレスの重複チェックの結果。
  - [Tentative]：IP アドレス重複チェックの最終結果はありません。
  - 有効（Valid）：IPアドレス衝突チェックが完了し、IPアドレスの衝突が検出されませんでした。
  - 有効（重複あり）（Valid-Duplicated）：IP アドレス重複チェックが完了し、重複する IP アドレスが検出されました。
  - 重複（Duplicated）：デフォルト IP アドレスの重複 IP アドレスが検出されました。
  - 遅延（Delayed）：DHCP クライアントが起動時に有効化される場合、DHCP アドレスを検出する時間を確保するために、IP アドレスの割り当てが 60 秒遅延します。
  - [Not Received]：DHCP アドレスに関するステータスです。DHCP クライアントが検出プロセスを開始すると、実際のアドレスが取得される前に、ダミーの IP アドレス 0.0.0.0 が割り当てられます。このダミー アドレスの状態は、「未受信」です。

ステップ 3 [Add] をクリックします。

ステップ 4 インターフェイスを選択します。この IP 設定に関連するインターフェイスとしてポート、LAG、VLAN、またはループバックを選択し、関連リストからインターフェイスを選択します。

ステップ 5 IP アドレスタイプを選択します。次のいずれかのオプションを選択してください。

- [ダイナミック IP アドレス]：IP アドレスを DHCP サーバーから受け取ります。
- [スタティックIPアドレス]：IP アドレスを入力し、[マスク] フィールドに入力します。
  - [Network Mask]：このアドレスの IP マスク。
  - [Prefix Length]：IPv4 プレフィックスの長さ。
- [Renew IP Address Now]：[Enable] チェックボックスをオンにして有効にします。
- [Auto Configuration via DHCP]：ステータス（[Disabled] または [Enabled]）が表示されます。

ステップ 6 [Apply] をクリックします。IPv4 アドレス設定が実行コンフィギュレーション ファイルに書き込まれます。

注意 システムが、スタンバイ アクティブ ユニットの存在するスタッキングモードのいずれか 1 つである場合は、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により、アクティブ スタッキング ユニットのスイッチオーバー時にネットワークから切断しないようにすることをお勧めします。スタンバイ アクティブ ユニットがスタックを制御するようになると、DHCP を使用する場合には、スタックの元のアクティブ対応ユニットで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ります。

アウトオブバンド インターフェイスの設定

アウトオブバンド管理により、ネットワークオペレータは、管理機能にアクセスする際に信頼境界を確立し、それをネットワークリソースに適用することができます。ここでは、アウトオブバンド（OOB）インターフェイスで IPv4 アドレスを設定する方法について説明します。

ステップ 1 スイッチの Web ベースユーティリティにログインし、[IPv4 Configuration] > [IPv4 Interface] の順に選択します。

[IPv4 Interface] ページの [IPv4 Interface] テーブルには、次の情報が含まれています。

- [Interface]：IP アドレスが定義されているユニットまたはインターフェイス。これはループバックインターフェイスの場合もあります。
- [IP Address Type]：使用可能なオプションは次のとおりです。
  - [DHCP]：Dynamic Host Configuration Protocol（DHCP）サーバーから受信されたもの。
  - [Static]：手動で入力したもの。スタティック インターフェイスはユーザーが作成した非 DHCP インターフェイスです。
  - [Default]：設定が行われる前にデフォルトでデバイスに存在するデフォルトのアドレス。
- [IP Address]：インターフェイスに設定されている IP アドレス。
- [Mask]：設定されている IP アドレスマスク。

- [Status]：IP アドレス重複チェックの結果。
  - [Tentative]：IP アドレス重複チェックの最終結果はありません。
  - [Valid]：IP アドレスのコリジョンチェックが完了しており、IP アドレスのコリジョンは検出されませんでした。
  - [Valid-Duplicated]：IP アドレス重複チェックが完了しており、IP アドレスの重複が検出されました。
  - [Duplicated]：デフォルト IP アドレスの、IP アドレスの重複が検出されました。
  - [Delayed]：DHCP クライアントが始動時に有効なら、DHCP アドレス検出のための時間を取るため、IP アドレスの割り当ては 60 秒間遅延されます。
  - [Not Received]：DHCP アドレスのみに関するステータスです。DHCP クライアントが検出プロセスを開始すると、実際のアドレスが取得される前に、ダミーの IP アドレス 0.0.0.0 が割り当てられます。このダミーアドレスのステータスは [Not Received] です。

ステップ 2 [Add] をクリックして、静的 IP アドレスを手動で割り当てます。

ステップ 3 [Interface] エリアから [Out of Band] を選択します。

ステップ 4 [IP Address Type] エリアから [Static IP Address] を選択します。

ステップ 5 [IP Address] フィールドにアウトオブバンド インターフェイスの IP アドレスを入力します。

ステップ 6 [Mask] エリアのオプションボタンをクリックし、対応するサブネットマスクを入力します。次のオプションがあります。

- [Network Mask]：このアドレスの IP マスク。
- [Prefix Length]：IPv4 プレフィックスの長さ。

ステップ 7 [Apply] をクリックして [Close] をクリックします。

セッションが自動的に終了し、スイッチへの接続は失われます。これは、アウトオブバンドポートに新しい管理 IP アドレスを適用するためです。

以上で、スイッチに IPv4 管理インターフェイスアドレスが正常に設定されます。

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 ルートを設定および表示できます。トラフィックをルーティングするときに、ネクスト ホップは最長プレフィックス照合（LPM アルゴリズム）に従って決定されます。宛先 IPv4 アドレスは、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可能性があります。デバイスは、最も高いサブネットマスク、つまり最長プレフィックス照合を持つ一致したルートを使用します。複数のデフォルト ゲートウェイが同じメトリック値で定義されている場合は、すべての設定済みデフォルト ゲートウェイの中から最も低い IPv4 アドレスが使用されます。

IP スタティックルートを定義するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [IPv4 Static Routes] をクリックします。

IPv4 スタティック ルート テーブルが表示されます。各エントリについて、次のフィールドが表示されます。

- [Destination IP Prefix]：宛先 IP アドレスプレフィックス。
- [Prefix Length]：宛先 IP の IP ルートプレフィックス。
- [Route Type]：ルートは拒否ルート、リモートルートのうちどれか。
- [Next Hop Router IP Address]：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。
- [Metric]：このホップのコスト（低い値が推奨されます）。
- [Outgoing Interface]：このルートの送信インターフェイス。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドの値を入力します。

- [Destination IP Prefix]：宛先 IP アドレスプレフィックスを入力します。
- [Mask]：次のフィールドを選択して値を入力します。
  - [Network Mask]：マスク形式の、宛先 IP の IP ルートプレフィックス（ルートネットワークアドレス内のビット数）。
  - [Prefix Length]：IP アドレス形式の、宛先 IP の IP ルートプレフィックス。
- [Route Type]：ルートタイプを選択します。
  - [Reject]：ルートを拒否し、すべてのゲートウェイを通じた宛先ネットワークへのルーティングを停止します。これにより、このルートの宛先 IP が指定されたフレームが着信した場合、ドロップされます。この値を選択すると、ネクストホップ IP アドレス、メトリック、および IP SLA トラックの各コントロールが無効になります。
  - [Remote]：このルートがリモートパスであることを示します。
- [Next Hop Router IP Address]：ルート上のネクストホップルータ 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 サーバーから IP アドレスを取得する、直接接続された IP サブネットを介してスタティックルートを設定することはできません。

- [メトリック]：次のいずれかを選択します。
  - [デフォルトを使用]：デフォルトのメトリックを使用する場合に選択します。
  - [ユーザー定義]：ネクスト ホップへの管理距離を入力します。範囲は 1 ～ 255 です。

ステップ 4 [Apply] をクリックします。IP スタティック ルートが実行コンフィギュレーション ファイルに保存されます。

IPv4転送テーブル

IPv4 転送テーブルを表示するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [IPv4 Forwarding Table] の順にクリックします。

IPv4 転送ルート テーブルが表示されます。各エントリについて、次のフィールドが表示されます。

- 宛先 IP プレフィックス（Destination IP Prefix）：宛先 IP アドレスのプレフィックス。
- プレフィックス長（Prefix Length）：宛先 IP の IP ルート プレフィックス。
- ルート タイプ（Route Type）：ルートがローカル、拒否、またはリモート ルートかどうか。
- ネクスト ホップ ルータ IP アドレス（Next Hop Router IP Address）：ネクスト ホップ IP アドレス。
- [Route Owner]：次のいずれかのオプションを選択できます。
  - [デフォルト]：デフォルト システム コンフィギュレーションによって設定されたルート。
  - [スタティック]：手動で作成されたルート。
  - [ダイナミック]：IP ルーティング プロトコルによって作成されたルート。
  - [DHCP]：DHCP サーバーから受け取ったルート。
  - [直接接続]：デバイスが接続されるサブネット。
  - [Rejected]：ルートは拒否されました。
- メトリック（Metric）：このホップのコスト（より低い値が優先）。
- アドミニストレーティブ ディスタンス（Administrative Distance）：ネクスト ホップまでのアドミニストレーティブ ディスタンス（より低い値が優先）。これは、スタティックルートには関係ありません。
- 発信インターフェイス（Outgoing Interface）：このルートの発信インターフェイス。

ステップ 2 [Refresh] アイコンをクリックしてデータを更新します。

RIPv2

このセクションでは、Routing Information Protocol（RIP）バージョン 2 の機能について説明します。

（注） この機能は、ファームウェア 3.1 以降でのみサポートされます。

Routing Information Protocol（RIP）は、ローカルエリア ネットワークおよびワイドエリア ネットワーク向けのディスタンスベクタープロトコルの実装です。ルータをアクティブまたはパッシブ（サイレント）のいずれかとして分類します。アクティブ ルータは、それらのルートを他のルータにアドバタイズします。パッシブ ルータはアドバタイズメントに基づいて、それらのルートをリッスンして更新しますが、アドバタイズはしません。通常、ルータはアクティブ モードで RIP を実行しますが、ホストはパッシブ モードを使用します。

デフォルト ゲートウェイはスタティック ルートであり、設定によって有効な場合は、他のすべてのスタティック ルータと同じ方法で RIP によってアドバタイズされます。IP ルーティングを有効にすると、RIP が完全に機能します。IP ルーティングを無効にすると、RIP はパッシブ モードで稼動します。つまり、受信した RIP メッセージからルートを学習するだけで、それらを送信しません。

（注） IP ルーティングを有効にするには、IPv4 インターフェイスページに移動します。デバイスは RIP バージョン 2 をサポートします。以下の標準規格に基づいています。

- RFC2453 RIP バージョン 2、1998 年 11 月
- RFC2082 RIP-2 MD5 認証、1997 年 1 月
- RFC1724 RIP バージョン 2 拡張 MIB

受信した RIPv1 パケットはドロップされます。

RIP のイネーブル化

- RIP は、グローバルに、インターフェイスごとに有効にする必要があります。
- RIP は、有効になっている場合にのみ設定できます。
- RIP をグローバルに無効にすると、システムの RIP 設定が削除されます。
- インターフェイス上の RIP を無効にすると、指定したインターフェイスの RIP 設定が削除されます。
- IP ルーティングを無効にすると、RIP メッセージは送信されませんが、RIP メッセージを受信した場合、それらはルーティング テーブル情報を更新するために使用されます。

（注） RIP は、手動で設定されている IP インターフェイスでのみ定義できます。つまり、IP アドレスを DHCP サーバから受信したインターフェイス、または IP アドレスがデフォルトの IP アドレスであるインターフェイスでは RIP を定義できません。

RIPv2プロパティ

デバイスで RIPv2 を有効化または無効化するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [RIPv2] > [RIPv2 Properties] の順にクリックします。

ステップ 2 必要に応じて、次のオプションを選択します。

- [RIP]：次のオプションを使用できます。
  - [Enable]：RIP を有効にします。
  - [Disable]：RIP を無効にします。RIP を無効にすると、システムの RIP 設定は削除されます。
  - シャットダウン（Shutdown）：シャットダウンするための RIP のグローバルな状態を設定します。
- RIP アドバタイズメント（RIP Advertisement）：選択すると、すべての RIP IP インターフェイスでルーティング アップデートの送信が有効になります。
- デフォルト ルートのアドバタイズメント（Default Route Advertisement）：選択すると、RIP ドメインへのデフォルト ルートの送信が有効になります。このルートは、デフォルト ルートして機能します。
- [Default Metric]：デフォルトメトリックの値を入力します。

ステップ 3 [Redistribute Static Route]：手動で定義した（リモート）ルートを有効にする場合に選択します。

ステップ 4 [Redistribute Static Route] が有効な場合、[Redistribute Static Metric] フィールドのオプションを選択します。次のオプションを使用できます。

- [Default Metric]：RIP では、伝播するスタティックルートの設定にデフォルトメトリック値が使用されるようになります。
- [Transparent]：RIP では、ルーティング テーブル メトリックが RIP メトリックとして使用されるようになります。
  - スタティック ルートのメトリック値が 15 以下の場合、この値は、このスタティック ルートをアドバタイズするときに RIP プロトコルで使用されます。
  - スタティック ルートのメトリック値が 15 より大きい場合は、スタティック ルートは RIP を使用して他のルータにアドバタイズされません。
- ユーザ定義メトリック（User Defined Metric）：メトリックの値を入力します。

ステップ 5 [Redistribute Connected Route]：RIP が有効になっていない定義済みの IP インターフェイス（ローカルに定義されている）に対応する RIP ルートを有効にする場合に選択します。

ステップ 6 [Redistribute Connected Route] が有効な場合、[Redistribute Connected Metric] フィールドのオプションを選択します。次のオプションを使用できます。

- [Default Metric]：RIP では、伝播するスタティックルートの設定にデフォルトメトリック値が使用されるようになります。
- 透過型（Transparent）：RIP が、伝播されたスタティック ルート設定の RIP メトリックとして、ルーティング テーブル メトリックをを使用するようにします。この結果、次のように動作します。
  - スタティック ルートのメトリック値が 15 以下の場合、この値は、このスタティック ルートをアドバタイズするときに RIP プロトコルで使用されます。
  - スタティック ルートのメトリック値が 15 より大きい場合は、スタティック ルートは RIP を使用して他のルータにアドバタイズされません。
- ユーザ定義メトリック（User Defined Metric）：メトリックの値を入力します。

ステップ 7 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

RIPv2設定

IP インターフェイス上で RIP を設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [RIPv2] > [RIPv2 Settings] の順にクリックします。

ステップ 2 RIP パラメータは、IP インターフェイスごとに表示されます。新しい IP インターフェイスを追加するには、[Add] をクリックして、次のフィールドを入力します。

- IP アドレス（IP Address）：レイヤ 2 インターフェイスで定義されている IP インターフェイスを選択します。
- シャットダウン（Shutdown）：インターフェイスで RIP 構成を保持するが、インターフェイスを非アクティブに設定します。
- パッシブ（Passive）：指定した IP インターフェイスで RIP ルート更新メッセージの送信を許可するかどうかを指定します。このフィールドが有効になっていない場合は、RIP アップデートが送信されません（パッシブ）。
- オフセット（Offset）：指定した IP インターフェイスのメトリック数値を指定します。これには、インターフェイスの速度に基づいて、このインターフェイスを使用するための追加コストが反映されます。
- [Default Route Advertisement]：このオプションは、RIPv2プロパティ （238 ページ）ページでグローバルに定義されます。グローバルな定義を使用することもできれば、特定のインターフェイスに対してこのフィールドを定義することもできます。次のオプションを使用できます。

- [Global]：[RIPv2 Properties] に定義されているグローバル設定を使用します。画面
- [Disable]：この RIP インターフェイス上でデフォルトルートをアドバタイズしません。
- 有効化（Enable）：この RIP インターフェイス上でデフォルト ルートをアドバタイズします。

- デフォルト ルート アドバタイズメントのメトリック（Default Route Advertisement Metric）：このインターフェイスのデフォルト ルートのメトリックを入力します。
- 認証モード（Authentication Mode）：指定した IP インターフェイスの RIP 認証状態（有効/無効）。次のオプションを使用できます。
  - [None]：認証が実行されません。
  - テキスト（Text）：以下に入力されたキー パスワードが認証に使用されます。
  - MD5：以下で選択したキー チェーンの MD5 ダイジェストが認証に使用されます。
- キー パスワード（Key Password）：認証タイプとして [Text] を選択した場合は、使用するパスワードを入力します。
- キー チェーン（Key Chain）：認証モードとして [MD5] を選択した場合は、ダイジェスト対象のキーチェーンを入力します。このキーチェーンは、この項に記載されているように作成されます。
- [Distribute-list In]：[Access List Name] で指定した 1 つ以上の IP アドレスに対して RIP 着信ルートのフィルタリングを設定する場合に選択します。このフィールドが有効な場合は、次の [Access List Name] を選択します。
- [Access List Name]：指定した IP インターフェイスに割り当てる RIP 着信ルートフィルタリングのアクセスリスト名（IP アドレスの一覧を含む）を選択します。
- [Distribute-list Out]：[Access List Name] で指定した 1 つ以上の IP アドレスに対して RIP 発信ルートのフィルタリングを設定する場合に選択します。このフィールドが有効な場合は、次の [Access List Name] を選択します。
- [Access List Name]：指定した IP インターフェイスに割り当てる RIP 発信ルートフィルタリングのアクセスリスト名（IP アドレスの一覧を含む）を選択します。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

RIPv2統計情報

IP アドレスごとの RIP 統計情報カウンタを表示するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [RIPv2] > [RIPv2 Statistics] の順にクリックします。

次のフィールドが表示されます。

- IP インターフェイス（IP Interface）：レイヤ 2 インターフェイスで定義されている IP インターフェイス。
- 受信済み不良パケット（Bad Packets Received）：IP インターフェイスで RIP によって識別された不良パケットの数を指定します。
- 受信済み不正ルート（Bad Routes Received）：IP インターフェイスで RIP によって受信および識別された不正ルートの数を指定します。不正なルートとは、ルートパラメータが正しくないことを意味します。たとえば、IP 宛先がブロードキャストアドレスになっていたり、メトリックが 0 または 16 を超えていたりした場合です。
- 送信の更新（Update Sent）：IP インターフェイスで RIP によって送信されたパケットの数を指定します。

ステップ 2 すべてのインターフェイス カウンタをクリアするには、[Clear All Interface Counters] をクリックします。

RIPv2ピアルータデータベース

RIP ピアルータデータベースを表示するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [RIPv2] > [RIPv2 Peer Router Database] の順にクリックします。

ピア ルータ データベースに関する次のフィールドが表示されます。

- ルータの IP アドレス（Router IP Address）： レイヤ 2 インターフェイスで定義されている IP インターフェイス。
- 受信済み不良パケット（Bad Packets Received）：IP インターフェイスで RIP によって識別された不良パケットの数を指定します。
- 受信済み不正ルート（Bad Routes Received）：IP インターフェイスで RIP によって受信および識別された不正ルートの数を指定します。不正なルートとは、ルートパラメータが正しくないことを意味します。たとえば、IP 宛先がブロードキャストになっていたり、メトリックが 0 または 16 を超えていたりした場合です。
- 最終更新時間（Last Updated）：RIP がリモート IP アドレスから RIP ルートを最後に受信した時間を示します。

ステップ 2 すべてのカウンタをクリアするには、[Clear All Interface Counters] をクリックします。

アクセス リスト

アクセスリストは、デバイス上のトラフィックをフィルタ処理する permit および deny ステートメントで構成されます。これらのステートメントはトップダウン方式で実行されます。つま

り、トラフィックをアクセスリストで照合する際、アクセスリストは上から下に解析され、一致が検索されます。最初に一致したステートメントにより、トラフィックが許可されるか拒否されるかが決定されます。そのため、アクセスリストのステートメントの順序は非常に重要です。アクセスリストでは、限定性の最も高いものから最も低いものへとステートメントを順に並べる必要があります。これにより、意図しない一致が最小限に抑えられます。一致するものがない場合は、アクセスリストのすべてのステートメントの後には「すべて拒否」が暗黙的に存在します。

アクセスリストはスイッチが動作するために必要であり、セキュリティにとって不可欠です。

アクセスリスト設定

アクセスリストのグローバル設定を設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [Access List] > [Access List Settings] の順にクリックします。

ステップ 2 新しいアクセス リストを追加するには、[Add] をクリックして [Add Access List] ページを開き、次のフィールドを入力します。

- [Name]：アクセスリストの名前を定義します。
- [Source IPv4 Address]：送信元 IPv4 アドレスを入力します。次のオプションを使用できます。
  - 任意（Any）：すべての IP アドレスを含めます。
  - [User defined]：IP アドレスを入力します。
- [Source IPv4 Mask]：送信元 IPv4 アドレスマスクのタイプと値を入力します。次のオプションを使用できます。
  - [Network mask]：ネットワークマスクを入力します。
  - [Prefix length]：プレフィックス長を入力します。
- アクション（Action）：アクセス リストのアクションを選択します。次のオプションを使用できます。
  - [Permit]：アクセスリスト内の 1 つ以上の IP アドレスからのパケットのエントリを許可します。
  - [Deny]：アクセスリスト内の 1 つ以上の IP アドレスからのパケットのエントリを拒否します。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

送信元 IPv4 アクセス リスト

IP アドレスを使用してアクセスリストに入力するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [Access List] > [Source IPv4 Access List] の順にクリックします。

ステップ 2 アクセス リストのパラメータを変更するには、[Add] をクリックし、次のフィールドのいずれかを変更します。

- [Access List Name]：アクセスリストの名前。
- [Source IPv4 Address]：送信元 IPv4 アドレス。次のオプションを使用できます。
  - 任意（Any）：すべての IP アドレスを含めます。
  - [User defined]：IP アドレスを入力します。
- 送信元 IPv4 マスク（Source IPv4 Mask）：送信元 IPv4 アドレスのマスクのタイプと値。次のオプションを使用できます。
  - [ネットワークマスク]：ネットワーク マスク（255.255.0.0 など）を入力します。
  - [Prefix length]：プレフィックス長を入力します。
- [Action]：アクセスリストに対するアクション。次のオプションを使用できます。
  - [Permit]：アクセスリスト内の 1 つ以上の IP アドレスからのパケットのエントリを許可します。
  - [Deny]：アクセスリスト内の 1 つ以上の IP アドレスからのパケットのエントリを拒否します。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

ARP

デバイスは、直接接続されている IP サブネットに存在するすべての既知のデバイス用の ARP（Address Resolution Protocol）テーブルを保持します。直接接続されている IP サブネットとは、デバイスの IPv4 インターフェイスが接続されているサブネットのことです。デバイスがローカル デバイスにパケットを送信またはルーティングする必要がある場合、ARP テーブルを検索してデバイスの 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 アドレスの両方が含まれています。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。デバイスは、受信する ARP パケットからダイナミック アドレスを作成します。ダイナミック アドレスは、設定された時間が過ぎるとエージ アウトします。

（注） マッピング情報は、ルーティングと生成されたトラフィックの転送に使用されます。

ARP テーブルを定義するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [ARP] の順にクリックします。

ステップ 2 パラメータを入力します。

- [ARP エントリのエージングアウト] : ARP テーブル内でダイナミック アドレスを保 持する期間（単位：秒）を入力します。テーブルに登録されている期間が [ARP Entry Age Out] の時間を超えると、そのダイナミックアドレスはエージアウトします。ダイナミックアドレスは、エージアウトするとテーブルから削除され、再度学習された場合のみテーブルに戻されます。
- [ARP テーブルエントリのクリア] : システムから削除する ARP エントリのタイプを 選択します。
  - [All] : すべてのスタティックアドレスとダイナミックアドレスをただちに削除します。
  - [Dynamic] : すべてのダイナミックアドレスをただちに削除します。
  - [Static] : すべてのスタティックアドレスをただちに削除します。
  - 通常のエージ アウト（Normal Age Out）：設定されている ARP エントリ エージ アウト時間に基づいてダイナミック アドレスを削除します。

ステップ 3 [Apply] をクリックします。ARP グローバル設定が実行コンフィギュレーション ファイルに書き込まれます。

ARP テーブルには以下のフィールドが表示されます。

- [Interface] : IP デバイスが存在する、直接接続されている IP サブネットの IPv4 インターフェイス。
- [IP アドレス] : IP デバイスの IP アドレス。
- [MAC アドレス] : IP デバイスの MAC アドレス。
- [ステータス] : エントリのタイプ（手動で入力されたか、動的に学習されたか）。

ステップ 4 [Add] をクリックします。

ステップ 5 パラメータを入力します。

- [IP バージョン] : このホストでサポートされている IP アドレス形式。IPv4 だけがサポートされます。
- [Interface] : IPv4 インターフェイスをポート、LAG、または VLAN 上に設定できます。デバイスに設定されている IPv4 インターフェイスの一覧から、目的のインターフェイスを選択します。
- [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。
- [MAC アドレス] : ローカル デバイスの MAC アドレスを入力します。

ステップ 6 [Apply] をクリックします。ARP エントリが実行コンフィギュレーション ファイルに保存されます。

ARP プロキシ

プロキシ ARP 手法は、ネットワーク上にないネットワークアドレスに対する ARP クエリに応答するために、特定の IP サブネット上のデバイスによって使用されます。

（注） ARP プロキシ機能は、デバイスが L3 モードのときにのみ使用できます。

ARP プロキシはトラフィックの宛先を認識し、返信で別の MAC アドレスを提供します。別のホストの ARP プロキシとして機能することで、LAN トラフィックの宛先をホストに効果的に指示できます。キャプチャされたトラフィックは通常、別のインターフェイスを使用するか、またはトンネルを使用して、プロキシによって目的の宛先にルーティングされます。プロキシ目的で、異なる IP アドレスの ARP クエリ要求を受け、ノードが自身の MAC アドレスで応答するプロセスを、パブリッシングということがあります。

すべての IP インターフェイスで ARP プロキシを有効にするには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [ARP Proxy] の順にクリックします。

ステップ 2 [ARP Proxy] を選択して、デバイスがリモート ノードに関する ARP 要求にデバイス MAC アドレスで応答できるようにします。

ステップ 3 [Apply] をクリックします。ARP プロキシが有効になり、実行コンフィギュレーション ファイルが更新されます。

UDPリレー/IPヘルパー

一般的にスイッチは、IP サブネット間の IP ブロードキャストパケットのルーティングを行いません。ただし、この機能を使用すると、デバイスは、その IPv4 インターフェイスから受信した特定の UDP ブロードキャスト パケットを特定の宛先 IP アドレスにリレーできます。

特定の IPv4 インターフェイスから受信した UDP パケットの特定の宛先ポートへのリレーを設定するには、UDP リレーを追加します。

ステップ 1 [IPv4 Configuration] > [UDP Relay/IP Helper] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 設定されている UDP 宛先ポートに基づいてデバイスがリレーする UDP ブロードキャスト パケットの送信元となる [Source IP Interface] を選択します。このインターフェイスは、デバイスに設定されている IPv4 インターフェイスのいずれかである必要があります。

ステップ 4 デバイスがリレーするパケットの [UDP Destination Port] 番号を入力します。ドロップダウンメニューから既知のポートを選択するか、またはポート オプション ボタンをクリックして番号を手動で入力します。

ステップ 5 リレーする UDP パケットを受信する [Destination IP Address] を入力します。このフィールドが 0.0.0.0 である場合、UDP パケットは破棄されます。このフィールドが 255.255.255.255 である場合、UDP パケットはすべての IP インターフェイスにフラッディングされます。

ステップ 6 [Apply] をクリックします。UDP リレー設定が実行コンフィギュレーション ファイルに書き込まれます。

DHCP スヌーピング/リレー

ここでは、Dynamic Host Configuration Protocol（DHCP）スヌーピング/リレーについて説明します。DHCP リレー エージェントとは、クライアントとサーバー間で DHCP パケットを転送するホストです。リレー エージェントは、同一の物理サブネット上にないクライアントとサーバー間で要求および応答を転送するために使用されます。リレーエージェント転送は、IP ルータの通常の転送とは異なります。通常の転送では、IP データグラムがネットワーク間である程度透過的にスイッチングされます。これとは対照的に、リレーエージェントは DHCP メッセージを受信すると、DHCP メッセージを新たに生成して他のインターフェイスから送信します。

DHCP スヌーピングは、対応ネットワークスイッチのオペレーティングシステムに組み込まれたレイヤ 2 のセキュリティ技術であり、許容できないと判断した DHCP トラフィックをドロップします。DHCP スヌーピングは通常、不正な DHCP サーバーによる DHCP クライアントへの IP アドレスの提供を防止するために使用されます。

プロパティ

DHCP リレーは、DHCP パケットを DHCP サーバーに転送します。このデバイスは、IP アドレスが設定されていない VLAN から受信した DHCP メッセージを転送できます。IP アドレスのない VLAN で DHCP リレーを有効にすると、Option 82 が自動的に挿入されます。

DHCP スヌーピング/リレーのプロパティを設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping/Relay] > [Properties] の順にクリックします。

ステップ 2 次のフィールドを設定します。

- [DHCP Relay]：DHCP リレーを有効にする場合に選択します。
- [DHCPスヌーピングステータス]：DHCP スヌーピングを有効にする場合に選択します。
- Option 82 パス スルー（Option 82 Pass Through）：選択すると、パケットを転送する際に異種の Option 82 情報をそのままにします。
- MAC アドレスの確認（Verify MAC Address）：選択すると、レイヤ 2 ヘッダーの送信元 MAC アドレスが、DHCP で信頼できるポートの DHCP ヘッダー（ペイロードの一部）に表示されるクライアント ハードウェア アドレスに一致することを確認します。
- データベースのバックアップ（Backup Database）：選択すると、デバイスのフラッシュ メモリに DHCP スヌーピング バインディング データベースをバックアップします。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

ステップ 4 DHCP サーバを定義するには、**[Add]** をクリックします。[DHCPサーバーを追加] ダイアログが表示されます。IP バージョンが示されています。

ステップ 5 DHCP サーバの IP アドレスを入力し、**[Apply]** をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

オプション82の設定

Option 82（DHCP リレーエージェント情報オプション）は、ポートおよびエージェント情報を中央 DHCP サーバに渡して、割り当てられた IP アドレスがネットワークに物理的に接続されている場所を示します。オプション 82 の主な目的は、DHCP サーバが IP アドレスを取得する最適な IP サブネット（ネットワーク プール）を選択できるようにすることです。

オプション 82（有効になっている場合）は、DHCP スヌーピングおよび IP アドレスが設定されている DHCP リレーインターフェイスに適用されます。オプション 82 が有効になっていない場合でも、IP アドレスのない VLAN で DCHP リレーが有効になっていれば、この VLAN で受信された DHCP パケットにはオプション 82 情報が挿入されます。

DHCP メッセージ内のオプション 82 データのフォーマットとデバイスのステータスを設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping /Relay] > [Option 82 Settings] の順にクリックします。

次のフィールドに入力します。

- [オプション82挿入]：[有効] チェックボックスをオンにすると、オプション 82 情報がパケット内に挿入されます。
- [Numeric Token Format]：必要に応じて [Hexadecimal] または [Ascii] を選択します。このパラメータによって、次のトークンに使用するフォーマットが定義されます。
  - $int-ifindex$
  - $int-portid$
  - $switch-moduleid$
  - $vlan-id$

  たとえば、VLAN ID が 35 の $vlan-id$ トークンがあるとします。VLAN ID 35 は、16 進バイト 0x23 または ASCII 表現の値 0x3335 のどちらかで送信できます。下記の表に、各種トークンの詳細情報を示しています。

ステップ 2 [回線IDテンプレート] に入力します。デフォルトの回線 ID を使用する場合は [デフォルトを使用] を選択します。回線 ID を設定する場合は [ユーザー定義] を選択します。テキスト ボックスを使用して回線 ID テンプレートに入力します。テンプレートは、自由形式のテキストと事前定義済みトークンから成る文字列です（下記表を参照）。トークンを入力するには、手動で入力する方法と、ドロップダウンを使用して利用可能トークンリストからトークンを選択し、矢印ボタンをクリックして回線IDテキストに追加する方法があります。実際のサブオプション バイトの内容と、選択されたサブオプションのテキスト表現を確認するには、[プレビュー] ボタンを使用します。

ステップ 3 [リモートIDテンプレート] に入力します。該当するテキスト ボックスとドロップダウン リストを使用して、回線 ID テンプレートと同じ要領で入力します

（注） [サブオプションペイロードの合計] には、両サブオプションの予約済みバイト数が動的に更新されて表示されます。ペイロードは247以下である必要があります。バイト数は、サブオプションに含まれるトークンの予約済みの長さと、サブオプションで使用される自由形式テキストの文字数を加算した値に基づいています。

ステップ 4 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

ドロップダウンボックスから利用できるトークンを下記の表に示します。

オプション	説明	予約済みバイト数	16進数フォーマットでの使用バイト数	ASCII フォーマットでの使用バイト数
$int-ifindex$	DHCP クライアントリクエストが受信されたインターフェイスの ifIndex。 値は ifTable MIB エントリの ifIndex フィールドから取得されます。	4	2	4

オプション	説明	予約済みバイト数	16進数フォーマットでの使用バイト数	ASCII フォーマットでの使用バイト数
$int-portid$	個々のユニット（スタンドアロンユニットまたはスタッキング ユニット）に関連するインターフェイス番号。 物理インターフェイスの場合、この値の先頭は、個々のユニットの第 1 ポートでは 1、そのユニットの第 2 ポートでは 2、そのユニットの最終ポートでは N となります。 LAG インターフェイスの場合、この値は、LAG ID に基づいてグローバルに決定されます（個々のユニットには基づきません）。例：1,2,3…	2	1	2

オプション	説明	予約済みバイト数	16進数フォーマットでの使用バイト数	ASCII フォーマットでの使用バイト数
$int-name$	DHCP クライアント リクエストが受信されたインターフェイスのフル ネーム。 この名前は、このインターフェイスの情報を設定または表示する際にCLI が使用するインターフェイス フル ネーム フォーマットに基づいています。	32	該当なし	インターフェイス名を ASCII で表す場合に使用される実際のバイト数（最大で、予約済みバイト数の限度まで）
$int-abrvname$	DHCP クライアント リクエストが受信されたインターフェイスの略称。 このパラメータは、このインターフェイスの情報を設定または表示する際にCLI が使用するインターフェイス略称フォーマットに基づいています。	8	該当なし	

オプション	説明	予約済みバイト数	16進数フォーマットでの使用バイト数	ASCII フォーマットでの使用バイト数
$int-desc-16$	DHCP クライアントパケットが受信されたインターフェイスに関するインターフェイス記述。最大で（先頭の）16 バイトまで。 この変数の値は、インターフェイスレベルの「description」コマンドを使用してユーザーがインターフェイスに追加した記述から取得されます。 記述の長さが 16 バイトを超える場合でも、使用できる最大バイト数は（先頭の）16 バイトです。 ユーザーによって定義された記述のないインターフェイスの場合は、インターフェイス略称フォーマットが使用されます。	16	該当なし	インターフェイス記述を ASCII で表す場合に使用される実際のバイト数（最大で、予約済みバイト数の限度まで）

オプション	説明	予約済みバイト数	16進数フォーマットでの使用バイト数	ASCII フォーマットでの使用バイト数
$int-desc-32$	DHCP クライアント パケットが受信されたインターフェイスに関するインターフェイス記述。最大で（先頭の）32 バイトまで。 この変数の値は、インターフェイス レベルの「description」コマンドを使用してユーザーがインターフェイスに追加した記述から取得されます。 記述の長さが 32 バイトを超える場合でも、使用できる最大バイト数は（先頭の）32 バイトです。 ユーザーによって定義された記述のないインターフェイスの場合は、インターフェイス略称フォーマットが使用されます。	32	該当なし	インターフェイス記述を ASCII で表す場合に使用される実際のバイト数（最大で、予約済みバイト数の限度まで）
$int-desc-64$		64	該当なし	

オプション	説明	予約済みバイト数	16進数フォーマットでの使用バイト数	ASCII フォーマットでの使用バイト数
	DHCP クライアント パケットが受信されたインターフェイスに関するインターフェイス記述の全部分（最大で 64 バイトまで）。 この変数の値は、インターフェイスレベルの「description」コマンドを使用してユーザーがインターフェイスに追加した記述から取得されます。 ユーザーによって定義された記述のないインターフェイスの場合は、インターフェイス略称フォーマットが使用されます。			
$int-mac$	DHCP クライアント リクエストが受信された物理インターフェイスの MAC アドレス。 このフィールドの形式は常に 16 進数フォーマットとなり、区切り文字はありません（例：000000112205）。	6	6	該当なし

オプション	説明	予約済みバイト数	16進数フォーマットでの使用バイト数	ASCII フォーマットでの使用バイト数
$switch-mac$	オプション 82（リレー エージェント）を挿入するデバイスのベース MAC アドレス このフィールドの形式は常に 16 進数フォーマットとなり、区切り文字はありません（例：000000112200）。	6	6	該当なし
$switch-hostname-16$	デバイスのホスト名の先頭バイト。最大 16 バイトまで。	16	該当なし	ホスト名を ASCII で表す場合に使用される実際のバイト数（最大で、予約済みバイト数の限度まで）
$switch-hostname-32$	デバイスのホスト名の先頭バイト。最大 32 バイトまで。	32	該当なし	
$switch-hostname-58$	デバイスのホストのフル ネーム。	58	該当なし	
$switch-module-id$	DHCP クライアント リクエストが受信されたユニットのユニット ID。 スタンドアロン システムの場合、ID は常に 1。	2	1	2
$vlan-id$	DHCP クライアントリクエストが受信された VLAN の VLAN ID。 値：1 ～ 4094	4	2	4

オプション	説明	予約済みバイト数	16進数フォーマットでの使用バイト数	ASCII フォーマットでの使用バイト数
$vlan-name-16$	DHCP クライアント パケットが受信された VLAN に関する、VLAN 名の先頭バイト。最大 16 バイトまで。 指定された VLAN に名前が設定されていない場合は、ifTable MIB エントリの当該 VLAN ifDescr MIB フィールドから値が取得されます。	16	該当なし	VLAN 名を ASCII で表す場合に使用される実際のバイト数（最大で、予約済みバイト数の限度まで）
$vlan-name-32$	DHCP クライアント リクエストが受信された VLAN のフル ネーム。 指定された VLAN に名前が設定されている場合は、ifTable MIB エントリの当該 ifDescr MIB フィールドから値が取得されます。	32	該当なし	

（注） 両サブオプションのペイロードの予約済みバイト数の合計が 247 バイトを超えることはできません。バイト数は動的に更新されず、画面下部に表示されます。バイト数は、サブオプションに含まれるトークンの予約済みの長さ（上記参照）と、サブオプションで使用される自由形式テキストの文字数を、加算した値に基づいています。

インターフェイスの設定

すべてのインターフェイスまたは VLAN で DHCP リレーおよびスヌーピングを有効化できます。DHCP リレーが機能するには、VLAN またはインターフェイスに IP アドレスを設定する必要があります。

DHCPv4 リレーの概要

DHCP リレーは、DHCP サーバに DHCP パケットをリレーします。デバイスは、IP アドレスを持たない VLAN から受信した DHCP メッセージをリレーできます。IP アドレスのない VLAN で DHCP リレーを有効にすると、Option 82 が自動的に挿入されます。この挿入は特定の VLAN 内のものであり、Option 82 の挿入のグローバル管理状態には影響しません。

DHCPv4 スヌーピングの概要

DHCP スヌーピングは、偽の DHCP 応答パケットの受信を防止し、DHCP アドレスをログに記録するためのセキュリティメカニズムを提供します。これを行うために、DHCP スヌーピングではデバイスのポートは信頼できるポートまたは信頼できないポートのいずれかとして扱われます。信頼できるポートは、DHCP サーバに接続しており、DHCP アドレスの割り当てが許可されているポートです。信頼できるポートで受信した DHCP メッセージは、デバイスをパススルーできます。信頼できないポートは、DHCP アドレスの割り当てが許可されていないポートです。デフォルトでは、すべてのポートは、ユーザが（[Interface Settings] ページで）信頼できると宣言するまで、信頼できないポートであると見なされます。

特定のインターフェイス上で DHCP スヌーピング/リレーを有効にするには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping/Relay] > [Interface Settings] の順にクリックします。

ステップ 2 インターフェイス上で DHCP リレーまたは DHCP スヌーピングを有効にするには、[追加] をクリックします。

ステップ 3 有効にするインターフェイスと機能（**DHCP リレー**、**DHCP スヌーピング**、または両方）を選択します。

（注） DHCP スヌーピング設定は、選択したインターフェイスに IP アドレスが設定されている場合にのみ使用できます。

ステップ 4 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

DHCPスヌーピングで信頼されたインターフェイス

信頼できないポート/LAG からのパケットは DHCP スヌーピング バインディング データベースに照らしてチェックされます（DHCP スヌーピング バインディング データベース （257 ページ）を参照）。デフォルトでは、インターフェイスは信頼されていません。インターフェイスを信頼できるものとして指定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping/Relay] > [DHCP Snooping Trusted Interfaces] の順にクリックします。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ステップ 3 [Trusted Interface] （信頼できる場合は [Yes]、信頼できない場合は [No]）を選択します。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

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 バインディング データベースのメンテナンスについては、次の点に注意してください。

- ステーションが別のインターフェイスに移っても、デバイスは DHCP スヌーピング バインディング データベースを更新しません。
- ポートがダウンしても、そのポートのエントリは削除されません。
- VLAN の DHCP スヌーピングが無効になると、その VLAN 用に収集されたバインド エントリが削除されます。
- データベースが一杯になった場合、DHCP スヌーピングはパケットの転送を続行しますが、新しいエントリは作成されません。IP ソースガードや ARP インスペクションの機能がアクティブの場合、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ていないクライアントは、ネットワークに接続できません。

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、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Snooping/Relay] > [DHCP Snooping Binding Database] の順にクリックします。

DHCP スヌーピング バインディング データベース内の IP ソースガードに関するフィールドが表示されます。

- Status
  - [アクティブ] : デバイス上で IP ソース ガードがアクティブです。
  - [Inactive] : デバイス上で IP ソースガードがアクティブではありません。
- 理由
  - 問題なし（No Problem）
  - リソースなし（No Resource）
  - スヌープ VLAN なし（No Snoop VLAN）
  - ポートを信頼（Trust Port）

ステップ 2 エントリを追加するには、[Add] をクリックします。サポートされるアドレス タイプは IPv4 です。

ステップ 3 次のフィールドに入力します。

- [VLAN ID]：パケットを受信すると予想される VLAN。
- [MAC Address]：パケットの MAC アドレス。
- [IP Address]：パケットの IP アドレス。
- インターフェイス（Interface）：パケットを受信するユニット/スロット/インターフェイス。
- [Type]：フィールドで可能な値は、次のとおりです。
  - [ダイナミック]：エントリのリース時間は制限されています。
  - [スタティック]：エントリは静的に設定されています。
- リース時間（Lease Time）：エントリがダイナミックの場合は、DHCP データベースでエントリがアクティブである時間を入力します。リース時間がない場合、[Infinite] をチェックします。

ステップ 4 [Apply] をクリックします。設定が定義され、デバイスが更新されます。

ステップ 5 設定を削除するには、[Clear Dynamic] をクリックします。

DHCP サーバ

DHCP サーバー機能により、デバイスを DHCPv4 サーバーとして設定できます。DHCPv4 サーバーは、IPv4 アドレスやその他の情報を別のデバイス（DHCP クライアント）に割り当てるために使用されます。DHCPv4 サーバーは、IPv4 アドレスを、IPv4 アドレスのユーザー定義プールから割り当てます。

これらのモードは、次のいずれかになります。

- スタティック割り当て（Static Allocation）：ホストのハードウェアアドレスまたはクライアント ID が手動で IP アドレスにマッピングされます。
- ダイナミック割り当て（Dynamic Allocation）：クライアントはリースされた IP アドレスを指定された期間（無限に設定可能）にわたって取得します。DHCP クライアントが割り当てられた IP アドレスを更新しない場合は、この期間の終了時に IP アドレスが無効になり、クライアントは別の IP アドレスを要求する必要があります。

DHCP サーバーのプロパティ

デバイスを DHCPv4 サーバーとして設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Properties] の順にクリックして、[Properties] ページを表示します。

ステップ 2 DHCP サーバとしてデバイスを設定するには、[Enable] を選択します。

ステップ 3 [Apply]をクリックします。デバイスは、直ちにDHCPサーバとして機能します。ただし、プールを作成するまでクライアントに IP アドレスを割り当てません。

ネットワーク プール

デバイスが DHCP サーバーとして機能している場合は、1 つ以上の IP アドレスのプールを定義する必要があります。デバイスはそれらのプールから、DHCP クライアントに IP アドレスを割り当てます。各ネットワーク プールには、特定のサブネットに属しているアドレスの範囲が含まれています。これらのアドレスは、そのサブネット内のさまざまなクライアントに割り当てられます。

クライアントが IP アドレスを要求すると、DHCP サーバとしてのデバイスは、次に従って IP アドレスを割り当てます。

- [Directly Attached Client]：デバイスは、DHCP 要求の受信元であるデバイスの IP インターフェイスで設定されているサブネットと一致するサブネットを持つネットワークプールのアドレスを割り当てます。

  メッセージが（DHCP リレー経由ではなく）直接到着した場合、プールはローカルプールであり、入力レイヤ 2 インターフェイスに定義されている IP サブネットのいずれかに属しています。この場合、プールの IP マスクは、IP インターフェイスの IP マスク、および IP サブネットに属しているプールの最小 IP アドレスと最大 IP アドレスと等しくなります。

- リモート クライアント ：デバイスは、DHCP リレー エージェントの IP アドレスに一致する IP サブネットに属しているネットワーク プールから IP アドレスを取得します。

  メッセージが DHCP リレー経由で到着した場合、使用されるアドレスは、プールの最小 IP アドレスと IP マスクで指定された IP サブネットに属します。このプールはリモートプールです。

最大 16 個のネットワーク プールを定義できます。

IP アドレスのプールを作成し、リース期間を定義するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Network Pools] の順にクリックします。

定義済みのネットワークプールが表示されます。これらのフィールドについては、次の [Add] ページで説明されています。次のフィールドが表示されます（[Add] ページには表示されません）。

- リースされたアドレスの数（Number of Leased Addresses）：プール内の割り当て（リース）済みのアドレスの数。

ステップ 2 [Add] をクリックして、新しいネットワーク プールを定義します。サブネット IP アドレスとマスク、またはマスク、アドレス プール開始、およびアドレス プール終了のいずれかを入力することに注意してください。

ステップ 3 次のフィールドに入力します。

- [Pool Name]：プール名を入力します。
- サブネット IP アドレス（Subnet IP Address）：ネットワーク プールが存在するサブネットを入力します。
- [Mask]：次のいずれかを入力します。
  - ネットワーク マスク（Network Mask）：プールのネットワーク マスクを確認し、入力します。
  - プレフィックス長（Prefix Length）：アドレス プレフィックスを構成するビットの数を確認し、入力します。
- アドレス プールの開始（Address Pool Start）：ネットワーク プールの範囲の最初の IP アドレスを入力します。
- アドレス プールの開始（Address Pool End）：ネットワーク プールの範囲の最後の IP アドレスを入力します。
- リース期間（Lease Duration）：DHCP クライアントがこのプールから IP アドレスを使用できる時間を入力します。最大 49,710 日のリース期間または無制限の期間を設定できます。
  - 無制限（Infinite）：リースの期間に制限はありません。
  - [Days]：リースの期間（日数）。範囲は 0 ～ 49,710 日です。
  - [Hours]：リースの時間数。時間数の値を追加する前に、日数の値を指定する必要があります。
  - [Minutes]：リースの分数。分数の値を追加する前に、日数の値と時間数の値を指定する必要があります。
- [Default Router IP Address (Option 3)]：DHCP クライアントのデフォルトルータを入力します。
- [Domain Name Server IP Address（Option 6)]：デバイス DNS サーバー（設定済みの場合）の 1 つを選択するか、または [Other] を選択して DHCP クライアントが利用可能な DNS サーバーの IP アドレスを入力します。
- ドメイン名（オプション 15）（Domain Name (Option 15)）：DHCP クライアントのドメイン名を入力します。
- [NetBIOS WINS Server IP Address (Option 44)]：DHCP クライアントが利用可能な NetBIOS WINS ネームネーバを入力します。
- NetBIOS ノード タイプ（オプション 46）（NetBIOS Node Type (Option 46)）：NetBIOS 名を解決する方法を選択します。有効なノード タイプは次のとおりです。
  - ハイブリッド（Hybrid）：b ノードと p ノードのハイブリッドな組み合せが使用されます。h ノードを使用するように設定した場合、コンピュータは常に p ノードを最初に試行し、p ノードが失敗した場合にのみ、b ノードを使用します。これはデフォルトです。
  - 混合（Mixed）：b ノードと p ノードの通信の組み合わせを、NetBIOS 名を登録して解決するために使用します。M ノードは最初に b ノードを使用し、その後必要に応じて、p ノードを使用します。M ノードでは、b ノードが優先されるため、通常は大規模なネットワークにとって最適な選択肢ではありません。ブロードキャストによってネットワークトラフィックが増加します。

- ピア ツー ピア（Peer-to-Peer）：NetBIOS ネーム サーバとのポイントツー ポイント通信が、コンピュータ名を IP アドレスに登録して解決するために使用されます。
- ブロードキャスト（Broadcast）：IP ブロードキャスト メッセージは、NetBIOS 名を IP アドレスに登録して解決するために使用されます。

- [SNTP Server IP Address (Option 4)]：デバイスの SNTP サーバー（設定済みの場合）の 1 つを選択するか、または [Other] を選択して DHCP クライアントのタイムサーバーの IP アドレスを入力します。
- ファイル サーバの IP アドレス（siaddr）（File Server IP Address (siaddr)）：設定ファイルのダウンロード元である TFTP/SCP サーバの IP アドレスを入力します。
- ファイル サーバのホスト名（sname/オプション 66）（File Server Host Name (sname/Option 66)）：TFTP/SCP サーバの名前を入力します。
- 設定ファイル名（file/オプション 67）（Configuration File Name (file/Option 67)）：設定ファイルとして使用されるファイルの名前を入力します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

除外されるアドレス

デフォルトでは、DHCP サーバは、プール内のすべてのプールアドレスをクライアントに割り当てることができると仮定します。1 つの IP アドレスまたは IP アドレスの範囲を除外することができます。除外アドレスは、すべての DHCP プールから除外されます。

除外されるアドレス範囲を定義するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Excluded Addresses] の順にクリックします。

定義済みの除外される IP アドレスが表示されます。

ステップ 2 除外する IP アドレスの範囲を追加するには、[Add] をクリックし、次のフィールドに入力します。

- 開始 IP アドレス（Start IP Address）：除外 IP アドレスの範囲の最初の IP アドレス。
- 終了 IP アドレス（End IP Address）：除外 IP アドレスの範囲の最後の IP アドレス。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

スタティックホスト

一部の DHCP クライアントに、変化しないを永続的な IP アドレスを割り当てることができます。このようなクライアントは、スタティック ホストと呼ばれます。スタティック ホストは、最大 120 個定義できます。

特定のクライアントに固定 IP アドレスを手動で割り当てるには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Static Hosts] の順にクリックします。

スタティック ホストが表示されます。表示されるフィールドについては、次のフィールドを除いて [Add] ページで説明されています。

- MACアドレス/クライアント識別子

ステップ 2 スタティック ホストを追加するには、[Add] をクリックし、次のフィールドに入力します。

IP アドレス	ホストに静的に割り当てられた IP アドレスを入力します。
ホスト名	ホスト名を入力します。ホスト名には、シンボルの文字列と整数を指定できます。
Mask	スタティックホストのネットワークマスクを入力します。 • ネットワーク マスク（Network Mask）：スタティック ホストのネットワーク マスクを確認し、入力します。 • プレフィックス長（Prefix Length）：アドレス プレフィックスを構成するビットの数を確認し、入力します。
識別子タイプ	特定のスタティックホストを識別する方法を設定します。 • クライアント識別子（Client Identifier）：16 進数の表記法で指定されたクライアントの一意の ID を入力します（例：01b60819681172）。 または： • [MAC Address]：クライアントの MAC アドレスを入力します。 選択したタイプに従って、クライアント識別子または MAC アドレスを入力します。
Client Name	標準の ASCII 文字セットを使用して、スタティックホストの名前を入力します。クライアント名にはドメイン名を含めることはできません。
デフォルトルータIPアドレス(オプション3)	スタティックホストのデフォルトルータを入力します。
ドメインネームサーバーIPアドレス(オプション6)	デバイス DNS サーバー（設定済みの場合）の 1 つを選択するか、または [Other] を選択して DHCP クライアントが利用可能な DNS サーバーの IP アドレスを入力します。
ドメイン名(オプション15)	スタティックホストのドメイン名を入力します。
NetBIOS WINSサーバーIPアドレス(オプション44)	スタティックホストで使用可能な NetBIOS WINS ネームサーバーを入力します。

NetBIOSノードタイプ(オプション46)	NetBIOS名の解決方法を選択します。有効なノードタイプは次のとおりです。 • ハイブリッド（Hybrid）：b ノードと p ノードのハイブリッドな組み合せが使用されます。h ノードを使用するように設定した場合、コンピュータは常に p ノードを最初に試行し、p ノードが失敗した場合にのみ、b ノードを使用します。これはデフォルトです。 • 混合（Mixed）：b ノードと p ノードの通信の組み合わせを、NetBIOS 名を登録して解決するために使用します。M ノードは最初に b ノードを使用し、その後必要に応じて、p ノードを使用します。M ノードでは、b ノードが優先されるため、通常は大規模なネットワークにとって最適な選択肢ではありません。ブロードキャストによってネットワークトラフィックが増加します。 • ピア ツー ピア（Peer-to-Peer）：NetBIOS ネーム サーバとのポイントツーポイント通信が、コンピュータ名を IP アドレスに登録して解決するために使用されます。 • ブロードキャスト（Broadcast）：IP ブロードキャスト メッセージは、NetBIOS 名を IP アドレスに登録して解決するために使用されます。
SNTPサーバーIPアドレス(オプション4)	デバイスの SNTP サーバー（設定済みの場合）の 1 つを選択するか、または [Other] を選択して DHCP クライアントのタイムサーバーの IP アドレスを入力します。
ファイルサーバーIPアドレス(siaddr)	設定ファイルのダウンロード元 TFTP/SCP サーバーの IP アドレスを入力します。
ファイルサーバーホスト名(sname/オプション66)	TFTP/SCP サーバーの名前を入力します。
コンフィギュレーションファイル名(file/オプション67)	設定ファイルとして使用されるファイルの名前を入力します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

DHCP オプション

デバイスが DHCP サーバとして動作している場合は、16 進数オプションを使用して DHCP オプションを設定できます。これらのオプションの説明は、RFC2131 で確認できます。これらのオプションの設定により、設定された DHCP オプションの要求（オプション 55 を使用）が含まれているパケットを持つ DHCP クライアントに送信される応答が決定されます。例：DHCP オプション 66 は、[DHCP Options] ページで TFTP サーバの名前を指定して設定します。オプション 66 が含まれているクライアント DHCP パケットを受信すると、TFTP サーバがオプション 66 の値として返されます。

1 つ以上の DHCP オプションを設定するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [DHCP Options] の順にクリックします。

それまでに設定された DHCP のオプションが表示されます。

ステップ 2 設定されていないオプションを設定するには、次のフィールドに入力します。

- [DHCP Server Pool Name equals to]：ネットワーク プール （259 ページ）で定義されているネットワークアドレスのプールの 1 つを選択し、[Go] をクリックして、そのネットワークアドレスのプールを基準にしたフィルタ処理を行います。

ステップ 3 [Add] をクリックして、次のフィールドに入力します。

- プール名（Pool Name）：定義されているコードの対象となるプール名が表示されます。
- コード（Code）：DHCP オプション コードを入力します。
- タイプ（Type）：DHCP オプションのパラメータのタイプに応じて、このフィールドのオプション ボタンを変更します。次のいずれかのコードを選択し、DHCPオプションパラメータの値を入力します。
  - 16 進（Hex）：DHCP オプションのパラメータの 16 進数値を入力するかどうかを選択します。16 進数値は、他のタイプの値の代わりに指定できます。たとえば、IP アドレス自体ではなく、IP アドレスの 16 進値を指定できます。

    16進数値の検証は行われません。そのため、不正な値を表す16進数値を入力した場合は、エラーが提供されず、クライアントはサーバからの DHCP パケットを処理できない可能性があります。
  - IP ：これが選択した DHCPオプションに関連する場合は、IP アドレスを入力するかどうかを選択します。
  - [IP List]：複数の IP アドレスをカンマで区切ったリストを入力します。
  - 整数（Integer）：選択した DHCP オプションのパラメータの整数値を入力するかどうかを選択します。
  - ブール（Boolean）：選択した DHCPオプションのパラメータがブール値かどうかを選択します。
- ブール値（Boolean Value）：タイプがブール値である場合は、返される値（True または False）を選択します。
- [Value]：タイプがブーリアンでない場合に、このコードについて送信する値を入力します。
- 説明（Description）：ドキュメンテーションの目的でテキストの説明を入力します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

アドレスバインディング

[Address Binding] ページを使用して、デバイスによって割り当てられた IP アドレスと対応する MAC アドレスを表示および削除します。

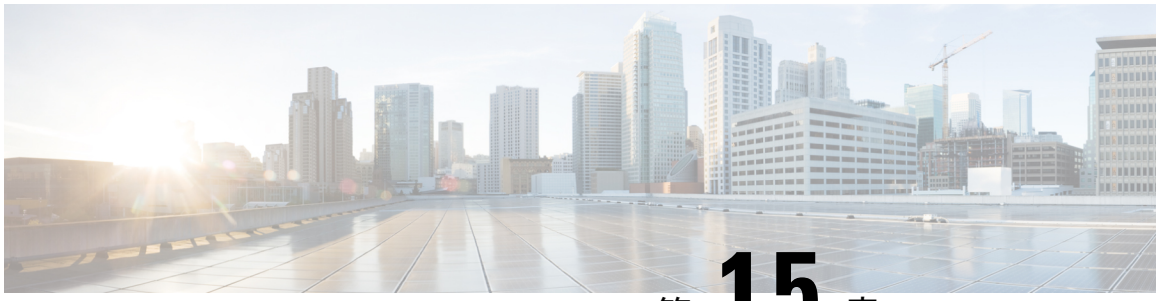
アドレスバインディングを表示または削除するには、次の手順を実行します。

ステップ 1 [IPv4 Configuration] > [DHCP Server] > [Address Binding] の順にクリックします。

アドレス バインドに関する次のフィールドが表示されます。

- [IP Address]：DHCP クライアントの IP アドレス。
- [Address Type]：DHCP クライアントのアドレスが MAC アドレスとして表示されるか、クライアント識別子を使用して表示されるかを示します。
- [MACアドレス/クライアント識別子]：MACアドレスとして、または16進表記（例：01b60819681172）として指定される、クライアントの固有識別子。
- リースの有効期限（Lease Expiration）：ホストの IP アドレスのリースの有効期日および時刻。
- タイプ（Type）：IP アドレスがクライアントに割り当てられた方法。オプションは次のいずれかです。
  - スタティック（Static）：ホストのハードウェア アドレスが IP アドレスにマッピングされています。
  - [Dynamic]：デバイスから動的に取得される IP アドレスが、指定された期間クライアントによって所有されている場合。指定された期間が終了するとIPアドレスは無効になり、クライアントは別の IP アドレスを要求する必要があります。
- [State]：次のオプションがあります。
  - 割り当て済み（Allocated）：IP アドレスが割り当てられています。スタティック ホストが設定されている場合は、その状態は割り当て済みです。
  - [Allocated]：IP アドレスは提供されているが受け入れられなかったため、割り当てられていません。
  - 期限切れ（Expired）：IP アドレスのリースの有効期限が切れています。
  - [Pre-Allocated]：エントリは、提供されたときから、クライアントから DHCP ACK が送信されるまでの間、事前割り当て済み状態になります。その後、割り当て済みになります。

ステップ 2 [Delete] をクリックします。実行コンフィギュレーション ファイルが更新されます。



第 15 章

IPv6 設定

この章は、次の項で構成されています。

IPv6グローバルコンフィギュレーション

インターネットプロトコルバージョン6（IPv6）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層プロトコルです。IPv6 は、展開されている主流のインターネット プロトコルである IPv4 を置き換えるように設計されました。IPv6 により、アドレス サイズが 32 ビットから 128 ビットのアドレスに増加するため、より柔軟に IP アドレスを割り当てることができます。IPv6 アドレスは 4 つの 16 進数の 8 つのグループとして記述されます。たとえば FE80:0000:0000:0000:0000:9C00:876A:130B などです。また、ゼロのグループを省略し、「::」で置き換えた省略形を使用することもできます。たとえば、FE80::9C00:876A:130B などです。IPv6 インターフェイスのアドレスは、ユーザーが手動で割り当てるか、または、DHCP サーバーから自動的に割り当てられます。

このセクションでは、デバイスの IPv6 アドレスを手動で、またはデバイスを DHCP クライアントにして定義することについて説明します。IPv6 グローバルパラメータおよび DHCPv6 クライアントの設定値を定義するには、次のようにします。

ステップ 1 [IPv6 Configuration] > [IPv6 Global Configuration] の順にクリックします。

ステップ 2 次のフィールドの値を入力します。

- [IPv6 Routing]：これを選択すると、IPv6 ルーティングが有効になります。これが有効になっていない場合、デバイスは（ルータではなく）ホストとして動作し、管理パケットは受信できますが、パケットの送信はできなくなります。ルーティングを有効にした場合、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、ネットワーク内のルータから送信された RA からオートコンフィグ操作を介してデバイスインターフェイスに割り当てられたすべてのアドレスが削除されます。

- ICMPv6 レート制限間隔（ICMPv6 Rate Limit Interval）：ICMP エラー メッセージが生成される頻度を入力します。

- ICMPv6 レート制限バケット サイズ（ICMPv6 Rate Limit Bucket Size）：間隔ごとにデバイスによって送信可能な ICMP エラー メッセージの最大数を入力します。

- IPv6ホップ リミット（IPv6 Hop Limit）：パケットが通過できる、最終的な宛先の途中にある中間ルータの最大数を入力します。別のルータにパケットが転送されるたびに、ホップ リミットが減少します。ホップ リミットがゼロに達すると、パケットは破棄されます。これにより、パケットが無限に転送されるのを防ぎます。

- DHCPv6 クライアント設定

  - 固有識別子（DUID）フォーマット（Unique Identifier (DUID) Format）：これは、DHCP サーバがクライアントを識別するために使用するDHCPクライアントの識別子です。次のいずれかのフォーマットを指定できます。

    [Link-Layer]：（デフォルト）。このオプションを選択した場合は、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（Enterprise Number）：このオプションを選択した場合は、次のフィールドに入力します。

  - エンタープライズ番号（Enterprise Number）：IANA によって管理される、ベンダーが登録したプライベート エンタープライズ番号。

  - [Identifier]：ベンダー定義の 16 進文字列（最大 64 文字の 16 進数）。文字列の数が偶数でない場合は、右側にゼロが追加されます。2 つの 16 進数文字は、それぞれピリオドまたはコロンで区切ることができます。

- DHCPv6一意の識別子(DUID)（DHCPv6 Unique Identifier (DUID)）：選択した識別子が表示されます。

ステップ 3 [Apply]をクリックします。IPv6グローバルパラメータおよびDHCPv6クライアント設定が更新されます。

IPv6インターフェイス

インターネットプロトコルバージョン6（IPv6）は、パケット交換インターネット通信に使用されるネットワーク層プロトコルです。IPv6は、最も広く使用されているインターネットプロ

トコルである IPv4 を置き換えるために作成されました。IPv6 では、IP アドレスのサイズが 32 ビットから 128 ビットに増加するため、IP アドレスをより柔軟に割り当てることができます。IPv6 アドレスは、FE80:0000:0000:0000:0000:9C00:876A:130B のように、4 桁の 16 進数の 8 つのグループで構成されます。

IPv4 しか使用できないネットワーク上で IPv6 ノード同士が通信するには、途中でマッピングする技術が必要です。この技術をトンネルと呼びます。トンネルを使用すれば、IPv6 にしか対応していないホストでも IPv4 サービスを利用できます。また、孤立した IPv6 ホストおよび IPv6 ネットワークが IPv4 インフラストラクチャを介して他の IPv6 ノードと接続できます。

IPv6 インターフェイスは、ポート、LAG、VLAN、ループバック インターフェイス、またはトンネルに設定できます。IPv6 インターフェイスを定義するには、次の手順を実行します。

ステップ 1 [IPv6 Configuration] > [IPv6 Interfaces] をクリックします。

ステップ 2 パラメータを入力します。

- IPv6 リンク ローカル デフォルト ゾーン（IPv6 Link Local Default Zone）：選択すると、デフォルト ゾーンを定義できるようになります。これは、指定されているインターフェイスなしで、またはデフォルト ゾーン 0 で到着したリンクローカル パケットを出力するために使用するインターフェイスです。
- IPv6 リンク ローカル デフォルト ゾーン インターフェイス（IPv6 Link Local Default Zone Interface）：デフォルト ゾーンとして使用するインターフェイスを選択します。これは、以前に定義されたトンネルまたはその他のインターフェイスになります。

ステップ 3 [Apply] をクリックしてデフォルト ゾーンを設定します。

IPv6 インターフェイス テーブルが次のフィールドとともに表示されます。

- [Tunnel Type]：[Manual]、[6to4]、および [ISATAP]。

ステップ 4 [Add] をクリックして、IPv6 インターフェイスを有効にする新しいインターフェイスを追加します。

ステップ 5 次のフィールドに入力します。

- [IPv6インターフェイス]：IPv6 アドレスの特定のポート、LAG、ループバック インターフェイス、または VLAN を選択します。

ステップ 6 インターフェイスを DHCPv6 クライアントとして設定して、インターフェイスが DHCPv6 サーバから情報（SNTP 設定や DNS 情報）を受信できるようにするには、[DHCPv6 Client] フィールドに入力します。

- [DHCPv6 Client]：インターフェイス上で DHCPv6 クライアント（ステートレスおよびステートフル）を有効にする場合に選択します。
- [高速コミット]：アドレス割り当てとその他の設定に対する 2 メッセージ交換の使用を有効にする場合に選択します。これが有効になっている場合は、クライアントが要請メッセージに高速コミット オプションを含めます。

- 最小情報更新時間（Minimum Information Refresh Time）：この値は、更新時間の最小値を指定するために使用します。サーバがこの値より小さい更新時間オプションを送信した場合は、この値が代わりに使用されます。[Infinite] または [User Defined] を選択して値を設定します。
- [Information Refresh Time]：この値は、DHCPv6 サーバーから受信する情報をデバイスが更新する頻度を示します。このオプションがサーバーから受信されない場合、ここに入力した値が使用されます。[Infinite] または [User Defined] を選択して値を設定します。

ステップ 7 追加の IPv6 パラメータを設定するには、次のフィールドに入力します。

- IPv6 アドレス自動設定（IPv6 Address Auto Configuration）：選択すると、ネイバーから送信されたルータ アドバタイズメントからの自動アドレス設定が有効になります。
- [DAD 試行回数]：このインターフェイスのユニキャスト IPv6 アドレスに対して Duplicate Address Detection（DAD; 重複アドレス検出）処理を実行しているとき に送信する、ネイバー送信要求メッセージの件数を入力します。DAD は、ユニ キャスト IPv6 アドレスを新規に割り当てる前に、そのアドレスが重複していないかどうかを検査する処理です。新しいアドレスは、DAD検証中は一時的な状態のままです。このフィールドに 0 を入力した場合は、指定したインターフェイスでの重複アドレス検出が無効になります。このフィールドに 1 を入力した場合は、フォローアップ伝送のない単一伝送が指定されます。
- [ICMPv6 メッセージの送信]：宛先到達不能メッセージを生成します。
- MLD バージョン（MLD Version）：IPv6 MLD のバージョン。
- IPv6 リダイレクト（IPv6 Redirects）：選択すると、ICMP IPv6 リダイレクト メッセージを送信できるようになります。これらのメッセージは、他のデバイスに対して、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通知します。

ステップ 8 [Apply] をクリックして、選択したインターフェイスで IPv6 処理を有効にします。通常の IPv6 インターフェイスには、次のアドレスが自動的に設定されます。

- デバイスの MAC アドレスに基づく EUI-64 形式のインターフェイス ID を使用したリンクローカル アドレス。
- すべてのノード リンク ローカル マルチキャスト アドレス（FF02::1）
- 要請ノード マルチキャスト アドレス（FF02::1:FFXX:X 形式）

ステップ 9 [Restart] をクリックして、DHCPv6 サーバーから受信するステートレス情報の更新を開始します。

ステップ 10 必要な場合は、[IPv6 Address Table] をクリックして、インターフェイスに IPv6 アドレスを手動で割り当てます。

ステップ 11 トンネルを追加するには、IPv6 トンネルテーブルの中でインターフェイスを選択して、[IPv6 Tunnel] をクリックします。

IPv6 トンネル

トンネルにより、IPv4 ネットワーク経由での IPv6 パケットの転送が実現されます。各トンネルには送信元IPv4アドレスがあり、手動トンネルの場合は宛先IPv4アドレスもあります。IPv6 パケットは、これらのアドレスの間でカプセル化されます。

ISATAP トンネル

デバイスは、1 つの Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）トンネルをサポートしています。ISATAP トンネルは、ポイントツーマルチポイント トンネルです。発信元アドレスは、デバイスの IPv4 アドレス（または IPv4 アドレスの 1 つ）です。ISATAP トンネルを設定する場合は、宛先 IPv4 アドレスはルータによって提供されます。次の点に注意してください。

- IPv6 リンク ローカル アドレスは、ISATAP インターフェイスに割り当てられます。最初の IP アドレスがインターフェイスに割り当てられ、次にインターフェイスがアクティブ化されます。
- ISATAP インターフェイスがアクティブな場合、ISATAP ルータ IPv4 アドレスは、ISATAP と IPv4 間のマッピングを使用して DNS 経由で解決されます。ISATAP DNS レコードが解決されない場合、ホストマッピングテーブル内の、ISATAPホストの名前とアドレスのマッピングが検索されます。
- DNS プロセスによって ISATAP ルータ IPv4 アドレスが解決されない場合は、ISATAP IP インターフェイスはアクティブのままです。システムには、DNSプロセスが解決されるまで ISATAP トラフィック用のデフォルト ルータがありません。

IPv6 トンネルを設定するには、次の手順を実行します。

ステップ 1 [IPv6 Configuration] > [IPv6 Tunnel] をクリックします。

ステップ 2 [Create ISATAP Tunnel] をクリックします。

ステップ 3 トンネル番号（1）とそのトンネルタイプ（ISATAP）が表示されます。

ステップ 4 次のフィールドを入力します。

- [送信元IPv4アドレス]：トンネルインターフェイスのローカル（送信元）IPv4アドレスを設定します。選択した IPv4 インターフェイスの IPv4 アドレスは、ISATAP トンネル インターフェイスを経由する IPv6 アドレスの一部を形成するために使用されます。IPv6 アドレスには、64 ビットのネットワーク プレフィックス fe80:: があり、残りの 64 ビットは 0000:5EFE と IPv4 アドレスを連結して形成されます。
  - 自動（Auto）：トンネル インターフェイス上で送信されるパケットの発信元アドレスとして、設定されているすべての IPv4 インターフェイスの中から最も低い IPv4 アドレスを自動的に選択します。

- 手動（Manual）：トンネルインターフェイス上で送信されるパケットの発信元アドレスとして使用するIPv4アドレスを指定します。IPv4アドレスが別のインターフェイスに移動した場合でも、トンネル インターフェイスのローカル アドレスは変更されません。

  （注） デバイスのIPv4アドレスが変化すると、トンネルインターフェイスのローカルアドレスも変化します。

- [Interface]：インターフェイスを指定します。

- [ISATAP Router Nam]：特定の自動トンネルルータドメイン名を表すグローバルストリングを設定するには、以下のいずれかのオプションを選択します。
  - デフォルトを使用（Use Default）：これは常に ISATAP です。
  - ユーザ定義（User Defined）：ルータのドメイン名を入力します。

ステップ 5 パラメータを入力します。

- ISATAP 要請間隔（ISATAP Solicitation Interval）：アクティブな ISATAP ルータが検出されない場合の ISATAP ルータ要請メッセージ間の秒数。この間隔は、[Default Value] または [User Defined] のいずれかの間隔です。
- ISATAP 堅牢性（ISATAP Robustness）：ルータ要請クエリの間隔を計算するために使用します。数値が大きいほど、クエリの頻度が高くなります。デフォルト値をそのまま使用するか、またはユーザー定義値を使用できます。

  （注） ISATAP トンネルは、基盤となる IPv4 インターフェイスが動作していない場合は動作しません。

ステップ 6 [Apply] をクリックし、実行コンフィギュレーション ファイルに ISATAP パラメータを保存します。

IPv6 アドレス

Ipv6 インターフェイスに IPv6 アドレスを割り当てるには、次の手順を実行します。

ステップ 1 [IPv6 Configuration] > [IPv6 Addresses] をクリックします。

ステップ 2 テーブルをフィルタ処理するには、インターフェイス名を選択し、[Go] をクリックします。インターフェイスがIPv6アドレステーブルに表示されます。これらのフィールドについては、次のフィールドを除いて [Add] ページで説明されています。

- アドレス送信元（Address Source）：アドレス送信元タイプ（DHCP、システム、スタティック）の 1 つが表示されます。
- [IPv6 Address Type]：IPv6 アドレスのタイプが表示されます。

- [IPv6 Address]：IPv6 アドレスが表示されます。
- [Preferred Lifetime]：優先ライフタイムのエントリが表示されます。
- 有効期間（Valid Lifetime）：エントリの有効期間が表示されます。
- 有効期限（Expiry Time）：有効期限が表示されます。

ステップ 3 [Add] をクリックします。

ステップ 4 フィールドの値を入力します。

オプション	説明
IPv6インターフェイス	IPv6 アドレスを定義するインターフェイスが表示されます。* が表示されている場合、これは IPv6 インターフェイスが設定されていますが、有効になっていないことを意味しています。
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（Link Local）：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 アドレス。リンク ローカル アドレスのプレフィックスは FE 80 で、ルーティングはできません。また、ローカル ネットワーク上の通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • グローバル（Global）：他のネットワークから表示可能で到達可能なグローバル ユニキャスト IPV6 タイプの IPv6 アドレス。 • エニーキャスト（Anycast）：IPv6 アドレスはエニーキャスト アドレスです。これは、通常は異なるノードに属するインターフェイスのセットに割り当てられます。エニーキャスト アドレスに送信されたパケットは、使用しているルーティング プロトコルの定義に従って、そのエニーキャスト アドレスが示す最も近いインターフェイスに送信されます。 （注） IPv6 アドレスが ISATAP インターフェイスにある場合、エニーキャストは使用できません。
IPv6 Address	インターフェイスには、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 アドレスが割り当てられますが、それに加え、受信されたルータ アドバタイズメントに基づいて、グローバル アドレスが自動的に割り当てられます。デバイスは、インターフェイスで最大 128 個のアドレスをサポートしています。各アドレスは、コロンで区切られた 16 ビット値を使用して 16 進数形式で指定された有効な IPv6 アドレスである必要があります。
Prefix Length	グローバル IPv6 プレフィックス部の長さ。0 ～ 128 の範囲の値を入力します。この値は、プレフィックス（アドレスのネットワーク部）を構成する、アドレスの上位ビットの数を意味します。

オプション	説明
EUI-64	EUI-64 パラメータを使用して、デバイスの MAC アドレスに基づく EUI-64 形式を使用することによりグローバル IPv6 アドレスのインターフェイス ID 部を識別する場合に選択します。

ステップ 5 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

IPv6 ルータ設定

次の項では、IPv6 ルータの設定方法について説明します。内容は次のとおりです。

ルータ アドバタイズメント

ルータ アドバタイズメント パケットには、ホストがインターネットで通信するために必要なレイヤ 3 IPv6 アドレスのネットワーク部など、IPv6 ホストの各種設定が含まれています。これにより、クライアントはアドレスのユニバーサルに一意のホスト部を生成し、アドレスを完成させます。この機能は、次のようにインターフェイスごとに有効化または抑制できます。

ステップ 1 [IPv6 Configuration] > [IPv6 Router Configuration] > [Router Advertisement] の順にクリックします。

ステップ 2 ルータ アドバタイズメント テーブルにリストされているインターフェイスを設定するには、[Edit] をクリックします。

ステップ 3 次のフィールドに入力します。

オプション	説明
ルータアドバタイズメントの抑制	インターフェイス上でIPv6ルータアドバタイズメントの伝送を抑制する場合は、[Yes] を選択します。
ルータ プリファレンス	ルータのプリファレンスとして、[Low]、[Medium]、または [High] のいずれかを選択します。ルータ アドバタイズメント メッセージは、このフィールドに設定されている優先順位で送信されます。優先順位が設定されていない場合、これらは中位の優先順位で送信されます。
アドバタイズメント間隔オプションを含める	選択すると、アドバタイズメント オプションがこのシステムで使用されます。このオプションは、訪問モバイル ノードに、そのノードがルータ アドバタイズメントを受信する予定である間隔を示します。ノードは、移動検出アルゴリズムでこの情報を使用できます。
ホップ リミット	これは、ルータがアドバタイズする値です。ゼロ以外の場合、ホストによってホップ限度として使用されます。

オプション	説明
マネージドアドレスコンフィギュレーションフラグ	接続されているホストに対して、アドレスを取得するためステートフル自動コンフィギュレーションを使用するよう指示する場合、このフラグを選択します。ホストは、ステートフルおよびステートレス自動設定を同時に使用できます。
他のステートフルコンフィギュレーションフラグ	[Other Stateful Configuration Flag]：接続されているホストに対して、その他の（アドレス以外の）情報を取得するためステートフル自動コンフィギュレーションを使用するよう指示する場合、このフラグを選択します。 （注） マネージドアドレス コンフィギュレーション フラグが設定されている場合、接続されているホストでは、ステートフル自動コンフィギュレーションを使用することにより、このフラグの設定には関係なく、その他の（アドレス以外の）情報を取得できます。
ネイバー要求再送信間隔	アドレスを解決する場合、またはあるネイバーに到達可能であるかどうかを試す場合に、ネイバー送信要求メッセージをネイバーに送信する際の再送信と再送信の間の時間を決定します（[User Defined]）。または、[Use Default] を選択して、システムのデフォルト値（1000）を使用します。
最大ルータアドバタイズメント間隔	ルータアドバタイズメントの時間間隔の最大値を入力します。 このコマンドを使用してルータがデフォルトルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメントの有効期間以内でなければなりません。他の IPv6 ノードとの同期を防ぐために、実際に使用される間隔は最小値と最大値の間の値からランダムに選択されます。
最小ルータアドバタイズメント間隔	ルータアドバタイズメントの時間間隔の最小値を入力するか（[User Defined]）、またはシステムデフォルトを使用する場合は [Use Default] を選択します。 （注） RA の間隔の最小値は、最大値の 75% 以上および 3 秒未満にはできません。
ルータアドバタイズメントライフタイム	このルータがデフォルトルータとして有効であり続ける残り時間を秒数で入力します。値がゼロの場合、それはデフォルトルータとして使用できなくなったことを示します。
Reachable Time	リモート IPv6 ノードが到達可能であると見なされる時間をミリ秒単位で入力するか（[User Defined]）、またはシステムデフォルトを使用する場合は [Use Default] オプションを選択します。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

IPv6プレフィックス

デバイスのインターフェイスに対してアドバタイズするプレフィックスを定義するには、次のようにします。

ステップ 1 [IPv6 Configuration] > [IPv6 Router Configuration] > [IPv6 Prefixes] の順にクリックします。

ステップ 2 必要に応じて、[Filter] フィールドを有効にして、[Go] をクリックします。フィルタに一致するインターフェイスのグループが表示されます。

ステップ 3 インターフェイスを追加するには、[Add] をクリックします。

ステップ 4 プレフィックスを追加する必要な IPv6 インターフェイスを選択します。

ステップ 5 次のフィールドに入力します。

オプション	説明
Prefix Address	IPv6 ネットワーク。この引数は、RFC 4293 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
Prefix Length	IPv6 プレフィックスの長さ。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示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
[Prefix Advertisement]	このプレフィックスをアドバタイズする場合に選択します。
有効なライフタイム	このプレフィックスが有効であり続ける時間、つまり無効になるまでの残り時間（秒数）。無効化されたプレフィックスから生成されたアドレスは、パケットの宛先または発信元アドレスとして表示されません。 • 無限（Infinite）：フィールドの無限を表す 4,294,967,295 に設定するには、この値を選択します。 • [User Defined]：値を入力します。
優先ライフタイム	このプレフィックスが優先であり続ける残りの時間（秒数）。この時間の経過後は、プレフィックスは新しい通信で発信元アドレスとして使用されなくなりますが、このようなインターフェイスで受信されたパケットは通常どおりに処理されます。優先有効期間は、有効期間より長くしてはなりません。 • 無限（Infinite）：フィールドの無限を表す 4,294,967,295 に設定するには、この値を選択します。 • [User Defined]：値を入力します。
オート コンフィギュレーション	インターフェイス上でステートレス自動設定を使用した IPv6 アドレスの自動設定を有効にして、インターフェイスの IPv6 処理を有効にします。アドレスは、ルータ アドバタイズメント メッセージで受信されたプレフィックスによって設定されます。

オプション	説明
プレフィックスステータス	次のオプションのいずれかを選択します。 • オンリンク（Onlink）：指定したプレフィックスをオンリンクとして設定します。指定したプレフィックスを含むアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。オンリンクプレフィックスは、接続されたプレフィックスとしてルーティングテーブルに挿入されます（L ビット セット）。 • 非オンリンク（No-Onlink）：指定したプレフィックスをオンリンクでないものとして設定します。非オンリンクプレフィックスは、接続されたプレフィックスとしてルーティング テーブルに挿入されますが、L ビット クリアでアドバタイズされます。 • オフリンク（Offlink）：指定したプレフィックスをオフリンクとして設定します。プレフィクスは L ビット クリアでアドバタイズされます。プレフィクスは、接続されたプレフィクスとしてルーティング テーブルに挿入されません。プレフィックスが接続されたプレフィックスとしてルーティング テーブルにすでに存在する場合（たとえば、IPv6 アドレスを追加してプレフィックスも設定された場合など）、そのプレフィックスは削除されます。

ステップ 6 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

IPv6デフォルトルータリスト

[IPv6 Default Router List] ページでは、デフォルトの IPv6 ルータ アドレスを設定および表示できます。このリストには、外部ネットワークとの間で送受信されるトラフィックを処理するための、このデバイスに対するデフォルトルータになり得るルータが表示されます（空の場合もあります）。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。デバイスは、1 つのスタティック IPv6 デフォルト ルータをサポートしています。ダイナミック デフォルト ルータは、デバイスの IPv6 インターフェイスにルータ アドバタイズメントを送信したルータです。

IP アドレスを追加または削除すると、次のイベントが発生します。

- IP インターフェイスを削除すると、すべてのデフォルト ルータの IP アドレスが削除されます。ダイナミック IP アドレスを削除することはできません。
- 複数のユーザ定義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。
- リンク ローカル タイプ（つまり「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定義するには、次の手順を実行します。

ステップ 1 [IPv6 Configuration] > [IPv6 Default Router List] をクリックします。

このページには、デフォルト ルータごとに次のフィールドが表示されます。

- [発信インターフェイス] : デフォルト ルータが接続されている発信 IPv6 インターフェイス。
- [デフォルトルータ IPv6 アドレス] : デフォルト ルータのリンク ローカル IP アドレス。
- [タイプ] : デフォルト ルータのタイプ。
  - スタティック（Static）：デフォルト ルータは [Add] ボタンを使用して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。
  - [Neighbor Discovery (ND)]：デフォルトルータは ND に設定されています。ネイバー探索プロトコルは、IPv6 ネットワーク内の異なるネイバーデバイス間の関係を識別するために使用されます。
- [Metric]：このホップのコスト。

ステップ 2 [Add] をクリックして、スタティック デフォルト ルータを追加します。

ステップ 3 次のフィールドに入力します。

- ネクスト ホップ タイプ（Next Hop Type）：パケットの送信先となる次の宛先の IP アドレス。これは、次の項目から構成されています。
  - グローバル（Global）：他のネットワークから表示可能で到達可能なグローバル ユニキャスト IPV6 タイプの IPv6 アドレス。
  - リンク ローカル（Link Local）：単独のネットワーク リンク上のホストを一意に識別する Ipv6 インターフェイスおよびIpv6アドレス。リンクローカルアドレスのプレフィックス部はFE80です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - ポイント ツー ポイント（Point to Point）：ポイントツーポイント トンネル。IPv6 ルーティング トンネルがサポートされる場合には、これがサポートされます。
- 発信インターフェイス（Outgoing Interface）：発信リンク ローカル インターフェイスが表示されます。
- デフォルトのルータの IPv6 アドレス（Default Router IPv6 Address）：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（Metric）：このホップのコストを入力します。

ステップ 4 [Apply] をクリックします。デフォルト ルータが実行コンフィギュレーション ファイルに保存されます。

IPv6ネイバー

[IPv6 Neighbors] ページでは、IPv6 インターフェイスの IPv6 ネイバーのリストを設定および表示できます。IPv6 ネイバー テーブル（IPv6 ネイバー探索キャッシュとも呼ぶ）には、デバイスと同じIPv6サブネットに存在するIPv6ネイバーのMACアドレスが表示されます。これは、IPv4 ARP テーブルの IPv6 版です。デバイスがそのネイバーと通信する必要がある場合、デバイスは IPv6 ネイバー テーブルを使用して、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、自動的に検出されたネイバー、または手動で設定されたエントリが表示されます。各エントリには、ネイバーが接続されているインターフェイス、をネイバーの 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 ネイバーを定義するには、次の手順を実行します。

ステップ 1 [IPv6 Configuration] > [IPv6 Neighbors] をクリックします。

オプションを選択して、クリアテーブルセクション内の IPv6 アドレスの一部またはすべてをクリアできます。

- [スタティックのみ] : スタティック IPv6 アドレス エントリを削除します。
- [ダイナミックのみ] : ダイナミック IPv6 アドレス エントリを削除します。
- [すべてのダイナミックおよびスタティック] : スタティック IPv6 アドレス エントリ とダイナミック IPv6 アドレス エントリを両方とも削除します。

ステップ 2 テーブルにネイバーを追加するには、[Add] をクリックします。

ステップ 3 次のフィールドが表示されます。

- [Interface] : 追加する隣接 IPv6 インターフェイスが表示されます。
- [IPv6 アドレス] : インターフェイスに割り当てられている IPv6 アドレスを入力しま す。有効な IPv6 アドレスを指定する必要があります。
- [MAC アドレス] : 入力した IPv6 アドレスに対応する MAC アドレスを入力します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ステップ 5 次に、IPv6 ネイバーテーブルに次の設定が表示されます。

- [インターフェイス] : 近隣 IPv6 インターフェイスのタイプ。
- [IPv6 アドレス] : ネイバーの IPv6 アドレス。
- [MAC アドレス] : 指定された IPv6 アドレスに対応する MAC アドレス。
- [タイプ] : 近隣探索キャッシュ情報エントリのタイプ（スタティックまたはダイナ ミック）。

- [状態] : IPv6 ネイバーのステータス。値は次のとおりです。
  - [未完了] : アドレス解決中です。ネイバーがまだ応答していません。
  - [到達可能] : ネイバーは到達可能であると認識されています。
  - [失効] : それまで認識されていたネイバーは到達不能になっています。トラフィックを送信する必要があるまで、到達可能性を確認するアクションは実行されません。
  - [遅延] : それまで認識されていたネイバーは到達不能になっています。インターフェイスは、事前定義された遅延時間にわたって遅延状態です。到達可能性の確認を受信しなかった場合、状態はプローブに変更されます。
  - [プローブ] : ネイバーが到達不能になっており、到達可能性を検査するためのユニキャスト ネイバー宛送信要求プローブを送信中です。
- ルータ（Router）：ネイバーがルータであるかどうかを指定します（[Yes] または [No]）。

ステップ 6 IP アドレスのタイプを [Static] から [Dynamic] に変更するには、アドレスを選択し、[Edit] をクリックし、[Edit IPv6 Neighbors] ページを使用します。

IPv6 プレフィックス リスト

一致条件に基づいてプレフィックスを許可または拒否するには、プレフィックス リストを permit または deny キーワードを指定して設定します。プレフィックスリストのどのエントリにも一致しないトラフィックには、暗黙の拒否が適用されます。プレフィックスリストエントリは、IP アドレスとビット マスクで構成されています。IP アドレスは、クラスフルなネットワーク、サブネット、または単一のホスト ルート用にできます。ビットマスクは 1 ～ 32 の数値です。

プレフィックス リストは、完全なプレフィックス長の一致、または ge キーワードと le キーワードが使用されている場合は範囲内の一致に基づいてトラフィックをフィルタリングするように設定されます。

プレフィックスリストを作成するには、次の手順を実行します。

ステップ 1 **[IPv6 Configuration]** > **[IPv6 Prefix List]** の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [List Name]：次のいずれかのオプションを選択します。
  - [Use existing list]：プレフィックスの追加先となる定義済みリストを選択します。
  - [新しいリストの作成]：作成する新しいリストの名前を入力します。

- シーケンス番号（Sequence Number）：プレフィックス リスト内でのプレフィックスの場所を指定します。次のオプションのいずれかを選択します。
  - 自動番号（Auto Numbering）：プレフィックス リストの最後のエントリの後に新しい IPV6 プレフィックスを配置します。シーケンス番号は、最後のシーケンス番号に 5 を加算した番号です。リストが空の場合は、最初のプレフィックスリスト エントリには番号 5 が割り当てられ、後続のプレフィックス リスト エントリは 5 ずつ増分します。
  - ユーザ定義（User Defined）：パラメータで指定された場所に新しい IPV6 プレフィックスを配置します。その番号のエントリが存在する場合、新しいものに置き換えられます。
- ルール タイプ（Rule Type）：プレフィックス リストのルールを入力します。
  - [Permit]：条件に一致するネットワークを許可します。
  - [Deny]：条件に一致するネットワークを拒否します。
  - [Description]：テキスト。
- [IPv6 Prefix]：IP ルートプレフィックス。
- プレフィックス長（Prefix Length）：IP ルート プレフィックス長。
- より大きい（Greater Than）：一致に使用する最小プレフィックス長。次のオプションのいずれかを選択します。
  - 制限なし（No Limit）：最小プレフィックス長を一致に使用しません。
  - ユーザ定義（User Defined）：照合される最小プレフィックス長。
- より小さい（Lower Than）：一致に使用する最大プレフィックス長。次のオプションのいずれかを選択します。
  - 制限なし（No Limit）：最大プレフィックス長を一致に使用しません。
  - ユーザ定義（User Defined）：照合される最大プレフィックス長。
- [Description]：プレフィックスリストの説明を入力します。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

IPv6 アクセス リスト

IPv6 アクセス リストは、[MLD Proxy] > [Global MLD Proxy Settings] > [SSM IPv6 Access List] ページで使用できます。

アクセスリストを作成する手順は、次のとおりです。

ステップ 1 [IPv6 Configuration] > [IPv6 Access List] の順にクリックします。リスト中のエントリのサブセットを表示するには、該当する検索条件をフィルタに入力して、[実行] をクリックします。

ステップ 2 アクセス リストを追加するには、[Add] をクリックして次のフィールドに入力します。

- [Access List Name]：次のいずれかを選択します。
  - [既存のリストの使用]：既存のアクセス リストを選択します。
  - 新しいリストを作成（Create new list）：新しいアクセス リストの名前を入力します。
- [Source IPv6 Address]：送信元 IPv6 アドレスを入力します。次のオプションを使用できます。
  - 任意（Any）：すべての IP アドレスを含めます。
  - [User Defined]：IP アドレスを入力します。
- プレフィックス長（Prefix length）：送信元 IPv6 プレフィックス長を入力します。
- アクション（Action）：アクセス リストのアクションを選択します。次のオプションを使用できます。
  - 許可（Permit）：アクセス リスト内の IP アドレスからのパケットのエントリを許可します。
  - 拒否（Deny）：アクセス リスト内の IP アドレスからのパケットのエントリを拒否します。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

IPv6ルート

IPv6 転送テーブルには、設定済みのさまざまなルートが含まれています。それらのルートの 1 つはデフォルトルート（IPv6 アドレスは「0」）です。このルートは、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するものです。デフォルト ルートに加えて、このテーブルには、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 ルートも含まれています。デバイスで使用されているデフォルト ルータが、デバイスの通信先 IPv6 サブネットとの間でトラフィックをルーティングしているルータでない場合に、ICMP リダイレクトメッセージが送信されます。

IPv6 ルートを表示するには：

[IPv6 Configuration] > [IPv6 Routes] の順にクリックします。

このページには、次のフィールドが表示されます。

- [IPv6 Prefix]：宛先 IPv6 サブネットアドレスの IP ルート アドレス プレフィックス。
- [Prefix Length]：宛先 IPv6 サブネットアドレスの IP ルートプレフィックス長。前にスラッシュ（/）を付けます。

- 発信インターフェイス（Outgoing Interface）：パケットを転送するために使用されるインターフェイス。
- [Next Hop]：パケット転送先アドレスのタイプ。通常、これは隣接するルータのアドレスです。次のいずれかのタイプを指定できます。
  - リンク ローカル（Link Local）：単独のネットワーク リンク上のホストを一意に識別する Ipv6 インターフェイスおよび Ipv6 アドレス。リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1つのリンク ローカルアドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - グローバル（Global）：他のネットワークから表示可能で到達可能なグローバルユニキャスト IPV6 タイプの IPv6 アドレス。
  - [Point to Point]：ポイントツーポイント トンネル。
- [Metric]：このルートを、IPv6 ルートテーブル内にある同一宛先の他ルートと比較する際に使用される値。すべてのデフォルトルートに同じ値が設定されています。
- ライフタイム（Lifetime）：パケットが削除されるまでに送信および再送信できる期間。
- [ルートタイプ] : 宛先アドレスが割り当てられた方法、および、エントリの取得に使 用された方式。以下の値を指定できます。
  - [S (Static)]：エントリは、ユーザーによって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 ルータから受信された ICMP リダイレクト ダイナミック ルートです。
  - ND（ルータ アドバタイズメント）：エントリは、ルータ アドバタイズメント メッセージから取得されます。

ステップ 1 新しいルートを追加するには、[Add]をクリックし、上記のフィールドに入力します。さらに、次のフィールドに入力します。

- [IPv6 Address]：新しいルートの IPv6 アドレスを追加します。

ステップ 2 [Apply] をクリックして、変更内容を保存します。

DHCPv6リレー

DHCPv6 リレーは、DHCPv6 メッセージを DHCPv6 サーバにリレーするために使用されます。これは RFC 3315 の中で定義されています。

DHCPv6 クライアントが DHCPv6 サーバーに直接接続されていない場合、この DHCPv6 クライアントが直接接続されている DHCPv6 リレーエージェント（デバイス）は、直接接続されている DHCPv6 クライアントから受信したメッセージをカプセル化し、DHCPv6 サーバーに転送します。

逆方向の場合は、リレー エージェントは DHCPv6 サーバから受信したパケットのカプセル化を解除して、それらを DHCPv6 クライアントに転送します。

ユーザは、パケットの転送先となる DHCP サーバのリストを設定する必要があります。2 つの DHCPv6 サーバ セットを設定することができます。

- グローバル宛先（Global Destinations）：パケットは常にこれらの DHCPv6 サーバにリレーされます。
- インターフェイス リスト（Interface List）：これは、インターフェイスごとの DHCPv6 サーバのリストです。DHCPv6 パケットがインターフェイスで受信されると、パケットは、インターフェイス リスト上のサーバ（存在する場合）とグローバル宛先リスト上のサーバの両方にリレーされます。

グローバル宛先

すべての DHCPv6 パケットのリレー先となる DHCPv6 サーバーのリストを設定するには、次の手順を実行します。

ステップ 1 **[IPv6 Configuration]** > **[DHCPv6 Relay]** > **[Global Destinations]** をクリックします。

ステップ 2 デフォルトの DHCPv6 サーバを追加するには、[Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- IPv6 アドレス タイプ（IPv6 Address Type）：クライアント メッセージを転送する宛先アドレスのタイプを入力します。アドレスタイプは、[Link Local]、[Global]、または [Multicast]（All_DHCP_Relay_Agents_and_Servers）のいずれかです。
- [DHCPv6 Server IP Address]：パケット転送先の DHCPv6 サーバーのアドレスを入力します。
- IPv6 インターフェイス（IPv6 Interface）：DHCPv6 サーバのアドレス タイプがリンク ローカルまたはマルチキャストの場合にパケットが送信される宛先インターフェイスを入力します。このインターフェイスは、VLAN、LAG、またはトンネルです。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

インターフェイスの設定

インターフェイスで DHCPv6 リレー機能を有効にし、DHCPv6 サーバーのリストを設定するには、次の手順を実行します。

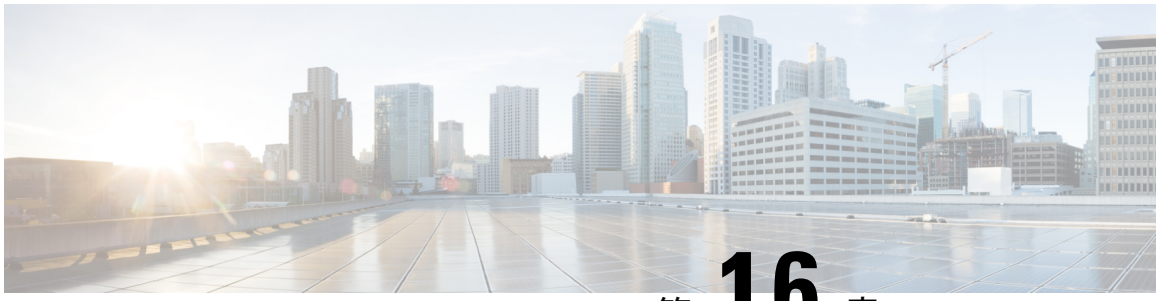
ステップ 1 **[IPv6 Configuration]** > **[DHCPv6 Relay]** > **[Interface Settings]** の順にクリックします。

ステップ 2 [Administration] > [Stack Management] をクリックします。

次のフィールドに入力します。

- [Source Interface]：DHCPv6 リレーを有効にするインターフェイス（ポート、LAG、VLAN、またはトンネル）を選択します。
- グローバル宛先のみを使用（Use Global Destinations Only）：選択すると、パケットが DHCPv6 グローバル宛先サーバのみに転送されます。
- IPv6 アドレス タイプ（IPv6 Address Type）：クライアント メッセージを転送する宛先アドレスのタイプを入力します。アドレスタイプは、[Link Local]、[Global]、または [Multicast]（All_DHCP_Relay_Agents_and_Servers）のいずれかです。
- [DHCPv6 Server IP Address]：パケット転送先の DHCPv6 サーバーのアドレスを入力します。
- [Destination IPv6 Interface]：ドロップダウンメニューから宛先 IPv6 インターフェイスを選択します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。



第 16 章

全般 IP 設定

IP インターフェイス アドレスは、ユーザが手動で設定するか、または DHCP サーバによって自動的に設定できます。この項では、デバイスの IP アドレスを手動で定義する、またはデバイスを DHCP クライアントにすることによって定義するための情報を提供します。

ポリシーベース ルーティング

ポリシーベース ルーティング（PBR）は、分類のために ACL を使用して、パケットのフィールドに基づいて、選択したパケットをネクスト ホップ アドレスにルーティングする手段を提供します。PBR により、ルーティング プロトコルから得られるルートへの依存が軽減されます。

ルート マップ

ルート マップは、PBR を設定するために使用する手段です。

ルートマップを追加するには、次の手順を実行します。

ステップ 1 [General IP Configuration] > [Policy Based Routing] > [Route Maps] の順にクリックします。

ステップ 2 [Add] をクリックして、パラメータを入力します。

- ルート マップ名（Route Map Name）：ルート マップを定義するために次のいずれかのオプションを選択します。
  - 既存のマップを使用（Use existing map）：以前に定義したルート マップを選択して新しいルールを追加します。
  - 新しいマップを作成（Create new map）：新しいルート マップの名前を入力します。

- シーケンス番号（Sequence Number）：指定されたルート マップでのルールの位置/優先順位を示す番号。ルート マップに複数のルール（ACL）が定義されている場合、シーケンス番号により、パケットが ACL と照合される順序（小さい番号から大きい番号の順）が決定されます。
- ルート マップ IP タイプ（Route Map IP Type）：ネクスト ホップ IP アドレスのタイプに応じて、IPv4 または IPv6 のいずれかを選択します。
- [Match ACL]：定義済みの ACL を選択します。パケットは、この ACL と照合されます。
- IPv6 ネクスト ホップ タイプ（IPv6 Next Hop Type）：ネクスト ホップ アドレスが IPv6 アドレスの場合は、次の特性のいずれかを選択します。
  - グローバル（Global）：他のネットワークから表示可能で到達可能なグローバル ユニキャスト IPV6 タイプの IPv6 アドレス。
  - リンク ローカル（Link Local）：単独のネットワーク リンク上のホストを一意に識別する Ipv6 インターフェイスおよびIpv6アドレス。リンクローカルアドレスのプレフィックス部はFE80です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。
- インターフェイス（Interface）：発信リンク ローカル インターフェイスが表示されます。
- ネクスト ホップ（Next Hop）：ネクスト ホップのルータの IP アドレス。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ルートマップバインディング

ルート マップにバインドされているインターフェイスで受信され、ルート マップ ルールに一致するすべてのパケットは、ルールで定義されているネクスト ホップにルーティングされます。

インターフェイスをルートマップにバインドするには、次の手順を実行します。

ステップ 1 [General IP Configuration] > [Policy Based Routing] > [Route Maps Binding] の順にクリックします。

ステップ 2 [Add] をクリックして、パラメータを入力します。

- [Interface]：インターフェイス（IP アドレスが付帯）を選択します。
- IPv4 ルート マップをバインド（Bound IPv4 Route Map）：インターフェイスにバインドする IPv4 ルート マップを選択します。
- IPv6 ルート マップをバインド（Bound IPv6 Route Map）：インターフェイスにバインドする IPv6 ルート マップを選択します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ポリシーベース ルート

定義されているルートマップを表示するには、次の手順を実行します。

ステップ 1 [General IP Configuration] > [Policy Based Routing] > [Policy Based Routes] の順にクリックします。

ステップ 2 以前に定義されたルート マップが表示されます。

- インターフェイス名（Interface Name）：ルート マップがバインドされているインターフェイス。
- [Route Map Name]：ルートマップの名前。
- ルート マップの状態（Route Map Status）：インターフェイスの状態。
  - [Active]：インターフェイスは起動しています。
  - [Interface Down]：インターフェイスは停止しています。
- ACL 名（ACL Name）：ルート マップに関連付けられている ACL。
- ネクスト ホップ（Next Hop）：ルート マップに一致するパケットのルーティング先。
- [Next Hop Status]：次に示すネクストホップの到達可能性。
  - アクティブ（Active）：ネクスト ホップ IP アドレスに到達可能です。
  - [Unreachable]：ネクストホップ IP アドレスに到達できないという事実のため、状態はアクティブではありません。
  - [Not Direct]：ネクストホップ IP アドレスはデバイスサブネットに直接アタッチされていないという事実のため、状態はアクティブではありません。

ドメインネームシステム

ドメイン ネーム システム（DNS）は、ホストを特定してアドレス指定するためにドメイン名を IP アドレスに変換します。

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

DNS の設定

[DNS Settings] ページを使用して、DNS 機能を有効にし、DNS サーバを設定し、デバイスで使用されるデフォルト ドメインを設定します。DNS 設定を行うには、次の手順を実行します。

ステップ 1 [General IP Configuration] > [DNS] > [DNS Settings] の順にクリックします。

ステップ 2 基本モードで、パラメータを入力します。

- サーバ定義（Server Definition）：DNS サーバを定義するために次のいずれかのオプションを選択します。
  - [By IP Address]：DNS サーバーの IP アドレスを入力します。
  - 無効（Disabled）：DNS サーバは定義されません。
- [Server IP Address]：前述の [By IP Address] を選択した場合は、DNS サーバーの IP アドレスを入力します。
- デフォルト ドメイン名（Default Domain Name）：非修飾ホスト名を完了するために使用する DNS ドメイン名を入力します。デバイスでこのドメイン名がすべての非完全修飾ドメイン名（NFQDN）に付加され、FQDN になります。

  （注） 非修飾名とドメイン名を区切る最初のピリオドは含めないようにしてください（cisco.com など）。

ステップ 3 拡張モードで、パラメータを入力します。

- DNS：選択すると、デバイスが DNS クライアントとして指定され、1 つまたは複数の設定済みの DNS サーバを通じて DNS 名を IP アドレスに解決できるようになります。
- [Polling Retries]：デバイスが DNS サーバーが存在しないと判断するまで、DNS クエリを DNS サーバーに送信する回数を入力します。
- [Polling Timeout]：DNS クエリに対する応答をデバイスが待機する秒数を入力します。
- ポーリング間隔（Polling Interval）：デバイスが再試行回数への到達後に DNS クエリ パケットを送信する頻度を（秒単位で）入力します。
  - [Use Default]：デフォルト値を使用する場合に選択します。

    この値 = 2*(ポーリング再試行回数 + 1)* ポーリング タイムアウト
  - ユーザ定義（User Defined）：ユーザ定義の値を入力する場合に選択します。
- [Default Parameters]：以下のデフォルトパラメータを入力します。
  - デフォルト ドメイン名（Default Domain Name）：非修飾ホスト名を完了するために使用する DNS ドメイン名を入力します。デバイスでこのドメイン名がすべての非完全修飾ドメイン名（NFQDN）に付加され、FQDN になります。

    （注） 非修飾名とドメイン名を区切る最初のピリオドは含めないようにしてください（cisco.com など）。
  - [DHCP Domain Search List]：[Details] をクリックして、デバイス上で設定されている DNS サーバーのリストを表示します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

[DNS Server Table] に、設定されている DNS サーバごとに次の情報が表示されます。

- [DNS Server]：DNS サーバーの IP アドレス。
- 優先順位（Preference）：各サーバには優先順位が設定されています。値が低いほど使用される可能性が高くなります。
- [Source]：サーバーの IP アドレスの送信元（スタティック、DHCPv4、DHCPv6 のいずれか）
- [Interface]：サーバーの IP アドレスのインターフェイス。

ステップ 5 最大 8 個の DNS サーバを定義できます。DNS サーバを追加するには、[Add] をクリックします。

ステップ 6 パラメータを入力します。

- [IP バージョン]：IPv6 の場合は [バージョン 6]、IPv4 の場合は [バージョン 4] を選択 します。
- [IPv6 アドレスタイプ]：IPv6 を使用する場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [リンクローカル]：IPv6 アドレスによって、同一ネットワーク リンク上のホスト が一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [グローバル]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
- [Link Local Interface]：IPv6 アドレスタイプがリンクローカルである場合、その受信元のインターフェイスを選択します。
- [DNS サーバー IP アドレス]：DNS サーバーの IP アドレスを入力します。
- 優先順位（Preference）：ドメインを使用する順序（低から高）を決定する値を選択します。これは実質的に、DNS クエリの間に非修飾名が完了する順序を決定します。

ステップ 7 [Apply] をクリックします。DNS サーバが実行コンフィギュレーション ファイルに保存されます。

検索リスト

検索リストには、ユーザー、DNS の設定 （289 ページ）ページ、および DHCPv4 と DHCPv6 のサーバーから受信した動的エントリによって定義される 1 つのスタティックエントリが含まれる場合があります。

デバイス上で設定されたドメイン名を表示するには、[General IP Configuration] > [DNS] > [Search List] の順にクリックします。

デバイスで設定されている DNS サーバごとに、次のフィールドが表示されます。

- ドメイン名（Domain Name）：デバイスで使用できるドメインの名前。
- [Source]：このドメインのサーバーのIPアドレスの送信元（スタティック、またはDHCPv4、または DHCPv6）。
- インターフェイス（Interface）：このドメインのサーバの IP アドレスのインターフェイス。
- 優先順位（Preference）：ドメインを使用する順序（低から高）。これは実質的に、DNS クエリの間に非修飾名が完了する順序を決定します。

ホストマッピング

ホスト名/IPアドレスのマッピングは、ホストマッピングテーブル（DNSキャッシュ）に格納されます。

このキャッシュには、次のタイプのエントリを含めることができます。

- スタティック エントリ（Static Entries）：これらは、キャッシュに手動で追加されるマッピング ペアです。最大 64 個のスタティック エントリを追加できます。
- [Dynamic Entries]：ユーザーが使用したためにシステムによって追加されたマッピングペアか、または DHCP によってデバイスに設定された IP アドレスごとに 1 つエントリがあるマッピングペアです。256 個のダイナミック エントリを追加できます。

名前解決は常にスタティックエントリを確認することによって開始され、続いてダイナミックエントリを確認し、外部 DNS サーバに要求を送信することによって終了します。ホスト名あたりの DNS サーバごとに 8 個の IP アドレスがサポートされています。

ホスト名とその IP アドレスを追加するには、次の手順を実行します。

ステップ 1 [General IP Configuration] > [DNS] > [Host Mapping] の順にクリックします。

ステップ 2 必要に応じて、[Clear Table] から次のオプションのいずれかを選択して、ホストマッピングテーブル内のエントリの一部またはすべてをクリアします。

- スタティックのみ（Static Only）：スタティック ホストを削除します。
- ダイナミックのみ（Dynamic Only）：ダイナミック ホストを削除します。
- すべてのダイナミック & スタティック（All Dynamic & Static）：スタティック ホストとダイナミック ホストを削除します。

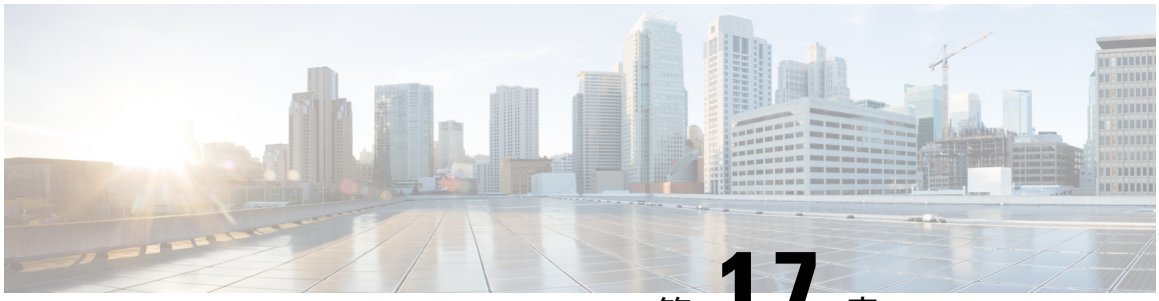
ステップ 3 ホストマッピングを追加するには、[Add] をクリックし、次を設定します。

- [IP バージョン]：IPv6 の場合は [バージョン 6]、IPv4 の場合は [バージョン 4] を選択 します。
- [IPv6 アドレスタイプ]：IPv6 を使用する場合、IPv6 アドレス タイプを選択します。次のオプションがあります。

- [リンクローカル] : IPv6 アドレスによって、同一ネットワーク リンク上のホスト が一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
- [グローバル] : IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。

- [Link Local Interface]：IPv6 アドレスタイプがリンクローカルである場合、その受信元のインターフェイスを選択します。
- [Host Name]：ユーザー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 文字の A ～ Z（大文字と小文字の区別なし）、数字の 0 ～ 9、下線、およびハイフンに制限されています。ピリオド（.）は、ラベルを区切るために使用されます。
- [IP Address]：単一のアドレス、または関連する 8 個以下の IP アドレスを入力します（IPv4 または IPv6）。

ステップ 4 [Apply] をクリックします。設定が実行コンフィギュレーション ファイルに保存されます。



第 17 章

セキュリティ

この章は、次の項で構成されています。

TACACS+クライアント

組織は Terminal Access Controller Access Control System（TACACS+）サーバを構築して、すべてのデバイスに対する一元化されたセキュリティを提供できます。この方法では、認証と認可は組織内のすべてのデバイスを単一サーバ上で処理することができます。

デバイスは、次のサービスを提供する TACACS+ サーバーを使用する TACACS+ クライアントとして機能します。[TACACS+] ページでは、TACACS+ サーバーの設定ができます。

- 認証（Authentication）：ユーザ名とユーザ定義のパスワードを使用してデバイスにログインしているユーザの認証を提供します。
- [Authorization]：ログイン時に実行されます。認証セッションが完了すると、認証されたユーザ名を使用して認可セッションを開始します。その後、TACACS+ サーバがユーザの権限を確認します。
- アカウンティング（Accounting）：TACACS+ サーバを使用してログイン セッションのアカウンティングを有効にします。これにより、システム管理者は TACACS+ サーバからアカウンティング レポートを生成できるようになります。

TACACS+ は IPv4 を使用する場合にのみサポートされます。

TACACS+ サーバーパラメータを設定するには、次の手順を実行します。

ステップ 1 [セキュリティ] > [TACACS+ クライアント] をクリックします。

ステップ 2 必要に応じて、[TACACS+ Accounting] を有効にします。

ステップ 3 次のデフォルト パラメータを入力します。

オプション	説明
Key String	暗号化モードまたはプレーンテキストモードのすべての TACACS+ サーバーとの通信に使用されるデフォルトのキーストリングを入力します。 ここで、キー文字列と個々の TACACS+ サーバのキー文字列の両方を入力する場合、個々の TACACS+ サーバに設定されているキー文字列が優先されます。
応答タイムアウト	デバイスと TACACS+ サーバーの間の接続がタイムアウトになるまでの経過時間を入力します。特定のサーバーに関する値が [Add TACACS+ Server] ページで入力されない場合、このフィールドの値が採用されます。
送信元IPv4インターフェイス	TACACS+ サーバーとの通信のために送られるメッセージで使用されるデバイス IPv4 送信元インターフェイスを選択します。
送信元IPv6インターフェイス	TACACS+ サーバーとの通信のために送られるメッセージで使用されるデバイス IPv6 送信元インターフェイスを選択します。 （注） 自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

ステップ 4 [Apply] をクリックします。TACACS+ のデフォルト設定が実行コンフィギュレーション ファイルに追加されます。それらの設定は、[Add] ページに同等のパラメータが定義されていない場合に使用されます。

各 TACACS サーバの情報は、TACACS+ サーバ テーブルに表示されます。このテーブルのフィールドは、[Status] フィールドを除き、[Add] ページで入力します。このフィールドは、サーバーがデバイスに接続されているかどうかを示します。

ステップ 5 TACACS+ サーバを追加するには、[Add] をクリックします。

ステップ 6 パラメータを入力します。

オプション	説明
サーバー指定方法	TACACS+ サーバーを識別する方法として、次のいずれか 1 つを選択します。 • [By IP address]：これを選択した場合は、[Server IP Address/Name] フィールドにサーバーの IP アドレスを入力します。 • [By name]：これを選択した場合は、[Server IP Address/Name] フィールドにサーバーの名前を入力します。
IP バージョン	送信元 IP アドレスのサポート対象 IP バージョン（IPv6 または IPv4）を選択します。
IPv6アドレス タイプ	IPv6アドレスタイプを選択します（IPv6が使用されている場合）。次のオプションがあります。 • [Link Local]：IPv6アドレスによって、単一ネットワークリンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [Global]：IPv6アドレスは、他のネットワークから表示可能で到達可能なグローバルユニキャスト IPV6 タイプです。
リンクローカルインターフェイス	リストからリンク ローカル インターフェイスを選択します（IPv6 アドレスタイプとしてリンクローカルが選択されている場合）。
サーバーのIPアドレス/名前	TACACS+ サーバーの IP アドレスまたは名前を入力します。
Priority	この TACACS+ サーバーの使用順序を入力します。ゼロは優先順位が最も高い TACACS+サーバかつ最初に使用されるサーバを示します。優先順位が最も高いサーバーとのセッションを確立できない場合、デバイスは次に優先順位が高いサーバーとの接続を試みます。
Key String	デバイスと TACACS+ サーバーの間の認証と暗号化に使用されるデフォルトのキーストリングを入力します。このキーは、TACACS+ サーバに設定されているキーと一致する必要があります。 キー文字列は、MD5を使用して通信を暗号化するために使用されます。デバイスのデフォルト キーを選択するか、暗号化（Encrypted）またはプレーン テキスト（Plaintext）形式でキーを入力することができます。（別のデバイスからの）暗号化キーストリングがない場合は、プレーンテキストモードでキーストリングを入力して [Apply] をクリックします。暗号化されたキー文字列が生成されて表示されます。

オプション	説明
応答タイムアウト	[User Defined] を選択して、デバイスと TACACS+ サーバーの間の接続がタイムアウトになるまでの経過時間を入力します。ページに表示されているデフォルト値を使用する場合は、[Use Default] を選択します。
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。
単一接続	すべての情報を単一の接続で受信できるようにするには、このフィールドを選択します。TACACS+ サーバーがこれをサポートしない場合、デバイスは複数接続に戻ります。

ステップ 7 [Apply] をクリックします。TACACS+ サーバがデバイスの実行コンフィギュレーション ファイルに追加されます。

ステップ 8 このページでプレーン テキスト形式でセンシティブ データを表示するには、[Display Sensitive Data As Plaintext] をクリックします。

RADIUS Client

Remote Authorization Dial-In User Service（RADIUS）サーバは、一元化された 802.1X または MAC ベースのネットワーク アクセス コントロールを提供します。デバイスは、一元化されたセキュリティを提供するために RADIUS サーバを使用できる RADIUS クライアントとなるように設定、および RADIUS サーバとして設定できます。組織は、デバイスを Remote Authorization Dial-In User Service（RADIUS）サーバとして使用して、一元化された 802.1X または MAC ベースのネットワーク アクセス コントロールをすべてのデバイスに対して提供できます。この方法では、認証と認可は組織内のすべてのデバイスを単一サーバ上で処理することができます。

RADIUS は、アクセスのセキュリティが必要なネットワーク環境で使用します。RADIUS サーバーのパラメータ値を設定するには、次の手順を実行します。

ステップ 1 [Security] > [RADIUS Client] をクリックします。

ステップ 2 RADIUS アカウンティング オプションを入力します。次のオプションを使用できます。

- [Port Based Access Control (802 1X, MAC Based, Web Authentication)]：802.1X ポートアカウンティングに RADIUS サーバーが使用されることを指定します。
- 管理アクセス（Management Access）：RADIUS サーバがユーザ ログイン アカウンティングに使用されることを指定します。
- [Both Port Based Access Control and Management Access]：ユーザー ログイン アカウンティングと 802.1X ポートアカウンティングの両方に RADIUS サーバーが使用されることを指定します。
- なし（None）：RADIUS サーバがアカウンティングに使用されないことを指定します。

ステップ 3 必要に応じて、デフォルトの RADIUS パラメータを入力します。[Default Parameters] で入力した値は、すべてのサーバに適用されます。特定のサーバの値が [Add RADIUS Server] ページで入力されていない場合、これらのフィールドの値がデバイスで使用されます。

- [リトライ回数] : RADIUS サーバーに要求を送信する最大試行回数を入力します。こ の回数送信しても要求が受け付けられなかった場合、エラーになります。
- 応答のタイムアウト（Timeout for Reply）：クエリを再試行するか、次のサーバに切り替える前にデバイスが RADIUS サーバからの応答を待機する秒数を入力します。
- デッド タイム（Dead Time）：サービス リクエストに応答していない RADIUS サーバがバイパスされるまでの経過時間（分数）を入力します。値が 0 の場合、サーバはバイパスされません。
- キー文字列（Key String）：デバイスと RADIUS サーバ間の認証と暗号化に使用されるデフォルト キー文字列を入力します。キーは、RADIUS サーバで設定されたキーと一致する必要があります。キー文字列は、MD5 を使用して通信を暗号化するために使用されます。暗号化（Encrypted）またはプレーン テキスト（Plaintext）形式でキーを入力することができます。（別のデバイスからの）暗号化キー文字列がない場合、プレーン テキスト モードでキー文字列を入力し、[Apply] をクリックします。暗号化されたキー文字列が生成されて表示されます。

これで、デフォルト キー文字列がオーバーライドされます（定義されている場合）。

- 送信元 IPv4 インターフェイス（Source IPv4 Interface）：RADIUS サーバと通信するためのメッセージで使用されるデバイスの IPv4 送信元インターフェイスを選択します。
- 送信元 IPv6 インターフェイス（Source IPv6 Interface）：RADIUS サーバと通信するためのメッセージで使用されるデバイスの IPv6 送信元インターフェイスを選択します。

（注） 自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

ステップ 4 [Apply] をクリックします。デバイスの RADIUS デフォルト設定が実行コンフィギュレーション ファイルで更新されます。

ステップ 5 RADIUS サーバーを追加するには、[Add] をクリックします。

ステップ 6 各 RADIUS サーバのフィールドに値を入力します。

- [サーバー指定方法] : RADIUS サーバーを IP アドレスで指定するか、名前で指定するか を選択します。
- IP バージョン（IP Version）：RADIUS サーバの IP アドレスのバージョンを選択します。
- [IPv6 アドレスタイプ] : IPv6 を使用する場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [リンクローカル] : IPv6 アドレスによって、同一ネットワーク リンク上のホスト が一意に識別されます。リンク ローカル アドレスのプレフィックスは FE 80 で、ルーティングはできません。また、ローカル ネットワーク上の通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。

- [グローバル] : IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。

- [リンクローカルインターフェイス] : リストからリンク ローカル インターフェイス（IPv6 アドレス タイプとしてリンク ローカルが選択されている場合）を選択します。•
- [Server IP Address/Name] : RADIUS サーバーを、IP アドレスまたは名前で入力します。
- [プライオリティ] : RADIUS サーバーのプライオリティを入力します。優先順位によって、デバイスがユーザ認証のために通信を試みるサーバの順序が決まります。デバイスは最初に、優先順位が最も高い RADIUS サーバとの接続を開始します。ゼロが最も高い優先順位です。
- キー文字列（Key String）：デバイスと RADIUS サーバ間の通信の認証と暗号化に使用されるキー文字列を入力します。キーは、RADIUS サーバで設定されたキーと一致する必要があります。キーは、暗号化（Encrypted）またはプレーン テキスト（Plaintext）形式で入力することができます。[Use Default] を選択した場合、デバイスはデフォルト キー文字列を使用して、RADIUS サーバの認証を試みます。
- 応答のタイムアウト（Timeout for Reply）：最大試行回数に達した場合、[User Defined] を選択して、クエリを再試行するか、次のサーバに切り替える前にデバイスが RADIUS サーバからの応答を待機する秒数を入力します。[デフォルトを使用] を選択した場合、デバイスはデフォルトのタイムアウト値を使用します。
- [Authentication Port] : 認証要求用の RADIUS サーバーポートの UDP ポート番号を入力します。
- アカウンティング ポート（Accounting Port）：アカウンティング要求用の RADIUS サーバ ポートの UDP ポート番号を入力します。
- 再試行回数（Retries）：[User Defined] を選択して、障害が発生したと見なされる前に、RADIUS サーバに送信される要求の数を入力します。[Use Default] を選択した場合、デバイスは再試行回数のデフォルト値を使用します。
- デッド タイム（Dead Time）：[User Defined] を選択して、サービス リクエストに応答していない RADIUS サーバがバイパスされるまでの経過時間（分数）を入力します。[Use Default] を選択した場合、デバイスはデッド タイムのデフォルト値を使用します。0 分を入力する場合、デッド タイムはありません。
- [使用タイプ] : RADIUS サーバーの認証タイプを入力します。次のオプションがあります。
  - ログイン（Login）：RADIUS サーバは、デバイスの管理を要求するユーザの認証に使用されます。
  - [802.1X] : RADIUS サーバーは 802.1X 認証に使用されます。
  - すべて（All）：RADIUS サーバは、デバイスの管理を要求するユーザの認証および 802.1X 認証に使用されます。

ステップ 7 [Apply] をクリックします。RADIUS サーバの定義がデバイスの実行コンフィギュレーション ファイルに追加されます。

ステップ 8 ページでプレーン テキスト形式でセンシティブ データを表示するには、[Display Sensitive Data As Plaintext] をクリックします。

RADIUS サーバ

組織のすべてのデバイスを対象として802.1XまたはMACに基づくネットワークアクセスの一元的な制御を行うために、デバイスをRemote Authorization Dial-In User Service（RADIUS）サーバーとして使用することができます。この方法により、すべてのデバイスに関する認証と認可を 1 つのサーバーで扱うことができます。

デバイスが RADIUS クライアントとして設定されている場合、次のサービスに RADIUS サーバを使用できます。

- 認証：ユーザー名およびユーザー定義のパスワードを使用して、通常のユーザーおよび 802.1X ユーザーを認証する機能を提供します。
- 認可：ログイン時に実行します。認証セッションが完了すると、認証されたユーザー名を使用して認可セッションが開始します。その後、RADIUSサーバがユーザの権限を確認します。

アカウンティング：RADIUSサーバーを使用した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。これにより、システム管理者はRADIUS サーバからアカウンティング レポートを生成できるようになります。RADIUSサーバのアカウンティングに使用されるユーザが設定可能な TCP ポートは、RADIUS サーバの認証と認可に使用されるのと同じ TCP ポートです。

RADIUSサーバーグローバル設定

デバイスは、RADIUSサーバとして設定できます。RADIUSサーバーのグローバルパラメータ値を設定するには、次のようにします。

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Global Settings] の順にクリックします。

ステップ 2 次のパラメータを入力します。

- RADIUS サーバのステータス（RADIUS Server Status）：RADIUS サーバ機能のステータスを有効にする場合に選択します。
- 認証ポート（Authentication Port）：認証要求用の 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（Accounting Port）：アカウンティング要求用の RADIUS サーバ ポートの UDP ポート番号を入力します。

トラップの設定

- RADIUS アカウンティング トラップ（RADIUS Accounting Traps）：RADIUS アカウンティング イベントのトラップを生成する場合に選択します。
- RADIUS 認証の失敗トラップ（RADIUS Authentication Failure Traps）：失敗したログインのトラップを生成する場合に選択します。
- RADIUS 認証の成功トラップ（RADIUS Authentication Success Traps）：成功したログインのトラップを生成する場合に選択します。

ステップ 3 [Apply] をクリックします。デバイスの RADIUS デフォルト設定が実行コンフィギュレーション ファイルで更新されます。

RADIUSサーバーキー

RADIUS サーバーキーを設定するには、次の手順を実行します。

ステップ 1 [Security] > **[RADIUS Server]** > **[RADIUS Server Keys]** の順にクリックします。

ステップ 2 必要に応じて、デフォルトの RADIUS キーを入力します。[Default Key] に入力した値は、（[ADD RADIUS Server] ページで）デフォルト キーを使用するように設定されているすべてのサーバに適用されます。

- デフォルト キー（Default Key）：デバイスと RADIUS サーバ間の認証と暗号化に使用されるデフォルト キー文字列を入力します。次のオプションのいずれかを選択します。
  - 既存のデフォルト キーを保持（Keep existing default key）：デバイスは、指定されたサーバに対して、既存のデフォルト キー文字列を使用して RADIUS クライアントの認証を試みます。
  - 暗号化（Encrypted）：MD5 を使用して通信を暗号化するには、暗号化された形式でキーを入力します。
  - プレーン テキスト（Plaintext）：プレーン テキスト モードでキー文字列を入力します。
- MD5 Digest（MD5 ダイジェスト）：ユーザが入力したパスワードの MD5 ダイジェストが表示されます。

ステップ 3 [Apply] をクリックします。デバイスの RADIUS デフォルト設定が実行コンフィギュレーション ファイルで更新されます。

ステップ 4 秘密キーを追加するには [Add] をクリックして、次のフィールドに入力します。

- NAS アドレス（NAS Address）：RADIUS クライアントが含まれているスイッチのアドレス。
- 秘密キー（Secret Key）：RADIUS クライアントが含まれているスイッチのアドレス。
  - [Use default key]：指定されたサーバーに対して、デバイスは既存のデフォルトキーストリングを使用して、RADIUS クライアントの認証を試行します。
  - 暗号化（Encrypted）：MD5 を使用して通信を暗号化するには、暗号化された形式でキーを入力します。

- プレーン テキスト（Plaintext）：プレーン テキスト モードでキー文字列を入力します。

ステップ 5 [Apply] をクリックします。デバイスのキーが実行コンフィギュレーション ファイルで更新されます。

RADIUS サーバー グループ

デバイスをRADIUSサーバーとして使用するユーザーのグループを設定するには、次の手順を実行します。

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Groups] の順にクリックします。

ステップ 2 [Add] をクリックして、次のフィールドに入力します。

- [Group Name]：グループの名前を入力します。
- 権限レベル（Privilege Level）：グループの管理アクセス権限レベルを入力します。
- 時間範囲（Time Range）：このグループに時間範囲を適用する場合に選択します。
- 時間範囲名（Time Range Name）：[Time Range] を選択した場合、使用する時間範囲を選択します。時間範囲を定義するには、[Edit]をクリックします。このフィールドは、時間範囲が作成済みである場合にのみ表示されます。
- VLAN：ユーザの VLAN を選択します。
  - [None]：VLAN ID は送信されません。
  - [VLAN ID]：送信される VLAN ID。
  - VLAN 名（VLAN Name）：送信される VLAN 名。

ステップ 3 [Apply]をクリックします。RADIUSグループの定義がデバイスの実行コンフィギュレーション ファイルに追加されます。

RADIUSサーバーユーザー

ユーザを追加するには、次の手順を実行します。

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Users] の順にクリックします。

現在のユーザが表示されます。

ステップ 2 [Add] をクリックします。

- [User Name]：ユーザーの名前を入力します。

- [Group Name]：以前に定義したグループを選択します。
- [Password]：次のいずれかのオプションを入力します。
  - 暗号化（Encrypted）：キー文字列は MD5 を使用して通信を暗号化するために使用されます。暗号化を使用するには、暗号化された形式でキーを入力します。
  - [Plaintext]：（別のデバイスからの）暗号化キーストリングがない場合は、プレーンテキストモードでキーストリングを入力します。暗号化されたキー文字列が生成されて表示されます。

ステップ 3 [Apply] をクリックします。ユーザ定義がデバイスの実行コンフィギュレーション ファイルに追加されます。

RADIUS サーバアカウンティング

RADIUS サーバは、FLASH のサイクル ファイルに最後のアカウンティング ログを保存します。アカウンティング ログは表示することができます。

RADIUS サーバーアカウンティングを表示するには、次の手順を実行します。

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Accounting] をクリックします。

RADIUS アカウンティング イベントが次のフィールドとともに表示されます。

- [User Name]：ユーザーの名前。
- イベント タイプ（Event Type）：値は次のいずれかです。
  - [Start]：セッションが開始されました。
  - [Stop]：セッションは停止されました。
  - 日付/時刻変更（Date/Time Change）：デバイスの日付/時刻が変更されました。
  - リセット（Reset）：デバイスが指定された時間にリセットされました。
- 認証方式（Authentication Method）：ユーザによって使用されている認証方式。イベント タイプが日付/時刻変更またはリセットの場合、N/A と表示されます。
- NAS アドレス（NAS Address）：RADIUS クライアントが含まれているスイッチのアドレス。イベント タイプが日付/時刻変更またはリセットの場合、N/A と表示されます。
- ユーザ アドレス（User Address）：認証されたユーザがネットワーク管理者の場合、これはその管理者の IP アドレスで、ユーザがステーションの場合、これはそのステーションの MAC アドレスです。イベント タイプが日付/時刻変更またはリセットの場合、N/A と表示されます。
- [Event Time]：イベントの時間。

ステップ 2 ユーザまたはイベントの詳細情報を表示するには、ユーザまたはイベントを選択して、[Details] をクリックします。

次のフィールドが表示されます。

（注） このページのフィールドは、閲覧しているアカウントのタイプとそのアカウントで受信した詳細情報によって異なります。常にすべてのフィールドが表示されるわけではありません。

- [Event Time]：上記参照。
- [Event Type]：上記参照。
- [User Name]：上記参照。
- [Authentication Method]：上記参照。
- [NAS IPv4 Address]：上記の [NAS Address] 参照。
- [NAS Port]：NAS アドレスのスイッチで使用されるポート。
- [User Address]：上記参照。
- アカウンティングセッション時間（Accounting Session Time）：上記のイベント時間（Event Time）を参照してください。
- セッションの終了理由（Session Termination Reason）：セッションの終了理由（ユーザの要求など）が表示されます。

RADIUSサーバー拒否ユーザー

RADIUS サーバーを使用して認証を試行し、拒否されたユーザーを表示するには、次の手順を実行します。

ステップ 1 [Security] > **[RADIUS Server]** > **[RADIUS Rejected Users]** の順にクリックします。

拒否されたユーザが次のフィールドとともに表示されます。

- [Event Type]：次のいずれかのオプションが表示されます。
  - Rejected：ユーザーは拒否されました。
  - 時間変更（Time Change）：デバイスの時計が管理者によって変更されました。
  - リセット（Reset）：デバイスが管理者によってリセットされました。
- ユーザ名（User Name）：拒否されたユーザの名前。
- ユーザ タイプ（User Type）：ユーザに関連する次の認証オプションのいずれかが表示されます。

- [Login]：管理アクセスユーザー
- [802.1x]：802.1x ネットワーク アクセス ユーザー
- [N/A]：リセットイベント用

- [Reason]：ユーザーが拒否された理由。
- [Time]：ユーザーが拒否された時間。

ステップ 2 拒否されたユーザの詳細情報を表示するには、そのユーザを選択して、[Details] をクリックします。

次のフィールドが表示されます。

（注） このページのフィールドは、閲覧しているアカウントのタイプとそのアカウントで受信した詳細情報によって異なります。常にすべてのフィールドが表示されるわけではありません。

- [Event Time]：上記参照。
- [User Name]：上記参照。
- [User Type]：上記参照。
- 拒否理由（Rejection Reason）：ユーザが拒否された理由。
- NAS IP アドレス（NAS IP Address）：Network Accessed Server（NAS）のアドレス。NAS は、RADIUS クライアントを実行しているスイッチです。

拒否されたユーザのテーブルをクリアするには、[Clear] をクリックします。

RADIUSサーバー不明NASエントリ

NAS が RADIUS サーバーに認識されていないことが原因の認証拒否を表示するには、次の手順を実行します。

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Unknown NAS Entries] の順にクリックします。

次のフィールドが表示されます。

- イベント タイプ
  - 不明な NAS（Unknown NAS）：不明な NAS イベントが発生しました。
  - 時間変更（Time Change）：デバイスの時計が管理者によって変更されました。
  - リセット（Reset）：デバイスが管理者によってリセットされました。
- IPアドレス（IP Address）：不明な NAS の IP アドレス。

• [Time]：イベントのタイムスタンプ。

ステップ 2 エントリを削除するには、[Clear] をクリックします。

RADIUSサーバー統計情報

RADIUS サーバの統計情報を表示する手順は、次のとおりです。

ステップ 1 [Security] > [RADIUS Server] > [RADIUS Server Statistics] の順にクリックします。

ステップ 2 次のオプションから統計情報ソースを選択します。

- • [Global]：すべてのユーザーの統計情報
  • [Specific NAS]：特定の NAS の統計情報。

ステップ 3 [Refresh Rate] を選択します。

ステップ 4 次の統計情報が表示されます。

認証ポート上の着信パケット数	認証ポートで受信したパケットの数。
不明なアドレスからの着信アクセス要求数	不明な NAS アドレスからの着信アクセス要求数。
重複着信アクセス要求数	受信した再送されたパケットの数。
送信済みアクセス許可数	送信されたアクセス許可の数。
送信済みアクセス拒否数	送信されたアクセス拒否の数。
送信済みアクセスチャレンジ数	送信されたアクセスチャレンジの数。
着信無効アクセス要求数	受信した不正なアクセス要求の数。
不正な認証コードを伴う着信認証要求数	パスワードが正しくない着信パケットの数。
その他の誤りを伴う着信認証パケット数	その他の誤りを伴う着信認証パケットの数。
不明なタイプの着信認証パケット数	不明なタイプの着信認証パケットの数。
アカウンティングポート上の着信パケット数	アカウンティングポート上の着信パケットの数。
不明なアドレスからの着信認証要求数	不明なアドレスからの着信認証要求の数。
着信重複アカウンティング要求数	着信重複アカウント要求の数。
送信済みアカウンティング応答数	送信済みアカウンティング応答の数。
着信無効アカウンティング要求数	無効アカウンティング要求の数。

不正な認証コードを伴う着信アカウンティング要求数	不正な認証コードを伴う着信アカウンティング要求の数。
その他の誤りを伴う着信アカウンティングパケット数	その他の誤りを伴う着信アカウンティングパケットの数。
着信未記録アカウンティング要求数	着信未記録アカウンティング要求の数。
不明なタイプの着信アカウンティングパケット数	タイプ不明の着信アカウンティングパケットの数。

ステップ 5 カウンタをクリアするには、[Clear Counters] をクリックします。

ステップ 6 カウンタを更新するには、[Refresh] をクリックします。

ログイン設定

デフォルトのユーザー名/パスワードは、**cisco/cisco** です。デフォルトのユーザー名とパスワードで初めてログインすると、新しいパスワードを入力するように求められます。パスワードの複雑性は、デフォルトで有効になっています。選択したパスワードが十分に複雑でない場合は、別のパスワードを作成するように求められます。

ステップ 1 [Security] > [Login Settings] をクリックします。

ステップ 2 [Password Aging] セクションで、[Enable] をオンにしてパスワードエージングを有効にします。[Password Aging] チェックボックスをオフにすると、[Password Aging Time] が無効になります。

ステップ 3 次に、以下の項目を設定します。

オプション	説明
パスワードエージング時間	これを行うには、日数を入力します。（範囲：1 ～ 365、デフォルト：180） （注） パスワードの有効期限の 10 日前に警告メッセージが表示されます。有効期限日が過ぎると、ログインしているユーザーはパスワードの変更が強制されます。パスワードが変更されるまでデバイスへのアクセスは許可されません。
最近のパスワード防御	この機能を有効にするには[Enable]をオンにします。この機能はデフォルトではディセーブルになっています。
パスワード履歴カウント	最近のパスワード防御の数を定義します。範囲は 1 ～ 24 で、デフォルトは 12 です。

オプション	説明
最小パスワード長	パスワードの文字数を入力します。（範囲：8 ～ 64、デフォルト：8）
許容される文字の繰り返し	文字を連続して繰り返すことはできません。許容される文字の繰り返し回数を入力します。（範囲：1 ～ 16、デフォルト：3）
文字クラスの最小数：	文字クラスの最小数を入力します。（範囲：0～4、デフォルト：3）

（注） パスワードの複雑さのルールは次のとおりです。

- デフォルトのパスワードの最小長は 8 文字です。パスワードは、8 ～ 64 文字の範囲で設定できます。
- 文字の繰り返し：文字を連続して繰り返すことはできません。デフォルトでは、許可される最小繰り返し数は 3 です。
- 最近のパスワード防御：このアカウントで過去に使用したことのあるパスワードとは異なるパスワードを要求する場合の、過去のパスワードの数を指定します。デフォルトは 12 で、3 ～ 24 の範囲で設定できます。
- 文字クラスの最小数：パスワードに使用する必要があるさまざまな文字クラスの数（クラスとは、大文字、小文字、数字、特殊文字です）。デフォルトでは、最小数は 3 で、0 ～ 4 の範囲で設定できます（0 と 1 は機能的に同じです）。
- ユーザーによって設定または変更されたパスワード（以降「シークレット」）は、次のファイルの一般的なパスワードのリストと比較する必要があります。シークレットにリスト内の単語が含まれている場合、ユーザーは次のエラーメッセージを受け取り、別のパスワードを再入力する必要があります：「パスワードが拒否されました：パスワードは辞書の英単語と一致してはならず、一般的に使用されるパスワードを含んではなりません」
- 連続文字：3 つ以上の連続した文字または数字、またはこれらの連続した値を逆に並べたものをパスワードに使用することはできません。次のような他の文字に置き換えられる文字もこの制限に含まれます。「s」の代わりの「$」、「a」の代わりの「@」、「o」の代わりの「0」、「l」の代わりの「1」、「i」の代わりの「!」、「e」の代わりの「3」。禁止されているパスワードの例：「efg123!$」、「abcd765%」、「kji!$378」、qr$58!230。連続文字は大文字と小文字のあらゆる組み合わせで（AbC または aBC など）禁止されています。
- コンテキスト固有の単語（プロジェクトおよびベンダー名）：パスワードには、ユーザー名、「cisco」または「cbs」、またはその派生語を含めてはなりません。これらの単語の逆読みや大文字と小文字の組み合わせもこの制限の対象となります。次のような他の文字に置き換えられる文字もこの制限に含まれます：「s」の代わりの「$」、「a」の代わりの「@」、「o」の代わりの「0」、「l」の代わりの「1」、「i」の代わりの「!」、「e」の代わりの「3」は使用できません。たとえば、C!$c0678! は許可されていません。

ログインロックダウン

デバイスのアドレスがわかっている場合、悪意のあるユーザーが辞書攻撃を試みる可能性があります。辞書攻撃とは、数千、時には数百万ものログイン情報でログインを試行する自動化されたプロセスです。辞書攻撃の目的は、実際にデバイスへの管理アクセス権を取得することです。

これらの攻撃を防ぐために、特定の時間範囲内で許可されるログイン試行回数を制限するようにデバイスを設定し、失敗した試行が指定の回数に達した後に続く静音モード時間を定義する

ことができます。指定の時間（within seconds）内に、指定された回数の接続試行が失敗した（attempt tries）場合、デバイスは指定の期間（block-for seconds）の間、追加のログイン試行を受け入れません。これは、ユーザーがログイン情報を忘れ、何度かログインを試みてもログインできなかった場合にも発生する可能性があります。

（注） 指定の時間内に指定された回数のログイン試行が失敗すると、デバイスは静音モードに入ります。telnet、SSH、SNMP、HTTP、HTTPS を含め、静音モードの間は接続要求を受け付けなくなります。静音モードの時間が終了すると、デバイスは接続要求の受け入れを再開します。静音モードの開始時間と終了時間は、Syslog メッセージで示されます。

失敗した試行回数は、各失敗した試行が測定される期間全体を通じてカウントする必要があります。待機時間中は、失敗した試行はカウントされません。待機時間が終了すると、失敗した試行のカウントが再開されます。タイマーが切れる前でも、この機能を無効にすることで待機時間を終了できます。

ステップ 1 [Login Response Delay] で、[Enable] をオンにして、ログイン応答遅延を有効にします。

ステップ 2 次に、以下の項目を設定します。

オプション	説明
Response Delay Period	応答遅延期間を秒数で入力して設定します。（範囲：1 ～ 10、デフォルト：1）
Quiet Period Enforcement	[Enable] をオンにして、待機時間を適用します。
Quiet Period Length	待機時間の長さを秒数で入力して設定します。（範囲：1 ～ 65535、デフォルト：300）
Triggering Attempts	トリガーの試行回数を入力します。（範囲：1 ～ 100、デフォルト：4）
Triggering Interval	トリガー間隔の秒数を入力します。（範囲：1 ～ 3600、デフォルト：60）
待機時間アクセスプロファイル （316 ページ）。 （注） このリンクをクリックすると、[Security] → [Management Access Method] → [Access Profiles] ページに移動します。	デフォルト設定は [Console Only] です。 （注） このドロップダウンには、既存のすべてのアクセスプロファイルのオプションが含まれています。

ログイン保護ステータス

[Login Protection Status] ページは、試行された攻撃やログインエラーを追跡して表示します。（ログインエラーがログイン情報を忘れたユーザーに起因するか、実際の攻撃に起因するかは区別されません）。[Refresh] ボタンをクリックするとデータが更新されます。

- [Quiet Mode Status]：アクティブまたは非アクティブのいずれかのステータスになります。
- [Quiet Mode Remaining Time]：このフィールドは、[Quiet Mode Status] がアクティブな場合にのみ表示されます。
- [Login Failures in the Last 60 Seconds]：[Quiet Period Length] パラメータで定義された時間の経過中に発生したログインエラーの数を表示します。[Quiet Period Length] は、[Security] > [Login Settings] ページで設定された秒単位の値です。

ログインエラーテーブルには、次の項目が表示されます。

- [Username]：ユーザーの名前
- [IP Address]：ユーザーの IP アドレス
- [Service]：使用されているサービス。これは、HTTP、HTTPS、Telnet、SSH、またはSNMPのいずれかです。
- [Count]：試行されたログインエラーの数。
- [Most Recent Attempt Time]：失敗したログインが試行された最近の時間。

キー管理

このセクションでは、RIPなど、アプリケーションやプロトコルのキーチェーンの設定方法について説明します。

Key Chain

新しいキー チェーンを作成するには、次の手順を実行します。

ステップ 1 [Security] > [Key Management] > [Key Chain Settings] をクリックします。

ステップ 2 新しいキー チェーンを追加するには、[Add] をクリックして [Add Key Chain] ページを開き、次のフィールドに入力します。

- [Key Chain]：キーチェーンの名前。
- [Key Identifier]：キーチェーンを識別する整数の ID。
- [Key String]：キーチェーンストリングの値。次のいずれかのオプションを入力します。

- [User Defined (Encrypted)]：暗号化バージョンを入力します。
- [User Defined (Plaintext)]：プレーンテキストバージョンを入力します。

（注） [Accept Life Time] と [Send Life Time] の両方の値を入力することができます。[Accept Life Time] は、受信しているパケットのキー識別子が有効な場合に表示されます。[Send Life Time] は、送信しているパケットのキー識別子が有効な場合に表示されます。

- [Accept Life Time/Send Life Time]：このキーを含むパケットが受け入れられる時点を指定します。次のオプションのいずれかを選択します。
  - [Always Valid]：キー識別子の存続期間に制限はありません。
  - [User Defined]：キーチェーンの存続期間には制限があります。このオプションが選択されている場合は、次のフィールドに値を入力します。

（注） [User Defined] を選択すると、システム時刻を手動で設定するか、または SNTP から設定する必要があります。そうしないと、[Accept Life Time] と [Send Life Time] は常に失敗します。

次のフィールドは、[Accept Life Time] フィールドと [Send Life Time] フィールドに関係しています。

- [Start Date]：キー識別子が有効になる最も早い日付を入力します。
- [Start Time]：[Start Date] において、キー識別子が有効になる最も早い時刻を入力します。
- [End Time]：キー識別子が有効である最後の日付を指定します。次のオプションのいずれかを選択します。
  - [Infinite]：キー識別子の存続期間に制限はありません。
  - [Duration]：キー識別子の存続期間には制限があります。このオプションが選択されている場合は、次のフィールドに値を入力します。
- [Duration]：キー識別子が有効である時間の長さ。次のフィールドに入力します。
  - [Days]：キー識別子が有効である日数。
  - [Hours]：キー識別子が有効である時間数。
  - [Minutes]：キー識別子が有効である分数。
  - [Seconds]：キー識別子が有効である秒数。

ステップ 3 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

キー設定

既存のキー チェーンにキーを追加するには、次の手順を実行します。

ステップ 1 [Security] > [Key Management] > [Key Settings] をクリックします。

ステップ 2 新しいキー文字列を追加するには、[Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [Key Chain]：キーチェーンの名前。
- [Key Identifier]：キーチェーンを識別する整数の ID。
- [Key String]：キーチェーンストリングの値。次のいずれかのオプションを入力します。
  - [User Defined (Encrypted)]：暗号化バージョンを入力します。
  - [User Defined (Plaintext)]：プレーンテキストバージョンを入力します。

  （注） [Accept Life Time] と [Send Life Time] の両方の値を入力することができます。[Accept Life Time] は、受信しているパケットのキー識別子が有効な場合に表示されます。[Send Life Time] は、送信しているパケットのキー チェーンが有効な場合に表示されます。[Accept Life Time] のフィールドのみ説明されています。[Send Life Time] には同じフィールドがあります。

- [Accept Life Time]：このキーを含むパケットがいつ受け入れられるかを指定します。次のオプションのいずれかを選択します。
  - [Always Valid]：キー識別子の存続期間に制限はありません。
  - [User Defined]：キーチェーンの存続期間には制限があります。このオプションが選択されている場合は、次のフィールドに値を入力します。
- [Start Date]：キー識別子が有効になる最も早い日付を入力します。
- [Start Time]：[Start Date] において、キー識別子が有効になる最も早い時刻を入力します。
- [End Time]：キー識別子が有効である最後の時刻を指定します。次のオプションのいずれかを選択します。
  - [Infinite]：キー識別子の存続期間に制限はありません。
  - [Duration]：キー識別子の存続期間には制限があります。このオプションが選択されている場合は、次のフィールドに値を入力します。
- [Duration]：キー識別子が有効である時間の長さ。次のフィールドに入力します。
  - [Days]：キー識別子が有効である日数。
  - [Hours]：キー識別子が有効である時間数。
  - [Minutes]：キー識別子が有効である分数。

- [Seconds]：キー識別子が有効である秒数。

ステップ 4 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

ステップ 5 センシティブデータを（暗号化形式ではなく）常にプレーンテキストとして表示するには、[Display Sensitive Data As Plaintext] をクリックします。

管理アクセス方式

このセクションでは、さまざまな管理方式のアクセス ルールについて説明します。

アクセスプロファイルにより、さまざまアクセス方式でデバイスにアクセスしているユーザの認証および認可方法が決まります。アクセスプロファイルは、特定の送信元からの管理アクセスを制限できます。

アクティブなアクセスプロファイルおよび管理アクセス認証方式の両方にパスしたユーザにのみ、デバイスへの管理アクセスが付与されます。

デバイスでは一度に 1 つのアクセス プロファイルのみアクティブにできます。

アクセス プロファイルは 1 つまたは複数のルールで構成されます。ルールは、アクセス プロファイル内の優先順位の順序（上から下）で実行されます。

ルールは、次の要素を含むフィルタで構成されます。

- [Access Methods]：デバイスにアクセスして管理するための方式。
  - Telnet
  - セキュア Telnet（SSH）
  - Hypertext Transfer Protocol（HTTP）
  - セキュア HTTP（HTTPS）
  - Simple Network Management Protocol（SNMP）
  - All of the above
- [Action]：インターフェイスまたは送信元アドレスへのアクセスを許可するか拒否するか。
- [Interface]：Web ベースの設定ユーティリティへのアクセスを許可または拒否されるポート、LAG、または VLAN。
- [Source IP Address]：IP アドレスまたはサブネット。管理方式へのアクセスは、ユーザ グループ間で異なることがあります。たとえば、1 つのユーザ グループは HTTPS セッションを使用してのみデバイス モジュールにアクセスでき、別のユーザ グループは HTTPS と Telnet の両方のセッションを使用してデバイス モジュールにアクセスできる場合があります。

アクセスプロファイル

[Access Profiles] ページには定義されているアクセス プロファイルが表示されます。また、アクティブにする 1 つのアクセス プロファイルを選択することができます。

ユーザがアクセス方式を介してデバイスへのアクセスを試みると、デバイスは、この方式によるデバイスへの管理アクセスがアクティブなアクセスプロファイルによって明示的に許可されているかどうかをチェックします。一致するアクセスプロファイルが見つからない場合、アクセスは拒否されます。

デバイスへのアクセスの試みが、アクティブなアクセスプロファイルに違反している場合、デバイスは、システム管理者にそのアクセスの試みを警告する Syslog メッセージを生成します。

コンソール専用アクセスプロファイルをアクティブ化した場合、それを非アクティブにする唯一の方法は、管理ステーションからデバイスの物理コンソールポートに直接接続することです。

詳細については、プロファイル ルール （318 ページ）を参照してください。

[Access Profiles] ページを使用してアクセス プロファイルを作成し、最初のルールを追加します。アクセスプロファイルに1つのルールしか含めない場合は、それで終了です。プロファイルにルールを追加するには、[Profile Rules] ページを使用します。

ステップ 1 [Security] > [Mgmt Access Method] > [Access Profiles] をクリックします。

このページには、すべてのアクセス プロファイル（アクティブおよび非アクティブ）が表示されます。

ステップ 2 アクティブなアクセスプロファイルを切り替えるには、[Active Access Profile] ドロップダウンメニューからプロファイルを選択し、[Apply] をクリックします。これで、選択したプロファイルがアクティブなアクセス プロファイルになります。

（注） [Console Only] を選択した場合、警告メッセージが表示されます。そのまま続行すると、Web ベースの設定ユーティリティからただちに切断されて、デバイスはコンソールポートからでなければアクセスできなくなります。これは、コンソール ポートを提供するデバイス タイプにのみ適用されます。

ステップ 3 [OK] をクリックしてアクティブなアクセス プロファイルを選択するか、[Cancel] をクリックして操作を中止します。

ステップ 4 [Add] をクリックして、[Add Access Profile] ページを開きます。このページでは、新しいプロファイルと 1 つのルールを設定できます。

ステップ 5 [Access Profile Name] を入力します。名前は最大 32 文字で指定できます。

ステップ 6 パラメータを入力します。

- [ルールプライオリティ] : ルールのプライオリティを入力します。パケットがルールに一致した場合、ユーザ グループはデバイスへのアクセスを許可または拒否されます。パケットは最初の一致に基づき照合されるため、ルールの優先順位はパケットとルールのマッチングにとって重要です。最も高い優先順位は「1」です。
- [管理方式] : ルールの対象となるアクセス方式を選択します。次のオプションがあります。

- [All]：すべての管理方式をこのルールに割り当てます。
- Telnet：Telnetアクセスプロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
- セキュア Telnet（SSH）（Secure Telnet (SSH)）：SSH アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
- HTTP：HTTPアクセスプロファイル条件を満たすデバイスへのアクセスを要求するユーザを許可または拒否します。
- セキュア HTTP（HTTPS）（Secure HTTP (HTTPS)）：HTTPS アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
- SNMP：SNMP アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザを許可または拒否します。

- [アクション]：このルールに割り当てる処理を選択します。次のオプションがあります。
  - 許可（Permit）：ユーザがプロファイルの設定と一致している場合、デバイスへのアクセスを許可します。
  - [Deny]：ユーザーがプロファイルの設定に一致する場合、デバイスへのアクセスを拒否します。
- [インターフェイスに適用]：このルールに割り当てるインターフェイスを選択します。次のオプションがあります。
  - [All]：すべてのポート、VLAN、および LAG に適用されます。
  - [ユーザー定義]:選択したインターフェイスに適用されます。
- [インターフェイス]：[ユーザー定義] を選択した場合は、インターフェイス番号を入 力します。
- [送信元 IP アドレスに適用]：このアクセス プロファイルに割り当てる送信元 IP アド レスのタイプを選択します。[Source IP Address] フィールドはサブネットワークに対して有効です。次のいずれかの値を選択します。
  - [All]：すべてのタイプの IP アドレスに適用されます。
  - [ユーザー定義]：フィールドで指定したタイプの IP アドレスだけが割り当てられ ます。
- IP バージョン（IP Version）：送信元 IP アドレスのバージョン（バージョン 6 またはバージョン 4）を入力します。
- [IP アドレス]：送信元 IP アドレスを入力します。
- [マスク]：送信元 IP アドレスに対するサブネット マスクの形式を選択し、いずれか のフィールドに値を入力します。
  - ネットワーク マスク（Network Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。

- プレフィックス長（Prefix Length）：プレフィックス長を選択し、送信元 IP アドレス プレフィックスを構成するビットの数を入力します。

ステップ 7 [Apply] をクリックします。アクセス プロファイルが実行コンフィギュレーション ファイルに書き込まれます。これで、このアクセス プロファイルをアクティブなアクセス プロファイルとして選択できます。

プロファイル ルール

アクセスプロファイルには、デバイスの管理とアクセスが許可されているユーザ、および使用される可能性があるアクセス方式を判断するための最大128個のルールを含めることができます。

アクセスプロファイル内の各ルールには、照合するためのアクションと条件（1つ以上のパラメータ）が含まれています。各ルールには優先順位があり、優先順位が一番低いルールが最初にチェックされます。着信パケットがルールと一致すると、そのルールに関連付けられたアクションが実行されます。アクティブなアクセスプロファイル内で一致するルールが見つからない場合、そのパケットはドロップされます。

たとえば、IT 管理センターに割り当てられている IP アドレスを除くすべての IP アドレスからデバイスへのアクセスを制限することができます。この方法でもデバイスは管理でき、追加のセキュリティ レベルを得ることができます。

プロファイルルールをアクセスプロファイルに追加するには、次の手順を実行します。

ステップ 1 [Security] > [Mgmt Access Method] > [Profile Rules] の順にクリックします。

ステップ 2 [Filter] フィールドで、アクセス プロファイルを選択します。[Go] をクリックします。

選択したアクセス プロファイルがプロファイル ルール テーブルに表示されます。

ステップ 3 [Add] をクリックしてルールを追加します。

ステップ 4 パラメータを入力します。

- [アクセスプロファイル名] : アクセス プロファイルを選択します。
- [ルールプライオリティ] : ルールのプライオリティを入力します。パケットがルールに一致した場合、ユーザ グループはデバイスへのアクセスを許可または拒否されます。パケットは最初の一致に基づき照合されるため、ルールの優先順位はパケットとルールのマッチングにとって重要です。
- [管理方式] : ルールの対象となるアクセス方式を選択します。次のオプションがあります。
  - [All] : すべての管理方式をこのルールに割り当てます。
  - Telnet：Telnetアクセスプロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
  - セキュア Telnet（SSH）（Secure Telnet (SSH)）：Telnet アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。

- [HTTP]：HTTPアクセスをこのルールに割り当てます。デバイスへのアクセスを要求しているユーザーがHTTPアクセスプロファイル基準を満たす場合、そのユーザーは許可または拒否されます。
- セキュア HTTP（HTTPS）（Secure HTTP (HTTPS)）：HTTPS アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザに対してアクセスを許可または拒否します。
- SNMP：SNMP アクセス プロファイル条件を満たすデバイスへのアクセスを要求するユーザを許可または拒否します。

- [Action]：次のいずれかのオプションを選択します。
  - 許可（Permit）：このルールに定義されているインターフェイスと IP ソースからのユーザに対するデバイス アクセスを許可します。
  - 拒否（Deny）：このルールに定義されているインターフェイスとIP ソースからのユーザに対するデバイス アクセスを拒否します。
- [インターフェイスに適用]：このルールに割り当てるインターフェイスを選択します。次のオプションがあります。
  - [All]：すべてのポート、VLAN、および LAG に適用されます。
  - [ユーザー定義]：選択したポート、VLAN、または LAG が割り当てられます。
- [Interface]：前述のフィールドで [User Defined] オプションを選択した場合は、インターフェイス番号を入力します。
- [送信元 IP アドレスに適用]：このアクセス プロファイルに割り当てる送信元 IP アドレスのタイプを選択します。[Source IP Address] フィールドはサブネットワークに対して有効です。次のいずれかの値を選択します。
  - [All]：すべてのタイプの IP アドレスに適用されます。
  - [ユーザー定義]：フィールドで指定したタイプの IP アドレスだけが割り当てられ ます。
- [IP バージョン]：送信元 IP アドレスのサポート対象 IP バージョン（IPv6 またはIPv4）を選択します。
- [IP アドレス]：送信元 IP アドレスを入力します。
- [マスク]：送信元 IP アドレスに対するサブネット マスクの形式を選択し、いずれか のフィールドに値を入力します。
  - ネットワーク マスク（Network Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。
  - プレフィックス長（Prefix Length）：プレフィックス長を選択し、送信元 IP アドレス プレフィックスを構成するビットの数を入力します。

ステップ 5 [Apply] をクリックすると、ルールがアクセス プロファイルに追加されます。

管理アクセス認証

SSH、Telnet、HTTP、HTTPS など、さまざまな管理アクセス方式に認証方式を割り当てることができます。認証処理は、ローカルで、またはサーバーで実行可能です。

認可が有効になっている場合は、ユーザのアイデンティティと読み取り/書き込み権限の両方が検証されます。承認処理が有効になっていない場合、ユーザーの ID だけが検証されます。

使用される認可および認証方式は、認証方式の選択順序によって決まります。最初に選択した認証方式が使用不能の場合、次に選択した認証方式が使用されます。たとえば、[RADIUS]、[Local] の順に認証方式を選択した場合、設定されたすべての RADIUS サーバーに対してプライオリティ順にクエリが送られて応答がなければ、ユーザーはローカルに承認/認証されます。

認可が有効になっていて、認証方式が失敗した場合、またはユーザの権限レベルが不十分な場合、ユーザはデバイスへのアクセスを拒否されます。つまり、ある認証方式で認証に失敗した場合、デバイスは認証の試行を停止します（そのまま続行して次の認証方式を使用することはありません）。

同様に、承認処理が無効になっていて、ある方式で認証に失敗した場合、デバイスは認証の試行を停止します。

アクセス方式の認証方式を定義するには、次の手順を実行します。

ステップ 1 [Security] > [Management Access Authentication] をクリックします。

ステップ 2 管理アクセス方式の [Application]（タイプ）を入力します。

ステップ 3 [Authorization] を選択し、後述の方式の一覧から選択して、ユーザの認証と認可の両方を有効にします。フィールドが選択されていない場合は、認証のみ実行されます。認可が有効になっている場合、ユーザの読み取り/書き込み権限がチェックされます。この権限レベルは、[User Accounts] ページで設定します。

ステップ 4 矢印を使用して、[Optional Methods] 列と [選択した方式（Selected Methods] 列の間で認証方式を移動させます。最初に選択した方式が最初に使用される方式です。

- RADIUS：ユーザは RADIUS サーバで認可および認証されます。1 つまたは複数の RADIUS サーバを設定しておく必要があります。Web ベースの設定ユーティリティへのアクセスを付与する RADIUS サーバの場合、その RADIUS サーバが cisco-avpair = shell:priv-lvl=15 を返す必要があります。
- TACACS+：ユーザは TACACS+ サーバで認可および認証されます。1 つまたは複数の TACACS+ サーバを設定しておく必要があります。
- None（なし）：ユーザは認可も認証もされなくてもデバイスにアクセスできます。
- ローカル（Local）：ローカルデバイスに保存されたデータと照らしてユーザ名とパスワードがチェックされます。ユーザ名とパスワードのペアは [User Accounts] ページで定義します。

（注） 認証方式の [Local] または [None] は、常に最後に選択する必要があります。[Local] または [None] の後に選択して認証方式はすべて無視されます。

ステップ 5 [Apply] をクリックします。選択した認証方式がアクセス方式と関連付けられます。

セキュア センシティブ データ管理

SSD は、デバイスの機密データ（パスワードやキーなど）の保護、ユーザー資格情報および SSD ルールに基づき暗号化された機密データや機密データへのプレーンテキストでのアクセスの許可 / 拒否、機密データを含むコンフィギュレーション ファイルの改ざんからの保護を実施します。

さらに、SSD では、センシティブ データを含むコンフィギュレーション ファイルをセキュアにバックアップおよび共有することができます。

SSD によって、ユーザは、プレーンテキストのセンシティブ データを保護しないレベルから、デフォルト パスフレーズに基づく暗号化による最小限の保護、ユーザ定義のパスフレーズに基づく暗号化による強力な保護まで、必要なレベルの保護をセンシティブ データに柔軟に設定できます。

SSD は、SSD 規則に従って、認証された承認済みのユーザにのみ、センシティブ データへの読み取りアクセス許可を付与します。デバイスは、ユーザ認証プロセスを通じて、ユーザに対する管理アクセスを認証および承認します。

SSD を使用しているかどうかにかかわらず、管理者は、ローカル認証データベースを使用して認証プロセスの安全性を確保したり、ユーザ認証プロセスで使用される外部認証サーバへの通信の安全性を確保したりすることが推奨されます。

要約すると、SSD は、SSD 規則、SSD プロパティ、およびユーザ認証によって、デバイス上のセンシティブ データを保護します。さらに、デバイスの SSD 規則、SSD プロパティ、およびユーザ認証の設定は、それ自体が SSD によって保護されているセンシティブ データです。

SSD プロパティ

SSD プロパティは、SSD 規則と組み合わせて、デバイスの SSD 環境を定義および制御する一連のパラメータです。SSD 環境は、次のようなプロパティで構成されています。

- センシティブ データを暗号化する方法を制御する。
- コンフィギュレーション ファイルのセキュリティの強度を制御する。
- 現在のセッション内でセンシティブ データを表示する方法を制御する。

SSD プロパティを設定するには、次の手順を実行します。

ステップ 1 [Security] > [Secure Sensitive Data Management] > [Properties] の順にクリックします。

次のフィールドが表示されます。

- 現在のローカル パスフレーズ タイプ（Current Local Passphrase Type）：現在、デフォルト パスフレーズまたはユーザ定義のパスフレーズのいずれが使用されているかが表示されます。

ステップ 2 [Configuration File Passphrase Control]：次のオプションを選択します。

- 無制限（Unrestricted）（デフォルト）：設定ファイルを作成するときに、デバイスはそのパスフレーズを含めます。これによって、デバイスは設定ファイルを受け入れ、ファイルからパスフレーズを学習できます。
- 制限付き（Restricted）：デバイスは、パスフレーズが設定ファイルにエクスポートされるのを制限します。制限モードは、パスフレーズがないデバイスからコンフィギュレーション ファイル内の暗号化されたセンシティブ データを保護します。ユーザが設定ファイルでパスフレーズを公開したくない場合には、このモードを使用する必要があります。

ステップ 3 次に、[Configuration File Integrity Control] を有効にします。

ステップ 4 現在のセッションの読み取りモードを選択します。

- [プレーンテキスト]：ユーザーはプレーンテキストの機密データにのみアクセスを許可されます。ユーザーには SSD パラメータへの読み取り権限と書き込み権限も付与されます。
- [暗号化]：ユーザーは暗号化された機密データにのみアクセスを許可されます。

ステップ 5 [Change Local Passphrase] をクリックして、新しいローカルパスフレーズを入力します。

- デフォルト（Default）：デバイスのデフォルト パスフレーズを使用します。
- ユーザ定義（プレーン テキスト）（User Defined (Plaintext)）：新しいパスフレーズを入力します。
- パスフレーズの確認（Confirm Passphrase）：新しいパスフレーズを確認します。

ステップ 6 [Apply] をクリックします。設定が実行コンフィギュレーション ファイルに保存されます。

SSDルール

SSD 読み取りアクセス許可が [Plaintext-only] または [Both] のユーザのみが、SSD 規則を設定できます。

SSD ルールを設定するには、次の手順を実行します。

ステップ 1 [Security] > [Secure Sensitive Data Management] > [SSD Rules] の順にクリックします。

現在、定義されている規則が表示されます。[Rule Type] フィールドは、規則がユーザ定義の規則であるか、またはデフォルトの規則であるかを示します。

ステップ 2 新しい規則を追加するには、[Add] をクリックします。次のフィールドに入力します。

- ユーザ（User）：規則が適用されるユーザを定義します。次のオプションのいずれかを選択します。

- 特定のユーザ（Specific User）：選択して、この規則が適用される特定のユーザ名を入力します（このユーザは必ずしも定義されている必要はありません）。
- 既定のユーザ（cisco）（Default User (cisco)）：この規則は既定のユーザに適用されることを示します。
- レベル 15（Level 15）：この規則は、権限レベル 15 を持つすべてのユーザに適用されることを示します。
- すべて（All）：この規則は、すべてのユーザに適用されることを示します。

- チャネル（Channel）：規則が適用される入力チャネルのセキュリティ レベルを定義します。次のオプションのいずれかを選択します。
  - セキュア（Secure）：この規則は、SNMP および XML チャネルを含まない、セキュア チャネル（コンソール、SCP、SSH、HTTPS）のみに適用されることを示します。
  - [Insecure]：ルールが、セキュアでないチャネル（Telnet、TFTP および HTTP）にのみ適用されることを示します。SNMP と XML チャネルは含みません。
  - セキュア XML SNMP（Secure XML SNMP）：この規則が HTTPS またはプライバシー保護付きの SNMPv3 経由の XML にのみ適用されるように指定します。
  - 非セキュア XML SNMP（Insecure XML SNMP）：この規則が HTTP または SNMPv1/v2 およびプライバシー保護なしの SNMPv3 経由の XML にのみ適用されるように指定します。
- 読み取りアクセス許可（Read Permission）：読み取りアクセス許可と規則を関連付けます。有効な値は次のとおりです。
  - [Exclude]：最も低い読み取りアクセス許可。ユーザはいかなる形式でも、センシティブ データの取得は許可されません。
  - プレーン テキストのみ（Plaintext Only）：上記より高い読み取りアクセス許可です。ユーザは、プレーン テキストのみのセンシティブ データの取得が許可されます。
  - 暗号化のみ（Encrypted Only）：中程度の読み取りアクセス許可です。ユーザは、暗号化のみのセンシティブ データの取得が許可されます。
  - 両方（プレーン テキストと暗号化）（Both (Plaintext and Encrypted)）：最高の読み取りアクセス許可です。ユーザは暗号化およびプレーン テキストの両方のアクセス許可を保持し、暗号化形式とプレーン テキストのセンシティブ データの取得が許可されます。
- デフォルト読み取りモード（Default Read Mode）：すべてのデフォルト読み取りモードは、規則の読み取りアクセス許可に従います。次のオプションが存在しますが、規則の読み取りアクセス許可に応じて、一部は拒否されることがあります。
  - 除外（Exclude）：センシティブ データの読み取りを許可しません。
  - 暗号化（Encrypted）：センシティブ データは暗号化形式で表示されます。
  - プレーン テキスト（Plaintext）：センシティブ データはプレーン テキストで表示されます。

ステップ 3 [Apply] をクリックします。設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 4 選択した規則に対して、次のアクションを実行できます。

- ルールの [追加]、[編集]、もしくは [削除]、または [デフォルトへの復元]。
- すべての規則をデフォルトに復元（Restore All Rules to Default）：ユーザが変更したデフォルト規則をデフォルト規則に復元します。

SSL Server

セキュア ソケット レイヤ（SSL）機能は、デバイスへの HTTPS セッションを開くために使用します。HTTPS セッションは、デバイス上に存在するデフォルト証明書で開くこともできます。デフォルトの証明書は証明機関（CA）によって署名されていないため、一部のブラウザではデフォルトの証明書を使用すると警告が表示されます。信頼できる CA によって署名された証明書を使用することをお勧めします。デフォルトでは、デバイスには変更可能な証明書が含まれています。HTTPS はデフォルトで有効になっています。

SSLサーバー認証設定

セキュアソケットレイヤ（SSL）認証は、ユーザーとサーバーがやり取りするためのセキュアな接続を作成するためのプロトコルです。サーバーとユーザーは、すべての Web インタラクションに関与します。ユーザーは、機密性の高い個人情報を Web サイトに入力することが多く、人やシステムが危険にさらされます。より適切な認証によって、特に金融、医療、または個人データを保存するサイトのセキュリティが強化されます。安定した、検証可能でセキュアなユーザーインタラクションが求められています。サーバーは、ユーザーが実在の人物であることを確認する手段として、情報を収集します。これはいくつかの方法で実行できます。

ステップ 1 [Security] > [SSL Server] > [SSL Server Authentication Settings] の順にクリックします。

ステップ 2 デバイスには 2 つの証明書が含まれています。そのうちの 1 つだけが、HTTPS セッションに使用できるアクティブな証明書です。どちらがアクティブな証明書かを定義するには、[SSL Active Certificate Number] で、アクティブな証明書（**1** または **2**）を選択します。

ステップ 3 [Apply] をクリックします。

ステップ 4 [HTTPS Session Logging] セクションで、[Enable] をオンにして有効にします。HTTPS セッションロギングを有効にすることにより、ユーザーは、デバイスによって生成された syslog メッセージを介して、HTTPS セッションのセットアップと切断の進行状況を追跡できます。

ステップ 5 [Apply] をクリックします。

新しい証明書の作成または生成

デバイスにある証明書を置換するために、新しい自己署名証明書が必要になる場合があります。新しい証明書を作成するには、次の手順を実行します。

ステップ 1 証明書を選択して [編集] をクリックします。

ステップ 2 次のフィールドに入力します。

- [Certificate ID]：置換する証明書 ID を選択します。
- [Regenerate RSA Key]：チェックボックスを選択して、RSA キーを再生成します。
- [Key Length]：2 つのオプション（2048 ビットまたは 3072 ビット）のいずれかからキーの長さを選択します。
- 共通名（Common Name）：デバイスの完全修飾 URL または IP アドレスを指定します。指定しない場合、デフォルトでデバイスの最小の IP アドレスになります（証明書が生成されるとき）。
- 組織単位（Organization Unit）：組織単位または部署名を指定します。
- [Organization Name]：組織名を指定します。
- ロケーション（Location）：ロケーションまたは都市名を指定します。
- 都道府県（State）：都道府県名を指定します。
- 国（Country）：国名を指定します。
- [Duration]：証明書の期間を定義します。

ステップ 3 [Generate] をクリックします。新しい証明書が生成され、既存の証明書が置き換えられます。

ステップ 4 新しい証明書要求を生成する場合は、証明書を選択して [Generate Certificate Request] をクリックします。

（注） 証明書要求とは、証明書が署名のために CA にエクスポートされ、署名された証明書としてデバイスにインポートされることをいいます。CA によって署名された証明書は安全であると見なされます（対して、自己署名証明書は安全とは見なされません）。

ステップ 5 次のフィールドに入力します。

- [Certificate ID]：置換する証明書 ID を選択します。
- 共通名（Common Name）：デバイスの完全修飾 URL または IP アドレスを指定します。指定しない場合、デフォルトでデバイスの最小の IP アドレスになります（証明書が生成されるとき）。
- 組織単位（Organization Unit）：組織単位または部署名を指定します。
- [Organization Name]：組織名を指定します。
- ロケーション（Location）：ロケーションまたは都市名を指定します。
- 都道府県（State）：都道府県名を指定します。
- 国（Country）：国名を指定します。

- 証明書の要求（Certificate Request）：[Generate Certificate Request] ボタンを押すと、作成されたキーが表示されます。

ステップ 6 [Generate Certificate Request] をクリックします。これにより、認証局（CA）で入力する必要のある証明書が作成されます。[Certificate Request] フィールドから証明書キーをコピーします。

ステップ 7 CA によって署名された証明書をインポートするには、アクティブな証明書を選択し、[Import Certificate] をクリックします。

ステップ 8 次のフィールドに入力します。

- [Certificate ID]：証明書を選択します。
- [Certificate Source]：自動生成された証明書であることを表示します。
- 証明書（Certificate）：受信した証明書にコピーされます。
- [Import RSA Key-Pair]：新しい RSA キーペアへのコピーを有効にするには、このフィールドを選択します。
- 公開キー（Public Key）：RSA 公開キーにコピーされます。
- [Fingerprint(Hex)]：証明書のフィンガープリントを 16 進形式で表示します。
- 秘密キー（暗号化）（Private Key (Encrypted)）：RSA 秘密キーを選択し、暗号化された形式でコピーします。
- 秘密キー（プレーン テキスト）（Private Key (Plaintext)）：RSA 秘密キーを選択し、プレーン テキスト形式でコピーします。

ステップ 9 [Apply] をクリックして、変更内容を実行コンフィギュレーションに適用します。

ステップ 10 [Details] ボタンをクリックして、SSL 証明書の詳細を表示します。

ステップ 11 次に、[Display Sensitive Data as Encrypted] をクリックして、このキーを暗号化して表示します。このボタンをクリックすると、（[Apply] をクリックしたときに）秘密キーが暗号化された形式で設定ファイルに書き込まれます。テキストが暗号化された形式で表示されると、ボタンが [Display Sensitive Data As Plaintext] に変わり、再びプレーン テキストでテキストを表示できるようになります。

SSH サーバ

リモート ユーザは、SSH サーバ機能を使用して、デバイスへの SSH セッションを確立することができます。これは、セッションがセキュリティで保護されていることを除いて、Telnet セッションの確立と同様です。

デバイスは、SSH サーバとして、パスワードまたは公開キーのいずれかを使用してリモートユーザの認証を行う SSH ユーザ認証をサポートしています。同時に、リモートユーザは、SSH クライアントとして、SSH サーバ認証を行い、デバイス公開キー（フィンガープリント）を使用してデバイスを認証することができます。

SSH サーバには、次の動作モードがあります。

- [By Internally-generated RSA/DSA Keys]（デフォルト設定）：RSA キーと 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してデバイスの IP アドレスを指定すると、デバイスで自動的に認証され、セッションが開きます。
- [Public Key Mode]：ユーザはデバイスで定義されています。ユーザの RSA キーまたは DSA キーは、PuTTY などの外部 SSH サーバ アプリケーションで生成されます。公開キーはデバイスに入力されます。その後、ユーザは、外部 SSH サーバ アプリケーションを使用して、デバイスで SSH セッションを開くことができます。

SSH ユーザ認証

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にすでに設定されているユーザの SSH ユーザ名を作成する場合には、自動ログイン機能を設定することで、追加の認証を回避することができます。これは次のように動作します。

- [Enabled]：ユーザがローカルデータベースに定義されており、このユーザが公開キーを使用して SSH 認証をパスした場合、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はスキップされます。

（注） このような特定の管理方法（コンソール、Telnet、SSH など）に設定されている認証方法はローカル（RADIUS や TACACS+ 以外）である必要があります。

- [Not Enabled]：SSH公開キーによる認証が成功したら、ユーザー名がローカルユーザーデータベース内で設定されている場合でも、設定された認証方式によってユーザーが再度認証されます。

この機能はオプションで、管理アクセス認証（320ページ）で設定できます。必ずしもSSHでユーザ認証を実行する必要はありません。

認証を有効にして、ユーザを追加します。

ステップ 1 [Security] > [SSH Server] > [SSH User Authentication] の順にクリックします。

ステップ 2 次のフィールドを選択します。

- [SSH User Authentication by Password]：ローカルデータベース内で設定されたユーザー名/パスワードを使用して SSH クライアントユーザーの認証を実行する場合に選択します（ユーザ アカウント（70ページ）を参照）。
- [SSH Session Logging]：[Enable] をクリックすると、SSH セッションロギングが有効になります。SSH セッションロギングを使用すると、ユーザーは、デバイスによって生成された syslog メッセージを介して、SSH セッションのセットアップと切断の進行状況を追跡できます。
- [SSH User Authentication by Public Key]：公開キーを使用して SSH クライアント ユーザの認証を実行する場合に選択します。

- [Automatic Login]：このフィールドは、[SSH User Authentication by Public Key] 機能が選択された場合に有効にできます。

ステップ 3 [Apply] をクリックします。設定が実行コンフィギュレーション ファイルに保存されます。

設定したユーザに関する次のフィールドが表示されます。

- [SSH User Name]：ユーザのユーザ名。
- [Key Type]：RSA キーまたは DSA キーのいずれであるかを示します。
- [Fingerprint]：公開キーから生成されたフィンガープリント。

ステップ 4 [Add or Edit] をクリックしてユーザーを追加または編集し、次のフィールドに値を入力します。

- [SSH User Name]：ユーザー名を入力します。
- [Key Type]：[RSA] または [DSA] のいずれかを選択します。
- [Public Key]：PuTTYなどの外部 SSH クライアント アプリケーションによって生成された公開キーをこのテキスト ボックスにコピーします。

ステップ 5 [Apply] をクリックして、新しいユーザを保存します。

すべてのアクティブなユーザに関して、次のフィールドが表示されます。

- [IP Address]：アクティブユーザーの IP アドレス。
- [SSH User Name]：アクティブ ユーザのユーザ名。
- [SSH Version]：アクティブ ユーザが使用する SSH のバージョン。
- [Cypher]：アクティブユーザーの暗号。
- [Authentication Code]：アクティブ ユーザの認証コード。

SSH サーバ認証

リモート SSH クライアントは、SSH サーバー認証を実行することによって、想定された SSH ドライバへの SSH セッションが確立されるようにします。SSH サーバー認証を実行するには、リモート SSH クライアントにターゲット SSH サーバーの SSH サーバー公開キー（またはフィンガープリント）のコピーが保存されている必要があります。

[SSH Server Authentication] ページで、SSH サーバーとしてのデバイスの秘密/公開キーが生成/インポートされます。ユーザーは、SSH セッションで SSH サーバー認証を実行する場合に、このデバイスの SSH サーバー公開キー（またはフィンガープリント）をアプリケーションにコピーする必要があります。RSA と DSA の公開キーと秘密キーは、デバイスを工場出荷時の初期状態でブートすると自動的に生成されます。これらのキーは、適切なユーザ設定キーをユーザが削除した場合にも自動的に作成されます。

RSA キーまたは DSA キーを再生成、または別のデバイスで生成された RSA キーまたは DSA キーをコピーするには、次の手順を実行します。

ステップ 1 [Security] > [SSH Server] > [SSH Server Authentication] の順にクリックします。

各キーには、次のフィールドが表示されます。

- [Key Type]：RSA または DSA。
- [Key Source]：自動生成またはユーザ定義。
- [Fingerprint]：キーから生成されるフィンガープリント。

ステップ 2 RSA キーまたは DSA キーのいずれかを選択します。

ステップ 3 次のいずれかのアクションを実行できます。

- [Generate]：選択した種類のキーを生成します。
- [Edit]：別のデバイスからキーをコピーすることができます。次のフィールドに入力します。
  - [Key Type]：上記を参照してください。
  - [Public Key]：公開キーを入力します。
  - [Private Key]：[Plaintext] または [Encrypted] のいずれかを選択して、秘密キーを入力します。

    [Plaintext]：プレーンテキストとしてキーを入力します。

ステップ 4 [Apply] をクリックして設定を適用します。

ステップ 5 [Display Sensitive Data as Encrypted]：クリックすると、SSH 認証設定が暗号化されて表示されます。

SSH クライアント

SSH クライアントによりユーザーは、ネットワークが 1 つ以上のスイッチで構成されていて、さまざまなシステムファイルが 1 つの中央 SSH サーバーに保管されている場合に、ネットワークの管理作業を実行できます。ネットワークを通じて構成ファイルが転送される際、SSH プロトコルを利用するアプリケーションの 1 つであるセキュアコピー（SCP）により、ユーザー名/パスワードなどの機密データが盗まれないことが保証されます。

SSH クライアントは、信頼できる SSH サーバーとのみ通信します。SSH サーバ認証が無効になっている場合（デフォルト設定）、SSH サーバは信頼できるものと見なされます。SSH サーバ認証を有効にすると、ユーザは、信頼できるサーバのエントリを信頼できる SSH サーバテーブルに追加する必要があります。

一般に、SSH プロトコルはファイル転送と端末アクセスの 2 つの目的に使用できます。

SSH ユーザ認証

デバイス（SSH クライアント）が SSH サーバへの SSH セッションの確立を試行した場合、SSH サーバはクライアントを認証するためにさまざまな方式を使用します。パスワード方式が選択されている場合は、このページを使用して、SSH ユーザ認証方式を選択し、ユーザ名とパスワードをデバイスに設定するか、または、公開/秘密キー方式が選択されている場合は、RSA キーまたは DSA キーを生成使用します。

認証方式を選択し、ユーザー名/パスワード/キーを設定するには、次の手順を実行します。

ステップ 1 [Security] > [SSH Client] > [SSH User Authentication] の順にクリックします。

ステップ 2 [SSH User Authentication Method] を選択します。これは、Secure Copy（SCP）に定義されるグローバル方式です。次のいずれかのオプションを選択します。

- [By Password]：これはデフォルトの設定です。これが選択されている場合は、パスワードを入力するか、またはデフォルト パスワードを保持します。
- RSA 公開キーによる（By RSA Public Key）：これが選択されている場合は、[SSH User Key Table] ブロックで、RSA 公開キーと秘密キーを作成します。
- DSA 公開キーによる（By DSA Public Key）：これが選択されている場合は、[SSH User Key Table] ブロックで、DSA 公開キーと秘密キーを作成します。

ステップ 3 [Username] にユーザ名を入力するか（選択された方式に関係なく）、または既定のユーザの名前を入力します。これは、SSH サーバで定義されているユーザ名と一致している必要があります。

ステップ 4 [By Password] 方式が選択された場合は、パスワードを入力するか（[Encrypted] または [Plaintext] 形式）、またはデフォルトの暗号化パスワードのままにします。

ステップ 5 次のいずれかの操作を実行します。

- 適用（Apply）：選択した認証方式がアクセス方式に関連付けられます。
- デフォルトのクレデンシャルを復元（Restore Default Credentials）：デフォルトのユーザ名とパスワード（anonymous）を復元します。
- センシティブ データをプレーンテキストとして表示（Display Sensitive Data As Plaintext）：現在のページのセンシティブ データがプレーン テキストとして表示されます。

  [SSH User Key Table] には、各キーの次のフィールドが含まれています。

- [Key Type]：RSA または DSA。
- [Key Source]：自動生成またはユーザ定義。
- [Fingerprint]：キーから生成されるフィンガープリント。

ステップ 6 RSA または DSA キーを処理するには、RSA または DSA のどちらかを選択して、次のアクションのいずれかを実行します。

- [Generate]：新しいキーを生成します。

- 編集（Edit）：別のデバイスにコピー/貼り付けするためのキーを表示します。
- [Delete]：キーを削除します。
- [Details]：キーを表示します。

SSH サーバ認証

SSH サーバー認証を有効にし、信頼できるサーバーを定義するには、次の手順を実行します。

ステップ 1 [Security] > [SSH Client] > [SSH Server Authentication] の順にクリックします。

ステップ 2 [Enable] を選択し、SSH サーバ認証を有効にします。

- IPv4 送信元インターフェイス（IPv4 Source Interface）：IPv4 SSH サーバとの通信で使用されるメッセージの送信元 IPv4 アドレスとして使用される IPv4 アドレスを保持している送信元インターフェイスを選択します。
- IPv6 送信元インターフェイス（IPv6 Source Interface）：IPv6 SSH サーバとの通信で使用されるメッセージの送信元 IPv6 アドレスとして使用される IPv6 アドレスを保持している送信元インターフェイスを選択します。

（注） 自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

ステップ 3 [Apply] をクリックします。

ステップ 4 [追加] をクリックし、信頼済み SSH サーバーについての下記フィールドに入力します。

- サーバ定義（Server Definition）：SSH サーバを特定するための方法として、次のいずれかを選択します。
  - IP アドレスによる（By IP address）：これが選択されている場合は、下のフィールドにサーバの IP アドレスを入力します。
  - 名前による（By name）：これが選択されている場合は、[Server IP Address/Name] フィールドにサーバの名前を入力します。
- IP バージョン（IP Version）：IP アドレスで SSH サーバを指定するように選択した場合は、その IP アドレスが IPv4 または IPv6 アドレスのどちらであるかを選択します。
- IPv6 アドレス タイプ（IPv6 Address Type）：SSH サーバの IP アドレスが IPv6 アドレスの場合は、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [リンクローカル] : IPv6 アドレスによって、同一ネットワーク リンク上のホスト が一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つの

リンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。

- [グローバル] : IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。

- リンク ローカル インターフェイス（Link Local Interface）：インターフェイスのリストからリンク ローカル インターフェイスを選択します。
- サーバ IP アドレス/名前（Server IP Address/Name）：[Server Definition] での選択に応じて、SSH サーバの IP アドレスまたはその名前のいずれかを入力します。
- フィンガープリント（Fingerprint）：SSH サーバの（そのサーバからコピーされた）フィンガープリントを入力します。

ステップ 5 [Apply] をクリックします。信頼できるサーバ定義は、実行コンフィギュレーション ファイルに保存されます。

SSH サーバでのユーザ パスワードの変更

SSH サーバーのパスワードを変更するには、次の手順を実行します。

ステップ 1 **[Security]** > **[SSH Client]** > **[Change User Password on SSH Server]** をクリックします。

ステップ 2 次のフィールドに入力します。

- サーバ定義（Server Definition）：[By IP Address] または [By Name] のいずれかを選択して、SSH サーバを定義します。[Server IP Address/Name] フィールドにサーバのサーバ名または IP アドレスを入力します。
- IP バージョン（IP Version）：IP アドレスで SSH サーバを指定するように選択した場合は、その IP アドレスが IPv4 または IPv6 アドレスのどちらであるかを選択します。
- IPv6 アドレス タイプ（IPv6 Address Type）：SSH サーバの IP アドレスが IPv6 アドレスの場合は、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [リンクローカル] : IPv6 アドレスによって、同一ネットワーク リンク上のホスト が一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [グローバル] : IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
- リンク ローカル インターフェイス（Link Local Interface）：インターフェイスのリストからリンク ローカル インターフェイスを選択します。

- サーバ IP アドレス/名前（Server IP Address/Name）：[Server Definition] での選択に応じて、SSH サーバの IP アドレスまたはその名前のいずれかを入力します。
- ユーザ名（Username）：これは、サーバ上のユーザ名と一致している必要があります。
- 古いパスワード（Old Password）：これは、サーバ上のパスワードと一致している必要があります。
- 新しいパスワード（New Password）：新しいパスワードを入力し、[Confirm Password] フィールドでそれを確定します。

ステップ 3 [Apply] をクリックします。SSH サーバのパスワードが変更されます。

TCP/UDPサービス

[TCP/UDP Services] ページでは、デバイス上で TCP または UDP ベースのサービスを有効にできます（通常はセキュリティの理由により行う）。

デバイスには次の TCP/UDP サービスがあります。

- HTTP：出荷時設定では有効
- HTTPS：出荷時設定では有効
- SNMP：出荷時設定では無効
- Telnet：出荷時設定では有効
- SSH：出荷時設定では無効

TCP/UDP サービスを設定するには、次の手順を実行します。

ステップ 1 [Security] > [TCP/UDP サービス（TCP/UDP Services] をクリックします。

ステップ 2 表示されたサービスで、次の TCP/UDP サービスを有効化または無効化します。

- [HTTP Service]：HTTP サービスが有効/無効のどちらになっているかを示します。
- [HTTPS Service]：HTTPS サービスが有効/無効のどちらになっているかを示します。
- [SNMP Service]：SNMP サービスが有効/無効のどちらになっているかを示します。
- [Telnet Service]：Telnet サービスが有効/無効のどちらになっているかを示します。
- [SSH Service]：SSH サーバー サービスが有効/無効のどちらになっているかを示します。

ステップ 3 [Apply] をクリックします。サービスが実行コンフィギュレーション ファイルに書き込まれます。

TCP サービス テーブルには、サービスごとに次のフィールドが表示されます。

- [Service Name]：TCP サービスを提供するためにデバイスが使用するアクセス方式。

- [Type]：サービスが使用する IP プロトコル。
- [Local IP Address]：サービスを提供するためにデバイスが使用するローカル IP アドレス。
- [Local Port]：サービスを提供するためにデバイスが使用するローカル TCP ポート。
- [Remote IP Address]：サービスを要求しているリモートデバイスの IP アドレス。
- [Remote Port]：サービスを要求しているリモートデバイスの TCP ポート。
- [State]：サービスの状態。

UDP サービス テーブルには、次の情報が表示されます。

- [Service Name]：UDP サービスを提供するためにデバイスが使用するアクセス方式。
- [Type]：サービスが使用する IP プロトコル。
- [Local IP Address]：サービスを提供するためにデバイスが使用するローカル IP アドレス。
- [Local Port]：サービスを提供するためにデバイスが使用するローカル UDP ポート。
- [Application Instance]：UDP サービスのサービスインスタンス。

ストーム制御

ブロードキャスト、マルチキャスト、または不明なユニキャストフレームを受信した場合、それらのフレームが重複していると、すべての可能な出力ポートにコピーが送信されます。つまり、実際には、関連するVLANに属しているすべてのポートに送信されます。この方法では、1つの入力フレームが多数のポートに送信され、トラフィック ストームが発生する可能性が生まれます。

ストームプロテクションを使用すると、デバイスに入るフレーム数を制限して、この制限に対してカウントされるフレームの種類を定義できます。

ブロードキャスト、マルチキャスト、または不明なユニキャストフレームのレートがユーザ定義のしきい値よりも高い場合、しきい値を超えた受信フレームは破棄されます。

ストーム制御の設定

ストーム制御を定義するには、次の手順を実行します。

ステップ 1 [Security] > [Storm Control] > [Storm Control Settings] をクリックします。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 パラメータを入力します。

- インターフェイス（Interface）：ストーム制御が有効になっているポートを選択します。

不明なユニキャスト ストーム制御

- ストーム制御状態（Storm Control State）：選択して、ユニキャスト パケットのストーム制御を有効にします。
- レートしきい値（Rate Threshold）：不明なパケットを転送する最大レートを入力します。この値は、キロビット/秒または使用可能な全帯域幅のパーセンテージで入力できます。
- ストームでトラップ（Trap on Storm）：選択して、ポートでストームが発生した場合にトラップを送信します。これが選択されていない場合、トラップは送信されません。
- [Shutdown on Storm]：ポートでストームが発生したときにポートをシャットダウンする場合に選択します。これが選択されていない場合は、余剰トラフィックが破棄されます。

マルチキャスト ストーム制御

- ストーム制御状態（Storm Control State）：選択して、マルチキャスト パケットのストーム制御を有効にします。
- マルチキャスト タイプ（Multicast Type）：ストーム制御を実装するマルチキャスト パケットの種類を次から 1 つ選択します。
  - [All]：ポート上のすべてのマルチキャストパケットに対するストーム制御を有効にします。
  - [Registered Multicast]：ポート上の登録済みマルチキャストアドレスに対するストーム制御のみを有効にします。
  - [Unregistered Multicast]：ポート上の登録解除済みマルチキャストストーム制御のみを有効にします。
- レートしきい値（Rate Threshold）：不明なパケットを転送する最大レートを入力します。この値は、キロビット/秒または使用可能な全帯域幅のパーセンテージで入力できます。
- ストームでトラップ（Trap on Storm）：選択して、ポートでストームが発生した場合にトラップを送信します。これが選択されていない場合、トラップは送信されません。
- [Shutdown on Storm]：ポートでストームが発生したときにポートをシャットダウンする場合に選択します。これが選択されていない場合は、余剰トラフィックが破棄されます。

ブロードキャスト ストーム制御

- ストーム制御状態（Storm Control State）：選択して、ブロードキャスト パケットのストーム制御を有効にします。
- レートしきい値（Rate Threshold）：不明なパケットを転送する最大レートを入力します。この値は、キロビット/秒または使用可能な全帯域幅のパーセンテージで入力できます。
- ストームでトラップ（Trap on Storm）：選択して、ポートでストームが発生した場合にトラップを送信します。これが選択されていない場合、トラップは送信されません。
- [Shutdown on Storm]：ポートでストームが発生したときにポートをシャットダウンする場合に選択します。これが選択されていない場合は、余剰トラフィックが破棄されます。

ステップ 4 [Apply] をクリックします。ストーム制御が変更されて、実行コンフィギュレーション ファイルが更新されます。

ストーム制御統計情報

ストーム制御統計情報を表示するには、次の手順を実行します。

ステップ 1 [Security] > [Storm Control] > [Storm Control Statistics] の順にクリックします。

ステップ 2 インターフェイスを選択します。

ステップ 3 [Refresh Rate] を入力します。統計情報の更新頻度を選択します。次のオプションを使用できます。

リフレッシュなし	統計情報は更新されません。
15 秒	統計情報は 15 秒ごとに更新されます。
[30 Sec]	統計情報は 30 秒ごとに更新されます。
[60 Sec]	統計情報は 60 秒ごとに更新されます。

不明なユニキャスト、マルチキャスト、およびブロードキャストストーム制御に関する次の統計情報が表示されます。

マルチキャストトラフィックタイプ	（マルチキャストトラフィックの場合のみ）すべて。
通過したバイト数	受信したバイト数。
ドロップされたバイト数	ストーム制御が原因でドロップされたバイト数。
最終ドロップ時刻	最後のバイトがドロップされた時刻。

ステップ 4 すべてのインターフェイス上のカウンタをすべてクリアするには、[Clear All Interfaces Counters] をクリックします。インターフェイス上のすべてのカウンタをクリアするには、選択して [Clear Interface Counters] をクリックします。

ポート セキュリティ

（注） ポート セキュリティは、802.1X が有効になっているポートまたは SPAN 宛先として定義されたポート上では有効にすることができません。

ネットワーク セキュリティは、特定のMACアドレスを持つユーザへのポートでのアクセスを制限することで向上できます。MAC アドレスは動的に学習することも、静的に設定することもできます。

ポートセキュリティは、受信および学習したパケットをモニタします。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定されます。

ポート セキュリティには次の 4 つのモードがあります。

- [Classic Lock]：ポート上で学習済みのすべての MAC アドレスがロックされます。新しい MAC アドレスは学習されません。学習済みの MAC アドレスは、エージングや再学習の対象にはなりません。
- 限定された動的ロック（Limited Dynamic Lock）：デバイスは許可されたアドレスの設定済みの制限まで MAC アドレスを学習します。上限数に達すると、デバイスはそれ以上 MAC アドレスを学習しません。このモードでは、学習済みの MAC アドレスがエージングと再学習の対象になります。
- [無期限セキュア]：ポートに関連付けられている現在のダイナミック MAC アドレスを保持します（スタート コンフィギュレーション ファイルにコンフィギュレーションが保存されている間）。ポートの許容最大アドレス数に達するまで、新しい MAC アドレスを「無制限セキュア」対象として学習することができます。再学習とエージングは無効になっています。
- リセット時の安全な削除（Secure Delete on Reset）：リセット後に、ポートに関連付けられている最新の動的MACアドレスを削除します。新しいMACアドレスは、Delete-On-Resetアドレスとして、ポートで許可されている最大アドレス数まで学習できます。再学習とエージングは無効になっています。

ポートで許可されていない新しい MAC アドレスからのフレームが検出された場合（クラシックロックモードで新しい MAC アドレスからのフレームが届いた場合か、限定ダイナミックロックモードで許容最大アドレス数を超過した場合）、保護メカニズムが働き、次のいずれかの処理が実行されます。

- フレームが破棄される
- フレームが転送される
- ポートがシャットダウンする

セキュア MAC アドレスから送信されたフレームが別のポートに届いた場合、そのフレームは転送されますが、そのポート上でその MAC アドレスが学習されることはありません。

次のいずれかの操作に加えて、トラップを生成し、デバイスのオーバーロードを回避するためにトラップの頻度と数を制限できます。

ポートセキュリティを設定するには、次の手順を実行します。

ステップ 1 [Security] > [Port Security] をクリックします。

ステップ 2 変更するインターフェイスを選択して、[Edit] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス] : インターフェイス名を選択します。
- [インターフェイスステータス] : ポートをロックする場合、チェックボックスをオン にします。
- [学習モード] : ポートのロック モードを選択します。このフィールドを設定するには、[Interface Status] のロックを解除する必要があります。[Learning Mode] フィールドは、[Interface Status] フィールドがロックされている場合にのみ有効になります。[Learning Mode] を変更するには、[Lock Interface] をクリアする必要があります。モードを変更したら、[Lock Interface] を元に戻すことができます。次のオプションがあります。
  - [クラシックロック] : すでに学習されている MAC アドレスの数にかかわらず、 ポートをすぐにロックします。
  - [限定ダイナミックロック] : 現在このポートに動的に関連付けられている MAC アドレスを削除し、ポートをロックします。ポートは、そのポートで許可されている最大数までアドレスを学習します。MAC アドレスの再学習とエージングの両方が有効になります。
  - セキュアな相手先固定（Secure Permanent）：ポートに関連付けられている現在の動的な MAC アドレスを保持し、そのポートで許可されているアドレスの最大数（[Max No. of Addresses Allowed] で設定）まで学習します。再学習とエージングは無効になっています。
  - リセット時の安全な削除（Secure Delete on Reset）：リセット後に、ポートに関連付けられている最新の動的 MAC アドレスを削除します。新しい MAC アドレスは、Delete-On-Reset アドレスとして、ポートで許可されている最大アドレス数まで学習できます。再学習とエージングは無効になっています。
- [最大 許可アドレス数] : [学習モード] で [限定ダイナミックロック] を選択した場合、 このポート上で学習できる MAC アドレスの上限数を入力します。数字の 0 は、スタティック アドレスのみインターフェイスでサポートされることを示します。
- [違反時アクション] : ロックされているポートに届いたパケットに適用する処理を選 択します。次のオプションがあります。
  - [Discard]：学習されていない送信元から届いたパケットを破棄します。
  - [Forward]：不明な送信元 MAC アドレスから届いたパケットを転送します。MAC アドレスは学習されません。
  - [Shutdown]：学習されていない送信元からのパケットを破棄し、ポートが再アクティブ化されるか、デバイスがリブートされるまで、ポートをシャットダウンします。
- [トラップ] : ロックされているポートにパケットが届いたときにトラップを有効にする場合、選択します。これは、ロック違反に関係します。[Classic Lock] の場合、受信したすべての新しいアドレスに関係します。[Limited Dynamic Lock] の場合、許可されているアドレス数を超過した新しいアドレスに関係します。
- [トラップ間隔] : トラップの最短間隔を入力します（単位：秒）。

ステップ 4 [Apply] をクリックします。ポート セキュリティが変更されて、実行コンフィギュレーション ファイルが更新されます。

802.1X 認証

802.1X 認証は、未認可クライアントが一般にアクセス可能なポートから LAN に接続することを制限します。802.1X 認証はクライアント/サーバ モデルです。このモデルでは、ネットワーク デバイスが次の固有の役割を持ちます。

- クライアントまたはサプリカント
- オーセンティケータ
- 認証サーバ

ネットワーク デバイスは、ポートごとにクライアント/サプリカント、オーセンティケータ、または両方として使用できます。

802.1X 認証プロパティ

[Properties] ページは、ポート/デバイス認証をグローバルに有効にするために使用されます。認証を機能させるには、認証をグローバルに有効にするとともに各ポートでも個別に有効にする必要があります。

ポートベースの認証を定義するには、次の手順を実行します。

ステップ 1 [Security] > [802.1X Authentication] > [Properties] の順にクリックします。

ステップ 2 パラメータを入力します。

- [ポートベース認証]：ポートベース認証を有効または無効にします。
- [認証方式]：ユーザー認証方式を選択します。次のオプションがあります。
  - [RADIUS、なし]：まずRADIUSサーバーを使用してポート認証を実行します。RADIUSサーバーから応答がない場合、認証処理は実行されず、セッションが許可されます。
  - [RADIUS]：RADIUSサーバー上でユーザーを認証します。認証が行われない場合、セッションは許可されません。
  - [None]：ユーザーを認証しません。セッションは許可されます。
- [Guest VLAN]：未認可ポート用にゲスト VLAN を使用できるようにする場合に選択します。ゲスト VLANが有効になっている場合は、すべての未認可ポートが、[Guest VLAN ID] フィールドで選択したVLAN に自動的に追加されます。ポートが後で許可された場合、そのポートはゲスト VLAN から削除されます。

ゲスト VLAN は、他の VLAN と同様に、レイヤ 3 インターフェイス（IP アドレスが割り当てられている）として定義できます。ただし、ゲスト VLAN IP アドレス経由ではデバイス管理が使用できません。

- [Guest VLAN ID]：VLAN のリストからゲスト VLAN を選択します。
- [Guest VLAN Timeout]：[Immediate]を選択するか[User Defined]に値を入力してタイムアウト時間を定義します。この値は次のように使用されます。

  リンクアップ後にソフトウェアで 802.1x サプリカントが検出されない場合、または認証に失敗した場合、ゲスト VLAN タイムアウトで設定した時間の経過後に、そのポートがゲスト VLAN に追加されます。

  ポート状態が [Authorized] から [Not Authorized] に変わる場合、[Guest VLAN Timeout] の時間が経過すると、そのポートはゲスト VLAN だけに追加されます。
- [トラップ設定]：トラップを有効にするには、次のオプションの中から 1 つ以上を選択します。
  - [802.1X Authentication Failure Traps]：選択すると、802.1X 認証が失敗したときにトラップが生成されます。
  - [802.1X Authentication Success Traps]：選択すると、802.1X 認証が成功したときにトラップが生成されます。
  - [MAC Authentication Failure Traps]：選択すると、MAC 認証が失敗したときにトラップが生成されます。
  - [MAC Authentication Success Traps]：選択すると、MAC 認証が成功したときにトラップが生成されます。
  - [サプリカント認証失敗トラップ]：選択すると、サプリカント認証が失敗したときにトラップが生成されます。
  - [サプリカント認証成功トラップ]：選択すると、サプリカント認証が成功したときにトラップが生成されます。
  - [Web Authentication Failure Traps]：選択すると、Web 認証が失敗したときにトラップが生成されます。
  - [Web Authentication Success Traps]：選択すると、Web 認証が成功したときにトラップが生成されます。
  - [Web Authentication Quiet Traps]：選択すると、待機時間が始まったときにトラップが生成されます。

    VLAN 認証テーブルにすべての VLAN が表示され、認証が有効になっているかどうかが表示されます。

ステップ 3 [Apply] をクリックします。802.1X プロパティは、実行コンフィギュレーション ファイルに書き込まれます。

VLAN での認証の有効/無効を変更するには、VLAN を選択し、[Edit] をクリックして、[Enable] または [Disable] のいずれかを選択します。

ポート認証

[Port Authentication] ページでは、各ポートのパラメータを設定できます。ホスト認証などのいくつかの設定は、ポートが [Force Authorized] 状態の間しか変更できないため、ポート制御を [Force Authorized] に変更してから設定を変更するようにお勧めします。設定が完了したら、ポート制御を元の状態に戻してください。

（注） 802.1X が定義されたポートが LAG のメンバーになることはできません。802.1X とポートのセキュリティは、同じポートで同時に有効にすることはできません。あるインターフェイス上でポートセキュリティを有効にした場合は、[Administrative Port Control] を [Auto] モードに変更できません。

802.1X 認証を設定するには、次の手順に従います。

ステップ 1 [Security] > [802.1X Authentication] > [Port Authentication] の順にクリックします。

このページには、すべてのポートの認証設定が表示されます。

[Add] ページで説明したフィールドに加えて、以下のフィールドがポートごとに表示されます。

- [Supplicant Status]：802.1X サプリカントが有効になっているインターフェイスに関して [Authorized] または [Unauthorized] のいずれかが示されます。
- [Supplicant Credentials]：サプリカント インターフェイスに使用されるクレデンシャル構造の名前。使用可能な値は、任意の名前か、N/A（サプリカントが有効になっていない場合）です。ポートに設定済みのサプリカント クレデンシャル名がある場合、ポート制御パラメータの値は [Supplicant] です。この値により、ポートから受信された他のポート制御情報が上書きされます。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]：ポートを選択します。
- [現在のポート制御]：現在のポート認可状態が表示されます。状態が [Authorized] の場合は、そのポートが認証されているか、[Administrative Port Control] が [強制認可（Force Authorized] になっています。反対に状態が [Unauthorized] の場合は、ポートが認証されていないか、[Administrative Port Control] が [Force Unauthorized] になっています。サプリカントをインターフェイス上で有効にすると、現在のポート制御がサプリカントになります。
- [管理ポート制御]：認可状態を選択します。次のオプションがあります。

- [Force Unauthorized]：インターフェイスを未承認状態に移行することにより、インターフェイスアクセスを拒否します。デバイスが、このインターフェイスを介してクライアントに認証サービスを提供することはありません。
- [Auto]：デバイスでのポートベース認証および認可を有効にします。デバイスとクライアントの間で交換される認証情報に基づいて、インターフェイスの状態は認可済みになったり未認可になったりします。
- [Force Authorized]：認証せずにインターフェイスを承認します。

- [RADIUS VLAN Assignment]：選択したポート上でダイナミック VLAN 割り当てを有効にする場合、選択します。
  - [Disable]：機能が有効になっていません。
  - [Reject]：RADIUS サーバーがサプリカントを許可したのにサプリカント VLAN を提供しなかった場合、そのサプリカントは拒否されます。
  - [Static]：RADIUS サーバーがサプリカントを許可したのにサプリカント VLAN を提供しなかった場合、そのサプリカントは許可されます。
- [Guest VLAN]：未認可ポート用にゲスト VLAN を使用できるようにする場合に選択します。
- [Open Access]：選択すると、認証が失敗した場合でもポートは正常に認証されます。
- [802.1X Based Authentication]：選択すると、ポートで 802.1X 認証が有効になります。
- [MAC-Based Authentication]：選択すると、サプリカント MAC アドレスに基づくポート認証が有効になります。このポートでは 8 つの MAC ベース認証のみを使用できます。

  （注） MAC ベース認証が成功するには、RADIUS サーバのサプリカントのユーザ名とパスワードが、サプリカント MAC アドレスである必要があります。MAC アドレスは、小文字で、ピリオドやハイフン（「.」や「-」）の区切り文字を使用せずに入力する必要があります（例：0020aa00bbcc）。

- [Web-Based Authentication]：選択すると、サプリカント MAC アドレスに基づく Web ベース認証が有効になります。
- [Periodic Reauthentication]：選択すると、[Reauthentication Period] で指定した間隔で、ポートの再認証試行が有効になります。
- [再認証期間]：選択したポートを再認証する間隔を入力します（単位：秒）。
- [Reauthenticate Now]：選択すると、ポートの再認証がすぐに有効になります。
- [認証状態]：設定されているポート認可状態が表示されます。次のオプションがあります。
  - [初期化]：起動処理中。
  - [Force Authorized]：ポート制御状態は Force Authorized（トラフィックを転 送）に設定されています。

- [Force-Unauthorized]：制御ポート状態が [Force-Unauthorized]（トラフィックの破棄）に設定されています。

  （注） [Force-Authorized] でも [Force-Unauthorized] でもない場合、ポートは自動モードになっていて、オーセンティケータには現在の認証状態が表示されます。ポートが認証されると、状態は [Authenticated] と表示されます。

- [Time Range]：選択すると、特定の時間範囲への認証の制限が有効になります。
- [時間範囲名]：[時間範囲] が選択されている場合は、[編集] ボタンをクリックすると、時間範囲のページにリダイレクトされます。そのページで、使用する時間範囲名を選択します。
- [Maximum WBA Login Attempts]：Web ベース認証で許可されるログイン試行の最大回数を入力します。[無制限] を選択して無制限にするか、[ユーザー定義] を選択して制限を設定します。
- [Maximum WBA Silence Period]：このインターフェイスで許可される Web ベース認証のサイレント期間の最大長を入力します。[無制限] を選択して無制限にするか、[ユーザー定義] を選択して制限を設定します。
- [Max Hosts]：このインターフェイスで許可される認可済みホストの最大数を入力します。

  [無制限] を選択して無制限にするか、[ユーザー定義] を選択して制限を設定します。

  （注） この値を 1 に設定すると、マルチセッション モードの Web ベース認証に対してシングルホスト モードがシミュレートされます。

- [Quiet Period]：待機時間の長さを入力します。
- [Resending EAP]：サプリカント（クライアント）からの、Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）要求/ID フレームに対する応答をデバイスが待機する時間（秒単位）を入力します。この時間内に応答がない場合、要求が再送信されます。
- [Max EAP Requests]：EAP 要求の最大送信回数を入力します。定義された期間内に応答が受信されなかった（サプリカントタイムアウト）場合は、認証プロセスが再開されます。
- [EAP Max Retries]：EAP 再試行の最大送信回数を入力します。
- [EAP Timeout]：タイムアウトになるまでの EAP 応答を待つ最大時間を入力します。
- [サプリカントタイムアウト]：サプリカントのタイムアウト時間を入力します（単位：秒）。この時間内に応答がない場合、EAP 要求がサプリカントに再送信されます。
- [Server Timeout]：デバイスが認証サーバに要求を再送信するまでの経過時間（秒単位）を入力します。
- [Supplicant]：802.1X を有効にする場合に選択します。
- [Credentials]：このサプリカントに使用するクレデンシャルをドロップダウン リストから選択します。このパラメータは、サプリカントがインターフェイスで有効になっている場合にのみ使用できます。クレデンシャルを設定できる [Supplicant Credentials] ページへのリンクを編集してください。
- [Supplicant Held Timeout]：RADIUS サーバから失敗応答を受信した後にサプリカントが認証を再び開始するまでの待機時間を入力します。

ステップ 4 [Apply] をクリックします。ポート設定は、実行コンフィギュレーション ファイルに書き込まれます。

ホストおよびセッション認証

[Host and Session Authentication] ページでは、ポートでの 802.1X の動作モードと、違反検出時に実行するアクションを定義できます。

ポートの 802.1X 詳細設定を定義するには、次の手順を実行します。

ステップ 1 [Security] > [802.1X Authentication] > [Host and Session Authentication] の順にクリックします。

すべてのポートの認証パラメータが示されます。次のフィールドを除くすべてのフィールドは、[Edit]ページに示されます。

- [Number of Violations]：単一ホストモードで、そのインターフェイスが、サプリカントの MAC アドレスとは異なる MAC アドレスを持つホストから受信したパケット数が表示されます。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]：ホスト認証を有効にするポート番号を入力します。
- [Host Authentication]：いずれかのモードを選択します。
  - [Single-Host]：許可されたクライアントが存在する場合にポートが許可されます。1 つのポートでは 1 つのホストのみ認可されます。
  - [Multi-Host (802.1x)]：許可されたクライアントが少なくとも 1 つ存在する場合にポートが許可されます。
  - [Multi-Sessions]：シングルホストおよびマルチホストモードとは異なり、マルチセッションモードのポートには認証ステータスがありません。このステータスは、ポートに接続している各クライアントに割り当てられます。

[Single Host Violation Settings]：ホスト認証が [Single-Host] の場合にのみ選択できます。

- [Action on Violation]：サプリカントの MAC アドレスとは異なる MAC アドレスを持つホストから、シングルセッションモードかシングルホストモードで受信したパケットに適用する処理を選択します。次のオプションがあります。
  - [保護(破棄)]：パケットを破棄します。
  - [制限(転送)]：パケットを転送します。
  - [シャットダウン]：パケットを廃棄し、ポートを停止します。ポートは、再アクティブ化されるかデバイスが再起動するまで、シャットダウンした状態になります。
- [トラップ]：選択すると、トラップが有効になります。

- [Trap Frequency]：ホストにトラップを送信する頻度を定義します。このフィールドの値を定義できるのは、複数ホストが無効になっている場合だけです。

ステップ 4 [Apply] をクリックします。設定は、実行コンフィギュレーション ファイルに書き込まれます。

サプリカントクレデンシャル

802.1X オーセンティケータとしての機能に加えて、スイッチ自体を、ネイバーからのポートアクセス権限を求める802.1Xサプリカントとして設定できます。このサプリカントは、RFC3748で規定されている EAP MD5-Challenge 方式をサポートします。この方式では、クライアントが、その名前とパスワードによって認証されます。サプリカントがインターフェイスで有効になっている場合、そのインターフェイスは未認可になります。802.1X認証プロセスが成功すると、インターフェイスの状態が認可済みに変更されます。このページでは、802.1Xサプリカントとして設定されたインターフェイスで使用できるクレデンシャルを作成および設定することができます。

サプリカントのログイン情報を追加するには、次の手順を実行します。

ステップ 1 **[Security]** > **[802.1X Authentication]** > [Supplicant Credentials] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [クレデンシャル名]：クレデンシャルを識別するための名前。
- [User Name]：クレデンシャル名に関連付けられるユーザ名を入力します。
- [Description]：ユーザを説明するテキストを入力します。
- [Password]：パスワードのタイプ（[Encrypted] または [Plaintext]）を選択し、パスワードを追加します。

ステップ 4 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

MACベース認証設定

MAC ベース認証は、802.1X のサプリカント機能を持たない装置（プリンタおよび IP Phone など）へのネットワーク アクセスを可能にする、802.1X 認証に代わるものです。MAC ベース認証は、接続装置の MAC アドレスを使用してネットワーク アクセスを許可または拒否します。

MAC ベース認証を設定するには、次の手順を実行します。

ステップ 1 [Security] > [802.1X Authentication] > [MAC-Based Authentication Settings] の順にクリックします。

ステップ 2 次のフィールドに入力します。

- [MAC認証タイプ]：次のいずれかのオプションを選択します。
  - [EAP]：スイッチ（RADIUS クライアント）と RADIUS サーバー（MAC ベースのサプリカントを認証するサーバー）の間のトラフィックに対し、RADIUS と EAP カプセル化を使用します。
  - [RADIUS]：スイッチ（RADIUS クライアント）と RADIUS サーバー（MAC ベースのサプリカントを認証するサーバー）の間のトラフィックに対して、RADIUS（EAP カプセル化なし）を使用します。

  ユーザ名の形式

  MAC ベースの認証では、サプリカント ユーザー名はサプリカント デバイスの MAC アドレスに基づいています。このMACベースのユーザー名の形式は、次のように定義されます。このユーザー名は、認証プロセスの一部としてスイッチから RADIUS サーバーへ送信されます。
- [グループサイズ]：MAC アドレスで区切り文字で囲まれ、ユーザー名として送信される ASCII 文字の数。
- [グループ区切り]：MACアドレス内で定義される文字グループを区切る区切り文字として使用される文字。
- [大文字小文字]：ユーザー名を小文字または大文字で送信します。

  MAC認証パスワード
- [Password]：スイッチがRADIUSサーバーでの認証に使用するパスワードを定義します。次のオプションのいずれかを選択します。
  - [デフォルトの使用(ユーザー名)]：定義されているユーザー名をパスワードとして使用する場合は、このオプションを選択します。
  - [暗号化]：パスワードを暗号化形式で定義します。
  - [プレーンテキスト]：パスワードをプレーンテキスト形式で定義します。
- [パスワードMD5ダイジェスト]：MD5 Digest パスワードを表示します。

ステップ 3 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。暗号化されたパスワードを表示するには、[機密データを平文で表示] をクリックします。

認証済みホスト

認証済みユーザーの詳細情報を表示するには、[Security] > [802.1X Authentication] > [Authenticated Hosts] の順にクリックします。

このページには、次のフィールドが表示されます。

- [User Name]：各ポートで認証されたサプリカントの名前。
- [Port]：ポート番号。

- [Session Time (DD:HH:MM:SS)]：そのポートでサプリカントが認証および認可されていた時間の長さ。
- [認証方式]：最後のセッションの認証に使用された方式。
- [Authentication Server]：RADIUS サーバー。
- [MAC アドレス]：サプリカントの MAC アドレスが表示されます。
- [VLAN ID]：ポートの VLAN。

ロック済みクライアント

ログインに失敗してロックアウトされたクライアントを表示し、ロック済みクライアントをロック解除するには、次の手順を実行します。

ステップ 1 **[Security]** > **[802.1X Authentication]** > [Locked Client] の順にクリックします。

次のフィールドが表示されます。

- [Interface]：ロックされたポート。
- [MACアドレス]：ロック済みステーションの MAC アドレスが表示されます。
- [Remaining Time (Sec)]：ポートがロックされるまでの残り時間。

ステップ 2 ポートを選択します。

ステップ 3 [Unlock] をクリックします。

Web認証のカスタマイズ

このページでは、さまざまな言語の Web ベース認証ページを設計できます。

最大 4 つの言語を追加できます。

（注） 最大 5 人の HTTP ユーザと 1 人の HTTPS ユーザが同時に Web ベース認証を要求できます。これらのユーザが認証されると、さらに別のユーザが認証を要求できます。

Web ベース認証用の言語を追加するには、次の手順を実行します。

ステップ 1 [Security] > [802.1X Authentication] > [Web Authentication Customization] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 [Language] ドロップダウン リストから言語を選択します。

ステップ 4 この言語をデフォルト言語にする場合は、[Set as Default Display Language] を選択します。エンドユーザが言語を選択していない場合はデフォルト言語のページが表示されます。

ステップ 5 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

Web 認証ページをカスタマイズするには、次の手順に従います。

ステップ 6 [Security] > [802.1X Authentication] > [Web Authentication Customization] の順にクリックします。

このページには、カスタマイズ可能な言語が表示されます。

ステップ 7 [Edit Login Page] をクリックします。

ステップ 8 [Edit labeled 1] をクリックします。次のフィールドが表示されます。

- [言語]：ページの言語が表示されます。
- [Color Scheme]：いずれかのコントラスト オプションを選択します。

  [Custom] カラー スキームが選択されている場合は、次のオプションを使用できます。

  - [Page Background Color]：背景の色の ASCII コードを入力します。選択した色がテキスト フィールドに表示されます。
  - [Page Text Color]：テキストの色の ASCII コードを入力します。選択した色がテキスト フィールドに表示されます。
  - [Header and Footer Background Color]：ヘッダーとフッターの背景の色の ASCII コードを入力します。選択した色がテキスト フィールドに表示されます。
  - [Header and Footer Text Color]：ヘッダーとフッターのテキストの色の ASCII コードを入力します。選択した色がテキスト フィールドに表示されます。
  - [Hyperlink Color]：テキストの色の ASCII コードを入力します。選択した色がテキスト フィールドに表示されます。

- [現在のロゴ画像]：現在のログ画像を含むファイルの名前が表示されます。
- [ロゴ画像]：次のいずれかのオプションを選択します。
  - [None]：ロゴを使用しません。
  - [デフォルト]：デフォルトのロゴを使用します。
  - [Other]：カスタマイズしたロゴを入力する場合に選択します。

    [Other] ロゴ オプションが選択されている場合は、次のオプションを使用できます。

  - [Logo Image Filename]：ロゴ ファイル名を入力するか、[Browse] をクリックして画像を選択します。
  - [Application Text]：ロゴに添えるテキストを入力します。
  - [Window Title Text]：ログイン ページのタイトルを入力します。

ステップ 9 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 10 [Edit labeled 2] をクリックします。次のフィールドが表示されます。

- [Invalid User Credentials]：エンドユーザが無効なユーザ名またはパスワードを入力したときに表示されるメッセージのテキストを入力します。
- [Service Not Available]：認証サービスを使用できないときに表示されるメッセージのテキストを入力します。

ステップ 11 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 12 [Edit labeled 3] をクリックします。次のフィールドが表示されます。

- [Welcome Message]：エンドユーザがログオンしたときに表示されるメッセージのテキストを入力します。
- [Instructional Message]：エンドユーザに表示される指示を入力します。
- [RADIUS Authentication]：RADIUS 認証が有効になっているかどうかが示されます。有効になっている場合は、ログイン ページにユーザ名とパスワードを含める必要があります。
- [Username Textbox]：選択すると、ユーザ名のテキスト ボックスが表示されます。
- [Username Textbox Label]：ユーザ名のテキスト ボックスの前に表示されるラベルを選択します。
- [Password Textbox]：選択すると、パスワードのテキスト ボックスが表示されます。
- [Password Textbox Label]：パスワードのテキスト ボックスの前に表示されるラベルを選択します。
- [Language Selection]：選択すると、エンドユーザが言語を選択できるようになります。
- [Language Dropdown Label]：言語選択ドロップダウンのラベルを入力します。
- [Login Button Label]：ログイン ボタンのラベルを入力します。
- [Login Progress Label]：ログイン プロセス中に表示されるテキストを入力します。

ステップ 13 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 14 [Edit labeled 4] をクリックします。次のフィールドが表示されます。

- [Terms and Conditions]：選択すると、契約条件のテキスト ボックスが有効になります。
- [Terms and Conditions Warning]：契約条件入力の指示として表示されるメッセージのテキストを入力します。
- [Terms and Conditions Content]：契約条件として表示されるメッセージのテキストを入力します。

ステップ 15 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 16 [Edit labeled 5] では、次のフィールドが表示されます。

- [Copyright]：選択すると、著作権のテキストの表示が有効になります。
- [著作権のテキスト]：著作権のテキストを入力します。

ステップ 17 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ステップ 18 [Edit Success Page] をクリックします。

ステップ 19 ページの右側にある [Edit] をクリックします。

ステップ 20 [Success Message] に、エンドユーザが正常にログインしたときに表示されるテキストを入力します。

ステップ 21 [Apply] をクリックするとし、設定が実行コンフィギュレーション ファイルに保存されます。

ログインまたは成功メッセージをプレビューするには、[Preview] をクリックします。

GUI インターフェイスのデフォルト言語を Web ベース認証のデフォルト言語として設定するには、[Set Default Display Language] をクリックします。

サービス拒絶防御

サービス妨害（DoS）攻撃では、ハッカーはデバイスをユーザが使用できない状態にしようとします。

DoS 攻撃では、デバイスが外部の通信要求で満たされ、正当なトラフィックに応答できないようになります。この攻撃では通常、デバイスの CPU がオーバーロードになります。

デバイスによって使用される DoS 攻撃に対抗する方法の 1 つは、セキュアコアテクノロジー（SCT）を利用する方法です。SCTはデフォルトで有効になっており、無効化できません。シスコデバイスは、エンドユーザ（TCP）トラフィックに加えて、管理トラフィック、プロトコル トラフィック、およびスヌーピング トラフィックを処理する高度なデバイスです。SCT を使用することで、デバイスは、受信するトラフィック量に関係なく、管理およびプロトコル トラフィックを受信して処理できます。これは、CPU に対する TCP トラフィックのレートを制限することで実現されます。

セキュリティスイート設定

（注） DoS 防御を有効化する前に、ポートにバインドされているすべてのアクセス コントロール リスト（ACL）または高度な QoS ポリシーをアンバインドする必要があります。ポートで DoS 防御機能がアクティブ化されている間、ACL と拡張QoSポリシーは非アクティブ化されます。

DoS 防御のグローバル設定を構成し、SCT をモニタするには、次の手順を実行します。

ステップ 1 [Security] > [Denial of Service Prevention] > [Security Suite Settings] をクリックします。

CPU 保護メカニズム：有効化（CPU Protection Mechanism: Enabled）は SCT が有効であることを示します。

ステップ 2 [CPU Utilization] の横の [Details] をクリックするとCPU 使用率 （41 ページ）ページに移動し、CPU リソース利用率情報が表示されます。

ステップ 3 この機能を設定するには、[TCP SYN Protection] の横にある [Edit] をクリックします。

ステップ 4 [DoS防御] を設定します。

- [Disable]：すべてのタイプのサービス妨害機能を無効にします（デバイスレベルの TCP SYN 保護は除く）。
- [System-Level Prevention]：Stacheldraht（分散型）、Invasor（トロイの木馬）、Back Orifice（トロイの木馬）、Martian アドレスからの攻撃の防御を有効にします。
- [System-Level and Interface-Level Prevention]：システムレベルの防御に加えて、インターフェイスレベルの設定（SYN フィルタリング、SYN レート保護、ICMP フィルタリング、IP フラグメント化）を有効化して設定できます。

ステップ 5 [システムレベルの防御] または [システムレベルおよびインターフェイスレベルの防御] を選択した場合、次の [DoS防御] オプションの 1 つまたは複数を有効にしてください。

- [Stacheldraht Distribution]：送信元 TCP ポートが 16660 に等しい TCP パケットを破棄します。
- [Invasor Trojan]：宛先 TCP ポートが 2140 に等しく、送信元 TCP ポートが 1024 に等しい TCP パケットを破棄します。
- [Back Orifice Trojan]：宛先 UDP ポートが 31337 に等しく、送信元 UDP ポートが 1024 に等しい UDP パケットを破棄します。

ステップ 6 必要に応じて、以下をクリックします。

- [Martian Addresses]：[Edit] をクリックするとMartianアドレス （352 ページ）ページに移動します。
- [SYN Filtering]：[Edit] をクリックするとSYN フィルタリング （354 ページ）ページに移動します。
- [SYN Rate Protection]：（レイヤ 2 のみ）[Edit] をクリックするとSYNレート保護 （354 ページ）ページに移動します。
- [ICMP Filtering]：[Edit] をクリックするとICMPフィルタリング （355 ページ）ページに移動します。
- [IP Fragmented]：[Edit] をクリックするとIPフラグメントフィルタリング （356 ページ）ページに移動します。

ステップ 7 [Apply]をクリックします。サービス妨害（DoS）防御セキュリティ スイートの設定が、実行コンフィギュレーション ファイルに書き込まれます。

SYN保護

ネットワーク ポートは、SYN 攻撃でデバイスを攻撃するためにハッカーによって使用される可能性があります。SYN 攻撃は TCP リソース（バッファ）と CPU パワーを消費します。

CPU は SCT を使用して保護されているため、CPU への TCP トラフィックは制限されます。ただし、1 つまたは複数のポートが高いレートの SYN パケットで攻撃された場合、CPU は攻撃者のパケットのみ受け取るためサービス妨害が発生します。

SYN 保護機能を使用している場合、CPU は各ネットワーク ポートから CPU に送られる 1 秒あたりの SYN パケットの入力をカウントします。

SYN 保護を設定するには、次の手順を実行します。

ステップ 1 [Security] > [Denial of Service Prevention] > [SYN Protection] をクリックします。

ステップ 2 パラメータを入力します。

- [Block SYN-FIN Packets]：選択すると、この機能が有効になります。すべてのポートで、SYN と FIN の両方のフラグを持つすべての TCP パケットがドロップされます。
- [SYN Protection Mode]：次の 3 つのモードから選択します。
  - [Disable]：特定のインターフェイスでこの機能が無効になります。
  - [Report]：SYSLOG メッセージを生成します。しきい値を超えた場合、ポートのステータスが [Attacked] に変わります。
  - [Block and Report]：TCP SYN 攻撃が見つかった場合、システム宛ての TCP SYN パケットはドロップされて、ポートのステータスが [Blocked] に変わります。
- [SYN Protection Threshold]：SYN パケットがブロックされるまでの 1 秒あたりの SYN パケット数（「自分への MAC を含む SYN を拒否」ルールがポートに適用されます）。
- [SYN Protection Period]：SYN パケットのブロックを解除するまでの秒数（「自分への MAC を含む SYN を拒否」ルールはポートからバインド解除されます）。

ステップ 3 [Apply] をクリックします。SYN 保護が定義され、実行コンフィギュレーション ファイルが更新されます。

SYN 保護インターフェイス テーブルに、（ユーザのリクエストに応じて）すべてのポートまたは LAG に関する次のフィールドが表示されます。

- [Current Status]：インターフェイスのステータス。次の値が可能です。
  - [Normal]：このインターフェイスで攻撃は検出されませんでした。
  - [Blocked]：トラフィックはこのインターフェイスでは転送されません。
  - [Attacked]：このインターフェイスで攻撃が検出されました。
- [Last Attack]：システムで最後に検出された SYN-FIN 攻撃の日付と、それに対するシステムのアクション。

Martianアドレス

[Martian Addresses] ページでは、ネットワーク上で確認された攻撃を示す IP アドレスを入力できます。それらのアドレスからのパケットは破棄されます。デバイスは、IP プロトコルの観点

からは不正な一連の予約済み Martian アドレスをサポートします。サポートされている予約済み Martian アドレスは次のとおりです。

- [Martian Addresses] ページで不正と定義されているアドレス。
- ループバックアドレスなど、プロトコルの観点からは不正なアドレス。次の範囲内のアドレスが含まれます。
  - 0.0.0.0/8（ただし送信元アドレスとしての 0.0.0.0/32 を除く）：このブロックのアドレスは、このネットワーク上の送信元ホストを参照します。
  - 127.0.0.0/8：インターネットホストのループバックアドレスとして使用されます。
  - 192.0.2.0/24：ドキュメンテーションおよびコード例で TEST-NET として使用されます。
  - 224.0.0.0/4（送信元 IP アドレスとして）：IPv4 マルチキャストアドレス割り当てで使用されます。以前は「クラス D アドレス空間」と呼ばれていました。
  - 240.0.0.0/4（ただし宛先アドレスとしての 255.255.255.255/32 を除く）：予約済みアドレス範囲。以前は「クラス E アドレス空間」と呼ばれていました。

DoS 防御用の新しい Martian アドレスを追加することもできます。Martian アドレスを含むパケットは破棄されます。

Martian アドレスを定義するには、次の手順を実行します。

ステップ 1 [Security] > [Denial of Service Prevention] > [Martian Addresses] をクリックします。

ステップ 2 [Reserved Martian Addresses] を選択し、[Apply] をクリックして、[System Level Prevention] リストに予約済の Martian アドレスを含めます。

ステップ 3 Martian アドレスを追加するには、[Add] をクリックします。

ステップ 4 パラメータを入力します。

- [IP Version]：サポートされる IP バージョンを示します。現時点では、IPv4 のサポートのみ提供されています。
- [IP Address]：拒否する IP アドレスを入力します。次の値が可能です。
  - [From Reserved List]：予約済みリストからウェルノウン IP アドレスを選択します。
  - [New IP Address]：IP アドレスを入力します。
- [Mask]：拒否する IP アドレスの範囲を定義するために IP アドレスのマスクを入力します。値は次のとおりです。
  - [Network Mask]：ドット付き 10 進表記でのネットワークマスク。
  - [Prefix Length]：サービス拒絶防御を有効にする対象の IP アドレス範囲を定義するための IP アドレスプレフィックスを入力します。

ステップ 5 [Apply] をクリックします。

SYN フィルタリング

[SYN Filtering] ページでは、SYN フラグを含み、1 つまたは複数のポートに送信される TCP パケットをフィルタリングできます。

SYN フィルタを定義するには、次の手順を実行します。

ステップ 1 [Security] > [Denial of Service Prevention] > [SYN Filtering] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [Interface]：フィルタを定義するインターフェイスを選択します。
- [IPv4アドレス]：フィルタを定義する対象の IP アドレスを入力するか、[すべてのアドレス] を選択します。
- ネットワーク マスク（Network Mask）：フィルタが有効になっているネットワーク マスクを IP アドレス形式で入力します。次のいずれか 1 つを入力します。
  - [Mask]：ドット付き 10 進表記のネットワークマスク。
  - [プレフィックス長]：DoS 防御を有効にする対象の IP アドレス範囲を定義するための IP アドレス プレフィックス長を入力します。
- TCP ポート（TCP Port）：フィルタ処理されている宛先 TCP ポートを選択します。
  - [Known ports]：リストからポートを選択します。
  - [User Defined]：ポート番号を入力します。
  - [すべてのポート]：すべてのポートをフィルタするには、このフィールドを選択します。

ステップ 4 [Apply] をクリックします。SYN フィルタが定義され、実行コンフィギュレーション ファイルが更新されます。

SYNレート保護

[SYN Rate Protection] ページでは、入力ポートで受信する SYN パケットの数を制限できます。そのため、パケット処理のために開かれる新しい接続数をレート制限することで、サーバに対する SYN フラッドの影響を緩和できます。

SYN レート保護を定義するには、次の手順を実行します。

ステップ 1 [Security] > [Denial of Service Prevention] > [SYN Rate Protection] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- インターフェイス（Interface）：レート保護が定義されているインターフェイスを選択します。
- [IPアドレス]：SYN レート保護を定義する対象の IP アドレスを入力するか、[すべてのアドレス] を選択します。IP アドレスを入力する場合は、マスクまたはプレフィックス長を入力します。
- [Network Mask]：送信元 IP アドレスのサブネットマスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - マスク（Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。
  - [プレフィックス長]：[プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。
- SYN レート制限（SYN Rate Limit）：受信する SYN パケットの数を入力します。

ステップ 4 [Apply] をクリックします。SYN レート保護が定義され、実行コンフィギュレーションが更新されます。

ICMPフィルタリング

[ICMP Filtering] ページでは、特定の送信元からの ICMP パケットをブロックできます。ブロックすることで、ICMP 攻撃の発生時にネットワークの負荷を軽減できます。

ICMP フィルタリングを設定するには、次の手順を実行します。

ステップ 1 [Security] > [Denial of Service Prevention] > [ICMP Filtering] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- インターフェイス（Interface）：ICMP フィルタリングが定義されているインターフェイスを選択します。
- [IPアドレス]：ICMP パケット フィルタリングをアクティブにする対象の IPv4 アドレスを入力するか、または [すべてのアドレス] を選択してすべての送信元アドレスからの ICMP パケットをブロックします。IP アドレスを入力する場合は、マスクまたはプレフィックス長を入力します。
- ネットワーク マスク（Network Mask）：送信元 IP アドレスのサブネット マスクの形式を選択し、いずれかのフィールドに値を入力します。
  - マスク（Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。

- [プレフィックス長] : [プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。

ステップ 4 [Apply] をクリックします。ICMP フィルタリングが定義され、実行コンフィギュレーションが更新されます。

IPフラグメントフィルタリング

IP フラグメンテーションは、ネットワーク層のデータが大きすぎて、データリンク層を介して一度に送信できない場合に発生します。その場合、ネットワーク層のデータがいくつかの断片（フラグメント）に分割されます。このプロセスが IP フラグメンテーションと呼ばれます。

フラグメント化された IP のフィルタ処理を設定し、フラグメント化された IP パケットをブロックするには、次の手順を実行します。

ステップ 1 [Security] > [Denial of Service Prevention] > [IP Fragments Filtering] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- インターフェイス（Interface）：IP フラグメンテーションが定義されているインターフェイスを選択します。
- [IPアドレス] : フラグメント化 IP パケットをフィルタリングする対象の IP ネットワークを入力するか、または [すべてのアドレス] を選択してすべてのアドレスからの IP フラグメント化パケットをブロックします。IP アドレスを入力する場合は、マスクまたはプレフィックス長を入力します。
- [Network Mask]：送信元 IP アドレスのサブネットマスクの形式を選択し、次のいずれかのフィールドに値を入力します。
  - マスク（Mask）：送信元 IP アドレスが所属するサブネットを選択し、ドット付き 10 進表記でサブネット マスクを入力します。
  - [プレフィックス長] : [プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。

ステップ 4 [Apply] をクリックします。IP フラグメンテーションが定義され、実行コンフィギュレーション ファイルが更新されます。

IP ソース ガード

IP ソース ガードは、ホストがネイバーの IP アドレスを使用しようとしたときに発生するトラフィック攻撃を防ぐために使用できるセキュリティ機能です。

IP ソース ガードが有効になっている場合、デバイスは、DHCP スヌーピング バインディング データベースに含まれている IP アドレスにのみクライアント IP トラフィックを送信します。このデータベースには、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のアドレスが含まれます。パケットがデータベース内のエントリと一致した場合、デバイスはそのパケットを転送します。一致しない場合、パケットはドロップされます。

ポートで IP ソース ガードが有効になっている場合：

- DHCP スヌーピングによって許可される DHCP パケットが受け入れられます。
- 送信元 IP アドレス フィルタリングを有効になっている場合：
  - IPv4 トラフィック：ポートに関連付けられている送信元 IP アドレスを持つトラフィックのみ許可されます。
  - 非 IPv4 トラフィック：許可されます（ARP パケットを含む）。

IP ソースガードのプロパティ

IP ソース ガードをグローバルに有効にするには、次の手順を実行します。

ステップ 1 [Security] > [IP Source Guard] > [Properties] の順にクリックします。
ステップ 2 [Enable] を選択して、IP ソース ガードをグローバルに有効にします。
ステップ 3 [Apply] をクリックして、IP ソース ガードを有効にします。

インターフェイスの設定

IP ソース ガードが信頼できないポートや LAG で有効になっている場合、DHCP スヌーピングによって許可された DHCP パケットが送信されます。送信元 IP アドレス フィルタリングが有効になっている場合、パケット送信は次のように許可されます。

- [IPv4 traffic]：特定のポートに関連付けられている送信元 IP アドレスを含む IPv4 トラフィックだけが許可されます。
- [Non IPv4 traffic]：IPv4 以外のトラフィックはすべて許可されます。

インターフェイスで IP ソース ガードを設定するには、次の手順を実行します。

ステップ 1 [Security] > [IP Source Guard] > [Interface Settings] をクリックします。
ステップ 2 [Filter] フィールドからポート/LAG を選択して、[Go] をクリックします。このユニット上のポートまたは LAG が次の情報とともに表示されます。

- [IP Source Guard]：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。

- DHCP スヌーピングの信頼できるインターフェイス（DHCP Snooping Trusted Interface）：信頼できる DHCP インターフェイスであるかどうかを示します。

ステップ 3 ポートまたは LAG を選択し、[Edit] をクリックします。[IP Source Guard] フィールドの [Enable] を選択すると、インターフェイスで IP ソースガードが有効になります。

ステップ 4 [Apply] をクリックして、設定を実行コンフィギュレーション ファイルにコピーします。

IP ソースガード バインディング データベース

IP ソースガードでは、信頼されていないポートからのパケットをチェックするために DHCP スヌーピング バインディング データベースを使用します。デバイスが 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の数が多すぎる場合、余分なエントリが非アクティブステータスで維持されます。エントリはリース時間が期限切れになると削除されるため、非アクティブなエントリがアクティブになることがあります。

「DHCP スヌーピング/リレー （246 ページ）」を参照してください。

（注） バインディングデータベースのページには、IP ソースガードが有効になったポートで定義された 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のみが表示されます。

DHCP スヌーピングを表示し、消費された TCAM リソースを確認するには、次の手順を実行します。

ステップ 1 [Security] > [IP Source Guard] > [Binding Database] をクリックします。

[Supported IP Format and TCAM Resources Consumed] が表示されます。

ステップ 2 DHCP スヌーピングでは、データベースの管理に TCAM リソースが使用されます。デバイスで非アクティブ エントリをアクティブ化する試行をどの程度の頻度で行うかを選択するために、[挿入非アクティブ] フィールドを設定します。次のオプションがあります。

- 再試行頻度（Retry Frequency）：TCAM リソースがチェックされる頻度。
- 実行しない（Never）：非アクティブなアドレスの再アクティブ化を試みない。

ステップ 3 [Apply] をクリックすると上記の変更が実行コンフィギュレーションに保存されます。また、[Retry Now] をクリックすると TCAM リソースが検査されます。

次のエントリが表示されます。

- [VLAN ID]：パケットを受信すると予想される VLAN。
- [MAC Address]：照合される MAC アドレス。
- [IP Address]：照合される IP アドレス。

- インターフェイス（Interface）：パケットが予測されるインターフェイス。
- [Status]：インターフェイスがアクティブであるかどうかを表示します。
- タイプ（Type）：エントリのタイプ（動的または静的）が表示されます。
- [Reason]：インターフェイスがアクティブでない場合、その理由を表示します。次の理由があります。
  - [No Problem]：インターフェイスはアクティブです。
  - [No Snoop VLAN]：VLAN で DHCP スヌーピングが有効になっていません。
  - [Trusted Port]：ポートが信頼されるようになりました。
  - リソースの問題（Resource Problem）：TCAM リソースが使い果たされました。

ステップ 4 これらのエントリのサブセットを表示するには、関連の検索条件を入力して [Go] をクリックします。

ARP インスペクション

ARP を使用すると、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内での IP 通信が可能になります。

悪意のあるユーザは、サブネットに接続されているシステムの ARP キャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイヤ 2 ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。この状況は、ARP は、ARP 要求を受信していないホストからの Gratuitous 応答も許可するため発生します。攻撃が開始されると、攻撃を受けたデバイスからのトラフィックはすべて、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されます。

ホスト A、B、および C は、インターフェイス A、B、および C 上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。それぞれの IP アドレスと MAC アドレスはカッコ内に表示されています。たとえば、ホスト A は IP アドレス IA と MAC アドレス MA を使用します。ホスト A が IP レイヤにあるホスト B と通信する必要がある場合、ホスト A は IP アドレス IB と関連付けられている MAC アドレスに ARP 要求をブロードキャストします。ホスト B は ARP 応答を使用して応答します。スイッチとホスト A は、ホスト B の MAC と IP を使用して、それぞれの ARP キャッシュを更新します。

ホスト C は、IP アドレスが IA（または IB）で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛てのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。このため、ホスト C はそのトラフィックを代行受信できます。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。これが、従来の中間者攻撃です。

ARP インスペクションプロパティ

ARP インスペクションのプロパティを設定するには、次の手順を実行します。

ステップ 1 [Security] > [ARP Inspection] > [Properties] の順にクリックします。

次のフィールドに入力します。

- [ARP Inspection Status]：ARP インスペクションを有効にする場合に選択します。
- [ARP Packet Validation]：検証チェックを有効にする場合に選択します。
- [Log Buffer Interval]：次のいずれかのオプションを選択します。
  - [Retry Frequency]：ドロップされたパケットに関する SYSLOG メッセージの送信を有効にします。入力した頻度でメッセージが送信されます。
  - [Never]：ドロップされたパケットに関する SYSLOG メッセージが無効になります。

ステップ 2 [Apply] をクリックします。設定が定義され、実行コンフィギュレーション ファイルが更新されます。

ARP インスペクション インターフェイス設定

信頼されていないポート/LAG からのパケットは ARP アクセスルールテーブルに対してチェックされ、さらに DHCP スヌーピングが有効になっていれば DHCP スヌーピング バインディング データベースに対してチェックされます（DHCP スヌーピング バインディング データベース （257 ページ）を参照）。

デフォルトでは、ポートや LAG は、ARP インスペクションで信頼されていません。

ポートや LAG の ARP 信頼ステータスを変更するには、次の手順を実行します。

ステップ 1 [Security] > [ARP Inspection] > [Interface Settings] をクリックします。

ポートと LAG およびそれぞれの ARP 信頼/非信頼ステータスが表示されます。

ステップ 2 あるポート/LAG を「信頼できる」または「信頼できない」に設定するには、そのポート/LAG を選択して [Edit] をクリックします。

ステップ 3 [Trusted] または [Untrusted] を選択し、[Apply] をクリックして、実行コンフィギュレーション ファイルに設定を保存します。

ARPアクセスコントロール

ARP インスペクション テーブルにエントリを追加するには、次の手順を実行します。

ステップ 1 [Security] > [ARP Inspection] > [ARP Access Control] の順にクリックします。

ステップ 2 エントリを追加するには、[Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [ARP Access Control Name]：ユーザーが作成した名前を入力します。
- [IP Address]：パケットの IP アドレス。
- [MAC Address]：パケットの MAC アドレス。

ステップ 4 [Apply] をクリックします。設定が定義され、実行コンフィギュレーション ファイルが更新されます。

ARPアクセスコントロールルール

作成済みの ARP アクセス コントロール グループにルールを追加するには、次の手順を実行します。

ステップ 1 [Security] > [ARP Inspection] > [ARP Access Control Rules] の順にクリックします。

ARP アクセス コントロール ルール テーブルに、現在定義されているアクセスルールが表示されます。

特定のグループを選択するには、[Filter] を選択し、コントロール名を選択して [Go] をクリックします。

ステップ 2 グループに追加のルールを追加するには、[Add] をクリックします。

ステップ 3 [ARP Access Control Name] を選択し、次のフィールドに入力します。

- [IP Address]：パケットの IP アドレス。
- [MAC Address]：パケットの MAC アドレス。

ステップ 4 [Apply] をクリックします。設定が定義され、実行コンフィギュレーション ファイルが更新されます。

ARP インスペクション VLAN 設定

VLAN 上の ARP インスペクションを有効にして、アクセス コントロール グループを VLAN と関連付けるには、次の手順を実行します。

ステップ 1 [Security] > [ARP Inspection] > [VLAN Settings] の順にクリックします。

ステップ 2 VLAN 上の ARP インスペクションを有効にするには、[Available VLANs] リストから [Enabled VLANs] リストに VLAN を移動します。

ステップ 3 ARP アクセス コントロール グループと VLAN を関連付けるには、[Add] をクリックします。VLAN 番号を選択し、定義済みの [ARP Access Control Name] を選択します。

ステップ 4 [Apply] をクリックします。設定が定義され、実行コンフィギュレーション ファイルが更新されます。

IPv6 ファースト ホップ セキュリティ

IPv6 ファースト ホップ セキュリティ（FHS）は、IPv6 が有効なネットワークでのセキュアなリンク操作を実現するために設計された機能のスイートです。これは、ネイバー探索プロトコルと DHCPv6 メッセージに基づいています。

この機能では、レイヤ 2 スイッチが各種の規則に従って、ネイバー探索プロトコル メッセージ、DHCPv6 メッセージ、およびユーザー データ メッセージをフィルタリングします。

IPv6 ファースト ホップ セキュリティのコンポーネント

IPv6 ファースト ホップ セキュリティには、次の機能があります。

- IPv6 ファースト ホップ セキュリティの共通機能
- RA ガード
- ND インスペクション
- ネイバー バインド整合性
- DHCPv6 ガード
- IPv6 ソース ガード

これらのコンポーネントは、VLAN で有効または無効にできます。機能ごとに、vlan_default と port_default という 2 つの空の事前定義済みポリシーが存在します。最初のポリシーは、ユーザ定義ポリシーに接続されていない各 VLAN に接続され、2 番目のポリシーは、ユーザ定義ポリシーに接続されていない各インターフェイスと VLAN に接続されます。

FHS の設定

[FHS Settings] ページを使用して、指定した VLAN グループで FHS 共通機能を有効にし、ドロップされたパケットのロギング用のグローバル設定値を設定します。必要に応じて、ポリシーを追加できます。また、パケットドロップロギングもシステム定義のデフォルトポリシーに追加できます。

IPv6 ファースト ホップ セキュリティの共通パラメータを設定するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [FHS Settings] をクリックします。

現在定義されているポリシーが表示されます。ポリシーごとに、それがデフォルトポリシーなのか、ユーザー定義のポリシーなのかを示す [Policy Type] が表示されます。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

- FHS VLAN リスト（FHS VLAN List）：IPv6 ファースト ホップ セキュリティを有効にする 1 つまたは複数の VLAN を入力します。
- パケット ドロップ ロギング（Packet Drop Logging）：選択すると、パケットがファーストホップ セキュリティ ポリシーによってドロップされたときにSYSLOGが作成されます。これは、ポリシーが定義されていない場合のグローバル デフォルト値です。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 4 必要な場合は、[Add] をクリックして FHS ポリシーを作成します。

次のフィールドに入力します。

- ポリシー名（Policy Name）：ユーザ定義のポリシー名を入力します。
- パケット ドロップ ロギング（Packet Drop Logging）：選択すると、パケットがこのポリシー内のファーストホップ セキュリティ ポリシーの結果としてドロップされたときに SYSLOG が作成されます。
  - 継承（Inherited）：VLAN またはグローバル設定の値を使用します。
  - 有効化（Enable）：ファーストホップ セキュリティの結果としてパケットがドロップされたときに SYSLOG が作成されます。
  - [Disable]：ファースト ホップ セキュリティによってパケットがドロップされてもSYSLOGは作成されません。

ステップ 5 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 6 このポリシーをインターフェイスに接続するには：

- [Attach Policy to VLAN]：クリックすると「ポリシー適用(VLAN) （374 ページ）」ページにジャンプし、このポリシーを VLAN にアタッチできます。
- [Attach Policy to Interface]：クリックすると「ポリシー適用(ポート) （374 ページ）」ページにジャンプし、このポリシーをポートにアタッチできます。

RAガード設定

[RA Guard Settings] ページを使用して、指定した VLAN グループで RA ガード機能を有効にし、この機能のグローバル設定値を設定します。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト RA ガード ポリシーを設定できます。

RA ガードを設定するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [RA Guard Settings] をクリックします。

現在定義されているポリシーが表示されます。ポリシーごとに、それがデフォルトポリシーなのか、ユーザー定義のポリシーなのかを示す [Policy Type] が表示されます。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

- RA ガード VLAN リスト（RA Guard VLAN List）：RA ガードを有効にする 1 つまたは複数の VLAN を入力します。

次に説明する他の設定フィールドに入力します。

ステップ 3 ポリシーを追加するには、[Add] をクリックし、次のフィールドに入力します。

- ポリシー名（Policy Name）：ユーザ定義のポリシー名を入力します。
- デバイス ロール（Device Role）：RA ガードの対象ポートに接続されているデバイスのロールを指定するために、次のオプションのいずれかが表示されます。
  - 継承（Inherited）：デバイス ロールは、VLAN またはシステム デフォルト（クライアント）から継承されます。
  - [Host]：デバイスロールはホストです。
  - ルータ（Router）：デバイス ロールはルータです。
- 管理設定フラグ（Managed Configuration Flag）：このフィールドには、IPv6 RA ガード ポリシー内でのアドバタイズされた管理アドレス設定フラグの検証を指定します。
  - 継承（Inherited）：機能は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - 検証なし（No Verification）：アドバタイズされた管理アドレス設定フラグの検証を無効にします。
  - オン（On）：アドバタイズされた管理アドレス設定フラグの検証を有効にします。
  - オフ（Off）：フラグの値は 0 である必要があります。
- その他の設定フラグ（Other Configuration Flag）：このフィールドには、IPv6 RA ガード ポリシー内でのアドバタイズされたその他の設定フラグの検証を指定します。
  - 継承（Inherited）：機能は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - 検証なし（No Verification）：アドバタイズされたその他の設定フラグの検証を無効にします。
  - オン（On）：アドバタイズされたその他の設定フラグの検証を有効にします。
  - オフ（Off）：フラグの値は 0 である必要があります。
- RA アドレス リスト（RA Address List）：フィルタ処理するアドレスのリストを指定します。
  - 継承（Inherited）：値は、VLAN またはシステムのデフォルト（検証なし）から継承されます。
  - [No Verification]：アドバタイズされたアドレスは検証されません。
  - [Match List]：照合される IPv6 アドレスリスト。

- RA プレフィックス リスト（RA Prefix List）：フィルタ処理するアドレスのリストを指定します。
  - 継承（Inherited）：値は、VLAN またはシステムのデフォルト（検証なし）から継承されます。
  - [No Verification]：アドバタイズされたプレフィックスは検証されません。
  - [Match List]：照合されるプレフィックスリスト。
- [Minimal Hop Limit]：RA ガードポリシーが、受信したパケットの最小ホップ限度をチェックするかどうかを示します。
  - 継承（Inherited）：機能は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - リミットなし（No Limit）：ホップ カウント制限の下限値の検証を無効にします。
  - ユーザ定義（User Defined）：ホップカウント制限がこの値以上であることを確認します。
- [Maximal Hop Limit]：RA ガードポリシーが、受信したパケットの最大ホップ限度をチェックするかどうかを示します。
  - 継承（Inherited）：機能は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - リミットなし（No Limit）：ホップカウント制限の上限値の検証を無効にします。
  - ユーザ定義（User Defined）：ホップカウント制限がこの値以下であることを確認します。高位境界の値は、低位境界の値以上でなければなりません。
- [Minimal Router Preference]：このフィールドは、RA ガードポリシーで、RA メッセージ内のアドバタイズされたデフォルト ルータ プリファレンスの最小値を検証するかどうかを示します。
  - 継承（Inherited）：機能は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - 検証なし（No Verification）：アドバタイズされたデフォルト ルータ プリファレンスの下限値の検証を無効にします。
  - 低（Low）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最小値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
  - 中（Medium）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最小値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
  - 高（High）：許容されるアドバタイズされたデフォルトルータ プリファレンスの最小値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
- [Maximal Router Preference]：このフィールドは、RA ガードポリシーで、RA メッセージ内のアドバタイズされたデフォルト ルータ プリファレンスの最大値を検証するかどうかを示します。
  - 継承（Inherited）：機能は、VLAN またはシステムのデフォルト（クライアント）から継承されます。

- 検証なし（No Verification）：アドバタイズされたデフォルト ルータ プリファレンスの上限値の検証を無効にします。
- 低（Low）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最大値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
- 中（Medium）：許容されるアドバタイズされたデフォルト ルータ プリファレンスの最大値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。
- 高（High）：許容されるアドバタイズされたデフォルトルータプリファレンスの最大値を指定します。次の値が許容されます：low、medium、および high（RFC4191 を参照）。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 5 システム定義のデフォルト ポリシーまたは既存のユーザ定義ポリシーを設定するには、ポリシーテーブルでポリシーを選択し、[Edit] をクリックします。

ステップ 6 このポリシーをインターフェイスに接続するには：

- [Attach Policy to VLAN]：クリックすると「ポリシー適用(VLAN)（374 ページ）」ページにジャンプし、このポリシーを VLAN にアタッチできます。
- [Attach Policy to Interface]：クリックすると「ポリシー適用(ポート)（374 ページ）」ページにジャンプし、このポリシーをポートにアタッチできます。

DHCPv6ガード設定

[DHCPv6 Guard Settings] ページを使用して、指定した VLAN グループで DHCPv6 ガード機能を有効にし、この機能のグローバル設定値を設定します。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト DHCPv6 ガード ポリシーを設定できます。

DHCPv6 ガードを設定するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [DHCPv6 Guard Settings] をクリックします。

現在定義されているポリシーが表示されます。ポリシーごとに、それがデフォルトポリシーなのか、ユーザー定義のポリシーなのかを示す [Policy Type] が表示されます。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

- [DHCPv6 Guard VLAN List]：DHCPv6 ガードが有効になっている VLAN を 1 つ以上入力します。
- [Device Role]：デバイスロールを表示します。[追加] ページの定義を参照してください。
- [Minimal Preference]：このフィールドは、受信したパケットのアドバタイズされた最小プリファレンス値を、DHCPv6 ガードポリシーでチェックするかどうかを示します。
  - 検証なし（No Verification）：受信したパケットのアドバタイズされた最小設定値の検証を無効にします。

- ユーザ定義（User Defined）：アドバタイズされた設定値がこの値以上であることを確認します。この値は最大設定値未満である必要があります。

- [Maximal Preference]：このフィールドは、受信したパケットのアドバタイズされた最大プリファレンス値を、DHCPv6 ガードポリシーでチェックするかどうかを示します。この値は最小設定値より大きくなければなりません。
  - 検証なし（No Verification）：ホップ カウント制限の下限の検証を無効にします。
  - ユーザ定義（User Defined）：アドバタイズされた設定値がこの値以下であることを確認します。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

既存のポリシーが表示されます。[Policy Type] フィールド以外のフィールドが下に表示されます。これは、ポリシーがユーザ定義とデフォルトのどちらかを示します。

ステップ 4 必要に応じて、[Add] をクリックして DHCPv6 ポリシーを作成します。

ステップ 5 次のフィールドに入力します。

- ポリシー名（Policy Name）：ユーザ定義のポリシー名を入力します。
- デバイス ロール（Device Role）：DHCPv6 ガードの対象ポートに接続されているデバイスのロールを指定するには、[Server] または [Client] のいずれかを選択します。
  - 継承（Inherited）：デバイスの権限は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - クライアント（Client）：デバイスのロールはクライアントです。
  - サーバ（Server）：デバイスのロールはサーバです。
- 応答プレフィックスを一致（Match Reply Prefixes）：選択すると、DHCPv6 ガード ポリシー内での受信した DHCP 応答メッセージ内のアドバタイズされたプレフィックスの検証が有効になります。
  - 継承（Inherited）：値は、VLAN またはシステムのデフォルト（検証なし）から継承されます。
  - [No Verification]：アドバタイズされたプレフィックスは検証されません。
  - [Match List]：照合される IPv6 プレフィックスリスト。
- サーバ アドレスを一致（Match Server Address）：選択すると、DHCPv6 ガード ポリシー内での受信した DHCP 応答メッセージ内の DHCP サーバおよびリレーの IPv6 アドレスの検証が有効になります。
  - 継承（Inherited）：値は、VLAN またはシステムのデフォルト（検証なし）から継承されます。
  - 検証なし（No Verification）：DHCP サーバおよびリレーの IPv6 アドレスの検証を無効にします。
  - 一致リスト（Match List）：一致させる IPv6 プレフィックスのリスト。
- [Minimal Preference]：このフィールドは、受信したパケットのアドバタイズされた最小プリファレンス値を、DHCPv6 ガードポリシーでチェックするかどうかを示します。

- 継承（Inherited）：最小設定は、VLANまたはシステムのデフォルト（クライアント）から継承されます。
- 検証なし（No Verification）：受信したパケットのアドバタイズされた最小設定値の検証を無効にします。
- ユーザ定義（User Defined）：アドバタイズされた設定値がこの値以上であることを確認します。この値は最大設定値未満である必要があります。

- [Maximal Preference]：このフィールドは、受信したパケットのアドバタイズされた最大プリファレンス値を、DHCPv6 ガードポリシーでチェックするかどうかを示します。この値は最小設定値より大きくなければなりません。
  - 継承（Inherited）：最小設定は、VLANまたはシステムのデフォルト（クライアント）から継承されます。
  - 検証なし（No Verification）：ホップ カウント制限の下限の検証を無効にします。
  - ユーザ定義（User Defined）：アドバタイズされた設定値がこの値以下であることを確認します。

ステップ 6 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 7 このポリシーをインターフェイスに接続するには：

- [Attach Policy to VLAN]：クリックすると「ポリシー適用(VLAN)（374 ページ）」ページにジャンプし、このポリシーを VLAN にアタッチできます。
- [Attach Policy to Interface]：クリックすると「ポリシー適用(ポート)（374 ページ）」ページにジャンプし、このポリシーをポートにアタッチできます。

NDインスペクション設定

[Neighbor Discovery (ND) Inspection Settings] ページを使用して、指定した VLAN グループで ND インスペクション機能を有効にし、この機能のグローバル設定値を設定します。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト ND インスペクション ポリシーを設定できます。

ND インスペクションを設定するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [ND Inspection Settings] をクリックします。

既存のポリシーが表示されます。[Policy Type] フィールド以外のフィールドが下に表示されます。これは、ポリシーがユーザ定義とデフォルトのどちらかを示します。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

- ND インスペクション VLAN リスト（ND Inspection VLAN List）：ND インスペクションを有効にする 1 つまたは複数の VLAN を入力します。
- デバイス ロール（Device Role）：次に説明するデバイス ロールが表示されます。
- 安全でないメッセージをドロップ（Drop Unsecure）：選択すると、IPv6 ND インスペクション ポリシー内で CGA または RSA 署名オプションのないメッセージのドロップが有効になります。
- [Minimal Security Level]：非セキュアなメッセージがドロップされない場合、メッセージが転送されるための最低限のセキュリティレベルを選択します。
  - 検証なし（No Verification）：セキュリティ レベルの検証を無効にします。
  - ユーザ定義（User Defined）：転送するメッセージのセキュリティ レベルを指定します。
- 送信元 MAC を検証（Validate Source MAC）：選択すると、リンク層アドレスと照らし合わせた送信元 MAC アドレスのチェックがグローバルに有効になります。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 4 必要に応じて、[Add] をクリックして ND インスペクション ポリシーを作成します。

ステップ 5 次のフィールドに入力します。

- ポリシー名（Policy Name）：ユーザ定義のポリシー名を入力します。
- デバイス ロール（Device Role）：ND インスペクションの対象ポートに接続されているデバイスのロールを指定するには、次のオプションのいずれかを選択します。
  - 継承（Inherited）：デバイスの権限は、VLAN またはシステムのデフォルト（クライアント）から継承されます。
  - ホスト（Host）：デバイスのロールはホストです。
  - ルータ（Router）：デバイスのロールはルータです。
- 安全でないメッセージをドロップ（Drop Unsecure）：次のいずれかのオプションを選択します。
  - 継承（Inherited）：VLAN またはシステムのデフォルト（無効）の値を継承します。
  - 有効化（Enable）：選択すると、IPv6 ND インスペクション ポリシー内で CGA または RSA 署名オプションのないメッセージのドロップが有効になります。
  - 無効化（Disable）：IPv6 ND インスペクション ポリシー内で CGA または RSA 署名オプションのないメッセージのドロップが無効になります。
- [Minimal Security Level]：非セキュアなメッセージがドロップされない場合、メッセージが転送されるための最低限のセキュリティレベルを選択します。
  - 継承（Inherited）：VLAN またはシステムのデフォルト（無効）の値を継承します。
  - 検証なし（No Verification）：セキュリティ レベルの検証を無効にします。
  - ユーザ定義（User Defined）：転送するメッセージのセキュリティ レベルを指定します。

- 送信元 MAC を検証（Validate Source MAC）：リンク層アドレスと照らし合わせた送信元 MAC アドレスのチェックをグローバルに有効にするかどうかを指定します。
  - 継承（Inherited）：VLAN またはシステムのデフォルト（無効）の値を継承します。
  - 有効化（Enable）：リンク層アドレスと照らし合わせた送信元MACアドレスのチェックが有効になります。
  - 無効化（Disable）：リンク層アドレスと照らし合わせた送信元 MAC アドレスのチェックが無効になります。

ステップ 6 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 7 このポリシーをインターフェイスに接続するには：

- [Attach Policy to VLAN]：このポリシーを VLAN にアタッチする手順については、ポリシー適用(VLAN)（374 ページ）を参照してください。
- [Attach Policy to Interface]：このポリシーをインターフェイスにアタッチする手順については、ポリシー適用(ポート)（374 ページ）を参照してください。

ネイバーバインディング設定

ネイバー バインド テーブルは、デバイスに接続されている IPv6 ネイバーのデータベース テーブルであり、ネイバー探索プロトコル（NDP）スヌーピングなどの情報ソースから作成されます。このデータベース（またはバインド）テーブルは、スヌーピングを防止し、攻撃をリダイレクトするためにさまざまな IPv6 ガード機能で使用されます。

[Neighbor Binding Settings] ページを使用して、指定した VLAN グループでネイバー バインド機能を有効にし、この機能のグローバル設定値を設定します。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト ネイバー バインド ポリシーを設定できます。

ネイバー バインドを設定するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [Neighbor Binding Settings] をクリックします。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

ネイバーバインディング VLANリスト	ネイバーバインディングが有効になっている VLAN を 1 つまたは複数入力します。
Device Role	デバイスのグローバルなデフォルトロール（境界）を表示します。
ネイバーバインディング ライフタイム	アドレスがネイバー バインディング テーブルに留まる時間の長さを入力します。

ネイバーバインディングロギング	選択すると、ネイバー バインディング テーブルのメインイベントのロギングが有効になります。
アドレスプレフィックス検証	選択すると、アドレスの IPv6 ソースガード検証が有効になります。

グローバルアドレスバインディングコンフィギュレーション

NDPメッセージからのバインディング	許可されるグローバル IPv6 アドレスの設定方法のグローバル設定を IPv6 ネイバー バインディング ポリシー内で変更するには、次のオプションのいずれかを選択します。 • [Any]：NDP メッセージからバインドされたグローバル IPv6 に対して、任意の設定方法（ステートレスおよび手動）を許可します。 • ステートレス（Stateless）：NDP メッセージからバインドされるグローバル IPv6 に対して、ステートレス自動設定のみが許可されます。 • 無効化（Disable）：NDP メッセージからのバインディングが無効になります。
DHCPv6メッセージからのバインディング	DHCPv6 からのバインドが許可されます。

ネイバーバインディングエントリ限度

VLAN毎のエントリ数	グローバル値を使用する場合は [Inherited]、エントリ数の限度を設定しない場合は [No Limit]、このポリシーに特別な値を設定する場合は [User Defined] を選択します。
インターフェイス毎のエントリ数	グローバル値を使用する場合は [Inherited]、エントリ数の限度を設定しない場合は [No Limit]、このポリシーに特別な値を設定する場合は [User Defined] を選択します。
MACアドレス毎のエントリ数	グローバル値を使用する場合は [Inherited]、エントリ数の限度を設定しない場合は [No Limit]、このポリシーに特別な値を設定する場合は [User Defined] を選択します。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 4 必要に応じて、[Add] をクリックしてネイバー バインド ポリシーを作成します。

ステップ 5 次のフィールドに入力します。

[Policy Name]	ユーザー定義のポリシー名を入力します。

Device Role	次のオプションの**いずれか**を選択して、ネイバー バインディング ポリシーのポートにアタッチされているデバイスのロールを指定します。 • 継承（Inherited）：デバイスの権限は、VLAN またはシステムのデフォルト（クライアント）から継承されます。 • 境界（Perimeter）：ポートは、IPv6 ファースト ホップ セキュリティをサポートしていないデバイスに接続されています。 • 内部（Internal）：ポートは、IPv6 ファーストホップセキュリティをサポートしているデバイスに接続されています。
ネイバーバインディング ロギング	次のオプションのいずれかを選択して、ロギングを指定します。 • 継承（Inherited）：ロギング オプションは、グローバル値と同じです。 • 有効化（Enable）：バインディング テーブル メイン イベントのロギングを有効にします。 • 無効化（Disable）：バインディング テーブル メイン イベントのロギングを無効にします。
アドレスプレフィックス検証	次のオプションのいずれかを選択して、アドレスの検証を指定します。 • 継承（Inherited）：検証オプションは、グローバル値と同じです。 • [Enable]：アドレスの検証を有効にします。 • [Disable]：アドレスの検証を無効にします。

グローバルアドレスバインディングコンフィギュレーション

アドレスバインディング設定の継承	グローバル アドレス バインディング設定の使用を有効にします。
NDPメッセージからのバインディング	許可されるグローバル IPv6 アドレスの設定方法のグローバル設定を IPv6 ネイバー バインディング ポリシー内で変更するには、次のオプションのいずれかを選択します。 • [Any]：NDP メッセージからバインドされたグローバル IPv6 に対して、任意の設定方法（ステートレスおよび手動）を許可します。 • ステートレス（Stateless）：NDP メッセージからバインドされるグローバル IPv6 に対して、ステートレス自動設定のみが許可されます。 • 無効化（Disable）：NDP メッセージからのバインディングが無効になります。
DHCPv6メッセージからのバインディング	DHCPv6 からのバインドを有効にする場合に選択します。

ネイバーバインディングエントリ限度

VLAN毎のエントリ数	グローバル値を使用する場合は [Inherited]、エントリ数の限度を設定しない場合は [No Limit]、このポリシーに特別な値を設定する場合は [User Defined] を選択します。
インターフェイス毎のエントリ数	グローバル値を使用する場合は [Inherited]、エントリ数の限度を設定しない場合は [No Limit]、このポリシーに特別な値を設定する場合は [User Defined] を選択します。
MACアドレス毎のエントリ数	グローバル値を使用する場合は [Inherited]、エントリ数の限度を設定しない場合は [No Limit]、このポリシーに特別な値を設定する場合は [User Defined] を選択します。

ステップ 6 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ステップ 7 このポリシーをインターフェイスに接続するには：

ポリシーをVLANにアタッチ	クリックするとポリシー適用(VLAN)（374ページ）ページにジャンプし、このポリシーを VLAN にアタッチできます。
ポリシーをインターフェイスにアタッチ	クリックするとポリシー適用(ポート)（374 ページ）ページにジャンプし、このポリシーをポートにアタッチできます。

IPv6ソースガード設定

[IPv6 Source Guard Settings] ページを使用して、指定した VLAN グループで IPv6 ソース ガード機能を有効にします。必要な場合は、このページでポリシーを追加するか、またはシステム定義のデフォルト IPv6 ソース ガード ポリシーを設定できます。

IPv6 ソース ガードを設定するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [IPv6 Source Guard Settings] をクリックします。

既存のポリシーが表示されます。[Policy Type] フィールド以外のフィールドが下に表示されます。これは、ポリシーがユーザ定義とデフォルトのどちらかを示します。

ステップ 2 次のグローバル コンフィギュレーション フィールドに入力します。

- IPv6 ソース ガード VLAN リスト（IPv6 Source Guard VLAN List）：IPv6 ソース ガードを有効にする 1 つまたは複数の VLAN を入力します。
- ポートの信頼（Port Trust）：デフォルトでポリシーが信頼できないポートを対象とすることが表示されます。これはポリシーごとに変更できます。

ステップ 3 必要に応じて、[Add] をクリックしてファースト ホップ セキュリティ ポリシーを作成します。

ステップ 4 次のフィールドに入力します。

- ポリシー名（Policy Name）：ユーザ定義のポリシー名を入力します。
- ポートの信頼（Port Trust）：ポリシーのポート信頼状態を選択します。
  - [Inherited]：ポリシーをポートにアタッチした時点では、信頼されていません。
  - [Trusted]：ポリシーをポートにアタッチした時点で、信頼済みです。

ステップ 5 [Apply] をクリックしてポリシーを接続します。

ステップ 6 このポリシーをインターフェイスにアタッチするには、[Attach Policy to Interface] をクリックします。

ポリシー適用(VLAN)

1 つまたは複数の VLAN にポリシーを接続するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [Policy Attachment (VLAN)] をクリックします。

すでに接続されているポリシーのリストが、そのポリシータイプ、ポリシー名、およびVLANリストとともに表示されます。

ステップ 2 VLAN にポリシーを接続するには、[Add] をクリックして次のフィールドに入力します。

- ポリシー タイプ（Policy Type）：インターフェイスに接続するポリシー タイプを選択します。
- [Policy Name]：インターフェイスにアタッチするポリシーの名前を選択します。
- [VLAN List]：ポリシーがアタッチされる VLAN を選択します。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ポリシー適用(ポート)

1 つまたは複数のポートまたは LAG にポリシーを接続するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [Policy Attachment (Port)] をクリックします。

すでに接続されているポリシーのリストが、そのインターフェイス、ポリシータイプ、ポリシー名、および VLAN リストとともに表示されます。

ステップ 2 ポートまたは LAG にポリシーを接続するには、[Add] をクリックして次のフィールドに入力します。

- [Interface]：ポリシーをアタッチするインターフェイスを選択します。
- ポリシー タイプ（Policy Type）：インターフェイスに接続するポリシー タイプを選択します。

- [Policy Name]：インターフェイスにアタッチするポリシーの名前を選択します。
- [VLAN List]：ポリシーがアタッチされる VLAN を選択します。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ネイバーバインディングテーブル

ネイバー バインド テーブルのエントリを表示するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [Neighbor Binding Table] をクリックします。

ステップ 2 次のテーブル クリア オプションのいずれかを選択します。

- スタティックのみ（Static Only）：テーブル内のすべてのスタティック エントリをクリアします。
- ダイナミックのみ（Dynamic Only）：テーブル内のすべてのダイナミック エントリをクリアします。
- [All Dynamic & Static]：テーブルに含まれるダイナミックなエントリとスタティックなエントリすべてをクリアします。

  ポリシーごとに、次のフィールドが表示されます（[Add]ページに存在しないフィールドのみが表示されます）。

- 発生元（Origin）：IPv6 アドレスを追加したプロトコル（ダイナミック エントリにのみ使用可能）。
  - [Static]：手動で追加したもの。
  - [NDP]：ネイバー探索プロトコルメッセージから学習したもの。
  - [DHCP]：DHCPv6 プロトコルメッセージから学習したもの。
- [State]：エントリの状態。
  - [Tentative]：新しいホストの IPv6 アドレスを検証中。ライフタイムが 1 秒未満であるため、期限切れ時間は表示されません。
  - 有効（Valid）：ホストの IPv6 アドレスがバインドされました。
- [Expiry Time (Sec.)]：エントリが確認されない場合、削除されるまでの残り時間（秒単位）。
- [TCAM Overflow]：[No] とマークされたエントリでは TCAM オーバーフローは発生しません。

ステップ 3 ポリシーを追加するには、[Add] をクリックし、次のフィールドに入力します。

- VLAN ID：エントリの VLAN ID。
- [IPv6 Address]：エントリの送信元 IPv6 アドレス。
- [Interface]：パケットを受信するポート。

- [MAC Address]：パケットのネイバー MAC アドレス。

ステップ 4 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を追加します。

ネイバープレフィックステーブル

ネイバープレフィックス テーブルに、NDP メッセージからバインドされたグローバル IPv6 アドレスのスタティック プレフィックスを追加できます。ダイナミックエントリが学習されます。

ネイバー プレフィックス テーブルにエントリを追加するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [Neighbor Prefix Table] をクリックします。

ステップ 2 ネイバー プレフィックス テーブルをクリアするには、[Clear Table] フィールドで次のオプションのいずれかを選択します。

- スタティックのみ（Static Only）：スタティック エントリのみをクリアします。
- ダイナミックのみ（Dynamic Only）：ダイナミック エントリのみをクリアします。
- すべてのダイナミック & スタティック（All Dynamic & Static）：スタティック エントリとダイナミック エントリをクリアします。

ステップ 3 既存のエントリについて、次のフィールドが表示されます。

- VLAN ID：プレフィックスが関連付けられる VLAN。
- [IPv6 Prefix]：IPv6 プレフィックス。
- [Prefix Length]：IPv6 プレフィックス長。
- 発生元（Origin）：エントリはダイナミック（学習されたもの）またはスタティック（手動で設定されたもの）です。
- 自動設定（Autoconfig）：プレフィックスはステートレス設定で使用できます。
- [Expiry Time]（秒）：エントリが削除されるまでの残り時間の長さ。

ステップ 4 [Add]をクリックしてテーブルに新しいエントリを追加し、新しいエントリについて上記のフィールドに入力します。

FHS の状態

FHS 機能のグローバル設定を表示するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [FHS Status] をクリックします。

ステップ 2 FHS の状態を報告するポート、LAG、または VLAN を選択します。

ステップ 3 次のフィールドが選択したインターフェイスに表示されます。

FHS の状態

現在のVLAN上のFHS状態	現在の VLAN で FHS が有効になっているかどうか。
パケットドロップロギング	現在のインターフェイスに対して（グローバル設定のレベルか、そのインターフェイスにアタッチされているポリシー内で）この機能が有効になっているかどうか。

RA ガードの状態

現在のVLAN上のRAガード状態	現在の VLAN で RA ガードが有効になっているかどうか。
Device Role	RA デバイスの役割。
マネージドコンフィギュレーションフラグ	マネージド設定フラグの検証が有効かどうか。
他のコンフィギュレーションフラグ	他の設定フラグの検証が有効かどうか。
RAアドレスリスト	照合される RA アドレスリスト。
RAプレフィックスリスト	照合される RA プレフィックスリスト。
最小ホップ限度	最小 RA ホップ限度の検証が有効かどうか。
最大ホップ限度	最大 RA ホップ限度の検証が有効かどうか。
最小ルータプリファレンス	最小ルータプリファレンスの検証が有効かどうか。
最大ルータプリファレンス	最大ルータプリファレンスの検証が有効かどうか。

DHCPv6 ガードの状態

現在VLAN上のDHCPv6ガード状態	現在の VLAN で DHCPv6 ガードが有効になっているかどうか。
Device Role	DHCP デバイスロール
一致リプレイプレフィックス	DHCP 応答プレフィックスの検証が有効かどうか。

一致サーバーアドレス	DHCP サーバーアドレスの検証が有効かどうか。
最小プリファレンス	最小プリファレンスの検証が有効かどうか。
最大プリファレンス	最大プリファレンスの検証が有効かどうか。

ND インスペクションの状態

現在のVLAN上のNDインスペクション状態	現在の VLAN で ND インスペクションが有効になっているかどうか。
Device Role	ND インスペクションのデバイスロール。
ドロップアンセキュア	非セキュアなメッセージをドロップするかどうか。
最低セキュリティレベル	非セキュアなメッセージがドロップされない場合、パケットが転送されるのに必要な最低セキュリティレベル。
ソースMACの検証	送信元 MAC アドレスの検証が有効かどうか。

ネイバー バインドの状態

現在のVLAN上のネイバーバインディング状態	現在の VLAN でネイバーバインディングが有効になっているかどうか。
Device Role	ネイバー バインディング デバイスのロール。
ロギングバインディング	ネイバー バインディング テーブルのイベントのロギングが有効かどうか。
アドレスプレフィックス検証	アドレスプレフィックスの検証が有効かどうか。
グローバルアドレスコンフィギュレーション	検証されるメッセージ。
VLAN毎の最大エントリ	VLAN ごとに許可されるダイナミック ネイバー バインディング テーブルの最大エントリ数。
インターフェイス毎の最大エントリ数	インターフェイスごとに許可されるネイバー バインディング テーブルの最大エントリ数。
MACアドレス毎の最大エントリ数	MAC アドレスごとに許可されるネイバー バインディング テーブルの最大エントリ数。

IPv6ソースガードステータス

現在のVLAN上のIPv6ソースガード状態	現在の VLAN で IPv6 ソースガードが有効になっているかどうか。

ポートの信頼性	ポートが信頼されているかどうか、およびその信頼状態の受信方法。

FHS統計情報

FHS 統計を表示するには：

ステップ 1 [Security] > [IPv6 First Hop Security] > [FHS Statistics] をクリックします。

ステップ 2 [Refresh Rate]（統計が更新されるまでの経過期間）を選択します。

ステップ 3 次のグローバル オーバーフロー カウンタが表示されます。

ネイバーバインディングテーブル	テーブルのサイズが最大値に達したためにテーブルに追加できなかったエントリ数。
ネイバープレフィックステーブル	テーブルのサイズが最大値に達したためにテーブルに追加できなかったエントリ数。
TCAM	TCAM オーバーフローが原因で追加できなかったエントリ数。

ステップ 4 インターフェイスを選択すると、次のフィールドが表示されます。

NDP（ネイバー探索プロトコルメッセージ）	次のタイプのメッセージについて、受信済みメッセージ数とドロップ済みメッセージ数が表示されます。 • RA：ルータ アドバタイズメント メッセージ • [REDIR]：リダイレクトメッセージ • NS：ネイバー要請メッセージ • NA：ネイバー アドバタイズメント メッセージ • RS：ルータ要請メッセージ

DHCPv6メッセージ	次のタイプのDHCPv6メッセージについて、受信済みメッセージ数とドロップ済みメッセージ数が表示されます。 • ADV：アドバタイズ メッセージ • [REP]：応答メッセージ • [REC]：再設定メッセージ • [REL-REP]：リレー応答メッセージ • LEAS-REP：リース クエリ応答メッセージ • [RLS]：リリース済みメッセージ • [DEC]：拒否済みメッセージ

次のフィールドがFHS ドロップ メッセージ テーブルに表示されます。

機能	ドロップされたメッセージのタイプ（DHCPv6 ガード、RA ガードなど）。
Count	ドロップされたメッセージの数。
理由	メッセージがドロップされた理由。

ステップ5 カウンタをクリアするには、[Clear Interface Counters]、[Clear All Interface Counters]、[Clear Global Counters] のいずれかをクリックします。

ステップ6 カウンタを更新するには、[Refresh] をクリックします。

証明書の設定

Cisco Business ダッシュボードプローブ（CBD）およびプラグアンドプレイ（PNP）機能では、CBD または PNP サーバーとの HTTPS 通信を確立するために CA 証明書が必要です。証明書設定機能により、これらのアプリケーションとデバイスマネージャは次のことを実行できます。

- 信頼された CA 証明書をインストールし、不要になった証明書を削除する
- デバイス設定ファイルに証明書を静的に追加する
- 信頼されていない証明書の失効リストを管理する

（注） 証明書の有効期限は、システムクロックが基準になります。デフォルトのシステムクロックを使用します。そうしなければ適切な検証は提供されません。そのため、最後のリブート以降にシステムクロックがアクティブに設定されていることを確認します（SNTP サービスの使用を推奨）。システムクロックが RTC に基づいておらず、また最後のリブート以降に設定されなかった場合、システムクロックが証明書の有効期間内であっても、証明書の検証は失敗します。

ダイナミック証明書

CBDおよびPNPアプリケーションは、動的に信頼された証明書をデバイスメモリにインストールできます。インストールされる証明書には次の属性が必要です。

- [Certificate name]：証明書を識別するために使用される文字列。
- [Owner]：証明書をインストールしたアプリケーション名（PNP、CBD など）。
- 証明書は PEM 形式です。

アプリケーションによってインストールされた特定のまたはすべてのダイナミック証明書を削除することもできます。

考慮事項

- 最大 512 のダイナミック証明書をデバイスにインストールできます。
- デバイスのリブート時にダイナミック証明書は削除されます。

スタティック証明書

リセットしても削除されない証明書をアプリケーションが追加する場合、またはスイッチのユーザーが証明書を追加する場合は、スタティック証明書を追加します。これらの証明書は、デバイス実行コンフィギュレーションに保存されるため、スタートアップ コンフィギュレーションにコピーできます。

スタティック証明書を追加するには、次の属性を指定する必要があります。

- [Certificate name]：証明書を識別するために使用される文字列です。
- [Owner]：証明書をインストールしたアプリケーション名（PNP、CBD など）。ユーザーが追加した場合は「static」になります。
- 証明書は PEM 形式です。

考慮事項

- 最大 256 のスタティック証明書をデバイスにインストールできます。
- 証明書の識別に使用する名前が異なっていれば、各アプリケーションまたは各ユーザーが追加する証明書は同じにできます。

CA 証明書設定

ユーザーは、インストールされているすべての証明書（動的および静的）に関する情報にアクセスできます。証明書ごとに次の情報が表示されます。

ステップ 1 [Security] > [Certificate Settings] > [CA Certificate Settings] の順にクリックします。

ステップ 2 新しい証明書をインポートするには、[Add] をクリックし、次の項目を入力します。

- [Certificate Name]：証明書の名前を入力します。
- [Certificate]：証明書を PEM 形式で貼り付けます（開始マーカー行と終了マーカー行を含みます）。

ステップ 3 新しい設定を適用するには、[Apply] をクリックします。

ステップ 4 既存の証明書の詳細を表示するには、リストから証明書を選択し、[Details] をクリックします。次のように表示されます。

オプション	説明
証明書名	証明書の名前または一意の識別子。
Type	これには、[signer]、[static]、または [dynamic] を選択できます。
Owner	これには、[signer]、[static]、[CBD]、または [PNP] を選択できます。
バージョン	証明書のバージョン。
Serial Number	証明書のシリアル番号。
Status	証明書のステータス。
Valid From	証明書の有効期限の開始日時。
Valid To	証明書の有効期限の終了日時。
発行元（Issuer）	証明書に署名したエンティティまたは CA。
Subject	証明書の識別名（DN）情報。
公開キータイプ	公開キーのタイプ。
公開キー長	公開キーの長さ（ビット単位）。
Signature Algorithm	CA が証明書に署名するために使用する暗号化アルゴリズム。
Certificate	PEM 形式の証明書の詳細。

ステップ 5 次のフィルタを使用して、特定の証明書を検索できます。

- [Type equals to]：このチェックボックスをオンにして、ドロップダウンリストから [Signer]、[Static]、または [Dynamic] を選択し、これらの証明書タイプでフィルタ処理します。

- [Owner equals to]：証明書を PEM 形式で貼り付けます（開始マーカー行と終了マーカー行を含みます）。

ステップ 6 1 つまたは複数の証明書を削除するには、証明書を選択して Delete を押します。スタティック証明書のみ削除できます。

CA 失効リスト

何らかの理由で証明書が信頼できなくなった場合は、ユーザーまたはいずれかのアプリケーションによって失効リストに追加されます。証明書が失効リストに含まれている場合は無効と見なされ、デバイスでは使用できなくなります。失効リストに証明書を追加しても、失効した証明書は証明書データベースから削除されません。証明書のステータスのみが、[Not Valid (Revoked)] に更新されます。証明書が失効リストから削除されると、その証明書のステータスは証明書データベースで自動的に更新されます。証明書を再インストールする必要はありません。

証明書を失効リストに追加または失効リストから削除するには、次の手順を実行します。

ステップ 1 [Security] > [Certificate Settings] > [CA Certificate Revocation List] の順にクリックします。

ステップ 2 [Add] をクリックして [Add Revoked Certificate] ダイアログボックスを開きます。

ステップ 3 次の詳細事項を入力します。

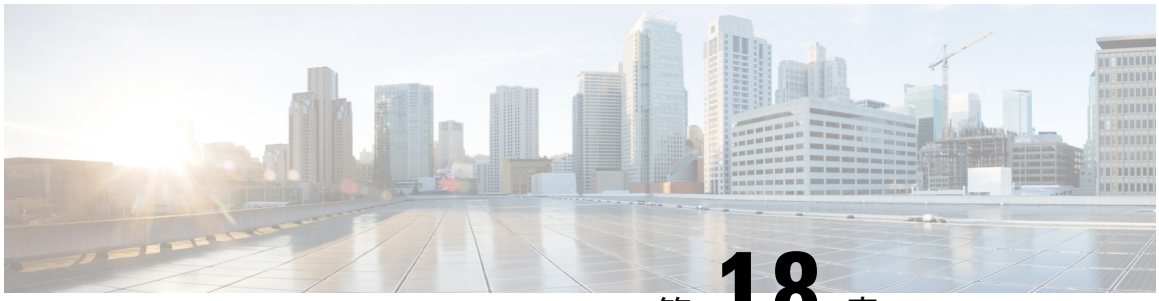
- [Issuer]：発行元を特定する文字列（「C=US、O=MyTrustOrg、CN=MyCommonName」など）（1 ～ 160 文字）。
- [Serial Number]：失効した証明書のシリアル番号。これは 16 進数のペアの文字列です（長さ 2 ～ 32）。

ステップ 4 [Apply] をクリックして証明書を追加します。

説明

- 最大 512 の証明書を失効リストに追加できます。
- 失効リストのエントリに一致するすべての証明書は無効と見なされます（証明書データベース内で異なる名前で特定された場合でも同様）。

ステップ 5 既存の証明書を削除するには、失効した CA 証明書テーブルから証明書を選択し、[Delete] をクリックします。



第 18 章

アクセス コントロール

アクセス コントロール リスト（ACL）機能は、セキュリティ メカニズムの一部です。ACL の定義は、特定のサービス品質（QoS）が与えられたトラフィック フローを定義するメカニズムの 1 つとして機能します。詳細については、「Quality of Service」を参照してください。ACL は、入力トラフィックのパターン（フィルタとアクション）を定義するネットワーク マネージャを有効にします。アクティブな ACL があるポートまたは LAG 上のデバイスに着信するパケットは、エントリが許可または拒否されます。この章は、次の項で構成されています。

MACベースACL

MAC ベースの ACL は、レイヤ 2 のフィールドに基づくトラフィックのフィルタリングに使用されます。MAC ベースの ACL は、一致するすべてのフレームをチェックします。MAC ベース ACL を定義するには、次の手順を実行します。

ステップ 1 [Access Control] > [MAC-Based ACL] をクリックします。

このページには、現在定義されているすべての MAC ベース ACL のリストが表示されます。

ステップ 2 [Add] をクリックします。

ステップ 3 [ACL名] フィールドに、新しい ACL の名前を入力します。ACL 名では大文字と小文字が区別されます。

ステップ 4 [Apply] をクリックします。MAC ベースの ACL は実行コンフィギュレーション ファイルに保存されます。

MAC ベースの ACE

（注） 各 MAC ベースのルールは、1 つの TCAM ルールを消費します。TCAM 割り当てはペアで実行されます。たとえば、最初の ACE には 2 つの TCAM ルールが割り当てられ、2 番目の TCAM ルールの方は次の ACE に割り当てられます。

ルール（ACE）を ACL に追加するには、次の手順を実行します。

ステップ 1 [Access Control] > [MAC-Based ACE] をクリックします。

ステップ 2 ACL を選択し、[Go] をクリックします。ACL における ACE の一覧が表示されます。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

- ACL 名（ACL Name）：ACE を追加する ACL の名前が表示されます。
- 優先順位（Priority）：ACE の優先順位を入力します。優先度の高い ACE は最初に処理されます。1 が最も高い優先順位です。
- [Action]：一致した場合に実行するアクションを選択します。次のオプションがあります。
  - [許可]：ACE 条件に一致するパケットを転送します。
  - 拒否（Deny）：ACE 条件に一致するパケットをドロップします。
  - [シャットダウン]：ACE 条件に一致するパケットをドロップし、パケットを受信したポートを無効にします。
- ロギング（Logging）：選択すると ACL ルールに一致する ACL フローのロギングが有効になります。
- 時間範囲（Time Range）：選択すると、特定の時間範囲への ACL の使用制限が有効になります。
- 時間範囲名（Time Range Name）：[Time Range] を選択した場合、使用する時間範囲を選択します。時間範囲を修正するには [Edit] をクリックします。
- [Destination MAC Address]：すべての宛先アドレスを受け入れる場合には [Any] を、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には [User defined] を、それぞれ選択します。
- 宛先 MAC アドレスの値（Destination MAC Address Value）：宛先 MAC アドレスを一致させる MAC アドレスとそのマスク（該当する場合）を入力します。
- [Destination MAC Wildcard Mask]：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、他の用途とは異なります。ここでビットを 1 と設定すると、その値を気にしないことを意味し、0 はその値を照合することを意味します。

（注） 0000 0000 0000 0000 0000 0000 1111 1111 というマスクを例に説明します。この場合、0 になっているビットは照合され、1 になっているビットは照合されません。2 進数値は 16 進数（16 進数 1 桁につき 4 ビット）に変換する必要があります。この例では、1111 1111 = FF であるので、マスクは 00:00:00:00:00:FF と記述されます。

- [Source MAC Address]：すべての送信元アドレスを許可する場合は [Any] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [User defined] を選択します。
- 送信元 MAC アドレスの値（Source MAC Address Value）：送信元 MAC アドレスを一致させる MAC アドレスとそのマスク（該当する場合）を入力します。
- [Source MAC Wildcard Mask]：MAC アドレスの範囲を定義するマスクを入力します。
- VLAN ID：一致する VLAN タグの VLAN ID セクションを入力します。
- [802.1p]：802.1p を使用する場合は [Include] を選択します。
- 802.1p の値（802.1p Value）：VPT タグに追加する 802.1p の値を入力します。
- 802.1p マスク（802.1p Mask）：VPT タグに適用するワイルドカード マスクを入力します。
- Ethertype：一致するフレーム Ethertype を入力します。

ステップ 5 [Apply] をクリックします。MAC ベースの ACE は実行コンフィギュレーション ファイルに保存されます。

IPv4 ベース ACL

ACL は、フローごとの QoS 処理のためのフロー定義の構成要素としても使用されます。IPv4 ベース ACL は、IPv4 パケットをチェックするために使用されます。IPv4 ベース ACL を定義するには、次の手順を実行します。

ステップ 1 [Access Control] > [IPv4-Based ACL] をクリックします。

このページには、現在定義されている IP v 4 ベースの ACL がすべて含まれています。

ステップ 2 [Add] をクリックします。

ステップ 3 [ACL名] フィールドに、新しい ACL の名前を入力します。名前は大文字と小文字が区別されます。

ステップ 4 [Apply] をクリックします。IPv4 ベースの ACL は実行コンフィギュレーション ファイルに保存されます。

IPv4ベースACE

（注） 各 IP v 4 ベースのルールは、1 つの TCAM ルールを消費します。TCAM の割り当ては、最初の ACE では一対で実行されます。2 つの TCAM ルールが割り当てられ、2 番目の TCAM ルールが次の ACE に割り当てられます。以降も同様です。

ルール（ACE）を IPv4 ベース ACL に追加するには、次の手順を実行します。

ステップ 1 [Access Control] > [IPv4-Based ACE] をクリックします。

ステップ 2 ACL を選択し、[Go] をクリックします。選択した ACL に現在定義されている IP ACE がすべて表示されます。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

ACL 名	ACE が追加されている ACL の名前が表示されます。
Priority	プライオリティを入力します。優先度の高い ACE は最初に処理されます。
Action	ACE に一致するパケットに割り当てられるアクションを、次のオプションから選択します。 • [許可]：ACE 条件に一致するパケットを転送します。 • 拒否（Deny）：ACE 条件に一致するパケットをドロップします。 • シャットダウン（Shutdown）：ACE 条件に一致するパケットをドロップし、パケットが向けられたポートを無効にします。ポートはエラー回復設定 （139 ページ）ページで再アクティブ化されます。
ログ	ACL ルールと一致する ACL フローのロギングを有効にする場合に選択します。
時間範囲	ACL の使用時間を指定した時間範囲に制限する場合に選択します。
時間範囲名	[Time Range] が選択されている場合は、[Edit] ボタンをクリックすると、時間範囲のページにリダイレクトされるので、使用する時間範囲名を選択します。システム時刻 （72 ページ）セクションでは、時間範囲について説明します。

プロトコル（Protocol）	特定のプロトコルまたはプロトコル ID に基づく ACE を作成する場合に選択します。[Any (IPv4)] を選択して、すべての IP プロトコルを受け入れます。それ以外の場合は、次のいずれかのプロトコルを選択します。 • [ICMP]：インターネット制御メッセージ プロトコル • [IGMP]：インターネット グループ管理プロトコル • [IP-in-IP]：IP-in-IP カプセル化 • [TCP]：トランスミッション コントロール プロトコル • [EGP]：外部ゲートウェイ プロトコル • [IGP]：内部ゲートウェイ プロトコル • [UDP]：ユーザ データグラム プロトコル • [HMP]：ホストマッピングプロトコル • [RDP]：信頼性の高いデータグラム プロトコル。 • [IDPR]：ドメイン間ポリシー ルーティング プロトコル • [IPV6]：IPv6 over IPv4 トンネリング • [IPV6:ROUT]：ゲートウェイ経由で IPv6 over IPv4 ルートに属するパケットを照合 • [IPV6:FRAG]：IPv6 over IPv4 フラグメント ヘッダーに属するパケットを照合 • [IDRP]：ドメイン間ルーティング プロトコル • [RSVP]：ReSerVation プロトコル • [AH]：認証ヘッダー • [IPV6:ICMP]：インターネット制御メッセージ プロトコル • [EIGRP]：Enhanced Interior Gateway Routing Protocol • [OSPF]：Open Shortest Path First • IPIP：IP in IP • [PIM]：Protocol Independent Multicast • [L2TP]：Layer 2 Tunneling Protocol • [ISIS]：IGP 固有のプロトコル • 一致させるプロトコル ID（Protocol ID to Match）：名前を選択せずにプロトコル ID を入力します。

送信元 IP アドレス	すべての送信元アドレスを許可する場合は [Any] を選択します。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 [User defined] を選択します。
送信元IPアドレス値	送信元 MAC アドレスが一致する IP アドレスとマスク（該当する場合）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ための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、他の用途とは異なります。ここでビットを 1 と設定すると、その値を気にしないことを意味し、0 はその値をマスクすることを意味します。 （注） 0000 0000 0000 0000 0000 0000 1111 1111 のマスクを指定する場合は、1 を 10 進数の整数に変換し、4 つのゼロごとに 0 を記述する必要があります。この例では 1111 1111 = 255 であるので、マスクは 0.0.0.255 と記述されます。
宛先IPアドレス	すべての宛先アドレスを許可する場合は [Any] を選択します。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 [User defined] を選択します。
宛先IPアドレス値	宛先 MAC アドレスが一致する IP アドレスとマスクを入力します（該当する場合）。
宛先IPワイルドカードマスク	宛先 IP ワイルドカードマスクを入力します。
Source Port	次のいずれかを選択します。 • [Any]：すべての送信元ポートに対して照合を実行します。 • リストから 1 つ（Single from list）：パケットを一致させる TCP/UDP 送信元ポートを 1 つ選択します。このフィールドは、800/6-TCP または 800/17-UDP が [IP Protocol] ドロップダウン メニューから選択されている場合にのみ有効です。 • 番号で 1 つ（Single by number）：パケットを一致させる TCP/UDP 送信元ポートを 1 つ入力します。このフィールドは、800/6-TCP または 800/17-UDP が [IP Protocol] ドロップダウン メニューから選択されている場合にのみ有効です。 • [Range]：0 ー 65535 の範囲を入力します。
Destination Port	使用可能ないずれかの値を選択します。これらは、前述の送信元ポート（Source Port）フィールドと同じです。 （注） 送信元または宛先ポートを入力する前に、ACL の IPv6 プロトコルを指定する必要があります。

TCP Flags	パケットのフィルタ処理に使用する TCP フラグを 1 つ以上選択します。フィルタリングされたパケットは転送またはドロップされます。TCP フラグによるパケットのフィルタリングはパケットの制御を増やし、ネットワーク セキュリティを向上させます。各フラグのタイプに対して、次のオプションのいずれかを選択します。 • 設定（Set）：フラグが SET の場合に一致します。 • [Unset]：フラグが Not SET の場合に照合します。 • 無視（Don't care）：TCP フラグを無視します。
Type of Service：タイプ オブ サービス	IP パケットのサービスタイプ。 • [任意]：任意のサービス タイプ。 • [DSCP to match]：照合する Differentiated Service Code Point（DSCP）。 • [照合する IP 優先度]：IP 優先度とは、適切な QoS を確実に提供するためにネットワークが使用する TOS（タイプ オブ サービス）のモデルです。このモデルでは、RFC 791 および RFC 1349 で説明されているように、IP ヘッダーのサービス タイプ バイトの 3 つの最上位ビットを使用します。
ICMP	ACL が ICMP に基づいている場合は、フィルタリングに使用する ICMP メッセージタイプを選択します。メッセージタイプの名前を選択するか、メッセージ タイプの番号を入力します。すべてのメッセージ タイプを受け入れる場合は、[Any] を選択します。 • 任意（Any）：すべてのメッセージ タイプは受け入れられます。 • リストから選択（Select from list）：ドロップダウン リストからメッセージ タイプを名前で選択します。 • [ICMP Type to Match]：フィルタリングに使用するメッセージタイプ番号。
ICMP Code	ICMP メッセージには、そのメッセージの処理方法を示すコードフィールドが設定されている場合があります。このコードでフィルタリングするかどうかを設定するには、次のオプションのいずれかを選択します。 • [Any]：すべてのコードを受け入れます。 • ユーザ定義（User Defined）：フィルタリング用に ICMP コードを入力します。

IGMP	ACL が IGMP に基づいている場合は、フィルタリングに使用する IGMP メッセージタイプを選択します。メッセージタイプの名前を選択するか、メッセージ タイプの番号を入力します。 • 任意（Any）：すべてのメッセージ タイプは受け入れられます。 • リストから選択（Select from list）：メッセージ タイプを名前で選択します。 • 一致させる IGMP の種類（IGMP Type to match）：フィルタリングに使用するメッセージ タイプの番号です。

ステップ 5 [Apply] をクリックします。IPv4 ベースの ACE は実行コンフィギュレーション ファイルに保存されます。

IPv6ベースACL

IPv6 ベース ACL は、IPv6 ベースのトラフィックをチェックします。ACL は、フローごとの QoS 処理のためのフロー定義の構成要素としても使用されます。IPv6 ベース ACL を定義するには、次の手順を実行します。

ステップ 1 [Access Control] > [IPv6-Based ACL] をクリックします。

このウィンドウには、定義された ACL とその内容のリストが含まれています。

ステップ 2 [Add] をクリックします。

ステップ 3 [ACL Name] フィールドに、新しい ACL の名前を入力します。名前は大文字と小文字が区別されます。

ステップ 4 [Apply] をクリックします。IPv6 ベースの ACL は実行コンフィギュレーション ファイルに保存されます。

IPv6ベースACE

（注） 各 IP v 6 ベースのルールは、2 つの TCAM ルールを消費します。

IPv6 ベース ACL を定義するには、次の手順を実行します。

ステップ 1 [Access Control] > [IPv6-Based ACE] をクリックします。

このウィンドウには、指定された ACL（ルールのグループ）の ACE（ルール）が含まれます。

ステップ 2 ACL を選択し、[Go] をクリックします。選択した ACL に現在定義されている IP ACE がすべて表示されます。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

ACL 名	ACE が追加されている ACL の名前が表示されます。
Priority	プライオリティを入力します。優先度の高い ACE は最初に処理されます。
Action	ACE に一致するパケットに割り当てられるアクションを、次のオプションから選択します。 • [許可]：ACE 条件に一致するパケットを転送します。 • 拒否（Deny）：ACE 条件に一致するパケットをドロップします。 • シャットダウン（Shutdown）：ACE 条件に一致するパケットをドロップし、パケットが向けられたポートを無効にします。ポートはエラー回復設定 （139 ページ）ページで再アクティブ化されます。
ログ	ACL ルールと一致する ACL フローのロギングを有効にする場合に選択します。
時間範囲	ACL の使用時間を指定した時間範囲に制限する場合に選択します。
時間範囲名	[Time Range] が選択されている場合は、[Edit] ボタンをクリックすると、時間範囲のページにリダイレクトされるので、使用する時間範囲名を選択します。システム時刻 （72 ページ）セクションでは、時間範囲について説明します。
プロトコル（Protocol）	次のオプションから特定のプロトコルに基づいて ACE を作成する場合に選択します。 • [Any (IPv6)]：すべての送信元 IPv6 アドレスが ACE に適用されます • [TCP]： 伝送制御プロトコルにより、2 つのホストが通信してデータストリームを交換できるため、TCP はパケット配信を保証し、パケットが送信された順序で送受信されることが保証されます。 • [UDP]：ユーザーデータグラムプロトコルはパケットを送信しますが、パケットの配信は保証しません。 • [ICMP]：パケットを Internet Control Message Protocol（ICMP）と照合します。 または • 一致させるプロトコル ID（Protocol ID to Match）：一致させるプロトコルの ID を入力します。
送信元 IP アドレス	すべての送信元アドレスを許可する場合は [Any] を選択します。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 [User defined] を選択します。

送信元IPアドレス値	送信元MACアドレスが一致するIPアドレスとマスク（該当する場合）を入力します。
送信元IPプレフィクス長	送信元 IP アドレスのプレフィックス長を入力します。
宛先IPアドレス	すべての宛先アドレスを許可する場合は [Any] を選択します。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 [User defined] を選択します。
宛先IPアドレス値	宛先MACアドレスが一致するIPアドレスとマスクを入力します（該当する場合）。
宛先IPプレフィクス値	IP アドレスのプレフィックス長を入力します。
Source Port	次のいずれかを選択します。 • [Any]：すべての送信元ポートに対して照合を実行します。 • リストから 1 つ（Single from list）：パケットを一致させる TCP/UDP 送信元ポートを 1 つ選択します。このフィールドは、800/6-TCP または 800/17-UDP が [IP Protocol] ドロップダウン メニューから選択されている場合にのみ有効です。 • [番号]：パケットを照合するTCP/UDP送信元ポートを1つ入力します。このフィールドは、800/6-TCP または 800/17-UDP が [IP Protocol] ドロップダウン メニューから選択されている場合にのみ有効です。
Destination Port	使用可能ないずれかの値を選択します。これらは、前述の送信元ポート（Source Port）フィールドと同じです。 （注） 送信元または宛先ポートを入力する前に、ACL の IPv6 プロトコルを指定する必要があります。
フロー ラベル	[IPv6 Flow label] フィールドに基づいて IPv6 トラフィックを分類します。これは IPv6 パケット ヘッダーに含まれる 20 ビットのフィールドです。送信元ステーションでは IPv6 フロー ラベルを使用して、同じフローに属する複数のパケットにラベルを付けることができます。すべてのフローラベルを受け入れ可能な場合は [任意] を選択します。または [ユーザー定義] を選択して、ACL で受け入れる特定のフロー ラベルを入力します。
TCP Flags	パケットのフィルタ処理に使用する TCP フラグを 1 つ以上選択します。フィルタリングされたパケットは転送またはドロップされます。TCPフラグによるパケットのフィルタリングはパケットの制御を増やし、ネットワークセキュリティを向上させます。各フラグのタイプに対して、次のオプションのいずれかを選択します。 • 設定（Set）：フラグが SET の場合に一致します。 • [Unset]：フラグが Not SET の場合に照合します。 • 無視（Don’t care）：TCP フラグを無視します。

Type of Service：タイプ オブ サービス	IP パケットのサービスタイプ。 • [任意]：任意のサービス タイプ。 • [DSCP to match]：照合する Differentiated Service Code Point（DSCP）。 • [照合する IP 優先度]：IP 優先度とは、適切な QoS を確実に提供するためにネットワークが使用する TOS（タイプ オブ サービス）のモデルです。このモデルでは、RFC 791 および RFC 1349 で説明されているように、IP ヘッダーのサービス タイプ バイトの 3 つの最上位ビットを使用します。
ICMP	ACL が ICMP に基づいている場合は、フィルタリングに使用する ICMP メッセージタイプを選択します。メッセージタイプの名前を選択するか、メッセージ タイプの番号を入力します。すべてのメッセージ タイプを受け入れる場合は、[Any] を選択します。 • 任意（Any）：すべてのメッセージ タイプは受け入れられます。 • リストから選択（Select from list）：ドロップダウン リストからメッセージ タイプを名前で選択します。 • [ICMP Type to Match]：フィルタリングに使用するメッセージタイプ番号。
ICMP Code	ICMP メッセージには、そのメッセージの処理方法を示すコードフィールドが設定されている場合があります。このコードでフィルタリングするかどうかを設定するには、次のオプションのいずれかを選択します。 • [Any]：すべてのコードを受け入れます。 • ユーザ定義（User Defined）：フィルタリング用に ICMP コードを入力します。

ステップ 5 [Apply] をクリックします。

ACLバインディング(VLAN)

ACL をインターフェイスにバインドすると、その ACE ルールが、このインターフェイスに届いたパケットに適用されます。ACL 内のどのACEにも一致しないパケットは、不一致のパケットをドロップするアクションを行うデフォルトのルールに一致します。各インターフェイスは 1 つの ACL にのみバインドできますが、ポリシー マップにグループ化し、そのポリシー マップをインターフェイスにバインドすることで、複数のインターフェイスを同じ ACL にバインドできます。ACL がインターフェイスにバインドされた後は、その ACL がバインドされている、または使用中のすべてのポートから削除されるまで、編集、変更、削除することはできません。

（注） インターフェイス（ポート、LAG または VLAN）をポリシーまたは ACL にバインドすることはできますが、ポリシーと ACL の両方にバインドすることはできません。同じクラス マップでは、フィルタリング条件として宛先 IPv6 アドレスを持つ IPv6 ACE では MAC ACL を使用できません。

ACL を VLAN にバインドするには、次の手順を実行します。

ステップ 1 [Access Control] > [VLAN] をクリックします。

ステップ 2 VLAN を選択して [Edit] をクリックします。

必要な VLAN が表示されない場合、新しい VLAN を追加します。

ステップ 3 次のいずれかを選択します。

MACベースACL	インターフェイスにバインドする MAC ベース ACL を選択します。
IPv4ベースACL	インターフェイスにバインドする IPv4 ベース ACL を選択します。
IPv6ベースACL	インターフェイスにバインドする IPv6 ベース ACL を選択します。
Default Action	次のオプションのいずれかを選択します。 • [Deny Any]：ACL に一致しないパケットは拒否（ドロップ）されます。 • [Permit Any]：ACL に一致しないパケットは許可（転送）されます。 （注） [Default Action] は、IP ソースガードがそのインターフェイス上でアクティブでない場合にのみ定義できます。

ステップ 4 [Apply] をクリックします。ACL のバインディングが変更され、実行コンフィギュレーション ファイルが更新されます。

（注） ACL が選択されていない場合、以前に VLAN にバインドされていた ACL はアンバインドされます。

ACLバインディング(ポート)

アクセスコントロールリスト（ACL）は、ポートに送信されるパケットのストリームをフィルタ処理するポートに適用される権限のリストです。ポートをバインドできるのはポリシーまた

はACLのいずれかです。両方にバインドすることはできません。ACL をポートまたは LAG にバインドするには、次の手順を実行します。

ステップ 1 [Access Control] > [ACL Binding（Port] をクリックします。

ステップ 2 インターフェイス タイプ [Ports/LAGs] （ポートまたは LAG）を選択します。

ステップ 3 [Go]をクリックします。選択されているインターフェイスのタイプごとに、そのタイプのすべてのインターフェイスが、現在の ACL のリストとともに表示されます（[Input ACL] および [Output ACL]）。

Interface	ACL が定義されているインターフェイスの ID。
MAC ACL	インターフェイスにバインドされているMACタイプのACL（存在する場合）。
IPv4 ACL	インターフェイスにバインドされているIPv4タイプのACL（存在する場合）。
IPv6 ACL	インターフェイスにバインドされているIPv6タイプのACL（存在する場合）。
Default Action	ACL のルールのアクション（[drop any] または [permit any]）。

ステップ 4 インターフェイスからすべての ACLをアンバインドするには、インターフェイスを選択し、[Clear] をクリックします。

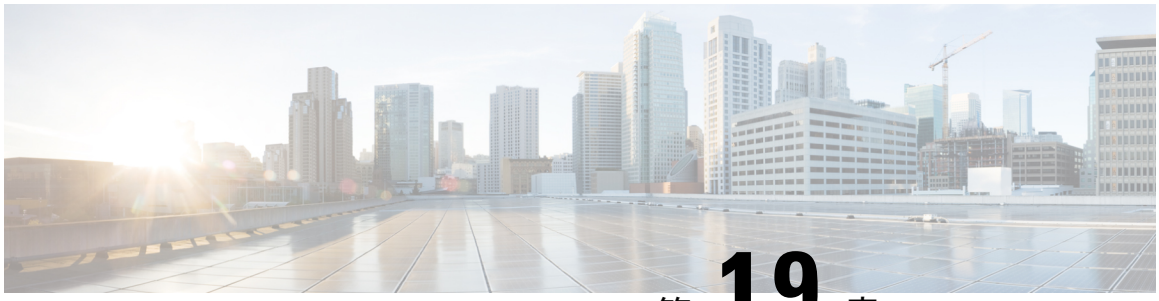
ステップ 5 インターフェイスを選択して、[Edit] をクリックします。

ステップ 6 入力 ACL と出力 ACL に関する以下の内容を入力します。

MACベースACL	インターフェイスにバインドする MAC ベース ACL を選択します。
IPv4ベースACL	インターフェイスにバインドする IPv4 ベース ACL を選択します。
IPv6ベースACL	インターフェイスにバインドする IPv6 ベース ACL を選択します。
Default Action	次のオプションのいずれかを選択します。 • [Deny Any]：ACL に一致しないパケットは拒否（ドロップ）されます。 • [Permit Any]：ACL に一致しないパケットは許可（転送）されます。 （注） [Default Action] は、IP ソースガードがそのインターフェイス上でアクティブでない場合にのみ定義できます。

ステップ 7 [Apply] をクリックします。ACL のバインディングが変更され、実行コンフィギュレーション ファイルが更新されます。

（注） ACL が選択されていない場合、以前にインターフェイスにバインドされていた ACL はアンバインドされます。



第 19 章

QoS

Quality of Service 機能をネットワーク全体に適用すると、必要な基準に従ってネットワークトラフィックが優先順位付けされ、重要なトラフィックが優先的に処理されます。この章は、次の項で構成されています。

一般

Quality of Service（QoS）は、トラフィックを優先順位付けするスイッチの機能であり、結果として、重要なネットワークトラフィックのパフォーマンスが向上します。QoS はスイッチによって異なります。スイッチのレベルが高いほど、そのスイッチで動作するネットワーク アプリケーション レイヤが高くなります。キューの数は、優先順位付けに使用される情報の種類と同様に異なります。

QoSプロパティ

Quality of Service（QoS）はトラフィックのタイプに基づいてトラフィックフローを優先順位付けし、遅延の影響を受けやすいアプリケーション（音声やビデオなど）のトラフィックの優先順位付けに適用したり、遅延に依存しないトラフィックの影響を制御したりできます。

QoS プロパティを設定するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [QoS Properties] をクリックします。

ステップ 2 QoS モードを設定します。次のオプションを使用できます。

- [Disable]：デバイスで QoS が無効になります。
- [Basic]：デバイスで QoS が基本モードで有効になります。
- [Advanced]：デバイスで QoS が拡張モードで有効になります。

ステップ 3 デバイス上のすべてのポート/LAG とそれらの CoS 情報を表示または修正するには、[Port/LAG] を選択し、[Go] をクリックします。

すべてのポート/LAG について、次のフィールドが表示されます。

- [インターフェイス] : インターフェイスのタイプ。
- [デフォルト CoS] : VLAN タグが設定されていない着信パケットに対するデフォル トの VPT 値。デフォルト CoS は 0 です。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

インターフェイスの QoS を設定するには、インターフェイスを選択し、[Edit] をクリックします。

ステップ 5 パラメータを入力します。

- [インターフェイス] : ポートまたは LAG を選択します。
- [デフォルト CoS] : VLAN タグが設定されていない着信パケットに割り当てる、デ フォルト CoS 値を選択します。

ステップ 6 [Apply] をクリックします。インターフェイスのデフォルト CoS 値が実行コンフィギュレーション ファイルに保存されます。

デフォルトの CoS 値を復元するには、[Restore CoS Defaults] をクリックします。

キュー

デバイスでは、インターフェイスごとに 8 つのキューがサポートされます。キュー番号 8 は、最もプライオリティの高いキューです。キュー番号 1 は、最もプライオリティの低いキューです。

キュー内のトラフィックを処理する方式には、絶対優先 と加重ラウンド ロビン（WRR）の 2 つがあります。

- 完全優先：プライオリティが最も高いキュー内のトラフィックが最初に送出されます。それより低いキュー内のトラフィックは、プライオリティが最高のキュー内のトラフィックが創出された後にのみ送出されます。したがって、プライオリティが最高のトラフィックは最大番号のキューに格納されます。
- [Weighted Round Robin (WRR)]：WRR モードでは、キューから送出されるパケット数は、キューのウェイトに比例します（キューのウェイトが大きいほど、送出されるフレームの数が多くなる）。たとえば、許容最大数の 4 個のキューがあり、4 個のキューすべてが WRR モードに設定されていて、デフォルトのウェイト設定が使用されている場合、すべてのキューが飽和状態になっていて輻輳が発生していると仮定すると、キュー 1 では帯域幅の 1/15、キュー 2 では 2/15、キュー 3 では 4/15、キュー 4 では 8/15 がそれぞれ使用されます。このデバイスで使用される WRR アルゴリズムの種類は、一般的な Deficit WRR（DWRR）ではなく Shaped Deficit WRR（SDWRR）です。

キューイング モードは [Queue] ページで選択できます。キューイング モードが SP の場合、プライオリティによって各キューの処理順序が決まります。まず、プライオリティが最高のキューから開始し、各キューが完了すると、プライオリティが次に高いキューに移ります。

キューイング モードが加重ラウンド ロビンの場合は、キューに割り当てられた帯域幅がすべて使用されるまでキューが処理され、その後に別のキューが処理されます。プライオリティの低いキューを WRR モードに設定し、プライオリティの高いキューを SP モードに設定することもできます。この場合、SP モードのキュー内のトラフィックは常に、WRR モードのキュー内のトラフィックよりも先に送出されます。SP モードのキューが空になると、WRR モードのキュー内のトラフィックの送出が開始されます。（各 WRR キューからの相対的な送出割合は、キューのウェイトに依存する）。

プライオリティ方式を選択し、WRR データを入力するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [Queue] をクリックします。

ステップ 2 パラメータを入力します。

- [キュー]：キュー番号が表示されます。
- [Scheduling Method]：次のオプションのいずれかを選択します。
  - [Strict Priority]：選択したキューおよびそれよりプライオリティの高いすべてのキューのトラフィック スケジューリングは、厳密にそのキューのプライオリティに基づきます。
  - [WRR]：選択したキューのトラフィック スケジューリングは、WRR に基づきます。送出時間は、空でない WRR モードのキュー間で配分されます。つまり、それらのキューには出力記述子が設定されています。この配分が発生するのは、SP モードのキューが空になっている場合のみです。
  - [WRR ウェイト]：WRR を選択した場合、このキューに割り当てる WRR ウェイトを入力します。
  - [WRR 帯域幅の %]：このキューに割り当てられている帯域幅の割合が表示されます。この値は、WRR ウェイトをパーセント値で表したものです。

ステップ 3 [Apply] をクリックします。キューが設定され、実行コンフィギュレーション ファイルが更新されます。

CoS/802.1p 値のキューへのマッピング

[CoS/802.1p to Queue] ページでは、802.1p プライオリティを出力キューにマッピングできます。[CoS/802.1p 値のキューへのマッピング テーブル（CoS/802.1p to Queue Table] では、着信パケットの出力キューが、パケットの VLAN タグ内の 802.1p プライオリティに基づいて決定されます。タグなし着信パケットの場合、802.1p プライオリティは、入力ポートに割り当てられているデフォルトの CoS/802.1p プライオリティです。

キューが 8 個の場合のデフォルトのマッピングを、以下の表に示します。

802.1p 値（0 ～ 7。プライオリティは 7 が最高）	キュー（キューが 8 個（1 ～ 8）の場合。プライオリティは 8 が最高）	7 個のキュー	注記
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	基幹アプリケーション：LVS 電話の SIP
4	5	4	ビデオ
5	8	7	音声：Cisco IP Phone のデフォルト
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 to Queue]）、キューのスケジュール方式と帯域割り当てを調整することにより、ネットワークでのサービス品質目標を達成できます。

CoS/802.1p 値からキューへのマッピングは、次のいずれかの場合にのみ適用されます。

- デバイスが QoS 基本モードかつ CoS/802.1p 信頼モードである場合。
- デバイスが QoS 拡張モードであり、CoS/802.1p が信頼されているフローにパケットが属する場合。

CoS 値を出力キューにマッピングするには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [CoS/802.1p to Queue] をクリックします。

ステップ 2 パラメータを入力します。

- [802.1p]：出力ポートを割り当てる 802.1p 値が表示されます。プライオリティは 0が最低、7 が最高です。
- [出力キュー] : 802.1p 値に割り当てる出力キューを選択します。サポートされる出力キュー数は 4 個または 8 個のいずれかです。キュー 4 またはキュー 8 が最高のプライオリティの出力キューで、キュー 1 が最低のプライオリティの出力キューです。

ステップ 3 それぞれの 802.1p プライオリティをマッピングする出力キューを選択します。

ステップ 4 [Apply]、[Cancel]、または [Restore Defaults] をクリックします。801.1p プライオリティ値がキューにマッピングされて実行コンフィギュレーション ファイルが更新されるか、入力された変更がキャンセルされるか、または以前に定義された値が復元されます。

DSCP値のキューへのマッピング

[DSCP (IP Differentiated Services Code Point) to Queue] ページでは、DSCP 値が出力キューにマッピングされます。[DSCP to Queue Table] では、着信パケットの出力キューが、パケットの DSCP 値に基づいて決定されます。着信パケットの元の VPT（VLAN プライオリティ タグ）値は変更されません。

DSCP 値とキューのマッピング、キューイングモード、および帯域割り当てを調整することにより、ネットワーク上でサービス品質目標を達成できます。

次の場合、DSCP 値のキューへのマッピングに IP パケットに適用できます。

- デバイスが QoS 基本モードであり、かつ DSCP が信頼モードである場合。
- デバイスが QoS 拡張モードであり、パケットが DSCP 信頼であるフローに属する場合。

非 IP パケットは、常にベスト エフォート キューに格納されます。

8 キューシステムでの DSCP からキューへのデフォルトマッピングを、以下の表に示します。7 が最高であり、8 はスタックコントロール用に使用されます。

DSCP	63	55	47	39	31	23	15	7
キュー	6	6	7	5	4	3	2	1
DSCP	62	54	46	38	30	22	14	6
キュー	6	6	7	5	4	3	2	1
DSCP	61	53	45	37	29	21	13	5
キュー	6	6	7	5	4	3	2	1
DSCP	60	52	44	36	28	20	12	4
キュー	6	6	7	5	4	3	2	1
DSCP	59	51	43	35	27	19	11	3
キュー	6	6	7	5	4	3	2	1
DSCP	58	50	42	34	26	18	10	2
キュー	6	6	7	5	4	3	2	1
DSCP	57	49	41	33	25	17	9	1

キュー	6	6	7	5	4	3	2	1
DSCP	56	48	40	32	24	16	8	0
キュー	6	6	6	7	6	6	1	1

8 キューシステムの場合の DSCP 値のキューへのデフォルトのマッピングを、以下の表に示します。8 が最高です。

DSCP	63	55	47	39	31	23	15	7
キュー	7	7	8	6	5	4	3	1
DSCP	62	54	46	38	30	22	14	6
キュー	7	7	8	6	5	4	3	1
DSCP	61	53	45	37	29	21	13	5
キュー	7	7	8	6	5	4	3	1
DSCP	60	52	44	36	28	20	12	4
キュー	7	7	8	6	5	4	3	1
DSCP	59	51	43	35	27	19	11	3
キュー	7	7	8	6	5	4	3	1
DSCP	58	50	42	34	26	18	10	2
キュー	7	7	8	6	5	4	3	1
DSCP	57	49	41	33	25	17	9	1
キュー	7	7	8	6	5	4	3	1
DSCP	56	48	40	32	24	16	8	0
キュー	7	7	7	8	7	7	1	2

DSCP をキューにマッピングするには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [DSCP to Queue] をクリックします。

[DSCP値のキューへのマッピング] ページには、[入力DSCP] フィールドが含まれています。このフィールドには着信パケットの DSCP 値とその関連クラスが表示されます。

ステップ 2 [出力キュー] で、DSCP 値をマッピングする出力キュー（トラフィック フォワーディング キュー）を選択します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。デフォルト設定に戻すには、[Restore Defaults] をクリックします。

帯域幅

（注） この設定は、[Advanced Setting] ビューでのみ使用できます。

[Bandwidth] ページには、各インターフェイスの帯域幅情報が表示されます。帯域幅情報を表示するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [Bandwidth] をクリックします。

このページのフィールドは、次のフィールドを除いて、下記の [Edit] ページで説明されています。

- **[入力レート制限]**：
  - [ステータス]：入力レート制限が有効になっているかどうかが表示されます。
  - [Rate Limit (KBits/sec)]：ポートの入力レート制限が表示されます。
  - [%]：ポートの入力レート制限を合計ポート帯域幅で割った値が表示されます。
  - [CBS (Bytes)]：データのバイトに含まれる入力インターフェイスの最大バーストデータサイズ。
- [Egress Shaping Rates]：
  - [Status]：出力シェーピング レートが有効になっているかどうかが表示されます。
  - [CIR (キロビット/秒)]：出力インターフェイスの最大帯域幅が表示されます。
  - [CBS (Bytes)]：データのバイトに含まれる出力インターフェイスの最大バーストデータサイズ。

ステップ 2 インターフェイスを選択して、[Edit] をクリックします。

ステップ 3 [ポート] または [LAG] インターフェイスを選択します。

ステップ 4 選択したインターフェイスに関する次のフィールドの値を入力します。

オプション	説明
入力レート制限	入力レート制限を有効にする場合、このフィールドを選択します。具体的な値はその下のフィールドで定義します（LAGとは無関係です）。
[Ingress Rate Limit (Kbits per sec)]	このインターフェイスで使用できる最大帯域幅を入力します（LAGとは無関係です）。
入力認定バーストサイズ(CBS)	データのバイトに含まれる入力インターフェイスの最大バーストデータサイズを入力します。帯域幅が一時的に許容範囲を超えて増加する

オプション	説明
	場合でも、この量を送信できます。このフィールドは、インターフェイスがポートの場合にのみ使用できます（LAG とは無関係です）。
出力シェーピングレート	このインターフェイスで出力シェーピングを有効にする場合、このフィールドを選択します。
認定情報レート（CIR）[にんていじょうほうれーとCIR]	出力インターフェイスの最大帯域幅を入力します。
出力認定バーストサイズ(CBS)	データのバイトに含まれる出力インターフェイスの最大バーストデータサイズを入力します。帯域幅が一時的に許容範囲を超えて増加する場合でも、この量を送信できます。

ステップ 5 [Apply] をクリックします。帯域幅設定は、実行コンフィギュレーション ファイルに書き込まれます。

キューあたりの出力シェーピング

この設定は、[Advanced Setting] ビューでのみ使用できます。

このデバイスでは、[Bandwidth] ページにおいてポート単位で入出力レートを制限できるだけでなく、選択した出力フレームの入出力レートをキュー単位、ポート単位で制限することもできます。出力レートを制限するには、出力負荷をシェーピングします。

このデバイスでは、管理フレーム以外のすべてのフレームを制限できます。制限されていないフレームは、レートの計算では無視されます。つまり、フレームのサイズは制限の合計に含まれません。

キューごとに出力シェーピングを設定するには、次の手順を実行します。

ステップ 1 **[Quality of Service]** > **[General]** > **[Egress Shaping per Queue]** をクリックします。

[Egress Shaping Per Queue] ページには、キューごとのレート制限（CIR）とバーストサイズ（CBS）が表示されます。

ステップ 2 インターフェイス タイプ（ポートまたは LAG）を選択し、[Go] をクリックします。

ステップ 3 ポート/LAG を選択して **[Edit]** をクリックします。

このページでは、インターフェイスごとに最大 8 個のキューに対して出力シェーピングを有効にすることができます。

ステップ 4 [Interface] を選択します。

ステップ 5 必要な各キューに関して、次のフィールドに入力します。

- [Enable Shaping]：選択すると、このキューで出力シェーピングが有効になります。

- [Committed Information Rate (CIR)]：最大レート（CIR）（Kbps 単位）を入力します。CIR は、送信できる平均最大データ量です。
- [Committed Burst Size (CBS)]：最大バースト サイズ（CBS）（バイト単位）を入力します。CBS は、バーストが CIR を超えても送信できるデータの最大バーストです。

ステップ 6 [Apply] をクリックします。帯域幅設定は、実行コンフィギュレーション ファイルに書き込まれます。

VLAN入力レート制限

この設定は、[Advanced Setting] ビューでのみ使用できます。

[VLAN 入力レート制限] ページで VLAN ごとにレート制限を実行すると、VLAN 上でのトラフィック制限が有効になります。VLAN 入力レート制限が設定されている場合、そのデバイス上のすべてのポートからの集約トラフィックが制限されます。

VLAN ごとのレート制限には、次の制約が適用されます。

- システム内で定義されている他のトラフィック ポリシングよりも低い優先度になります。たとえば、QoS レート制限と VLAN レート制限がパケットに適用されていて、それらのレート制限が競合する場合、QoS レート制限が優先されます。
- これはデバイス レベルで適用され、そのデバイス内部ではパケット プロセッサ レベルで適用されます。デバイス上に複数のパケット プロセッサがある場合、設定されている VLAN レート制限値が、各パケット プロセッサに個別に適用されます。ポート数が 24 個以下のデバイスの場合、パケット プロセッサは 1 個ですが、ポート数が 48 個以上のデバイスにはパケット プロセッサが 2 個あります。

レート制限は、ユニット中のパケット プロセッサごとに別個に計算されます。

VLAN 入力レート制限を定義するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [VLAN Ingress Rate Limit] をクリックします。

このページには、VLAN 入力レート制限テーブルが表示されます。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [VLAN ID]：VLAN を選択します。
- [Committed Information Rate (CIR)]：VLAN に受け入れ可能な平均最大データ量（Kbps 単位）を入力します。
- [Committed Burst Size (CBS)]：出力インターフェイスの最大バースト データ サイズ（バイト単位）を入力します。帯域幅が一時的に許容範囲を超えて増加する場合でも、この量を送信できます。LAG の場合は入力できません。

ステップ 4 [Apply] をクリックします。VLAN レート制限が追加され、実行コンフィギュレーション ファイルが更新されます。

iSCSI

この設定は、[Advanced Setting] ビューでのみ使用できます。

このページでは、iSCSI最適化をアクティブにすることができます。これは、iSCSIトラフィックを他のタイプのトラフィックより優先するメカニズムのセットアップを意味します。この機能がデバイス上で有効になっている場合は、すべてのインターフェイス上のiSCSIトラフィックに定義済みの優先順位が割り当てられ、iSCSIトラフィックはインターフェイス上で設定されたACLまたはポリシールールの影響を受けなくなります。

iSCSIトラフィックは、iSCSIターゲットが要求をリッスンするTCPポートによって（また、必要に応じて、iSCSIターゲットが要求をリッスンするIPv4アドレスによっても）識別されます。デフォルトで、ウェルノウンTCPポート3260と860を使用した2つのiSCSI IPv4フローがデバイス上で定義されます。iSCSIフローの最適化は双方向に、つまり、ターゲットへとターゲットからの両方向のストリームに適用されます。

iSCSIトラフィックに優先順位を付け、必要であればマーキングするためのメカニズムを有効にして設定するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [iSCSI] をクリックします。

ステップ 2 [iSCSI Status] フィールドで [Enable] チェックボックスをオンにして、デバイス上の iSCSI トラフィックの処理を有効にします。

ステップ 3 [サービス設定の品質] の下のフィールドに入力します。

- [VPT Assignment]：[Unchanged] を選択してパケット内の元の VLAN プライオリティ タグ（VPT）値をそのまま使用するか、[Reassigned] フィールドに新しい値を入力します。
- [DSCP Assignment]：[Unchanged] を選択してパケット内の元の DSCP 値をそのまま使用するか、[Reassigned] フィールドに値を入力します。
- [キュー割り当て]：iSCSI トラフィックのキュー割り当てを入力します。デフォルトで、キュー 7 に割り当てられます。

ステップ 4 [Apply] をクリックして設定を保存します。

iSCSI フロー テーブルに、定義されたさまざまな iSCSI フローが表示されます。ウェルノウン TCP ポート 3260 および 860 を使用した 2 つの iSCSI フローが表示されます。これらのフローの [Flow Type] は [Default] です。新しいフローを追加すると、その [Flow Type] が [Static] になります。

新しいフローを追加するには、次の手順に従います。

ステップ 5 [Add] をクリックして、次のフィールドに入力します。

- [TCP Port]：これは、iSCSI ターゲットが要求をリッスンする TCP ポートの番号です。スイッチ上で最大 8 つのターゲット TCP ポートを設定できます。
- [Target IP Address]：iSCSI ターゲット（データの保存先）の IP アドレスを指定します。これは、iSCSI トラフィックの送信元でもあります。[Any] を選択して TCP ポートパラメータに基づいてフローを定義することも、[User-Defined] フィールドに IP アドレスを入力して特定のターゲットアドレスを定義することもできます。

ステップ 6 [Apply] をクリックして設定を保存します。

デフォルト フローを復元する場合は、[Restore Default Flows] をクリックします。

TCP 輻輳回避

この設定は、[Advanced Setting] ビューでのみ使用できます。

[TCP Congestion Avoidance] ページでは、TCP 輻輳回避アルゴリズムをアクティブにすることができます。このアルゴリズムは、さまざまな送信元が同じバイト カウントのパケットを送信しているためにノードで輻輳が発生している場合に、その輻輳ノードでの TCP グローバル同期を無効にするか、または回避します。

TCP 輻輳回避を設定するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [General] > [TCP Congestion Avoidance] をクリックします。

ステップ 2 [Enable] をクリックして TCP 輻輳回避を有効にして、[Apply] をクリックします。

QoS 基本モード

QoS 基本モードでは、ネットワーク内の特定のドメインを信頼できるものとして定義できます。そのドメイン内では、必要となるサービスのタイプを表すために、パケットに802.1pプライオリティやDSCPのマークが付けられます。そのドメイン内のノードでは、それらのフィールドを使用して、パケットが特定の出力キューに割り当てられます。初期パケット分類およびそれらのフィールドのマーキングは、信頼できるドメインの入力において実行されます。

QoS のグローバルな設定

[Global Settings] ページには、デバイスで信頼を有効にするための情報が含まれています（後述の [Trust Mode] フィールドを参照）。QoS モードが基本モードの場合、この設定がアクティブになります。QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。

信頼設定を定義するには、以下の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Basic Mode] > [Global Settings] の順にクリックします。

ステップ 2 デバイスが基本モードまたは拡張モードになっているときに [Trust Mode] を選択します。パケットの CoS レベルと DSCP タグが個別のキューにマッピングされる場合、信頼モードが、パケットが割り当てられるキューを決定します。

- [CoS/802.1p]：トラフィックは、VLAN タグの VPT フィールドに基づいて、またはポートごとのデフォルト CoS/802.1p 値に基づいて（着信パケットに VLAN タグがない場合）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、[mapping CoS/802.1p to Queue] ページで設定できます。
- DSCP：すべての IP トラフィックは、IP ヘッダーの DSCP フィールドに基づいてキューにマッピングされます。DSCP のキューへの実際のマッピングは、[DSCP to Queue] ページで設定できます。トラフィックが IP トラフィックではない場合、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/802.1p と DSCP のうち、いずれか設定されているほう。

ステップ 3 着信パケット中の元の 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オーバーライドする場合は、[Override Ingress DSCP] を選択します。[Override Ingress DSCP] が有効にされると、デバイスで出力キューイングに新しい DSCP 値が使用されます。また、パケット中の元の DSCP 値も、新しい DSCP 値によって置き換えられます。

（注） フレームは、元の DSCP 値ではなく書き換え後の新しい値を使用して出力キューにマッピングされます。

ステップ 4 [DSCP Override Table] をクリックして、DSCP を再設定します。（「DSCP オーバーライド テーブル」を参照）。

ステップ 5 [DSCP In] には、着信パケットの DSCP 値が表示されます。これらの値を代替値に変更する必要があります。[DSCP Out] の値は、発信値がマッピングされることを示す場合に選択します。

ステップ 6 [Apply] をクリックします。実行コンフィギュレーション ファイルが新しい DSCP 値で更新されます。デフォルト設定に戻るには、[Restore Defaults] をクリックします。

QoS インターフェイス設定

[Interface Settings] ページでは、次のように、デバイスのポートごとに QoS を設定できます。

- インターフェイスに対して QoS 状態を無効にした場合：そのポートの着信トラ フィックはすべて、ベスト エフォート キューに格納されます。トラフィックの分類処 理およびプライオリティ設定処理は実行されません。
- ポートに対して QoS 状態を有効にした場合：そのポートに届いたトラフィックは、システム規模でグローバルに設定された信頼モード（CoS/802.1p 信頼モードまたは DSCP 信頼モード）に基づいて処理されます。

各インターフェイスの QoS 設定を入力するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Basic Mode] > [Interface Settings] をクリックします。

ステップ 2 フィルタを使用して [Interface Type] （[Port] または [LAG]）を選択し、[Go] をクリックして現在の設定を表示します。[QoS State] に、インターフェイスの QoS 状態（有効か無効か）が表示されます。

ステップ 3 インターフェイスを選択して、[Edit] をクリックします。

ステップ 4 [ポート] または [LAG] インターフェイスを選択します。

ステップ 5 [QoS State] で、このインターフェイスの QoS 状態（有効または無効）をクリックして設定します。

ステップ 6 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

QoS拡張モード

ACL に合致して着信が許可されたフレームは、暗黙的に、着信許可を出した ACL の名前がラベルとして付けられます。その後、それらのフローに、拡張モード QoS アクションを適用できます。

QoS 拡張モードでは、フローごとの QoS をサポートするポリシーがデバイスによって使用されます。ポリシーとそのコンポーネントには、次の特徴および関係性があります。

- ポリシーには 1 つ以上のクラス マップが含まれています。
- クラス マップは、関連する 1 つ以上の ACL でフローを定義します。クラス マップの中の許可（転送）アクションをともなう ACL ルール（ACE）のみに合致するパケットは、同じフローに属するものと見なされ、同じサービス品質が適用されます。そのようにして、1 つのポリシーに 1 つ以上のフローが含まれ、そのそれぞれにユーザ定義 QoS があります。
- クラス マップ（フロー）の QoS は、関連す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 種類があります。それぞれのポリサーは、QoS 仕様により設定されます。シングル ポリサーは、そのポリサーの QoS 仕様に基づいて QoS を単一のクラス マップに、したがって単一のフローに適用します。集約ポリサーは、1 つ以上のクラス マップに、したがって 1 つ以上のフローに QoS を適用します。集約ポリサーは、異なる複数のポリシーからのクラス マップをサポート可能です。

  2 レート 3 カラー（2R3C）機能がデバイスでサポートされます。この機能では、すべてのポリサーに 2 つのしきい値が割り当てられます。1 つ目のしきい値に到達すると、ユーザ設定の超過アクションが実行されます。2 つ目のしきい値に到達すると、ユーザー設定の違反アクションが実行されます。
- 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。1 つのポリシーとそのクラス マップを 1 つ以上のポートにバインドすることは可能ですが、各ポートは 1 つのポリシーにしかバインドされません。

グローバル設定

[Global Settings] ページには、デバイスで信頼を有効にするための情報が含まれています。QoS ドメインに入るパケットは、QoS ドメインのエッジで分類されます。

信頼設定を定義するには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Global Settings] をクリックします。

ステップ 2 デバイスが拡張モードになっているときに [Trust Mode] を選択します。パケットの CoS レベルと DSCP タグが個別のキューにマッピングされる場合、信頼モードが、パケットが割り当てられるキューを決定します。

- [CoS/802.1p]：トラフィックは、VLAN タグの VPT フィールドに基づいて、またはポートごとのデフォルト CoS/802.1p 値に基づいて（着信パケットに VLAN タグがない場合）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、[mapping CoS/802.1p to Queue] ページで設定できます。
- DSCP：すべての IP トラフィックは、IP ヘッダーの DSCP フィールドに基づいてキューにマッピングされます。DSCP のキューへの実際のマッピングは、[DSCP to Queue] ページで設定できます。トラフィックが IP トラフィックではない場合、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]：選択すると、非 IP トラフィックに信頼 CoS モードが使用され、IP トラフィックに信頼 DSCP が使用されます。

ステップ 3 [Default Mode Status] フィールドで、インターフェイスのデフォルトの拡張モード QoS 信頼モード（信頼できるかどうか）を選択します。これにより、拡張 QoS で基本 QoS の機能が提供されるため、拡張 QoS においてデフォルトで（ポリシーを作成することなく）CoS/DSCP を信頼できます。

ステップ 4 [QoS Advanced Mode] で、[Default Mode Status] が [Not Trusted] に設定されている場合、インターフェイスで設定されているデフォルトの CoS 値は無視され、すべてのトラフィックがキュー 1 に送られます。詳細については、[Quality of Service] > [QoS Advanced Mode] > [Global Settings] ページを参照してください。

ステップ 5 インターフェイス上にポリシーがある場合、デフォルトモードは無効になり、ポリシー設定に従ったアクションになって、合致しないトラフィックはドロップされます。

ステップ 6 DSCP オーバーライド テーブルに従って、着信パケット中の元の DSCP 値を新しい値でオーバーライドする場合は、[入力DSCPのオーバーライド] を選択します。[Override Ingress DSCP] が有効にされると、デバイスで出力キューイングに新しい DSCP 値が使用されます。また、パケット中の元の DSCP 値も、新しい DSCP 値によって置き換えられます。

（注） フレームは、元の DSCP 値ではなく書き換え後の新しい値を使用して出力キューにマッピングされます。

ステップ 7 [Override Ingress DSCP] を有効にした場合は、[DSCP Override Table] をクリックして DSCP を設定しなおします。

a) [DSCP Override Table] で、次のフィールドに入力します。

- [DSCP入力]：着信パケットの DSCP 値が表示されます。これらの値を代替値に変更する必要があります。

• [DSCP出力]：発信値がマッピングされることを示す場合に DSCP 出力値を選択します。

b) [Apply] をクリックします。デフォルト設定に戻るには、[Restore Defaults] をクリックします。

アウト オブ プロファイル DSCP リマーク

クラスマップ（フロー）にポリサーが割り当てられている場合、1 つまたは複数のフロー内のトラフィック量が QoS で指定されている制限を超えた場合に実行されるアクションを指定できます。トラフィックのうち、フローが QoS 制限を超過する原因となった部分は、アウトオブプロファイルパケットと呼ばれます。超過アクションがアウトオブプロファイル DSCP の場合、デバイスにより、アウトオブプロファイル IP パケットの元の DSCP 値が、アウトオブプロファイル DSCP リマークテーブルに基づく新しい値を使用してマッピングし直されます。デバイスは、新しい値を使用して、それらのパケットにリソースと出力キューを割り当てます。また、アウトオブプロファイルパケット中の元の DSCP 値も、デバイスによって新しい DSCP 値に物理的に置き換えられます。

アウト オブ プロファイル DSCP 超過アクションを使用するには、アウト オブ プロファイル DSCP リマーク テーブルで DSCP 値を再マッピングします。そうしない場合、アクションは空になります。これは、工場出荷時設定では、パケットが、このテーブルの DSCP 値により、その値そのものに再マッピングされるためです。この機能により、信頼 QoS ドメイン間で切り替えられる着信トラフィックの 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 値が変更されると、そのタイプのトラフィックのプライオリティが、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が識別されるようになります。これらの設定値は、システムが QoS 拡張モードの場合にアクティブになり、一度アクティブになるとグローバルにアクティブになります。これは、QoSプロパティ （399 ページ）で設定できます。

DSCP 値をマッピングするには、次の手順を実行します。

ステップ 1 **[Quality of Service]** > **[QoS Advanced Mode]** > **[Out of Profile DSCP Remarking]** の順にクリックします。このページで、デバイスを出入りするトラフィックの DSCP 値を設定することができます。

[DSCP In] には、着信パケットの DSCP 値が表示されます。これらの値を代替値に変更する必要があります。

ステップ 2 着信値のマッピング結果となる [DSCP Out] 値を選択します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが新しい DSCP リマーク テーブルで更新されます。

ステップ 4 このインターフェイスの CoS 情報を工場出荷時の設定に戻すには、[Restore Defaults] をクリックします。

クラスマッピング

クラス マップは、そこで定義されている ACL（アクセス制御リスト）を使用してトラフィック フローを定義します。MAC ACL、IP ACL、および IPv6 ACL を組み合わせて、クラス マップを作成できます。クラスマップは、すべて合致か、いずれかが合致という形でパケット条件に合致するように設定されます。パケット合致は、ファーストフィット方式で判定されます。つまり、最初に合致したクラスマップに関連付けられたアクションが、システムの実行するアクションになります。複数のパケットが同じクラスマップに合致する場合、それらのパケットは同じフローに属するものと見なされます。

（注） クラスマップの定義は QoS には影響しません。これは暫定的な手順であり、後でクラスマップを使用できるようにします。

より複雑なルールセットが必要になる場合、複数のクラスマップを、ポリシーと呼ばれるスーパーグループにまとめることができます。

同一のクラスマップでは、宛先IPv6アドレスがフィルタリング条件として設定されているIPv6 ACE と同時に MAC ACL を使用することはできません。

[Class Mapping] ページには、定義されているクラス マップとそのそれぞれを構成する ACL のリストが表示されます。このページで、クラスマップを追加または削除することができます。

クラスマップを定義するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Class Mapping] をクリックします。

クラス マップごとに、そこで定義されている ACL が、それらの ACL 間の関係とともに表示されます。最大 3 つの ACL を [Match] とともに表示できます。[Match] は [And] または [Or] のどちらかにすることができます。これは、ACL 間の関係を示しています。クラス マップは、3 つの ACL を And または Or のどちらかで結合した結果になります。

ステップ 2 [Add] をクリックします。

1 つまたは 2 つの ACL を選択し、クラス マップの名前を指定すると、新しいクラス マップが追加されます。クラス マップの ACL が 2 つの場合、フレームが両方の ACL に合致しなければならないのか、それとも選択された ACL のいずれか一方または両方に合致しなければならないのかを指定できます。

ステップ 3 パラメータを入力します。

- [Class Map Name]：新しいクラス マップの名前を入力します。
- [Match ACL Type]：クラス マップで定義されているフローに属すると見なされるためにパケットが合致しなければならない条件。次のオプションがあります。
  - [IP]：パケットは、クラスマップの IP ベース ACL のいずれかに合致しなければなりません。
  - [MAC]：パケットは、クラスマップの MAC ベース ACL のいずれかに合致しなければなりません。

- [IP and MAC]：パケットは、クラスマップの IP ベース ACL と MAC ベース ACL に合致しなければなりません。
- [IP or MAC]：パケットは、クラスマップの IP ベース ACL または MAC ベース ACL のいずれかに合致しなければなりません。

- [IP]：クラス マップの IPv4 ベース ACL または IPv6 ベース ACL を選択します。
- [MAC]：クラスマップの MAC ベースの ACL を選択します。
- [Preferred ACL]：パケットを IP と MAC のどちらと最初に照合するのかを選択します。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

集約ポリサー

定義済みのルールセットに一致するトラフィックのレートを測定できます。制限を適用するには、1 つ以上のクラスマップで ACL を使用して目的のトラフィックに一致させ、ポリサーを使用して照合トラフィックに QoS を適用します。

ポリサーは、QoS 仕様により設定されます。ポリサーには、次の 2 種類があります。

- シングル（標準）ポリサー：シングル ポリサーは、そのポリサー QoS 仕様に基づいて QoS を単一のクラスマップに、そして単一のフローに適用します。シングルポリサーを使用する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、各ポートにはそのシングルポリサーの独自のインスタンスがあります。したがって、それぞれが互いに独立したポートで、クラスマップ（フロー）に QoS を適用します。シングル ポリサーは、[Policy Table] ページで作成されます。
- 集約ポリサー：集約ポリサーは、1 つ以上のクラス マップに、そして 1 つ以上のフローに QoS を適用します。集約ポリサーは、異なる複数のポリシーからのクラスマップをサポート可能です。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。集約ポリサーは、[Aggregate Policer] ページで作成されます。

  集約ポリサーは、ポリサーを複数のクラスで共有する場合に定義されます。ある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。

各ポリサーは、次のパラメータを組み合わせたそれぞれ独自の QoS 仕様により定義されます。

- [Peak Enforcement]：選択すると、ピーク バースト サイズを超えた場合のアクションが有効になります。
- [Peak Information Rate (PIR)]：ピーク トラフィック レート（PIR）をキロビット/秒（kbps）単位で入力します。
- [Peak Burst Size (PBS)]：ピークバーストサイズ（PIR）をバイト単位で入力します。
- [Violate Action]：ピークサイズを超えた場合のアクションを次の中から 1 つ選択します。

- [Drop]：ピーク サイズに違反したフレームをドロップします。
- [Out-of-Profile DSCP]：事前に設定したDSCP値でピークサイズを超えているフレームをマークします。

- 最大許容レート（「認定情報レート（CIR）」と呼ばれる）（Kbps 単位）。
- トラフィック量（「認定バースト サイズ（CBS）」と呼ばれる）（バイト単位）。これは、定義されている最大レートを超える場合にも一時的なバーストとして通過を許可されるトラフィックです。
- 制限を超えるフレーム（「アウト オブ プロファイル トラフィック」と呼ばれる）に適用されるアクション。そのようなフレームは、そのまま通過させられるか、ドロップされるか、あるいは通過させられた上で新しいDSCP値に再マッピングされ、そのデバイス内の以降のすべての処理ではプライオリティが低いフレームとなるようにマークされます。
- 指定されたレートに基づいてトラフィックポリシングを設定し、オプションのアクションを実行します。 CIR とそれらのオプションの値およびアクションを入力します。

ポリサーをクラス マップに割り当てる処理は、クラス マップがポリシーに追加される時点で実行されます。ポリサーが集約ポリサーの場合は、[Aggregate Policer]ページを使用してそれを作成する必要があります。

集約ポリサーを定義するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Aggregate Policer] をクリックします。

このページには、既存の集約ポリサーが表示されます。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [集約ポリサー名]：集約ポリサーの名前を入力します。
- [Ingress Committed Information Rate (CIR)]：許可される最大帯域幅（bps単位）を入力します。帯域幅（405 ページ）の説明を参照してください。
- [Ingress Committed Burst Size (CBS)]：CIR を超えていても通過を許可される最大バースト サイズ（バイト単位）を入力します。帯域幅 （405 ページ）の説明を参照してください。
- [超過アクション]：CIR を超える着信パケットに対して実行するアクションを選択します。値は次のとおりです。
  - ドロップ（Drop）：定義済みの CIR 値を超えるパケットはドロップされます。
  - [Out of Profile DSCP]：定義されている CIR 値を超えるパケットの DSCP 値は、アウト オブ プロファイル DSCP リマーク テーブルに基づく値に再マッピングされます。
- [Peak Enforcement]：選択すると、ピーク バースト サイズを超えた場合のアクションが有効になります。

- [Peak Information Rate (PIR)]：ピーク トラフィック レート（PIR）をキロビット/秒（kbps）単位で入力します。
- [Peak Burst Size (PBS)]：ピークバーストサイズ（PIR）をバイト単位で入力します。
- [Violate Action]：ピークサイズを超えた場合のアクションを次の中から 1 つ選択します。
  - [Drop]：ピーク サイズに違反したフレームをドロップします。
  - [Out-of-Profile DSCP]：事前に設定した DSCP 値でピークサイズを超えているフレームをマークします。

ステップ 4 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

ポリシーテーブル

[Policy Table Map] ページには、システム内で定義されている拡張 QoS ポリシーのリストが表示されます。このページでは、ポリシーを作成および削除できます。インターフェイ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（ポリシーバインディング（420ページ）を参照）。

各ポリシーは、次のもので構成されます。

- ポリシーでトラフィック フローを定義する ACL の 1 つ以上のクラス マップ。
- ポリシーでトラフィック フローに QoS を適用する 1 つ以上の集約。

ポリシーが追加された後、[Policy Table] ページを使用してクラスマップを追加することができます。QoS ポリシーを追加するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Policy Table] をクリックします。

このページには、定義されているポリシーのリストが表示されます。

ステップ 2 [Policy Class Map Table] をクリックして、[Policy Class Maps] ページを表示するか、または [Add] をクリックして、[Add Policy Table] ページを表示します。

ステップ 3 [New Policy Name] フィールドに、新しいポリシーの名前を入力します。

ステップ 4 [Apply] をクリックします。QoS ポリシー プロファイルが追加され、実行コンフィギュレーション ファイルが更新されます。

ポリシークラスマップ

ポリシーには 1 つ以上のクラス マップを追加できます。クラス マップは、同じトラフィック フローに属すると見なされるパケットのタイプを定義します。

クラス マップをポリシーに追加するには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Policy Class Maps] をクリックします。

ステップ 2 [Filter] でポリシーを選択し、[Go] をクリックします。そのポリシー内のすべてのクラスマップが表示されます。

ステップ 3 新しいクラス マップを追加するには、[Add] をクリックします。

ステップ 4 次のパラメータを入力します。

[Policy Name]	クラスマップの追加先のポリシーが表示されます。
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を選択します。クラスマップは[Class Mapping] ページで作成されます。
アクション タイプ	一致するすべてのパケットの入力CoS/802.1pやDSCPの値に関するアクションを選択します。 • [Use default trust mode]：このオプションが選択されている場合は、グローバル信頼モードでデフォルトモードステータスを使用します。デフォルトモード ステータスが「Not Trusted」（信頼できない）の場合は、入力CoS/802.1pやDSCPの値が無視され、合致したパケットはベストエフォートとして送信されます。 • [Always Trust]：このオプションが選択されている場合は、デバイスがグローバル信頼モード（[Global Settings] ページで選択）に基づいて一致したパケットを信頼します。デフォルト モード ステータス（[Global Settings] ページで選択）は無視されます。 • [設定]：このオプションが選択されている場合は、[新しい値] ボックスに入力された値を使用することにより、合致パケットの出力キューが以下のように判別されます。 新しい値 (0..7) が CoS/802.1p プライオリティである場合は、そのプライオリティ値と [CoS/802.1p to Queue Table] を使用して、すべての合致パケットの出力キューを判別します。 新しい値 (0..63) が DSCP である場合は、新しい DSCP と [DSCP to Queue Table] を使用して、合致するIPパケットの出力キューを判別します。これら以外の場合は、新しい値 (1..8) を、すべての合致パケットの出力キュー番号として使用します。
トラフィックリダイレクト	一致するトラフィックをリダイレクトするかどうかを選択します。リダイレクトする場合は、トラフィックをリダイレクトするユニット/ポートを選択します。

トラフィックミラー	トラフィックフローをアナライザ イーサネット ポートにミラーリングするように設定します。このオプションが選択されている場合、トラフィックはSPANセッション ID 1 で指定された宛先ポートにミラーリングされます。SPAN セッション ID 1 でターゲットポートが指定されていない場合、ミラーアクションは無効です。トラフィック ミラー アクションをともなうポリシー クラス マップがインターフェイスに適用され、その同じインターフェイスが SPAN セッション 1 の送信元ポートとして定義されている場合は、特定のフローだけでなく、すべてのトラフィックがミラーリングされます。 トラフィック ミラー アクションが設定されている場合でも、インターフェイスに適用されたポリシー（およびACL）の追加のルールとアクションは依然として適用されます。次に例を示します。 • ミラー対象フローの ACL アクションが許可されている場合は、ミラーリングに加えて、フロートラフィックも転送されます。フロー ACL のアクションが拒否になっている場合、フロートラフィックはミラーリングされますが、出力ネットワーク インターフェイスに転送されません（ドロップ動作）。 • ポリシーが適用されるインターフェイス上のトラフィックフローがミラー対象のクラスマップ分類と一致しない場合は、デフォルトポリシーのデフォルトアクションに従います。
ポリシングタイプ	ポリシーのポリサー タイプを選択します。次のオプションがあります。 • [None]：ポリシーは使用されません。 • [Single]：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。

ステップ 5 [Police Type] が [Aggregate] の場合は、[Aggregate Policer] を選択します。

ステップ 6 [Police Type] が [Single] である場合は、次の QoS パラメータを入力します。

入力認定情報レート(CIR)	CIR を Kbps 単位で入力します。この説明については、帯域幅ページを参照してください。
入力認定バーストサイズ(CBS)	CBS をバイト単位で入力します。この説明については、帯域幅ページを参照してください。
超過アクション	CIR を超える着信パケットに割り当てるアクションを選択します。次のオプションがあります。 • ドロップ（Drop）：定義済みの CIR 値を超えるパケットはドロップされます。 • [Out of Profile DSCP]：定義されている CIR 値を超える IP パケットは、アウト オブ プロファイル DSCP リマーク テーブルに由来する新しい DSCP を使用して転送されます。

ピーク強制	ピークバーストサイズを超えたときにアクションを有効にする場合に選択します。
最大情報レート(PIR)	ピークトラフィックレート（PIR）をキロビット/秒（kbps）単位で入力します。
最大バーストサイズ(PBS)	ピークバーストサイズ（PIR）をキロビット/秒（kbps）単位で入力します。
違反アクション	ピークサイズを超えた場合のアクションを次の中から 1 つ選択します。 • [Drop]：ピーク サイズに違反したフレームをドロップします。 • [Out of Profile DSCP]：事前に設定した DSCP 値でピークサイズを超えているフレームをマークします。

ステップ 7 [Apply] をクリックします。

ポリシーバインディング

[Policy Binding] ページには、どのポリシープロファイルがどのポートにバインドされているかが表示されます。ポリシーは入力ポリシーまたは出力ポリシーとしてインターフェイスにバインドできます。ポリシープロファイルは、特定のポートにバインドされている場合、そのポートでアクティブになっています。ポートごとおよび方向ごとに設定できるポリシープロファイルは 1 つだけです。ただし、1 つのポリシーを複数のポートにバインドできます。

ポリシーがポートにバインドされている場合、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がフィルタリングされ、それに QoS が適用されます。

ポリシーを編集するには、まず、バインド先のすべてのポートからそのポリシーを削除（アンバインド）する必要があります。

（注） ポートは、ポリシーまたは ACL にバインドできますが、両方に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定義するには、次の手順を実行します。

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Policy Binding] をクリックします。

ステップ 2 必要に応じて、[Interface Type] を選択します。

ステップ 3 [Go] をクリックします。そのインターフェイスのポリシーが表示されます。

ステップ 4 [Edit] をクリックします。

ステップ 5 入力ポリシー/インターフェイスに関して次の項目を選択します。

- [Input Policy Binding]：入力ポリシーをインターフェイスにバインドする場合に選択します。
- [ポリシー名]：バインドする入力ポリシーを選択します。

- [Default Action]：パケットがポリシーと合致した場合のアクションを選択します。
  - [Deny Any]：インターフェイス上のパケットがいずれかのポリシーと合致するときに転送する場合に選択します。
  - [Permit Any]：インターフェイス上のパケットがいずれのポリシーにも一致しないときに転送する場合に選択します。

    （注） [Permit Any] を定義できるのは、IP ソースガードがインターフェイス上でアクティブでない場合のみです。

ステップ 6 出力ポリシー/インターフェイスに関して次の項目を選択します。

- [Output Policy Binding]：出力ポリシーをインターフェイスにバインドする場合に選択します。
- [ポリシー名]：バインドする出力ポリシーを選択します。
- [Default Action]：パケットがポリシーと合致した場合のアクションを選択します。
  - [Deny Any]：インターフェイス上のパケットがいずれかのポリシーと合致するときに転送する場合に選択します。
  - [Permit Any]：インターフェイス上のパケットがいずれのポリシーにも一致しないときに転送する場合に選択します。

    （注） [Permit Any] を定義できるのは、IP ソースガードがインターフェイス上でアクティブでない場合のみです。

ステップ 7 [Apply] をクリックします。QoS ポリシー バインディングが定義され、実行コンフィギュレーション ファイルが更新されます。

QoS 統計情報

QoS 統計情報機能により、パケットがキューから転送される速度の統計情報と、デバイス上で認定パケット、適合パケット、または超過パケットがドロップされる速度の統計情報を収集できます。

シングルポリサー統計

[Single Policer Statistics] ページには、インターフェイスから受信したプロファイル内パケットおよびアウト オブ プロファイル パケットのうち、ポリシーのクラス マップで定義されている条件を満たすものの数が示されます。

（注） デバイスがレイヤ 3 モードの場合、このページは表示されません。

ポリサー統計情報を表示するには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Statistics] > [Single Policer Statistics] の順にクリックします。

このページには、次のフィールドが表示されます。

- [Interface]：このインターフェイスに関する統計情報が表示されます。
- [ポリシー]：このポリシーに関する統計情報が表示されます。
- [Class Map]：このクラス マップに関する統計情報が表示されます。
- [プロファイル内バイト]：受信したプロファイル内バイトの数。
- [Out-of-Profile Bytes]：受信したアウト オブ プロファイル バイトの数。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]：統計情報を収集する対象のインターフェイスを選択します。
- [Policy Name]：ポリシー名を選択します。
- [Class Map Name]：クラス名を選択します。

ステップ 4 [Apply] をクリックします。統計情報に関する追加の要求が作成され、実行コンフィギュレーション ファイルが更新されます。

集約ポリサー統計

集約ポリサー統計情報を表示するには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Statistics] > [Aggregate Policer Statistics] をクリックします。

このページには、次のフィールドが表示されます。

- [集約ポリサー名]：統計の対象となるポリサー。
- [In-Profile Bytes]：受信されたプロファイル内パケットの数。
- [Out-of-Profile Bytes]：受信されたアウト オブ プロファイル パケットの数。

ステップ 2 [Add] をクリックします。

ステップ 3 [Aggregate Policer Name] で、統計情報表示の対象となる作成済みの集約ポリサーの 1 つを選択します。

ステップ 4 [Apply] をクリックします。統計情報に関する追加の要求が作成され、実行コンフィギュレーション ファイルが更新されます。

ステップ 5 特定の統計情報を削除するには、[Delete] をクリックします。

ステップ 6 選択したポリサーをクリアするには、[Clear Counters] をクリックします。

キュー統計情報

[Queues Statistics] ページには、転送されたパケットやドロップされたパケットなどに関する統計情報が、インターフェイスごと、キューごと、およびドロップ優先順位ごとに表示されます。

キュー統計情報を表示したり、表示する統計情報（カウンタセット）を定義したりするには、次の手順に従います。

ステップ 1 [Quality of Service] > [QoS Statistics] > [Queues Statistics] の順にクリックします。

このページには、次のフィールドが表示されます。

- [リフレッシュレート] : インターフェイスイーサネット統計情報がリフレッシュされるまでの時間を選択します。次のオプションを使用できます。
  - [No Refresh]：統計情報は更新されません。
  - [15 秒]：統計情報は 15 秒ごとにリフレッシュされます。
  - [30 Sec]：統計情報は 30 秒ごとに更新されます。
  - [60 Sec]：統計情報は 60 秒ごとに更新されます。

特定のユニットやインターフェイスを表示するには、フィルタでユニット/インターフェイスを選択して、[Go] をクリックします。

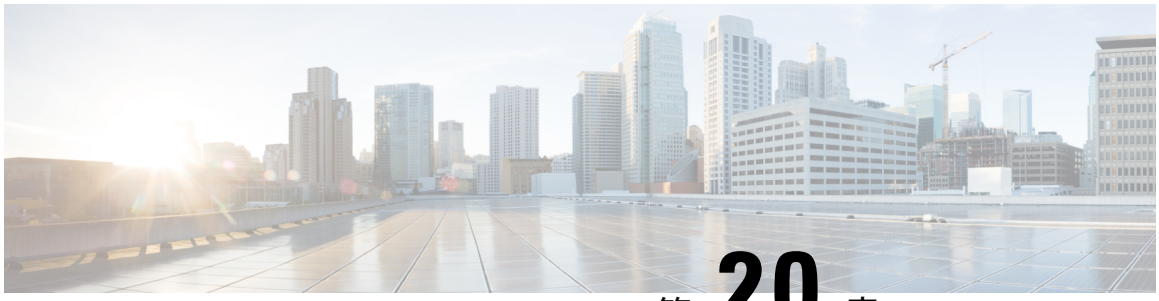
特定のインターフェイスを表示するには、フィルタでインターフェイスを選択して、[実行] をクリックします。

キュー統計情報テーブルに、各キューに関する次のフィールドが表示されます。

- [Queue]：このキューから転送またはテール ドロップされたパケット。
- [Transmitted Packets]：送信されたパケットの数。
- [テールドロップパケット数]：テール ドロップされたパケットの数。
- [送信バイト数]：送信されたバイトの数。
- [テールドロップバイト数]：テール ドロップされたバイトの数。

ステップ 2 選択したインターフェイスの統計情報カウンタをクリアするには、[Clear Interface Counters] をクリックします。

ステップ 3 すべてのインターフェイスの統計情報カウンタをクリアするには、[Clear All Interface Counters] をクリックします。



第 20 章

SNMP

この章では、ネットワークデバイスを管理する方法を提供する Simple Network Management Protocol（SNMP）機能について説明します。ここで説明する内容は、次のとおりです。

エンジン ID

エンジン ID は、それらを一意に識別するために SNMPv3 エンティティによって使用されます。SNMP エージェントは、正規の SNMP エンジンと見なされます。つまり、エージェントが着信メッセージ（Get、GetNext、GetBulk、Set）に応答して、マネージャにトラップ メッセージを送信します。エージェントのローカル情報は、メッセージ内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用されるローカル情報を保持します。デフォルトの SNMP エンジン ID は、エンタープライズ番号とデフォルトの MAC アドレスで構成されます。このエンジン ID は、ネットワーク内の 2 台のデバイスが同じエンジン ID を持つことがないように、管理ドメインで一意である必要があります。

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

⚠

注意 エンジン ID を変更すると、設定されているすべてのユーザとグループが消去されます。

SNMP エンジン ID を設定するには、次の手順を実行します。

ステップ 1 [SNMP] > [Engine ID] をクリックします。

ステップ 2 [Local Engine ID] に次のどちらを使用するかを選択します。

- デフォルトを使用（Use Default）：デバイスによって生成されたエンジン ID を使用することを選択します。デフォルトのエンジン ID はデバイスの MAC アドレスに基づくもので、次のような基準に従って定義されます。
  - 最初の 4 つのオクテット：最初のビット = 1、残りの部分が IANA エンタープライズ番号。
  - 5 番目のオクテット：3 に設定すると、それに続く MAC アドレスを指定します。
  - 第 6 ～ 11 オクテット：デバイスの MAC アドレスです。
- なし（None）：エンジン ID は使用されません。
- ユーザ定義（User Defined）：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。

  リモートのエンジン ID テーブルでは、すべてのリモート エンジン ID とその IP アドレスが表示されます。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

リモート エンジン ID テーブルは、エンジンの IP アドレスおよびエンジン ID の間のマッピングを示します。

エンジン ID の IP アドレスを追加するには：

ステップ 4 [Add] をクリックします。次のフィールドに入力します。

- サーバ定義（Server Definition）：IP アドレスまたは名前によってエンジン ID サーバを指定するかどうかを選択します。
- [IP バージョン]：サポートする IP 形式を選択します。
- [IPv6 アドレスタイプ]：IPv6 を使用する場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [リンクローカル]：IPv6 アドレスによって、同一ネットワーク リンク上のホスト が一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このアドレスはルーティング不能であり、ローカルネットワークでの通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [グローバル]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
- [リンクローカルインターフェイス]：リストからリンク ローカル インターフェイス（IPv6 アドレス タイプとしてリンク ローカルが選択されている場合）を選択します。

- サーバ IP アドレス/名前（Server IP Address/Name）：IP アドレスまたはログ サーバのドメイン名を入力します。
- [Engine ID]：エンジン ID を入力します。

ステップ 5 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

SNMP ビュー

ビューは、MIB サブツリーの集合のためのユーザ定義のラベルです。各サブツリー ID は、関連するサブツリーのルートのオブジェクト ID（OID）によって定義されます。目的のサブツリーのルートを指定するには、既知の名前を使用するか、または、OID を入力します。ビューページでは、SNMP ビューの作成および編集が有効です。デフォルトのビュー（Default および DefaultSuper）を変更することはできません。

ビューは、グループにアタッチすることも、基本アクセスモードを使用するコミュニティにアタッチする（SNMP グループ （428 ページ）を使用）こともできます。

SNMP ビューを設定するには、次の手順を実行します。

ステップ 1 [SNMP] > [Views] をクリックします。

各ビューには、次のフィールドが表示されます。

- オブジェクト ID サブツリー（Object ID Subtree）：ビューに含まれるか除外される MIB ツリー内のノード。
- オブジェクト ID サブツリー ビュー（Object ID Subtree View）：ノードが含まれるか除外されるかどうか。

ステップ 2 [Add] をクリックし、新しいビューを定義します。

ステップ 3 パラメータを入力します。

- [View Name]：0 ～ 30 文字でビューの名前を入力します。
- オブジェクト ID サブツリー（Object ID Subtree）：選択した SNMP ビューに含まれるか除外される MIB ツリー内のノードを選択します。オブジェクトを選択するオプションは次のとおりです。
  - リストから選択（Select from list）：MIB ツリーを移動できるようになります。
  - ユーザ定義（User Defined）：[Select from list] オプションで提供されていない OID を入力します。

ステップ 4 [Include in view] を選択または選択解除します。これを選択すると、選択した MIB はビューに含まれ、そうでないものは除外されます。

ステップ 5 [Apply] をクリックします。

ステップ 6 ビューの設定を確認するには、[Filter: View Name] リストからユーザ定義のビューを選択します。

- デフォルト（Default）：読み取りおよび読み取り/書き込みビューのデフォルトの SNMP ビューです。
- DefaultSuper：管理者ビューのデフォルトの SNMP ビューです。

SNMP グループ

SNMPv1 および SNMPv2 では、コミュニティストリングは、SNMP フレームとともに送信されます。コミュニティストリングは、SNMP エージェントにアクセスするためのパスワードとして機能します。ただし、フレームもコミュニティストリングも暗号化されません。したがって、SNMPv1 と SNMPv2 は安全ではありません。

SNMPv3 では、次のセキュリティ メカニズムを設定することができます。

- 認証（Authentication）：デバイスは SNMP ユーザが承認済みシステム管理者であることを確認します。これは、フレームごとに実行されます
- プライバシー（Privacy）：SNMP フレームは暗号化されたデータを伝送できます。

したがって、SNMPv3 では、3 つのレベルのセキュリティがあります。

- セキュリティなし（認証なし、プライバシーなし）
- 認証（認証あり、プライバシーなし）
- 認証およびプライバシー

SNMPv3 では、各ユーザが読み取りまたは書き込みできるコンテンツと、ユーザが受信する通知を制御する手段を提供します。グループは、読み取り/書き込み権限とセキュリティのレベルを定義します。グループは、SNMP ユーザーまたはコミュニティに関連付けられている場合に機能します。

（注） グループにデフォルト以外のビューを関連付けるには、まずSNMP ビュー （427 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、次の手順を実行します。

ステップ 1 [SNMP] > [Groups] をクリックします。

このページには、既存の SNMP グループおよびセキュリティ レベルが含まれています。

ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- [Group Name]：新しいグループ名を入力します。

- セキュリティ モデル（Security Model）：グループ、SNMPv1、v2、v3 にアタッチされる SNMP バージョンを選択します。

  さまざまなセキュリティ レベルの、3 つのタイプのビューを定義できます。セキュリティレベルごとに、以下のフィールドを入力して、読み取り、書き込み、通知用のビューを選択します。

- 有効化（Enable）：セキュリティ レベルを有効にするには、このフィールドを選択します。
- セキュリティ レベル（Security Level）：グループにアタッチするセキュリティ レベルを定義します。SNMPv1 および SNMPv2 は、認証もプライバシーもサポートしません。SNMPv3 を選択する場合、次のいずれかを選択します。
  - 認証なし、プライバシーなし（No Authentication and No Privacy）：認証とプライバシーのどちらのセキュリティ レベルもグループに割り当てられません。
  - [Authentication and No Privacy]：SNMP メッセージが認証され、SNMP メッセージの送信元が保証されますが、メッセージは暗号化されません。
  - 認証およびプライバシー（Authentication and Privacy）：SNMP メッセージを認証し、それらを暗号化します。
- ビュー（View）：選択すると、ビューに読み取り、書き込み、通知アクセスが関連付けられます。グループのアクセス権限は、グループに読み取り、書き込み、および通知アクセスがある MIB ツリーの範囲を制限します。
  - 読み取り（Read）：管理アクセスは、選択したビューの読み取り専用です。そうでない場合、このグループに関連付けられているユーザまたはコミュニティが、SNMP 自体を制御するものを除くすべての MIB を読み取ることができます。
  - [Write]：選択したビューに対する管理アクセス権限は、書き込みです。そうでない場合、このグループに関連付けられているユーザまたはコミュニティが、SNMP 自体を制御するものを除くすべての MIB を書き込むことができます。
  - 通知（Notify）：選択したビューに含まれるものにトラップの使用可能な内容が制限されます。それ以外の場合、トラップの内容は制限されません。これは、SNMPv3 でのみ選択できます。

ステップ 4 [Apply] をクリックします。SNMP グループは実行コンフィギュレーション ファイルに保存されます。

SNMP ユーザー

SNMPユーザは、ログイン クレデンシャル（ユーザ名、パスワード、および認証方式）と、グループおよびエンジン ID との関連付けによって動作するコンテキストおよび範囲によって定義されます。設定されたユーザーには、そのグループの属性が設定され、関連付けられたビュー内でアクセス権限が設定されます。

SNMPv3 ユーザを作成するには、まず次が存在しなければなりません。

- エンジン ID をデバイスで最初に設定する必要があります。これは、エンジン ID（425 ページ）で設定します。
- SNMPv3 グループが使用可能でなければなりません。SNMPv3 グループは、SNMP グループ（428 ページ）で定義します。

SNMP ユーザを表示し、新規で定義するには：

ステップ 1 [SNMP] > [Users] をクリックします。

このページには、既存のユーザが表示されます。このページのフィールドは、次のフィールドを除いて [Add] ページで説明されています。

- IP アドレス（IP Address）：エンジンの IP アドレスを表示します。

ステップ 2 [Add] をクリックします。

このページは、SNMP ユーザに SNMP アクセス制御権限を割り当てるための情報を提供します。

ステップ 3 パラメータを入力します。

- [User Name]：ユーザーの名前を入力します。
- エンジン ID（Engine ID）：ユーザを接続するローカルまたはリモート SNMP エンティティを選択します。ローカル SNMP エンジン ID を変更または削除すると、SNMPv3 ユーザ データベースが削除されます。通知メッセージを受信して情報をリクエストするには、ローカルおよびリモート ユーザの両方を定義する必要があります。
  - ローカル（Local）：ユーザはローカルのデバイスに接続されます。
  - リモート IP アドレス（Remote IP Address）：ユーザはローカルのデバイスだけでなく、別の SNMP エンティティに接続されます。リモートエンジン ID が定義されている場合、リモートデバイスはインフォームメッセージを受信できますが、情報を要求することはできません。
- グループ名（Group Name）：SNMP ユーザが所属する SNMP グループを選択します。SNMP グループは、[Add Group] ページで定義されます。

  （注） 削除されたグループに属しているユーザは残りますが、アクティブではありません。

- 認証方式（Authentication Method）：認証方式を選択します。これは割り当てられているグループ名に応じて変わります。グループの認証が不要な場合、ユーザーは認証を設定できません。次のオプションがあります。
  - [None]：ユーザー認証は使用されません。
  - [SHA]：SHA-1（セキュア ハッシュ アルゴリズム）認証方式でキーを生成するために使用されるパスワード。
  - [SHA224]：SHA-224（セキュア ハッシュ アルゴリズム 2 ベース）認証方式で 128 ビットに切り捨てたキーを生成するために使用されるパスワード。

- [SHA256]：SHA-256（セキュア ハッシュ アルゴリズム 2 ベース）認証方式で 192 ビットに切り捨てたキーを生成するために使用されるパスワード。
- [SHA384]：SHA-384（セキュア ハッシュ アルゴリズム 2 ベース）認証方式で 256 ビットに切り捨てたキーを生成するために使用されるパスワード。
- [SHA512]：SHA-512（セキュア ハッシュ アルゴリズム 2 ベース）認証方式で 384 ビットに切り捨てたキーを生成するために使用されるパスワード。

- [Authentication Password]：パスワードおよび認証方式を使用して認証を行う場合は、ローカルユーザーパスワードを [Encrypted] または [Plaintext] のいずれかに入力します。ローカルユーザーパスワードはローカルデータベースと比較されます。最大 32 文字の ASCII 文字を使用できます。
- プライバシー方式（Privacy Method）：次のいずれかのオプションを選択できます。
  - [None]：プライバシーパスワードは暗号化されません。
  - [AES]：プライバシーパスワードは AES に従って暗号化されます。
- [Privacy Password]：AES プライバシー方式が選択されている場合、16 バイト必要です（AES 暗号化キー）。このフィールドには 32 文字の 16 進数を指定する必要があります。暗号化またはプレーン テキストモードを選択できます。

ステップ 4 [Apply] をクリックして設定を保存します。

SNMP コミュニティ

SNMPv1 および SNMPv2 のアクセス権限は、[Communities] ページでコミュニティを定義することによって管理されます。コミュニティ名とは、SNMP 管理ステーションとデバイスの間で共有される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されます。

SNMPv3 はコミュニティではなくユーザと連携するため、コミュニティは SNMPv1 および v2 でのみ定義されます。ユーザは、アクセス権が割り当てられているグループに属します。[Communities] ページは、コミュニティにアクセス権を直接（基本モード）またはグループを通じて（拡張モード）関連付けます。

- 基本モード（Basic mode）：コミュニティのアクセス権は、読み取り専用、読み取り/書き込み、または SNMP 管理権限と一緒に設定できますまた、SNMP ユーザー（429 ページ）で定義されたビューを選択することで、コミュニティへのアクセスを、特定の MIB オブジェクトのみに制限できます。
- 拡張モード：コミュニティのアクセス権限は、SNMP グループ（428 ページ）で定義されたグループによって定義されます。特定のセキュリティ モデルを持つグループを設定できます。グループのアクセス権限は、読み取り、書き込み、および通知です。

SNMP コミュニティを定義するには、次の手順を実行します。

ステップ 1 [SNMP] > [Communities] をクリックします。

ステップ 2 [Add] をクリックして、新しい SNMP コミュニティを定義および設定します。

ステップ 3 次のフィールドを設定します。

SNMP管理ステーション	次のオプションのいずれかを選択します。 • [All]：すべての IP デバイスが SNMP コミュニティにアクセスできることを示します。 • [User Defined]：SNMP コミュニティにアクセスできる管理ステーションの IP アドレスを入力します。
IP バージョン	[IPv4] または [IPv6] を選択します。
IPv6 アドレス タイプ	サポートされる IPv6 アドレスタイプを選択します（IPv6 が使用される場合）。次のオプションがあります。 • [リンクローカル] : IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このアドレスはルーティング不能であり、ローカルネットワークでの通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [グローバル] : IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
リンクローカルインターフェイス	IPv6 アドレスタイプがリンクローカルの場合、 IPv6 アドレスを VLAN または ISATAP 経由で受信するかを選択します。
IP アドレス	SNMP 管理ステーションの IP アドレスを入力します。
Community String	デバイスに対する管理ステーションの認証に使用するコミュニティ名を入力します。

基本 (Basic)	このコミュニティタイプでは、どのグループにも接続できません。選択できるのはコミュニティ アクセス レベル（読み取り専用、読み取り/書き込み、またはSNMP管理）のみであり、必要に応じて、特定のビューではさらに制限します。デフォルトでは、MIB 全体に適用されます。これを選択した場合、次のフィールドに入力します。 • アクセス モード（Access Mode）：コミュニティのアクセス権を選択します。次のオプションがあります。 読み取り専用：管理アクセスは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。 読み取り/書き込み：管理アクセスは読み取り/書き込みです。デバイス構成に変更を行うことはできますが、コミュニティにはできません。 [SNMP Admin]：ユーザーは、すべてのデバイス設定オプションにアクセスし、コミュニティを変更できます。SNMP管理は、SNMP MIBを除くすべてのMIBの読み取り/書き込みに相当します。SNMP管理は、SNMP MIBへのアクセスに必要です。 • ビューの名前（View Name）：SNMP ビューを選択します（アクセスが付与される MIB サブツリーの集合）。
Advanced	選択したコミュニティに対してこのタイプを選択します。 • グループ名（Group Name）：アクセス権を決定する SNMP グループを選択します。

ステップ 4 [Apply] をクリックします。SNMP コミュニティが定義され、実行コンフィギュレーションが更新されます。

トラップの設定

[Trap Settings] ページでは、デバイスから SNMP 通知を送信するかどうか、およびどのケースで送信するかを設定することができます。

トラップ設定を定義するには、次の手順を実行します。

ステップ 1 [SNMP] > [Trap Settings] をクリックします。

ステップ 2 デバイスから SNMP 通知を送信できるように指定するには、[SNMP Notifications] で [Enable] を選択します。

ステップ 3 SNMP 認証失敗時の通知を有効にするには、[Authentication Notifications] で [Enable] を選択します。

ステップ 4 [Apply] をクリックします。SNMP トラップ設定は、実行コンフィギュレーション ファイルに書き込まれます。

通知受信者SNMPv1、2

通知の受信者は、SNMP通知の宛先、および各宛先に送信するSNMP通知の種類（トラップまたはインフォーム要求）を設定できます。SNMP通知とはデバイスからSNMP管理ステーションに送信されるメッセージであり、リンク アップ/ダウンなど、特定のイベントが発生したことを示します。

特定の通知をフィルタリングすることもできます。フィルタ処理を行うには、通知フィルタ（437ページ）でフィルタを作成し、そのフィルタをSNMP通知受信者に関連付けます。通知フィルタを使用すると、これから送信される通知の OID に基づいて、管理ステーションに送信される SNMP 通知のタイプをフィルタリングすることができます。

SNMPv1,2 で受信者を定義するには：

ステップ 1 [SNMP] > [Notification Recipients SNMPv1,2] をクリックします。

このページには、SNMPv1,2 の受信者が表示されます。

ステップ 2 次のフィールドに入力します。

- IPv4 送信元インターフェイスに通知（Informs IPv4 Source Interface）：IPv4 SNMP サーバと通信するための通知メッセージの送信元IPv4アドレスとして、IPv4アドレスが使用される送信元インターフェイスを選択します。
- IPv4 送信元インターフェイスをトラップ（Traps IPv4 Source Interface）：IPv6 SNMP サーバと通信するためのトラップ メッセージの送信元IPv6アドレスとして、IPv6アドレスが使用される送信元インターフェイスを選択します。
- IPv6 送信元インターフェイスに通知（Informs IPv6 Source Interface）：IPv4 SNMP サーバと通信するための通知メッセージの送信元IPv4アドレスとして、IPv4アドレスが使用される送信元インターフェイスを選択します。
- IPv6 送信元インターフェイスをトラップ（Traps IPv6 Source Interface）：IPv6 SNMP サーバと通信するためのトラップ メッセージの送信元IPv6アドレスとして、IPv6アドレスが使用される送信元インターフェイスを選択します。

（注） 自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

- [サーバー指定方法] : リモート ログ サーバーを IP アドレスで指定するか、名前で指定す るかを選択します。
- [IP Version] : IPv4 または IPv6 を選択します。
- IPv6 アドレス タイプ（IPv6 Address Type） : リンク ローカルまたはグローバルのいずれかを選択します。
  - [リンクローカル] : IPv6 アドレスによって、同一ネットワーク リンク上のホスト が一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80 です。このアドレスはルーティング不能であり、ローカルネットワークでの通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [グローバル] : IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
- [Link Local Interface] : IPv6 アドレスタイプがリンクローカルの場合、 IPv6 アドレスを VLAN または ISATAP 経由で受信するかを選択します。
- 受信者の IP アドレス/名前（Recipient IP Address/Name） : トラップが送信される場所の IP アドレスまたはサーバ名を入力します。
- UDP ポート（UDP Port） : 受信者のデバイスで通知のために使用する UDP ポートを入力します。
- 通知タイプ（Notification Type） : トラップまたは通知のどちらを送信するかを選択します。両方が必要な場合は、2 名の受信者を作成する必要があります。
- [Timeout] : デバイスがインフォーム要求を再送信するまでの待機時間を秒数で入力します。
- 再試行回数（Retries） : デバイスがインフォーム要求を再送信する回数を入力します。
- コミュニティストリング（Community String） : プルダウン メニューから、トラップ マネージャのコミュニティストリングを選択します。コミュニティストリング名は、SNMP コミュニティ （431 ページ）にリストされた名前から生成されます。
- 通知バージョン（Notification Version） : トラップの SNMP バージョンを選択します。SNMPv1 または SNMPv2 のいずれかをトラップのバージョンとして使用できますが、一度に有効にできるのは 1 つのバージョンのみです。
- 通知フィルタ（Notification Filter） : 選択すると、管理ステーションに送信される SNMP 通知タイプのフィルタリングが有効になります。フィルタは通知フィルタ （437 ページ）で作成されます。
- [Filter Name] : トラップに含める情報を定義した SNMP フィルタ（通知フィルタ （437 ページ）で定義）を選択します。

ステップ 5 [Apply] をクリックします。SNMP 通知の受信者設定は、実行コンフィギュレーション ファイルに書き込まれます。

通知受信者SNMPv3

SNMPv3 で受信者を定義するには：

ステップ 1 [SNMP] > [Notification Recipients SNMPv3] をクリックします。

ステップ 2 次の設定を行います。

- [Informs IPv4 Source Interface]：ドロップダウンリストから、IPv4 SNMP サーバーとの通信に使用する通知メッセージ内で、IPv4アドレスを送信元IPv4アドレスとして使用する送信元インターフェイスを選択します。
- [Traps IPv4 Source Interface]：ドロップダウンリストから、トラップメッセージ内で、IPv6 アドレスを送信元アドレスとして使用する送信元インターフェイスを選択します。8
- [Informs IPv6 Source Interface]：ドロップダウンリストから、IPv4 SNMP サーバーとの通信に使用する通知メッセージ内で、IPv4アドレスを送信元IPv4アドレスとして使用する送信元インターフェイスを選択します。
- [Traps IPv6 Source Interface]：ドロップダウンリストから、トラップメッセージ内で、IPv6 アドレスを送信元アドレスとして使用する送信元インターフェイスを選択します。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

- [サーバー指定方法]：リモート ログ サーバーを IP アドレスで指定するか、名前で指定す るかを選択します。
- [IP Version]：IPv4 または IPv6 を選択します。
- [IPv6アドレスタイプ]：IPv6を使用する場合、IPv6アドレス タイプを選択します。次のオプションがあります。
  - [リンクローカル]：IPv6 アドレスによって、同一ネットワーク リンク上のホスト が一意に識別されます。リンクローカルアドレスのプレフィックス部はFE80です。このアドレスはルーティング不能であり、ローカルネットワークでの通信にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。
  - [グローバル]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
- リンク ローカル インターフェイス（Link Local Interface）：プルダウン リストからリンク ローカル インターフェイスを選択します（IPv6 アドレス タイプにリンク ローカルが選択されている場合）。
- 受信者の IP アドレス/名前（Recipient IP Address/Name）：トラップが送信される場所の IP アドレスまたはサーバ名を入力します。
- UDP ポート（UDP Port）：受信者のデバイスで通知のために使用する UDP ポートを入力します。

- 通知タイプ（Notification Type）：トラップまたは通知のどちらを送信するかを選択します。両方が必要な場合は、2 名の受信者を作成する必要があります。
- [Timeout]：デバイスがインフォームまたはトラップを再送するまでに待機する時間（秒数）を入力します。タイムアウト：範囲 1 ～ 300、デフォルト 15
- 再試行回数（Retries）：デバイスがインフォーム要求を再送信する回数を入力します。再試行範囲：1 ～ 255、デフォルトは 3
- ユーザ名（User Name）：ドロップダウン リストから、SNMP 通知を送信するユーザを選択します。通知を受け取るには、そのユーザーがページで定義されていて、そのエンジン ID がリモートである必要があります。
- セキュリティ レベル（Security Level）：パケットに適用する認証のレベルを選択します。

  （注） このセキュリティ レベルは、どのユーザ名を選択したかによって異なります。このユーザ名が「認証なし」として設定された場合、セキュリティ レベルは「認証なし」のみとなります。ただし、[User Name] に [Authentication and Privacy] 権限が割り当てられている場合、[Security Leve] は [No Authentication]、[Authentication Only]、または [Authentication and Privacy] のいずれかになります。

  次のオプションがあります。

  - [No Authentication]：パケットは認証または暗号化されていないことを示します。
  - [Authentication]：パケットは認証されているが、暗号化されていないことを示します。
  - [Privacy]：パケットは認証および暗号化されていることを示します。

- 通知フィルタ（Notification Filter）：選択すると、管理ステーションに送信される SNMP 通知タイプのフィルタリングが有効になります。
- [Filter Name]：トラップに含まれる情報を定義する SNMP フィルタを選択します。

ステップ 5 [Apply] をクリックします。SNMP 通知の受信者設定は、実行コンフィギュレーション ファイルに書き込まれます。

通知フィルタ

[Notification Filter] ページでは、SNMP 通知フィルタと、チェック対象のオブジェクト ID（OID）を設定することができます。通知フィルタを使用すると、これから送信される通知の OID に基づいて、管理ステーションに送信される SNMP 通知のタイプをフィルタリングすることができます。

通知フィルタを定義する手順は次のとおりです。

ステップ 1 [SNMP] > [Notification Filter] をクリックします。

[Notification Filter] テーブルには、各フィルタの通知情報があります。テーブルでは、フィルタ名でフィルタ通知のエントリをフィルタリングできます。[Object ID Subtree Filter] には、設定された各フィルタの現在のステータスが表示されます。

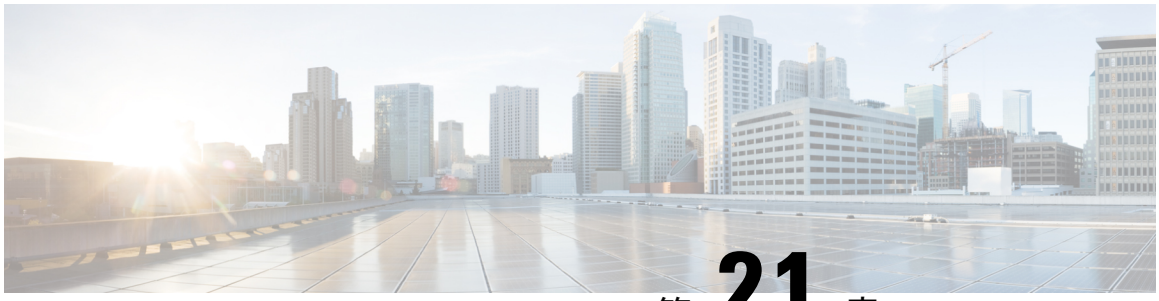
ステップ 2 [Add] をクリックします。

ステップ 3 パラメータを入力します。

- フィルタ名（Filter Name）：0 ～ 30 文字で名前を入力します。
- オブジェクト ID サブツリー（Object ID Subtree）：選択した SNMP フィルタに含まれるか除外される MIB ツリー内のノードを選択します。オブジェクトを選択するオプションは次のとおりです。
  - [Select from List]：MIB ツリー内を探索できます。上向き矢印を押すと選択したノードの親と兄弟のレベルに移動します。下向き矢印を押すと選択したノードの子のレベルまで下がります。1 つのノードからその兄弟に渡すには、ビューのノードをクリックします。兄弟をビューに移動するには、スクロール バーを使用します。
  - [オブジェクトID]：[フィルタに含める] オプションが選択されている場合にこのオプションを選択すると、入力したオブジェクト ID がビューに表示されます。

ステップ 4 [Include in filter] を選択または選択解除します。これを選択すると、選択した MIB はフィルタに含まれ、そうでないものは除外されます。

ステップ 5 [Apply] をクリックします。SNMP ビューが定義され、実行コンフィギュレーションが更新されます。



第 21 章

付録

この章は、次の項で構成されています。

スイッチのスタックの管理

スイッチは、単独で機能させることも、スイッチのスタックに接続することもできます。デフォルトで、デバイスはスタッカブルですが、スタックポートを備えていません。デフォルトでは、スイッチ上のすべてのポートがネットワークポートになっています。スタックポートのないスイッチは、それ自体だけによるスタック内のアクティブユニットと見なすことができます。また、スタックポートのないスイッチをスタンドアロンスイッチと見なすこともできます。複数のスイッチをスタックするには、スイッチ上で必要なネットワークポートをスタックポートとして再設定し、そのスタックポートを備えたスイッチをリングまたはチェーントポロジに接続します。

スタック内のスイッチ（ユニット）は、スタックポートを介して接続されます。その後、これらのスイッチは、単一の論理スイッチとして一括して管理されます。スタック ポートを Link Aggregation Group（LAG）のメンバーにすることによって、スタック ポートの帯域幅を増やすこともできます。

スタックは、単一のアクティブ/スタンバイと複数のメンバーのモデルに基づいています。スタックには次のような利点があります。

- ネットワーク容量を動的に拡張または縮小することができます。管理者は、ユニットを追加することで、スタック内のポート数を動的に増やしながら、一元管理を維持することができます。同様に、ユニットを除去して、ネットワーク容量を減らすことができます。
- スタック構成のシステムは、次の方法で冗長性をサポートしています。
  - スタンバイユニットは、元のアクティブユニットに障害が発生すると、そのスタックのアクティブユニットになります。
  - スタック システムは、チェーンとリングの 2 タイプのトポロジをサポートしています。リングトポロジでは、スタックポートのいずれかで障害が生じると、スタックはチェーントポロジとなり継続して機能します。
  - リング スタック内のポートでは、スタック ポート リンクのいずれかで障害が生じた場合のデータ パケット損失期間を短縮するために、ファスト スタック リンク フェールオーバーと呼ばれるプロセスがサポートされています。スタックが新しいチェーントポロジに回復するまで、スタック ユニットは、障害の生じたスタック構成ポートを介して送信されると想定されるパケットをループ バックし、ループ バックされたパケットを残りのスタック構成ポートを介して宛先へ送信します。ファスト スタック リンク フェールオーバーの間は、アクティブ/スタンバイユニットがアクティブのまま正常に機能しつづけます。

スタック内のユニットのタイプ

スタックは最大8つのユニットで構成されます。スタック内のユニットは、次のタイプのいずれかです。

- **アクティブ**：アクティブユニットの ID は、1 または 2 のいずれかにする必要があります。スタックは、それ自体を管理するアクティブユニット、スタンバイユニット、およびメンバーユニットを介して管理されます。
- **スタンバイ**：アクティブユニットに障害が発生すると、スタンバイユニットがアクティブロールを引き継ぎます（スイッチオーバー）。スタンバイユニットの ID は、1 または 2 のいずれかにする必要があります。
- **メンバー**：これらのユニットは、アクティブユニットによって管理されます。

ユニットのグループをスタックとして機能させるためには、アクティブ対応ユニットが存在している必要があります。アクティブ対応ユニットに障害が発生した場合、スタンバイユニット（アクティブロールを引き継ぐメインユニット）がある限り、スタックは機能し続けます。アクティブユニットに加えて、スタンバイユニットに障害が発生した場合、機能する唯一のユ

ニットはメンバーユニットです。これらも 1 分後に機能を停止します。これは、たとえば、1 分後に、アクティブユニットを使用せずに動作していたメンバーユニットの 1 つにケーブルをつないでもリンクが確立されないことを意味します。

スタック内のユニット数の下位互換性

スタック可能スイッチは、4 ユニットから 8 ユニットまでサポートします。これは、スイッチのモデルによって異なります。以前のソフトウェアリリースからのアップグレードは、構成ファイルを変更せずに実行できます。ハイブリッドスタックモードをサポートしていないファームウェアバージョンがスタックにロードされ、スタックが再起動されると、スタックはネイティブスタックモードに戻ります。ハイブリッドスタックモードのデバイスに、ハイブリッドスタックモードをサポートしていないファームウェアバージョンが読み込まれると、そのシステムモードはデフォルトのシステムモードに戻ります。スタックのユニット ID が手動で構成された場合、ID が 4 より大きいユニットは自動番号付与に切り替えられます。

スタックトポロジ

スタック内のユニットは、次のタイプのトポロジのいずれかで接続できます。

- チェーン トポロジ：各ユニットがネイバー ユニットに接続されているが、最初と最後のユニットの間にケーブル接続はありません。
- リング トポロジ：各ユニットがネイバー ユニットに接続されています。最後のユニットは、最初のユニットに接続されます。以下は、8ユニット スタックのリング トポロジを示しています。

リング トポロジの方が、チェーン トポロジより信頼性が高いです。リング内の 1 つのリンクの障害はスタックの機能に影響しませんが、一方、チェーン接続の 1 つのリンクの障害はスタックの分割を引き起こすことがあります。

トポロジディスカバリ

スタックは、トポロジディスカバリと呼ばれるプロセスによって確立されます。このプロセスは、スタック ポートのアップ/ダウン状態の変更によってトリガーされます。このプロセスをトリガーするイベントの例を次に示します。

- リングからチェーンへのスタック トポロジが変化する
- 2 つのスタックが 1 つのスタックにマージされる
- スタックが分割される
- 他のメンバーユニットがスタックに挿入される（たとえば、ユニットが障害のために、それ以前にスタックから切断されたため）。これは、チェーン トポロジで、スタックの中間のユニットで障害が生じた場合に発生することがあります。

トポロジディスカバリ中には、スタック内の各ユニットが、トポロジ情報を含むパケットを交換します。トポロジ ディスカバリ プロセスが完了すると、各ユニットには、スタック内のすべてのユニットのスタック マッピング情報が含まれます。

ユニット ID の割り当て

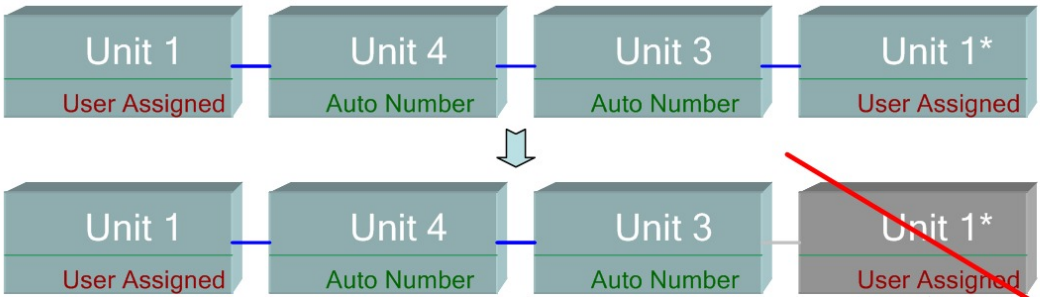
トポロジディスカバリが完了すると、スタック内の各ユニットに一意のユニット ID が指定されます。ユニット ID は、[System Mode and Stack Management] ページで、次の方法のいずれかで設定されます。

- **自動（Auto）**：ユニット ID は、トポロジディスカバリ プロセスによって指定されます。これがデフォルト設定です。
- **手動**：ユニット ID は、1 ～ 8 の整数に手動で設定されます。

重複ユニット ID

同じユニット ID を 2 つの個別のユニットに指定すると、それらの一方だけがそのユニット ID を使用してスタックに参加できます。自動番号付けを選択している場合、重複ユニットには、新しいユニット番号が指定されます。自動番号付けが選択されていない場合、重複ユニットはシャットダウンされます。2 つのユニットに手動で同じユニット ID が割り当てられたケースを以下に示します。ユニット 1 はスタックに参加せず、シャットダウンされます。アクティブ対応ユニット（1 または 2）の間のアクティブ選択プロセスで勝ち残れませんでした。

重複ユニットのシャットダウン



アクティブ選択プロセス

アクティブユニットは、マスター対応ユニット（1 または 2）から選択されます。アクティブユニットを選択する要因は、次の優先順位で考慮されます。

- [Force Active]：[Force Active] がユニットでアクティブになっている場合、そのユニットが選択されます。
- [System Up Time]：アクティブ対応ユニットは、10 分間のセグメント単位で測定される稼働時間を交換します。セグメント数が多いユニットが選択されます。両方のユニットが同じ時間セグメント数で、一方のユニットのユニット ID が手動で設定されていて、他方のユニットのユニット ID が自動的に設定されている場合は、手動定義のユニット ID を持つユニットが選択されます。それ以外の場合は、より小さいユニット ID を持つユニットが選択されます。両方のユニット ID が同じ場合は、最小の MAC アドレスを持つユニットが選択されます。

（注） スイッチ フェールオーバー プロセスでスタンバイユニットがアクティブとして選択されると、その稼働時間が保持されます。

- **ユニット ID**：両方のユニットの時間セグメント数が同じ場合、最小のユニット ID を持つユニットが選択されます。
- **MAC アドレス**：両方のユニット ID が同じ場合、最小の MAC アドレスを持つユニットが選択されます。

（注） スタックを動作させるためには、アクティブユニットが必要です。アクティブユニットは、アクティブの役割を引き受けるメインユニットとして定義されます。スタックには、アクティブ選択プロセスの後に、ユニット 1 およびユニット 2、またはどちらか一方が含まれている必要があります。そうしなかった場合は、スタックとそのすべてのユニットが、完全な電源オフとしてではなく、部分的にシャットダウンされますが、トラフィック通過機能は停止されます

スタックの変更

このセクションでは、スタックに変更を引き起こすことのあるさまざまなイベントについて説明します。次のいずれかの状況が発生すると、スタック トポロジが変更されます

- スタックとの間で1つまたは複数のユニットが接続されるか、切断される、またはその両方が発生する。
- スタック ポートのいずれかでリンクがアップまたはダウンする。
- スタックが、リング形態とチェーン形態の間で変化する。

スタックとの間でユニットが追加または削除されるか、その両方が発生した場合、トポロジの変更、マスター選択プロセス、および/またはユニット ID の割り当てがトリガーされます。

新しいユニットの接続

ユニットがスタックに挿入されると、スタック トポロジの変更がトリガーされます。ユニット ID が指定され（自動番号付けの場合）、ユニットはアクティブユニットによって設定されます。

既存のスタックに新しいユニットを接続すると、次のいずれかが発生することがあります。

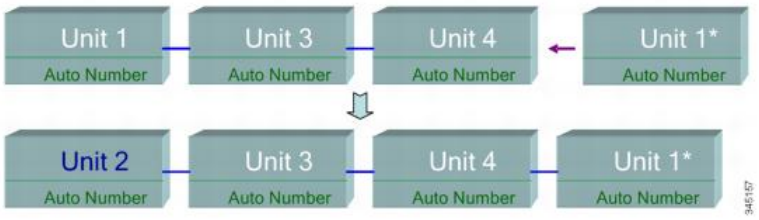
- 重複ユニット ID は存在しません。
  - ユーザ定義 ID を持つユニットが、自身のユニット ID を保持する。
  - 自動的に指定された ID を持つユニットが、自身のユニット ID を保持する。

- ファクトリー デフォルトのユニットは、使用可能な中で最小の ID で始まるユニット ID を自動的に受信する。

- 1 つ以上の重複ユニット ID が存在します。自動番号付けが、競合を解決し、ユニット ID を指定します。手動での番号付けの場合、1 つのユニットのみがそのユニット ID を保持し、その他はシャットダウンされます。
- スタック内のユニット数が、許可されるユニットの最大数を超えます。スタックに参加する新しいユニットはシャットダウンされ、SYSLOG メッセージが生成されて、マスターユニット上に表示されます

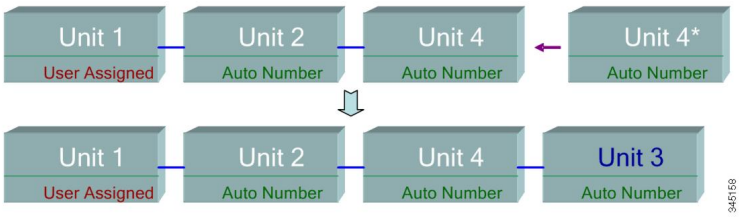
アクティブ対応ユニットがスタックに参加したときの自動番号付けの例を、以下に示します。ユニット ID が 1 の 2 つのユニットがあります。アクティブ選択プロセスでは、アクティブユニットとして最適なユニットが選択されます。最適なユニットは、10 分間のセグメントでより長い稼働時間を持つユニットです。その他のユニットは、バックアップとなります

自動番号付けされたアクティブ対応ユニット



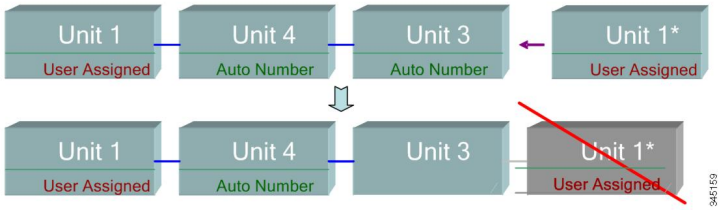
新しいユニットがスタックに参加したときの自動番号付与の例を以下に示します。既存のユニットはその ID を保持します。新しいユニットが使用可能な最小の ID を受け取ります。

自動番号ユニット



すでにユーザー指定されたユニット ID 1 のアクティブユニットが存在するスタックに、ユーザー指定のユニット ID 1 のアクティブ対応ユニットが参加したときに何が起きるかを、以下に示します。より新しいユニット 1 は、スタックに参加せず、シャットダウンされます。

ユーザー指定のアクティブ対応ユニット



スタック内のユニットの障害

アクティブユニットに障害が発生すると、スタンバイユニットがプライマリの役割を引き継ぎ、スタックは正常に動作しつづけます。

スタンバイスイッチがアクティブスイッチの代わりになることができるように、両方のユニットは常に予約された状態が維持されます。予約モードでは、アクティブスイッチとそのスタンバイスイッチがスタティック設定（スタートアップ コンフィギュレーション ファイルと実行コンフィギュレーション ファイルの両方に含まれる）と同期されます。スタンバイ スイッチ コンフィギュレーション ファイルは、前のアクティブスイッチに残ります。

STP 状態テーブル、動的に学習された MAC アドレス、動的に学習された SmartPort タイプ、MAC マルチキャスト テーブル、LACP、GVRP などのダイナミック プロセス状態情報は、同期されません。アクティブスイッチの設定中は、スタンバイユニットとすぐに同期されます。同期は、コマンドが実行されるとすぐに、実行されます。これは透過的です。

アクティブスイッチの設定中は、バックアップとすぐに同期されます。同期は、コマンドが実行されるとすぐに、実行されます。これは透過的です。

ユニットが動作中のスタックに挿入され、スタンバイユニットとして選択されると、アクティブスイッチはスタンバイユニットが最新の設定を保持できるようにそれと同期し、その後、SYNC COMPLETE SYSLOG メッセージを生成します。これは、スタンバイユニットとアクティブユニットが同一化したときにのみ表示される一意の SYSLOG メッセージで、次のように表示されます：%DSYNCH-I-SYNCH_SUCCEEDED: Synchronization with unit 2 is finished successfully.

アクティブ/スタンバイのスイッチオーバー

スタックのアクティブスイッチで障害が発生すると、スイッチオーバーが発生します。スタンバイユニットがアクティブとなり、そのプロセスとプロトコルスタックがすべて初期化され、スタック全体の責任を担います。その結果、このユニット内のトラフィック転送が一時的に中断されますが、メンバーユニットはアクティブのままです。

（注） STP が使用され、ポートのリンクがアップしている場合、STP ポートの状態は一時的に「ブロッキング」になり、トラフィックを転送したり、MAC アドレスを学習したりすることはできません。これによって、アクティブなユニット間のスパニング ツリー ループを防いでいます。

メンバーユニットの取り扱い

スタンバイユニットがアクティブスイッチになっている間、メンバーユニットはアクティブなままで、元のアクティブスイッチからの設定に基づいてパケットの転送を継続します。これにより、ユニット内でのデータ トラフィックの中断は最小限に抑えられます。スタンバイユニットがアクティブ状態への移行を完了したら、次の操作を実行することによって、メンバーユニットを一度に 1 つずつ初期化します。

- メンバーユニットの設定をクリアしてデフォルトにリセットします（新しいアクティブユニットからの間違った設定を回避するため）。その結果、メンバーユニットでのトラフィック転送が中断されます。
- 関連するユーザー設定をメンバーユニットに適用します。
- ポートの STP 状態、動的 MAC アドレス、アクティブユニットとメンバーユニットの間のリンク稼働/ダウンステータスといった動的情報を交換します。アクティブスイッチが STP に基づいてポートの状態を「転送中」に設定すると、メンバーユニットでのパケット転送が再開されます。

（注） MAC アドレスが学習または再学習されるまで、不明なユニキャスト MAC アドレスへのパケット フラッディングが発生します。

フェールオーバー後の元のアクティブユニットの再接続

フェールオーバー後に、元のアクティブスイッチが再接続されると、アクティブ選択プロセスが実行されます。元のアクティブスイッチ（ユニット 1）がアクティブユニットとして再選択されると、現在のアクティブスイッチ（元のバックアップユニットだったユニット 2）はリブートし、再度バックアップになります。

（注） アクティブユニットのフェールオーバー中も、スタンバイユニットの稼働時間は保持されます。

スタック内でのソフトウェアの自動同期

スタック内のすべてのユニットが同じソフトウェアバージョン（ファームウェアとブートコード）を実行する必要があります。スタック内の各ユニットは、実行しているファームウェアまたはブートコードが、アクティブユニットが実行しているものと異なっていた場合、自動的にアクティブユニットからファームウェアとブートコードをダウンロードします。ユニットは自動的に自身をリブートし、新しいバージョンを実行します。

スタック ポート

デフォルトでは、デバイス上のすべてのポートは、ネットワーク（アップリンク）ポートです。ユニットを接続するには、デバイスを接続するために使用するポートのタイプをスタックポートとして変更する必要があります。これらのポートは、ユニットの間でデータおよびプロトコル パケットを転送するために使用されます。

スタック ポート リンク アグリゲーション

隣接する2台のユニットが接続されている場合は、それらを接続しているスタック ポートが自動的にスタックLAGに割り当てられます。この機能によって、単一ポートの帯域幅を超えて、スタック ポートのスタック帯域幅を増やすことができます。ユニットあたり最大2つのスタック LAG を指定できます。

スタック LAG は、2 ～最大数（ユニット タイプに応じる）のスタック ポートで構成できます。

スタック ポートの状態

スタック ポートは、次のいずれかの状態になります。

- ダウン：ポートの動作状態がダウンであるか、またはスタック ポートの動作状態がアップであるが、そのポート上でトラフィックを渡すことができません。
- アクティブ：スタック ポートは、スタック ポートの動作状態がアップで、そのポートでトラフィックを渡すことができ、それがスタックLAGのメンバーであるスタックLAGに追加されました。
- スタンバイ：スタック ポートの動作状態がアップで、そのポートで双方向トラフィックを渡すことができるが、そのポートをスタック LAG に追加することはできず、そのポートはトラックを送信しません。ポートがスタンバイ状態になる考えられる理由は、次のとおりです。
  - 単一のネイバーと接続するために、異なる速度のスタック ポートが使用された。

下位互換性

次のモードは、デバイスの現在のソフトウェアバージョンで拡張されています。以前のソフトウェアバージョンでこれらの機能を使用する場合は、注意が必要です。

- **スタックポート LAG**：ソフトウェアがLAGのスタックポートをサポートしているユニットが、ソフトウェアがLAGのスタックポートをサポートしていないユニットに接続されている場合、ユニットを接続しているスタックポートはスタック LAG のメンバーにはなりません。ユニットはスタックポートを介して接続され、アクティブなスタックユニットはソフトウェアを他のユニットにコピーします。コピーされるソフトウェアは、アクティブユニットになるユニットによって異なります。
- **キューモード**：このモードは、4つのQoSキューから8つのQoSキューに変更できます。4キューモードが現在のソフトウェアバージョンのデフォルトキューモードであるため、

8 キューをサポートしていなかった以前のソフトウェアバージョンからアップグレードしても問題はありません。しかし、キューモードを 8 キューに変更するときは、その新しいキューモードで必要な QoS 目標を満たすように設定を調べて調整する必要があります。キューモードの変更は、システムのリブート後に有効になります。新しいキューモードと競合するキュー関連の設定は拒否されます。

- **スタッキングモード**：ハイブリッド スタッキング モードを含むようにスタッキングモードが拡張されました。デバイスは既存のスタッキングモード（ネイティブ スタッキング モード）で起動するため、以前のソフトウェアバージョンからアップグレードしても問題はありません。ハイブリッドスタッキングモードで構成されたデバイスから、ハイブリッドスタッキングをサポートしないソフトウェアバージョンにソフトウェアをダウングレードする場合は、最初にデバイスをネイティブ スタッキング モードに構成します。

スタック LAG の物理的な制約

- スタック LAG には、同じ速度のポートを含める必要があります。
- トポロジがリング/チェーンでないスタックにユニットを接続しようとすると（たとえば、1 つのユニットを 3 つ以上のネイバー ユニットに接続しようとする - スター トポロジ）、2 つのスタック LAG のみがアクティブになり、残りのスタック ポートはスタンバイ モード（非アクティブ）に設定されます。

ポート速度の自動選択

ケーブルがポートに接続されると、スタック構成ケーブル タイプが自動的に検出されます（自動検出はデフォルト設定）。システムはスタック ケーブル タイプを自動的に特定し、そのケーブルとポートでサポートされている最高速度を選択します。

ケーブル タイプが認識されない場合は、SYSLOG メッセージ（情報レベル）が表示されます。

リンク集約

概要

Link Aggregation Control Protocol（LACP）は、IEEE（802.3az）規格に含まれており、複数の物理ポートをまとめて 1 つの論理チャネル（LAG)にすることを可能にします。LAG は、帯域幅を増大させ、ポートの柔軟性を高め、2 つのデバイス間にリンク冗長性を提供します。リンク集約を使用すると、2 つのネットワークデバイス間にある複数のイーサネットリンクを 1 つのリンクに結合できます。最も一般的な組み合わせは、スイッチの、別のスイッチ、サーバー、ネットワーク接続ストレージ （NAS）デバイス、またはマルチポート WiFi アクセスポイントへの接続などです。

ネットワークデバイスと管理機能は、複数のイーサネット接続のリンク集約グループ（LAG）を 1 つのリンクとして扱います。たとえば、仮想ローカルエリアネットワーク（VLAN）に LAG を含めることができます。同じスイッチに複数の LAG を設定することも、同じ LAG に

複数のイーサネットリンクを追加することもできます（LAG あたりのリンクの最大数はデバイスによって異なります）。

一部のネットワークデバイスは、リンク集約セットアッププロセスでのエラーの防止に役立つ Link Aggregation Control Protocol（LACP）をサポートしています。

リンク集約の利点

リンク集約には、次の利点があります。

- 信頼性と可用性の向上：LAG 内のいずれかの物理リンクがダウンした場合、トラフィックは別の物理リンクに再割り当てされます。
- 物理リソースの有効活用：物理リンク全体へのトラフィックのロードバランシングが可能です。
- 帯域幅の増加：集約された物理リンクにより、個別のリンクよりも高い帯域幅が提供されます。
- コスト効率の改善：特に新しいケーブル配線が必要である場合、物理ネットワークのアップグレードには大きな費用がかかる可能性があります。リンク集約により、新しい機器を必要とせずに帯域幅を高めることができます。

リンク集約のセットアップ

次の手順では、ネットワーク内の2つのデバイス間でリンク集約をセットアップする方法について簡単に説明します。

ステップ 1 両方のデバイスがリンク集約をサポートしていることを確認します。

ステップ 2 2 つのデバイスのそれぞれでリンク集約グループ（LAG）を設定します。

ステップ 3 各デバイスで作成した LAG のポート速度、デュプレックスモード、フロー制御、および MTU サイズの設定が同じであることを確認します。

ステップ 4 LAG のメンバーであるすべてのポートが同じ仮想ローカルエリアネットワーク (VLAN) メンバーシップを持つことを確認します。LAG を VLAN に追加する場合は、最初に LAG をセットアップし、その LAG を VLAN に追加します。個別のポートを追加しないでください。

警告 各デバイスでLAGをセットアップするまでは、複数のイーサネットケーブルを使用してデバイスを相互に接続しないでください。2 つのデバイス間に複数の接続を形成し、どちらのデバイスにもループ防止機能がない場合、ネットワークループが形成されます。ネットワークループにより、ネットワークでの通常のトラフィックが遅くなる、または停止する可能性があります。

ステップ 5 LAGを追加する各デバイスのポートをメモして、正しいポートに接続していることを確認します。ポートメンバーのポート速度、デュプレックスモード、または MTU サイズの設定が異なる場合や、LAG のメンバーではないポートを間違って接続した場合は、LAG によってアラートが生成され、設定が拒否されます。

ステップ 6 イーサネットまたはファイバケーブルを使用して、各デバイスで LAG に追加したポートを接続します。

ステップ 7 各スイッチで接続された各ポートのポート LED が緑色で点滅していることを確認します。

ステップ 8 各デバイスの管理インターフェイスで、リンクが稼働状態であることを確認します。

LAG のロードバランシングの設定

ステップ 1 **ユーザー名**と**パスワード**を入力してシスコのスイッチにログインします。[Log In] をクリックします。デフォルトでは、ユーザー名とパスワードは*cisco*ですが、既存のネットワークで作業しているため、独自のユーザー名とパスワードが必要です。代わりにそれらのログイン情報を入力してください。

ステップ 2 [Port Management] > [LAG Management] の順に移動し、[Load Balance Algorithm] オプションを選択します。[MAC Address] または [IP/MAC Address] のいずれかを選択できます。[Apply] をクリックします。

（注） デフォルトでは、[MAC Address] は、[Load Balance Algorithm] に対して選択されるオプションです。

ステップ 3 次に、画面に成功通知が表示されます。[File Operations] をクリックしてスイッチの設定をスタートアップコンフィギュレーションに保存します。

ステップ 4 [File Operations] ページが開きます。[Running Configuration] で [Source File Name] が選択され、[Startup Configuration] で [Destination File Name] が選択されていることを確認します。[Apply] をクリックして、設定を保存します

UDLD

概要

Unidirectional Link Detection（UDLD）は、単方向リンクを有効にするため、光ファイバまたはツイストペア イーサネット ケーブルを介して接続されたデバイスを有効にするレイヤ 2 プロトコルです。隣接するデバイスが送信したトラフィックをローカルデバイスが受信するにもかかわらず、ローカルデバイスから送信されたトラフィックをネイバーが受信しない場合には、常に単一方向リンクが発生します。

UDLD の目的は、ネイバーがローカル デバイスからのトラフィックを受信しないポート（単方向リンク）を検出して、そのようなポートをシャットダウンすることです。プロトコルが単方向リンクを正しく検出するには、接続されているすべてのデバイスで UDLD をサポートする必要があります。ローカル デバイスのみが UDLD をサポートしている場合、このデバイスがリンクのステータスを検出することはできません。この状況では、リンクのステータスは未定義に設定されます。ユーザは、未定義の状態でポートがシャットダウンされるようにするか、それとも単に通知がトリガーされるようにするかどうかを設定できます。

UDLD の機能

ポートで UDLD を有効にすると、次のアクションが実行されます。

- UDLD は、ポートで検出状態を開始します。
  - この状態で、UDLD は、すべてのアクティブなインターフェイスで、すべてのネイバーに定期的にメッセージを送信します。これらのメッセージには、既知のネイバーすべてのデバイス ID が含まれます。これらのメッセージは、ユーザ定義のメッセージ時間に従って送信されます。
- UDLD は、隣接するデバイスから UDLD メッセージを受信します。これらのメッセージは、有効期限（メッセージ時間の 3 倍）が切れるまでキャッシュされます。有効期限の前に新しいメッセージが受信されると、以前のメッセージの情報が新しいメッセージの情報に置き換えられます。
- 有効期限が切れると、デバイスは、受信した情報を使用して次の操作を実行します。
  - ネイバー メッセージにローカル デバイス ID が含まれている場合：ポートのリンク ステータスが双方向に設定されます。
  - ネイバー メッセージにローカル デバイス ID が含まれていない場合：ポートのリンク ステータスが単一方向に設定され、ポートがシャットダウンされます。
- 有効期限の時間内に、隣接するデバイスからの UDLD メッセージが受信されない場合、ポートのリンク ステータスが未定義になり、次のいずれかが発生します。
  - デバイスが通常の UDLD モードの場合：通知が発行されます。
  - デバイスがアグレッシブ UDLD モードの場合：ポートがシャットダウンします。

インターフェイスが双方向または未定義の状態になっている間、デバイスは、メッセージ時間（秒）ごとに定期的にメッセージを送信します。前述の手順が繰り返し実行されます。

使用上のガイドライン

シスコは、UDLD がサポートされていないか無効になっているデバイスに接続されているポートで UDLD を有効にすることを推奨しません。UDLD をサポートしていないデバイスに接続されたポートで UDLD パケットを送信すると、ポートで利点のないトラフィックの増大が発生します。

加えて、UDLD の設定時に次の点を考慮してください。

- 単一方向リンクを持つポートをシャットダウンする緊急度に従って、メッセージ時間を設定します。メッセージの時間が短いほど、より多くの UDLD パケットが送信および分析されますが、リンクが単一方向である場合、ポートがより早くシャットダウンされます。
- UDLD を銅線ポートで有効にする場合、ポートごと有効にする必要があります。UDLD をグローバルに有効にする場合、光ファイバ ポートのみで有効にできます。
- ポートをシャットダウンしない場合には、リンクが単一方向であることが明らかでない限り、UDLD モードを通常に設定します。
- 単一方向リンクと双方向リンク両方の損失を求める場合、UDLD モードをアグレッシブに設定します。

Smartport の概要

SmartPort 機能は、共通の設定を保存および共有するのに便利です。同じ SmartPort マクロを複数のインターフェイスに適用すると、インターフェイスは共通設定を共有します。Smartport マクロは、CLI（コマンドライン インターフェイス）コマンドのスクリプトです

マクロ名、またはマクロに関連付けられている SmartPort タイプによって、Smartport マクロをインターフェイスに適用できます。マクロ名による SmartPort マクロの適用は、CLI でのみ実行できます。

Smartport タイプごとに、Smartport マクロをインターフェイスに適用する 2 種類の方法があります。

- 静的 SmartPort：インターフェイスに SmartPort タイプを手動で割り当てます。その結果、対応する SmartPort マクロがインターフェイスに適用されます。
- Auto Smartport：Auto Smartport では、インターフェイスにデバイスが接続された時点で、コンフィギュレーションが適用されます。インターフェイスからデバイスが検出されると、接続デバイスの Smartport タイプに対応する Smartport マクロ（指定されている場合）が自動的に適用されます。

Smartportは、組み込み（またはユーザー定義）マクロを適用できるインターフェイスです。これらのマクロは、通信要件をサポートし、さまざまなタイプのネットワーク デバイスの機能を活用するようにデバイスを迅速に設定するための手段をもたらすように設計されています。ネットワーク アクセス要件および QoS 要件は、インターフェイスが IP phone、プリンタ、またはルータやアクセス ポイント（AP）に接続されているかどうかによって異なります。

VLAN Description

各 VLAN には、1 ～ 4094 の範囲の値を持つ VLAN ID（VID）が設定されています。VLAN のメンバーは、VLANにデータを送受信できるブリッジ型ネットワーク内のデバイスのポートです。VLAN に送信されるそのポート宛のすべてのパケットが VLAN タグを付けられていない場合、ポートは VLAN のタグなしメンバーとなります。VLAN に送信されるそのポート宛のすべてのパケットが VLAN タグを付けられている場合、ポートは VLAN のタグ付きメンバーとなります。ポートは 1 つのタグなし VLAN にのみ属することができますが、複数のタグ付き VLAN に属することができます。

VLAN アクセスモードでは、1 つのポートは、1 つの VLAN にしか属せません。ポートが全般またはトランクモードの場合、1 つまたは複数の VLAN のメンバーになれます。VLAN は、セキュリティとスケーラビリティの問題を解決するために使用されます。VLAN トラフィックはVLAN内に留まり、VLANデバイスで終了します。また、物理的な再配置を必要とせずにデバイスを概念的にリンクすることにより、ネットワーク構成を簡素化します。

VLAN タグ付きフレームの場合、4 バイトの VLAN タグが各イーサネットフレームに適用されます。タグは、1 ～ 4094 の範囲の VLAN ID と、0 ～ 7 の範囲の VLAN 優先度タグ（VPT）で構成されます。フレームが VLAN 対応デバイスに入るときに、フレーム内の 4 バイトの VLAN

タグが、VLAN に属しているものとして、分類に使用されます。フレームに VLAN タグがない、またはパケットに優先順位タグしかない場合、フレームは、フレームを受信した入力ポートで定義されている PVID（ポート VLAN ID）に基づいて VLAN に分類されます。入力のフィルタリングが有効になっていて、入力ポートがパケットの属する VLAN のメンバーではない場合、フレームは入力ポートでドロップされます。VLAN タグの VID が 0 の場合のみ、フレームは優先タグ付きと見なされます。VLAN に属するフレームは VLAN に留まります。

これは、対象 VLAN の出力ポートのメンバーにのみフレームが送信または転送されることで実現されます。VLAN の出力ポートは、タグ付きまたはタグなしのいずれかにすることができます。

出力ポートの役割は次のとおりです。

- 出力ポートが対象 VLAN のタグ付きメンバーであり、元のフレームに VLAN タグがない場合、出力ポートはフレームに VLAN タグを追加します。
- 出力ポートが対象 VLAN のタグなしメンバーであり、元のフレームに VLAN タグが付いている場合、VLAN タグはフレームから削除されます。

VLAN の役割

レイヤ 2 は、VLAN が機能する場所です。すべての VLAN トラフィック（ユニキャスト、ブロードキャスト、およびマルチキャスト）は、VLAN 内に含まれます。イーサネット MAC レイヤでは、個別の VLAN に接続されているデバイスは直接接続できません。レイヤ 3 ルータだけが、異なる VLAN からのデバイスを相互に対話できるようにします。各 VLAN が IP サブネットを表す場合、それらの間で IP トラフィックをルーティングするために IP ルータが必要です。

IP ルータは、各ポートに接続されている VLAN が 1 つだけの標準ルータである可能性があります。標準 IP ルータとの間の VLAN タグなしトラフィックが必要です。各 IP ルータのインターフェイスは 1 つまたは複数の VLAN に接続でき、VLAN 認識型 IP ルータとすることができます。VLAN 認識型 IP ルータで送受信されるトラフィックは、VLAN タグ付きまたはタグなしのいずれも可能です。

隣接する VLAN 認識型デバイスは Generic VLAN Registration Protocol（GVRP）を使用して VLAN 情報を通信します。したがって、VLAN 情報は、ブリッジ化ネットワークを介して伝達されます。デバイスで交換される GVRP 情報に基づいて、VLAN 上のデバイスは静的にも動的にも作成できます。VLAN は静的にも動的にもできますが（GVRP に基づき）、同時に両方にはできません。GVRP の詳細については、「GVRP 設定」の項を参照してください。

QinQ

QinQ は、サービス プロバイダー ネットワークと顧客ネットワーク間の分離を提供します。デバイスは、ポートベースの c タグ付きサービスインターフェイスをサポートするプロバイダーブリッジとなります。

QinQ では、デバイスは、プロバイダーネットワークに転送するパケットに、サービスタグ（S タグ）と呼ばれる ID タグを追加します。S タグはさまざまな顧客間のトラフィックを分離するために使用されますが、顧客の VLAN タグも維持されます。

顧客のトラフィックは、それがcタグ付きまたはcタグなしのいずれであっても、TPID 0x8100のSタグ付きでカプセル化されます。Sタグにより、このトラフィックはプロバイダーブリッジネットワーク内で集合体として扱われます。この場合、ブリッジ処理はSタグVID（S-VID）のみに基づいて行われます。

Sタグは、トラフィックがネットワーク サービス プロバイダーのインフラストラクチャを介して転送されている間は保持され、後に出力デバイスにより削除されます。

QinQの他の利点として、お客様のエッジ デバイスでの設定は不要です。

プライベート VLAN

プライベートVLAN機能は、ポート間でのレイヤ2の分離を提供します。つまり、IPルーティングとは異なり、ブリッジング トラフィックのレベルで、同じブロードキャスト ドメインを共有するポートが相互に通信することはできません。プライベート VLAN 内のポートはレイヤ2ネットワークの任意の場所に配置できます。よって、これらのポートは同じスイッチ上にある必要はありません。プライベートVLANは、タグなしまたは優先順位タグ付きトラフィックを受信し、タグなしトラフィックを送信するように設計されています。

次の種類のポートはプライベート VLAN のメンバーにできます。

- プロミスキャス：無差別ポートは、同じプライベート VLAN のすべてのポートと通信できます。これらのポートは、サーバとルータに接続します。
- コミュニティ（ホスト）：コミュニティ ポートは、同じレイヤ2ドメインのメンバーであるポートのグループを定義できます。これらはレイヤ 2 で他のコミュニティおよび隔離ポートから分離されます。これらのポートは、ホスト ポートに接続します。
- 隔離（ホスト）：隔離ポートは、同じプライベート VLAN 内の他の隔離ポートおよびコミュニティ ポートからレイヤ 2 で完全に分離されます。これらのポートは、ホスト ポートに接続します。

プライベート VLAN には次の種類があります。

- プライマリ VLAN：プライマリ VLAN は、無差別ポートから隔離ポートおよびコミュニティ ポートにレイヤ 2 で接続する場合に使用します。プライベート VLAN ごとに、プライマリ VLAN が 1 つだけ使用できます。
- 隔離 VLAN（セカンダリ VLAN とも呼ばれる）：隔離 VLAN は、隔離ポートがプライマリ VLAN にトラフィックを送信する場合に使用します。プライベート VLAN ごとに、隔離 VLAN が 1 つだけ使用できます。
- コミュニティ VLAN（セカンダリ VLAN とも呼ばれる）：VLAN 内のポート（コミュニティ）のサブグループを作成するには、ポートをコミュニティ VLAN に追加する必要があります。コミュニティ VLAN は、コミュニティ ポートから、無差別ポートおよび同じコミュニティのコミュニティ ポートにレイヤ 2 で接続する場合に使用します。コミュニティごとに 1 つのコミュニティ VLAN が使用でき、複数のコミュニティ VLAN が同じプライベート VLAN のシステム内で共存できます。

ホスト トラフィックは隔離 VLAN とコミュニティ VLAN 上で送信されますが、サーバとルータのトラフィックは、プライマリ VLAN 上で送信されます。

共有 MAC アドレス ラーニングは、同じプライベート VLAN のメンバーであるすべての VLAN 間に存在します（ただしスイッチは独立した VLAN ラーニングをサポートします）。これによりユニキャスト トラフィックが有効になり、ホスト MAC アドレスが隔離 VLAN およびコミュニティ VLAN により学習されるのに対し、ルータとサーバの MAC アドレスはプライマリ VLAN により学習されます。

プライベート VLAN のポートは、1 つのプライベート VLAN にのみ追加できます。アクセスまたはトランク ポートなどの他の種類のポートは、プライベート VLAN を構成する個々 の VLAN に追加できます（これらは通常の 802.1Q VLAN であるため）。

プライベート VLAN は、異なるスイッチのポート間でトランク ポートを設定し、これらをプライベート VLAN 内のすべての VLAN に追加することで、複数のスイッチ経由で拡張するように設定できます。スイッチ間のトランク ポートは、プライベート VLAN のさまざまな VLAN（プライマリ、隔離、およびコミュニティ）のタグ付きトラフィックを送受信します。

スイッチでの VLAN の設定

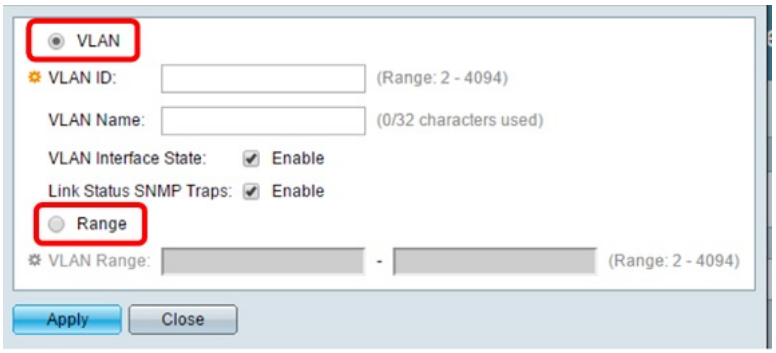
仮想ローカルエリアネットワーク（VLAN）を作成することで、スイッチ上で個別のブロードキャストドメインを設定できます。ブロードキャストドメインは、ルータなどのレイヤ 3 デバイスを使用して、互いに関連付けることができます。VLAN は、ホストの物理的な配置場所に関係なく、ホスト間でグループを形成するために主に使用されます。したがって、VLAN はホスト間にグループを形成することでセキュリティを向上させます。VLAN を作成しても、その VLAN が少なくとも 1 つのポートに手動で、または動的に接続されるまでは何の効果もありません。VLAN を設定する最も一般的な理由の 1 つは、音声用の VLAN と、データ用の VLAN を個別に設定するためです。そうすることで、同じネットワークを使用していても、両方のタイプのデータのパケットが送信されます。

VLAN の作成

ステップ 1 Web ベースのユーティリティにログインし、[VLAN Management] > [VLAN Settings] の順に選択します。

ステップ 2 [VLAN Table] エリアで、[Add] をクリックして新しい VLAN を作成します。

ステップ 3 次の図に示されているオプションのように、VLAN は 2 つの異なる方法で追加できます。目的の方法に対応するオプションボタンを選択します。



- [VLAN]：特定の VLAN を作成するには、この方法を使用します。
- [Range]：一定範囲の VLAN を作成するには、この方法を使用します。

ステップ 4 手順 3 で [VLAN] を選択した場合は、[VLAN ID] フィールドに VLAN ID を入力します。有効な範囲は 2 ～ 4094 です。

ステップ 5 [Vlan Name] フィールドに VLAN の名前を入力します。この例では、VLAN 名は「Accounting」です。最大で 32 文字を使用できます。

ステップ 6 VLAN インターフェイス状態を有効にするには、[VLAN Interface State] チェックボックスをオンにします（デフォルトでオンになっています）。有効にしないと、VLANは事実上シャットダウンされ、そのVLANを介した送受信は不可能になります。

ステップ 7 SNMP トラップの生成を有効にする場合は、[Link Status SNMP Traps] チェックボックスをオンにします。この設定はデフォルトでイネーブルになっています。

ステップ 8 手順 3 で [Range] を選択した場合は、[VLAN Range] フィールドに VLAN の範囲を入力します。有効な範囲は 2 ～ 4094 です。この例では、VLAN の範囲は 3 ～ 52 です。

（注） 一度に最大100個のVLANを作成できます。

ステップ 9 [Apply] をクリックします。

GVRP の設定

GVRP は COS スイッチでのみサポートされます。GVRP は、802.1Q トランクポートでのみ動作し、主に、トランキングスイッチ間を通過する必要がない VLAN からのトラフィックをプルーニングするために使用されます。GVRPを設定するには、次の手順を実行します。ポートが全般モードのままである状態を確保するために、GVRPに参加している各インターフェイスで、Smartport マクロ自動実行を無効にすることを強くお勧めします。

ステップ 1 目的の VLAN でスイッチを設定します。たとえば、次のように設定することができます。

- スイッチ 1 に、VLAN ID 1 をデフォルトとして割り当て、次に 300、400、および 500 を割り当てることができます。
- スイッチ 2 に、VLAN ID 1 をデフォルトとして割り当てることができます。
- スイッチ 3 に、VLAN ID 1 をデフォルトとして割り当て、次に 100 および 200 を割り当てることができます。

ステップ 2 インターフェイスで GVRP を有効にするには、全般モードで設定する必要があります。全般モードで設定しないと、スイッチは GARP メッセージを送信しません。

ステップ 3 GVRP をグローバルにイネーブルにします。デフォルトでは、スイッチに対して GVRP が有効になっていません。GVRP 動作用に 802.1Q ポートを設定する前に、まず、スイッチでGVRP を有効にする必要があります。

ステップ 4 802.1Q 動作用にポートを設定します。GVRP は、802.1Q トランキング用に設定されたポートでのみ動作します。

ステップ 5 ポートの GVRP を設定します。GVRP は、トランクの両側で正しく動作するように設定する必要があります。

ステップ 6 （任意）ポートの登録モードを設定します。デフォルトでは、GVRP ポートは **normal** 登録モードです。これらのポートは、近接スイッチからの GVRP Join メッセージを使用して、802.1Q トランクリンクで動作する VLAN をプルーニングします。相手側のデバイスが GVRP メッセージを送信できない場合やスイッチに VLAN をプルーニングさせたくない場合は、**fixed** モードを使用します。fixed モードのポートは、スイッチデータベースに存在するすべての VLAN に転送します。**forbidden** モードのポートは、VLAN 1 にのみ転送します。

音声 VLAN の設定

このトラブルシューティングのヒントは、音声 VLAN の設定に関するものです。

ステップ 1 スイッチ上で VLAN を作成します。たとえば、データ VLAN が 2 に設定され、音声 VLAN が 5 に設定されている場合は、[Auto Voice VLAN] タブで VLAN 5 を割り当てます。

ステップ 2 動作中の音声 VLAN が 5 に設定されていることを確認します。

ステップ 3 表示モードを**基本モード**から**拡張モード**に変更します。

ステップ 4 次に、[VLAN Management] の [Interface Settings] で、ポートモードを [Access] から [Trunk] に変更します。

ステップ 5 次に、[Port to VLAN Membership] で、IP フォンに接続されているポートについて、データ VLAN をタグなしとして設定し、音声 VLAN をタグ付きとして設定します。IP フォンに接続されているデスクトップおよびラップトップについても同じ手順を実行してください。

ステップ 6 [IP configuration] > [IPv4 Interface] の順に移動し、VLAN 2 と VLAN 5 の両方に IP を割り当てます。

ステップ 7 デバイスで DHCP サーバーが有効になっている場合に備えて、両方の VLAN 用に DHCP プールを作成します。（任意）

ステップ 8 [Smart port] タブに移動し、スマートポートが有効になっていることを確認します。

ステップ 9 [Device Detection] で、[IP Phone+Desktop] チェックボックスがオンになっていることを確認します。

ステップ 10 [Smartport Type] 設定に移動し、[IP Phone+Desktop] に関して [Macro] を選択します。

ステップ 11 [Edit] をクリックします。[Macro Type] で [Built-in Macro] が選択されていることを確認してください。

ステップ 12 [Macro Parameters] を変更します。

- [Parameter2] の値をデータ VLAN ID の値（今回はデータ VLAN が 2 であるため 2）に変更します。
- [Auto voice VLAN settings] で動作中の音声 VLAN が 5 と表示される場合は、[Parameter3] の値が自動的に 5 になります。

ステップ 13 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

音声 VLAN の削除

（注） 音声 VLAN を削除できず、「**VLAN xxx cannot be deleted because it is used as the agreed Voice VLAN**」というエラーメッセージが表示される場合は、**音声 VLAN** の動作が原因です。シスコのスイッチのファームウェア **2.5.5.x** 以前の場合、デフォルトでは [triggered auto voice VLAN] オプションが [enable] 設定されています。スイッチが他のスイッチから VSDP パケットを受信するか UC ルータから CDP パケットを受信すると、音声 VLAN が自動的に有効になります。

何らかの理由で**音声 VLAN** を削除する場合は、正常に削除するための一連の手順に従う必要があります。GUI を使用して、次の手順を実行してください。

ステップ 1 [VLAN Management] > [Voice VLAN] > [Properties] の順に選択し、[Dynamic Voice VLAN] を [Disable] に設定します。

ステップ 2 [VLAN Management] > [Voice VLAN] > [Properties] の画面で、[Voice VLAN Id] を [1] に設定します（これにより、セットアップで使用された音声 ID が削除され、値がデフォルトの 1 に設定されます）。

ステップ 3 [VLAN Management] > [VLAN Settings] に戻り、**音声 VLAN** として使用されていた VLAN を削除します。

（注） ただし、[Dynamic Voice VLAN] を再度有効にすると、削除した VLAN が自動的に再作成され、**音声 VLAN** として設定されます。

リンクフラッピングのトラブルシューティング

このトラブルシューティングのヒントは、Cisco Business スイッチのリンクフラッピングの問題を解決するために役立ちます。

（注） スタック構成のスイッチ間、または別のスイッチとのアップリンクを持つスイッチ間でリンクフラッピングが発生した場合は、次の手順に従って問題を解決してください。

ステップ 1 両方のスイッチが最新バージョンのファームウェアにアップグレードされていることと、両方のスイッチが同じファームウェアを実行していることを確認します。

ステップ 2 [Administration] > [Discovery-Bonjour] > [Disable] をクリックして、Bonjour プロトコルの検出を無効にします。

ステップ 3 [Port Management] > [Green ethernet] > [Properties] > [802.3 Energy Efficient Ethernet (EEE)] > [Disable] をクリックして、両方のスイッチで **EEE**（Energy Efficient Ethernet）を無効にします。

ステップ 4 [Port Management] > [Error Recovery] をクリックして、両方のスイッチで [Link Flap Prevention] を有効にします。[Link Flap Prevention] の [Enable] チェックボックスをオンにして有効にしてください。

ステップ 5 手順 1 ～ 4 を実行しても問題が解決しない場合は、**LLDP** を無効にします。[Administration] > [Discovery-LLDP Properties] > [LLDP Status] > [Disable] の順にクリックします。

手順 1 ～ 5 を実行してもリンクフラッピングを解決できない場合は、アップリンク/スタック構成に使用されているポートですべてのポートを削除します。

重要：スタック構成の場合は、スタック構成からポートを削除し、再設定する必要があります。

リンクフラップの識別

リンクフラップとは、スイッチ上の物理インターフェイスが継続的に稼働とダウンを繰り返す（1 秒間に 3 回以上、少なくとも 10 秒間）状態です。一般的な原因は通常、不良、サポート対象外、または非標準のケーブルや Small Form-Factor Pluggable（SFP）に関連しているか、その他のリンク同期に関する問題に関連しています。リンクフラップの原因は、断続的ものである場合と永続的なものである場合があります。

リンクフラップは物理的な干渉になりやすいため、ここでは、これを診断および防止するために実行できる手順について説明します。

ステップ 1 ケーブルとモニターの変更を試みます。問題が解決しない場合は、手順 2 に進みます。

ステップ 2 [Status and Statistics] > [Diagnostics] > [Copper Test] の順に移動します。

ステップ 3 ドロップダウンメニューからポートを選択し、[Copper Test] をクリックします。

ステップ 4 警告が表示されます。ポートが短時間シャットダウンされることに注意してください。[OK] を選択します。

ステップ 5 テスト結果が表示されます。「OK」と表示されるときは、多くの場合、ケーブルが原因ではありません。「OK」以外が表示される場合は、ケーブルを変更し、銅線テストを繰り返して、ケーブルが原因ではないことを確認します。

トポロジの分析

スイッチでの設定の問題ではなく物理的な問題であることを確認するには、スイッチに接続されているデバイスを分析する必要があります。次の点をチェックします。

1. スイッチに接続されているデバイスは何ですか。
   - スイッチに接続されている各デバイスを分析します。これらのデバイスで問題が発生したことはありますか。
2. どのポートが問題の原因で、どのデバイスがそれらのポートに接続されていますか。
   - 別のデバイスを接続してポートをテストし、問題が続くかどうかを確認します。
   - デバイスの別のポートが問題の原因になっているかどうかを確認します。
3. それはポートですか、それともデバイスですか。

- それがポートなのかデバイスなのかを判断することで、トラブルシューティング プロセスを続行する方法が決まります。
- それがデバイスである場合は、そのデバイスのサポート管理に連絡する必要がある場合があります。
- それがポートであると判断した場合は、問題が設定または物理的な問題に関連しているかどうかを確認します。

リンクフラップ防止の設定

リンクフラップ防止機能により、リンクフラップの発生によるスイッチおよびネットワーク動作の中断を最小限に抑えることができます。過剰なリンクフラップイベントが発生しているポートを *err-disable* に自動的に設定することにより、ネットワークトポロジが安定します。このメカニズムにより、フラッピングの根本原因をデバッグして特定するための時間も提供されます。リンクフラップおよびポートシャットダウンに関するアラートとして、Syslog メッセージまたは Simple Network Management Protocol（SNMP）トラップが送信されます。ユーザーまたはシステム管理者が明示的に有効にした場合にのみ、インターフェイスが再びアクティブになります。

ステップ 1 スイッチの Web ユーザーインターフェイス（UI）にログインします。

ステップ 2 **拡張モード**に変更します。

ステップ 3 [Port Management] > [Port Settings] の順に移動します。

ステップ 4 [Link Flap Prevention] の [Enable] チェックボックスをオンにします。[Apply] を押します。

ステップ 5 [Save] をクリックして設定を保存します。

スパニングツリー プロトコル

スパニングツリープロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークの正常な動作を実現するには、どの 2 つのステーション間でもアクティブ パスを 1 つにする必要があります。エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。

STP は、スパニングツリーアルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを 1 つ選択します。スパニングツリーアルゴリズムは、アクティブトポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチドレイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートが指定ポートの役割またはバックアップポートの役割にであるようなスイッチはルートスイッチです。少なくとも 1 つのポートに役割が指定されているスイッチは、指定スイッチを意味します。

STP は、ネットワーク上のエンドステーション間に一意のパスを作成し、それによってループをなくすことで、スイッチと相互接続リンクの配置においてツリー トポロジを提供します。

デバイスは、次のスパニング ツリー プロトコルのバージョンをサポートしています。

- 従来の STP：任意の 2 台のエンドステーション間に 1 本のパスが生成されるため、ループが解消されます。
- 高速 STP（RSTP）：ネットワークトポロジを検出し、スパニングツリーのより高速なコンバージェンスを提供します。これは、ネットワーク トポロジが自然にツリー構造化され、そのため、より高速なコンバージェンスが可能な場合に、最も効果的です。RSTP はデフォルトで有効になっています。
- 多重 STP（MSTP）：MSTP は RSTP に基づきます。レイヤ 2 ループを検出し、それに関与するポートがトラフィックを伝送するのを防ぐことで、軽減を試みます。ループはレイヤ 2 ドメイン単位で存在するため、STP ループをなくすためにポートがブロックされると、その状況が発生することがあります。トラフィックはブロックされていないポートに転送され、ブロックされているポートにはトラフィックは転送されません。これは、ブロックされたポートが常に未使用となるため、帯域幅の効率的な使用方法ではありません。MSTP は、各 STP インスタンスで個別にループを検出し、軽減できるように、いくつかの STP インスタンスを有効化することで、この問題を解決します。これにより、1 個のポートを 1 つまたは複数の STP インスタンスに対してブロックし、その他の STP インスタンスに対してはブロックしないように指定できます。異なる VLAN が異なる STP インスタンスに関連付けられている場合、それらのトラフィックは関連付けられた MST インスタンスの STP ポートの状態に基づいてリレーされます。結果として、帯域幅利用が改善されます。
- PVST+/RPVST+：（高速）Per VLAN Spanning Tree
  - PVST+ は、802.1Q STP 標準プロトコルの個別インスタンスを VLAN ごとに実行するプロトコルです。
  - Rapid PVST+ は、802.1Q RSTP 標準プロトコルの個別インスタンスを VLAN ごとに実行するプロトコルです。

    PVST/RPVST+ 動作の一環として、ポート上で定義された各 VLAN のために、個別の PVST フレームが送信されます。これにより、VLAN ごとの状態およびトポロジの維持が可能になります。

- SSTP：シスコのスイッチは、特別な共有スパニングツリープロトコル（SSTP）BPDU を使用して、PVST+ および高速 PVST+ スパニングツリートポロジ情報を交換します。これらは、SSTP BPDU をシスコの共有スパニングツリー MAC アドレスである 01-00-0C-CC-CC-CD に送信します。これらの BPDU の形式は、IEEE 標準 802.1Q の独自の拡張に基づいています。ネイティブ VLAN では、これらの BPDU はタグなしです。ポートは、複数の VLAN によってトランクモードで設定されている場合、それらの VLAN に関してタグ付けされたポートで SSTP BPDU を送信します。

スパニングツリープロトコル間の相互運用

IEEE 標準 MSTP（RSTP および STP を含む）と PVST+（および高速 PVST+）の相互運用には、2 つの主な側面があります。1 つ目は、MSTP および PVST+ を実行するスイッチとリージョンの間で共通のスパニングツリーの形成に関するものです。2 つ目は、MSTP リージョン間での PVST+ スパニングツリーのトンネリングに関するものです。

PVST+ で設定されたシスコのスイッチは、ポートで IEEE 標準 RSTP BPDU を受信すると、それらを認識し、SSTP 形式の BPDU と IEEE 標準 STP BPDU という 2 つのバージョンの BPDU をそのポートで送信します。同様に、高速 PVST+ で設定されたスイッチは、IEEE 標準 RSTP BPDU を認識し、RSTP BPDU を受信するポートで、SSTP 形式の BPDU と IEEE 標準 RSTP 形式の BPDU という 2 つのバージョンの BPDU を送信します。

MSTP と PVST+ がスパニングツリー インスタンスを VLAN にマッピングする方法には違いがあります。PVST+ はすべての VLAN に対してスパニングツリー インスタンスを作成しますが、MSTP は 1 つ以上の VLAN を各 MST インスタンスにマッピングします。PVST+ リージョンが MSTP リージョンと境界では、通常、一連の PVST+ インスタンスと一連の MST インスタンスが一致しません。そのため、PVST+ リージョンと MSTP リージョンは、単一の共通スパニングツリー インスタンス上で相互に通信する必要があります。

共通スパニングツリーを介した MSTP リージョンと PVST+ リージョンの間の相互運用は、次のように実現されます。

MST と PVST+ はどちらもループフリーのレイヤ 2 トポロジを提供しますが、それぞれが使用するアプローチは異なっています。

- MST は複数の VLAN を 1 つのインスタンスにマッピングします。このため、スパニングツリー インスタンスの数が削減されます。
- PVST+ は、スパニングツリー インスタンスごとにインスタンスを計算します。

PVST+ はインスタンス/VLAN ごとに BPDU を送信するため、VLAN 用に設定されたインスタンスによって MST に各 BPDU を個別に処理させることができます。

MST リージョンが PVST+ トポロジに接続されると、MST は PVST シミュレーションメカニズムを使用して PVST+ をシミュレートします。MST リージョンは、PVST+ スイッチに接続されているインターフェイスで PVST+ BPDU を送信（VLAN ごとに 1 つ）します。これらの BPDU はすべて、同じ情報を伝送し、同じルートブリッジをアドバタイズします。PVST+ トポロジに接続するインターフェイスは、「境界インターフェイス/ポート」と呼ばれます。PVST+ スイッチは、同じ情報を伝送する MST から各 VLAN の BPDU を受信するようになったため、ルートブリッジ、ルートポートなどを選択するときに、すべて同じ決定を行います。

MST リージョンがネットワークのルートブリッジになるようにネットワークを設定することが最も簡単です。PVST+ ドメインにルートブリッジがある場合、MST は、すべての VLAN に同じルートポートを使用します。MST リージョンにルートブリッジがある場合、異なるルートポートを使用してある程度のロードバランシングを実現するには、PVST+ スイッチで VLAN ごとのコストを変更します。

RSPAN の設定

SPAN（スイッチポートアナライザ）はポートミラーリングまたはポートモニタリングとも呼ばれ、ネットワークアナライザによる分析のためにネットワークトラフィックを選択します。シスコ スイッチ プローブ デバイスまたはその他のリモートモニタリング（RMON）プローブは、ネットワークアナライザとして使用できます。

ポートミラーリングは、1 つのデバイスポート、複数のデバイスポート、または仮想ローカルエリアネットワーク（VLAN）全体で検出されるネットワークパケットのコピーを、デバイスの別のポートのネットワークモニタリング接続に送信するネットワークデバイス機能です。この機能は、通常、侵入検知システムなど、ネットワークトラフィックのモニタリングを必要とするネットワークアプライアンスのために使用されます。データパケットは、モニタリングポートに接続しているネットワークアナライザにより、診断、デバッグ、およびパフォーマンスモニタリング用に処理されます。

リモート スイッチ ポート アナライザ（RSPAN）は、SPAN 拡張機能です。RSPAN は、ネットワーク全体にわたり複数スイッチのモニタリングを可能にし、アナライザポートをリモートスイッチ上に定義できるようにすることで、SPAN を拡張します。これは、ネットワーク キャプチャ デバイスを一元化できることを意味します。

RSPAN は、RSPAN セッションの送信元ポートからのトラフィックを RSPAN セッション専用の VLAN にミラーリングすることによって機能します。その後、この VLAN は他のスイッチにトランキングされ、RSPAN セッショントラフィックが複数のスイッチを通過できるようになります。RSPAN セッション VLAN からのトラフィックは、セッションの宛先ポートを含むスイッチの宛先ポートに単純にミラーリングされます。

各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。開始デバイスの送信元インターフェイスからのトラフィックは、リフレクタポートを介して RSPAN VLAN にコピーされます。これは設定が必要な物理ポートです。これは、RSPAN セッションを構築するためにのみ使用されます。リフレクタポートを指定する場合は「network」キーワードが必要であり、リンク上で非 RSPAN トラフィックが許可されます。

リフレクタ ポートには、次の特性があります。

- EtherChannel グループが SPAN の送信元として指定されている場合でも、EtherChannel グループに割り当てられる物理ポートにすることができます。ポートは、リフレクタ ポートとして設定されている間は、グループから削除されます。
- リフレクタ ポートとして使用されるポートは、SPAN の送信元または宛先にすることができず、一度に複数のセッションのリフレクタ ポートにすることもできません。

- すべての VLAN から認識されません。
- リフレクタ ポートではスパニングツリーが自動的にディセーブルになります。
- リフレクタポートは、すべてのモニタ対象送信元ポートで送受信されたトラフィックのコピーを受信します。

RSPAN トラフィックフロー

- 各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN を介してルーティングされます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。
- 開始デバイスの送信元インターフェイスからのトラフィックは、リフレクタポートを介して RSPAN VLAN にコピーされます。これは構成する必要がある物理ポートであり、リンクを介した他のトラフィックを許可する「network」キーワードが必要です。
- このリフレクタポートは、パケットを RSPAN VLAN にコピーするメカニズムとして機能します。
- 次に、RSPAN トラフィックは、中間デバイスのトランクポートを介して、最終的なスイッチの宛先セッションにルーティングされます。
- RSPAN VLAN は宛先スイッチによってモニタリングされ、宛先ポートにコピーされます。

RSPAN ポートメンバーシップルール

- すべてのスイッチ：RSPAN VLAN のメンバーシップはタグ付けのみが可能です。
- 開始スイッチ
  - SPAN 送信元インターフェイスは、RSPAN VLAN のメンバーになることは許可されていません。
  - リフレクタポートをこの VLAN のメンバーにすることはできません。
- 中間スイッチ
  - ミラーリングされたトラフィックの受け渡しに使用されていないすべてのポートから RSPAN メンバーシップを削除することをお勧めします。
  - 通常、RSPAN VLAN には 2 つのポートがあります。
- 最終スイッチ
  - ミラーリングされたトラフィックでは、送信元ポートが RSPAN VLAN のメンバーである必要があります。
  - RSPAN メンバーシップは、宛先インターフェイスを含む他のすべてのポートから削除する必要があります。

マルチキャスト

マルチキャストは、別々の場所にいる複数の受信者にメッセージを送信するための効率的な通信メカニズムを提供します。また、多対多および多対 1 の通信をサポートすることもできます。

マルチキャスト アプリケーションは、IP 上で User Datagram Protocol（UDP）を使用します。メッセージは送信元（「送信者」と呼ばれます）によって送信され、その情報の受信に関心のある別のデバイスがネットワーク上に存在しない場合でも送信されます（「ストリーム」と呼ばれます）。一方、受信者は、それらのメッセージを転送するようにネットワークに通知するために、特定のマルチキャストストリームに登録する必要があります。

IP マルチキャストは、ネットワーク リソース（特に、音声やビデオなどの帯域幅集約型サービス）を効率的に使用する方法です。IP マルチキャスト ルーティングにより、ホスト（ソース）は、IP マルチキャスト グループ アドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。送信側ホストは、マルチキャスト グループ アドレスをパケットの IP 宛先アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、マルチキャスト グループのメンバーに接続されたすべてのインターフェイスから着信した IP マルチキャスト パケットを転送します。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。

IP マルチキャスト ルーティングのデフォルト設定

次の表に、IP マルチキャスト ルーティングのデフォルト設定を示します。

表 *5 : IP* マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 kb/s

IGMP の概要

Internet Group Management Protocol（IGMP）は、マルチキャスト用に設計されたプロトコルです。IGMP を使用すると、ネットワーク内の異なるユーザー間でグループメンバーシップを確立できます。IGMP は、主に、ネットワーク内の異なるユーザー間でのマルチメディア ストリーミング（ビデオチャットなど）に使用されます。「スヌーピング」とは、通信において第三者が現在の接続データトラフィックをリッスンまたは観測する場合に使用される用語です。そのため、「IGMP スヌーピング」は、特にマルチキャストトラフィックをリッスンするプロ

セスを指します。IGMP スヌーピングを有効にすると、スイッチの特定ポートで登録済みのマルチキャストクライアントだけにマルチキャストトラフィックを転送できます。これにより、マルチキャストフレームは、VLAN内のすべてのユーザーではなく、VLAN内の特定のマルチキャストクライアントだけに転送されます。

マルチキャストは、1 つのホストからネットワーク内の選択されたホストにデータパケットを送信するために使用されるネットワークレイヤ技法です。下位レイヤでは、1 つのホストだけが受信する必要がある場合でも、スイッチはすべてのポートでマルチキャストトラフィックをブロードキャストします。Internet Group Management Protocol（IGMP）スヌーピングは、Internet Protocol バージョン 4（IPv4）マルチキャストトラフィックを目的のホストに転送するために使用されます。一方、マルチキャストリスナー検出（MLD）スヌーピングは、Internet Protocol バージョン 6（IPv6）マルチキャストトラフィックを目的のホストに転送するために使用されます。

IGMP が有効になっていると、IPv4 ルータとそのインターフェイスに接続されたマルチキャストホストの間で交換される IGMP メッセージが検出されます。その後、IPv4 マルチキャストトラフィックを制限するテーブルが維持され、それらのトラフィックが、受信する必要があるポートに動的に転送されます。

次の設定は、IGMP を設定するための前提条件です。

1. 仮想ローカルエリアネットワーク（VLAN）を設定します。
2. 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。

MLD が有効になっていると、IPv6 ルータとそのインターフェイスに接続されたマルチキャストホストの間で交換される MLD メッセージが検出されます。その後、IPv6 マルチキャストトラフィックを制限するテーブルが維持され、それらのトラフィックが、受信する必要があるポートに動的に転送されます。

IGMP_MLD プロキシ

IGMP/MLD プロキシは、簡潔な IP マルチキャスト プロトコルです。IGMP/MLD プロキシを使用して、エッジボック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することにより、これらのデバイスの設計とインストールがかなり簡単になります。プロトコル独立マルチキャスト（PIM）またはディスタンス ベクター マルチキャスト ルーティング プロトコル（DVMRP）などのより高度なマルチキャストルーティングプロトコルをサポートしていないため、デバイスのコストだけではなく、動作のオーバーヘッドも削減されます。

別の利点は、コアネットワークルータのマルチキャスト ルーティング プロトコルからプロキシデバイスを独立させることができる点です。その結果、プロキシデバイスは、任意のマルチキャストネットワークで簡単にセットアップできます。

IGMP/MLD プロキシ ツリー

IGMP/MLD プロキシは、堅牢なマルチキャスト ルーティング プロトコル（PIM など）を必要としない簡潔なツリートポロジで動作します。学習グループメンバーシップとプロキシ グループ メンバーシップ情報に基づく簡潔な IPM ルーティングプロトコルを使用し、それらの情報に基づいてマルチキャストパケットを転送するには、これで十分です。各プロキシデバイス

は、アップストリーム インターフェイスとダウンストリーム インターフェイスを識別して手動で設定する必要があります。

さらに、プロキシツリートポロジの IP アドレッシング方式は、プロキシデバイスが IGMP/MLD クエリア選出で確実に選出さ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。プロキシデバイスを除く他のマルチキャストルータがツリー内に存在しないようにし、より広いマルチキャスト構造にツリーのルートが接続されるようにする必要があります。

IGMP/MLD 転送を使用するプロキシデバイスは、単一のアップ ストリーム インターフェイスと 1 つ以上のダウン ストリーム インターフェイスを備えています。これらの指定は明示的に行われます。各インターフェイスのタイプを決定するプロトコルは存在しません。ダウンストリーム インターフェイスで、プロキシデバイスは IGMP/MLD のルータ部を実行し、アップストリーム インターフェイスでは、IGMP/MLD のホスト部を実行します。

転送ルールとクエリア

次のルールが適用されます。

- アップストリームインターフェイスで受信されたマルチキャスト パケットは、そのパケットを要求するすべてのダウンストリームインターフェイスに転送されます（ただし、プロキシ デバイスがそのインターフェイス上のクエリアである場合のみ）。
- プロキシ デバイスは、ダウンストリーム インターフェイスでクエリアにならない場合、ダウンストリーム インターフェイスで受信されたマルチキャスト パケットをドロップします。
- ダウンストリーム インターフェイスで受信されるマルチキャスト パケットは、プロキシデバイスがそのダウンストリーム インターフェイスでクエリアとなる場合、アップストリームインターフェイスで転送されます。プロキシデバイスがダウンストリームインターフェイスでクエリアとなる場合にのみ、パケットを要求するすべてのダウンストリームインターフェイスで転送されます。

マルチキャスト転送用の IGMP スヌーピングの設定

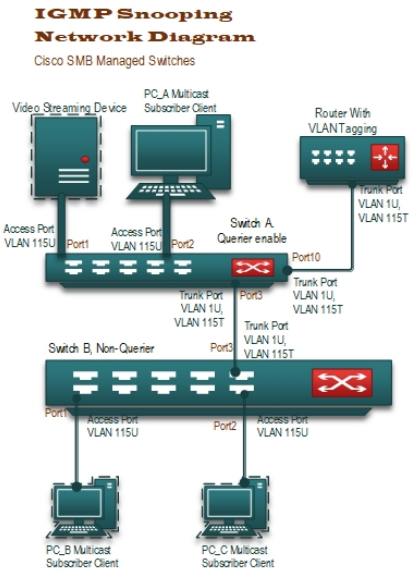
IGMP が機能するには IGMP クエリアが必要です。マルチキャストの処理にはマルチキャストルータの方が適していますが、設定が適切に行われているかぎり、Cisco Small Business スイッチはその役割の一部を果たすことができます。

IGMP スヌーピングはマルチキャストトラフィックが送信される VLAN に結び付けられるため、サブスクライバが存在する VLAN とは異なる VLAN にマルチキャストサーバーを配置することができます。

このセットアップでは、2 つの VLAN が使用されます。マルチキャストトラフィックが発生する 1 つ目の VLAN（VLAN 115）と 2 つ目の VLAN（今回は VLAN 1）はデフォルト設定されます。

ステップ 1 この VLAN 割り当ての場合、スイッチ B（非クエリアスイッチ）は、ポート 3 を介してスイッチ A（クエリア）にアップリンク接続されます。両方のポートが、トランク 1U、115T（VLAN 1 タグなし、VLAN 115 タグ付き）として設定されます。

a) スイッチ A のポート 1 には、マルチキャストサーバーが接続されます（VLAN 115U、アクセス）。
b) スイッチ A のポート 2 には、サブスクライバが接続されます（VLAN 115U、アクセス）。
c) スイッチ B のポート 1 には、サブスクライバが接続されます（VLAN 115U、アクセス）。
d) スイッチ B のポート 2 には、サブスクライバが接続されます（VLAN 115U、アクセス）。
e) スイッチ A のポート 10 には、ルータが接続されます（VLAN 1U、115T、トランク）。



ステップ 2 スイッチが接続されるルータのポートは、トランクポート VLAN 1U、115T である必要があります。対応する IP アドレスと DHPC 設定が適切に指定されていることを確認します。

ステップ 3 スイッチのメイン設定ページに移動し、[Multicast] > [IGMP Snooping] の順に選択します。このページの場所は、スイッチのモデルによって異なります。

ステップ 4 次の [Enable] チェックボックスをオンにします。

- IGMPスヌーピングステータス
- IGMPクエリアステータス

ステップ 5 次に、VLAN 115 を選択し、[Edit] をクリックします。

ステップ 6 IGMP スヌーピングステータスの [Enable] チェックボックスをオンにして有効にします。

ステップ 7 [MRouter Ports Auto Learn] チェックボックスをオンにして有効にします。このオプションは、スイッチがクエリア（マルチキャストルータ）の場所を自動的に学習するためのものです。そのため、スイッチがクエリアとして機能している場合は、このオプションをオンにしないでください。

ステップ 8 [Immediate Leave] チェックボックスをオンにして有効にします。このオプションは、IGMP スヌーピング機能への副作用を心配することなく、有効または無効にすることができます。有効にすると、デバイスポートに送信される不要な IGMP トラフィックのブロックにかかる時間が短縮されます。

ステップ 9 [Last Member Query Counter] はデフォルト設定のままにして、ウィンドウを閉じて次の手順に進みます。

ステップ 10 スイッチのメイン設定ページに戻り、[Multicast] > [IGMP Snooping] の順に選択します。このページの場所は、スイッチのモデルによって異なります。

ステップ 11 [IGMP Querier Status] チェックボックスをオンして有効にします。このスイッチがクエリアとして機能する場合にのみ、このオプションを有効にします。それ以外の場合は、オフのままにしておいてください。今回は、クエリアを 1 つだけ設定します。

ステップ 12 次に、VLAN 115 を選択し、[Edit] をクリックします。

ステップ 13 [IGMP Querier Status] チェックボックスをオンして、スイッチがクエリアとして機能できるようにします。このスイッチをクエリアとして機能させる場合にのみ、この手順を実行してください。ほとんどのセットアップでは、必要なクエリアは 1 つだけです。

ステップ 14 [IGMP Querier Election] チェックボックスをオンにします。VLAN で複数のクエリアが使用されており、2つ目のクエリアで IGMP クエリアステータスがグローバルに有効になっている場合は、このオプションを使用することにより、この環境を管理することができます。

ステップ 15 IGM クエリアのバージョン（バージョン 2 またはバージョン 3）を選択します。バージョン 3 を選択するのは VLAN 内に送信元固有の IP マルチキャスト転送を実行するスイッチやルータがある場合であるため、ほとんどの場合はバージョン 2 を選択します。

ステップ 16 [Querier Source IP address] で [User Defined] を選択し、クエリアとして機能するスイッチの IP アドレスを選択します。

ステップ 17 スヌーピングページでの調整が完了したので、全体を機能させ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する必要があります。スイッチの Web UI で、[Multicast] > [Properties] の順に移動します。

ステップ 18 [Bridge Multicast Filtering Status] チェックボックスをオンにして、スイッチが IGMP スヌーピングと連携してマルチキャストを処理できるようにします。この機能が有効になっていない場合（デフォルトではオフ）、すべてのポートがマルチキャストトラフィックに使用されます。

ステップ 19 VLAN 115 または特定の VLAN を選択します。「転送方式」を選択します。ここでは、[MAC Group Address] を選択していれば、[Multicast /MAC Group Address] テーブルに MAC アドレスが表示されますが、今回は [IP Group Address] を選択しているため、[Multicast /IP Multicast Group Address] テーブルにマルチキャスト IP アドレスが表示されます。

ステップ 20 デフォルトでは、[Multicast Router Port] は [None] に設定されています。ここでは何も調整する必要がありません。非クエリアスイッチでは、クエリアデバイスへのアップリンクポートが [Dynamic] として選択されます。これを確認するには、VLAN 115 を選択し、[Go] をクリックして、[Dynamic] 行でポート 3 が選択されていることを調べてください。これは、スイッチ B はクエリアではないものの、そのアップリンクポートでクエリアを検出したことを示しています。

ステップ 21 [Multicast] > [Forward All] の順にクリックし、これが [None] に設定されていることを確認します。通常、デフォルトで [None] に設定されています。これはクエリアスイッチにも当てはまります。

ステップ 22 [Multicast] > [Unregistered Multicast] の順にクリックします。デフォルト設定では [Forwarding all] が指定されています。つまり、登録済みまたは未登録のすべてのマルチキャストトラフィックが転送されます。未登録のトラフィックを転送したくない場合は、推奨設定の [Filtering] に設定し、マルチキャスト サーバー マシンが接続されているポートについてのみ [Forwarding] 設定が選択されたままにします。

ステップ 23 動作することを確認するためにテストします。VLC をビデオ ストリーミング プログラムおよびビデオ サブスクライバクライアントとして使用して、図のようにデバイスを接続します。VLC サーバーからビ

デオのストリーミングを開始し、クライアントを起動してストリームに登録します。結果は、次のとおりです。

VLC をビデオ ストリーミング プログラムおよびビデオ サブスクライバ クライアントとして使用して、図のようにデバイスを接続します。VLC サーバーからビデオのストリーミングを開始し、クライアントを起動してストリームに登録します。結果は、次のとおりです。

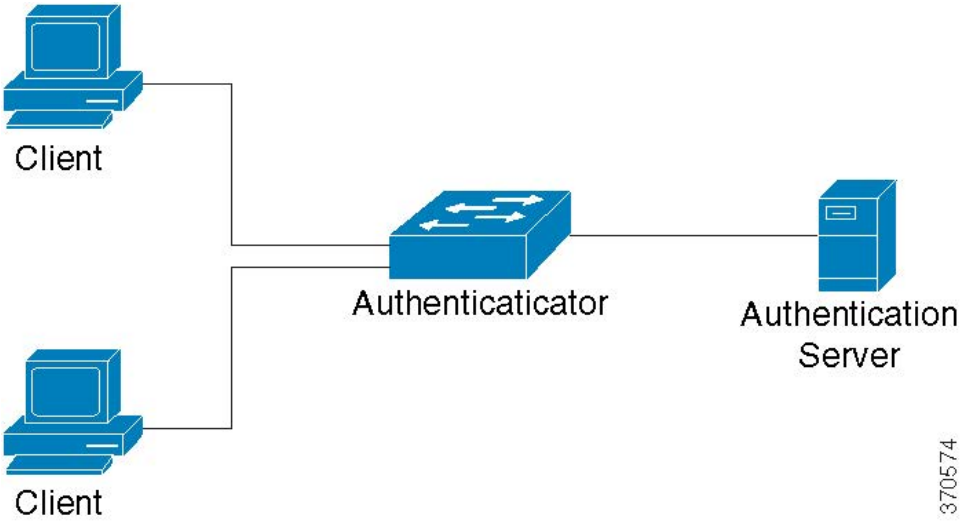
- マルチキャスト IP アドレスが VLAN 115 の [Multicast /IP Multicast Group Address] に正しく入力されていることを確認します。これは、クライアントがビデオストリームに正常に登録されていることを示しています。
- 複数のスイッチによるセットアップでは、クエリアとして機能していないスイッチがクエリアを正常に識別したことを確認します。非クエリアスイッチでは、クエリアデバイスへのアップリンクポートが [Dynamic] として選択されます。これを確認するには、VLAN 115 を選択し、[Go] をクリックして、[Dynamic] 行でポート 3 が選択されていることを調べてください。これは、このスイッチ B はクエリアではないものの、そのアップリンクポートでクエリアを検出したことを示しています。

ステップ 24 デフォルトでは、マルチキャストブリッジフィルタが有効になっていないかぎり、スイッチのすべてのポートでマルチキャストトラフィックが設定されます。サブスクライバが VLAN y に存在する場合、マルチキャストトラフィックが VLAN x から発信されると、上記の設定は機能しません。マルチキャスト TV を使用すると、この特別な設定に対応できます。

802_1x の概要

802.1X 認証は、未認可クライアントが一般にアクセス可能なポートから LAN に接続することを制限します。802.1X 認証はクライアント/サーバ モデルです。このモデルでは、ネットワーク デバイスが次の固有の役割を持ちます。

- クライアントまたはサプリカント
- オーセンティケータ
- 認証サーバ



ネットワーク デバイスは、ポートごとにクライアント/サプリカント、オーセンティケータ、または両方として使用できます。

クライアントまたはサプリカント

クライアントまたはサプリカントは、LAN へのアクセスを要求するネットワーク デバイスです。クライアントはオーセンティケータに接続されます。

クライアントは、認証に 802.1X プロトコルを使用する場合、802.1X プロトコルのサプリカントの部分と EAP プロトコルのクライアントの部分を実行します。

オーセンティケータ

オーセンティケータは、サプリカント ポートの接続先となる、ネットワーク サービスを提供するネットワーク デバイスです。ポートでは次の認証モードがサポートされています。

- 単一ホスト：ポートごとに単一のクライアントを受け入れる、ポートベースの認証をサポートします。
- 複数ホスト：ポートごとに複数のクライアントを受け入れる、ポートベースの認証をサポートします。
- 複数セッション：ポートごとに複数のクライアントを受け入れる、クライアントベースの認証をサポートします。

次の認証方式がサポートされます。

- 802.1X ベース：すべての認証モードでサポートされます。
- MAC ベース：すべての認証モードでサポートされます。
- Web ベース：マルチセッション モードでのみサポートされます。

802.1X ベース認証では、オーセンティケータが 802.1X メッセージ（EAPOL パケット）から EAP メッセージを抽出し、RADIUS プロトコルを使用してそれらを認証サーバに渡します。

MACベース認証またはWebベース認証では、オーセンティケータ自体が、ネットワーク アクセスを求めるクライアントの代わりにソフトウェアのEAPクライアントの部分を実行します。

オープンアクセス

802.1x環境で、オープン（モニタリング）アクセス機能は、実際の認証失敗と、設定ミスやリソース不足のために発生する失敗を区別するために役立ちます。オープンアクセスを使用することにより、システム管理者は、ネットワークに接続しているホストの設定上の問題を容易に把握し、不適切な状態をモニターして、これらの問題を修正できるようになります。

オープンアクセスがインターフェイスで有効になっている場合、スイッチはRADIUSサーバーの失敗をすべて成功と見なし、認証結果にかかわらず、インターフェイスに接続しているステーションのネットワークへのアクセスを許可します。通常の動作では、認証が有効になっているポート上のトラフィックは認証と認可が正常に完了するまでブロックされますが、オープンアクセスにより、その動作が変更されます。

認証のデフォルトの動作では、Extensible Authentication Protocol over LAN（EAPoL）を除くすべてのトラフィックがブロックされます。一方、オープンアクセスでは、認証（802.1Xベース、MACベース、またはWebベース）が有効になっている場合でも、すべてのトラフィックに対して無制限のアクセスを許可するオプションが管理者に提供されます。

RADIUSアカウンティングが有効になっている場合、認証試行をログに記録し、監査証跡を使用して、ネットワークに接続しているユーザやシステムを把握できます。

オーセンティケータの概要

ポート管理認証状態

ポート管理状態により、クライアントがネットワークへのアクセス権を付与されるかどうかが決まります。

次の値が有効です。

- force-authorized-Port認証は無効で、ポートはスタティック設定に従い、認証を行わずにすべてのトラフィックを送信します。スイッチは、802.1X EAPOL 開始メッセージを受信すると、EAP成功メッセージを格納した802.1XEAPパケットを送信します。これは、デフォルトの状態です。
- force-unauthorized-Port 認証は無効で、ポートはゲスト VLAN および非認証 VLAN 経由ですべてのトラフィックを送信します。スイッチは、802.1X EAPOL 開始メッセージを受信すると、EAP 失敗メッセージを格納した 802.1X EAP パケットを送信します。
- auto-Enables 802.1x 認証は、設定済みのポートホストモードおよびポートに設定されている認証方式に従って有効になります。

ポート ホスト モード

ポートに設定できるポートホストモードは次のとおりです。

- [Single-Host Mode]：許可されたクライアントが存在する場合にポートが許可されます。1つのポートでは1つのホストのみ認可されます。ポートが未承認でゲストVLANがイネーブルの場合、タグなしトラフィックはゲスト VLAN に再マッピングされます。タグ付きトラフィックは、ゲスト VLAN または非認証 VLAN に属していないかぎりドロップされます。ポートでゲスト VLAN が有効になっていない場合、非認証 VLAN に属しているタグ付きトラフィックだけがブリッジされます。

  ポートが認可されると、認可済みホストからのトラフィックは、タグなしのものもタグ付きのものも、スタティック VLAN メンバーシップ ポート設定に基づいてブリッジされます。他のホストからのトラフィックはドロップされます。許可ホストからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによって割り当てられた VLAN に再マッピングされるようにユーザが指定できます。タグ付きトラフィックは、RADIUS割り当て VLAN か非認証 VLAN に属していないかぎりドロップされます。

- [Multi-Host Mode]：許可されたクライアントが少なくとも 1 つ存在する場合にポートが許可されます。ポートが認可されておらず、ゲスト VLAN が有効になっている場合、タグなしトラフィックはゲスト VLAN に再マッピングされます。タグ付きトラフィックは、ゲスト VLAN または非認証 VLAN に属していないかぎりドロップされます。ポート上でゲスト VLAN が有効になっていない場合、認証されていない VLAN に属するタグ付きトラフィックだけがブリッジされます。

  ポートが認可されると、そのポートに接続されたすべてのホストからのトラフィックは、タグなしのものもタグ付きのものも、スタティック VLAN メンバーシップ ポート設定に基づいてブリッジされます。ユーザは、認可済みポートからのタグなしトラフィックが、認証プロセス中に、RADIUSサーバによって割り当てられているVLANに再マッピングされるように指定できます。タグ付きトラフィックは、RADIUS 割り当て VLAN か非認証 VLAN に属していないかぎりドロップされます。

- [Multi-Sessions Mode]：シングルホストおよびマルチホストモードとは異なり、マルチセッションモードのポートには認証ステータスがありません。このステータスは、ポートに接続している各クライアントに割り当てられます。非認証 VLAN に属しているタグ付きトラフィックは、ホストが認可されているどうかにかかわらず、常にブリッジされます。

  非認証 VLAN に属していない未認可ホストからのトラフィックは、タグ付きのものもタグなしのものも、ゲスト VLAN が VLAN で定義されていて有効になっている場合はゲストVLANに再マッピングされ、ゲストVLANがポートで有効になっていない場合はドロップされます。ユーザは、認可済みポートからのタグなしトラフィックが、認証プロセス中に、RADIUSサーバによって割り当てられているVLANに再マッピングされるように指定できます。タグ付きトラフィックは、RADIUS 割り当て VLAN か非認証 VLAN に属していないかぎりドロップされます。

複数の認証方法

スイッチで複数の認証方式が有効になっている場合は、次の認証方式の階層が適用されます。

- 802.1X 認証：最上位
- Web ベース認証

• MAC ベース認証：最下位

複数の方式を同時に実行できます。1 つの方式が正常に完了すると、クライアントが認可されて、優先順位の低い方式は停止され、優先順位の高い方式は続行されます。

同時に実行されている認証方式のいずれかが失敗すると、他の方式が続行されます。

優先順位の低い認証方式で認証されたクライアントに対して別の認証方式が正常に完了すると、新しい認証方式の属性が適用されます。新しい方式が失敗する場合、クライアントは古い方式で認可されたままになります。

802.1xベース認証

802.1x ベースのオーセンティケータは、透過的な EAP メッセージを 802.1x サプリカントと認証サーバーの間でリレーします。サプリカントとオーセンティケータの間で交換された EAP メッセージは802.1x メッセージ内にカプセル化され、オーセンティケータと認証サーバーの間で交換された EAP メッセージは RADIUS メッセージ内にカプセル化されます。

MAC ベースの認証

MAC ベース認証は、802.1X のサプリカント機能を持たない装置（プリンタおよび IP Phone など）へのネットワークアクセスを可能にする、802.1X 認証に代わるものです。MAC ベース認証は、接続装置の MAC アドレスに基づき、ネットワークアクセスを許可または拒否します。この場合、スイッチは、次のように、クライアントの MAC アドレスであるユーザー名とパスワードで EAP MD5 機能をサポートします。

Web ベース認証

スイッチを介したネットワークへのアクセスを要求するエンドユーザーは、Webベース認証を使用して認証されます。これにより、スイッチに直接接続されているクライアントを、ネットワークへのアクセス権が与えられる前に、キャプティブポータルメカニズムを使用して認証できます。

Web ベース認証はクライアントベースの認証であり、レイヤ 2 とレイヤ 3 の両方においてマルチセッションモードでサポートされます。この認証方式がポートごとに有効になっている場合、各ホストはネットワークにアクセスするためにそのホスト自体を認証する必要があります。したがって、有効になっているポートで認証されるホストと認証されないホストが存在する可能性があります。

ポートで Web ベース認証が有効になっている場合、スイッチは、ARP、DHCP、および DNS パケットを除き、未認可クライアントからのすべてのトラフィックをドロップします。スイッチにより、これらのパケットは転送されることが許可されます。そのため、未認可クライアントでも IP アドレスを取得し、ホスト名またはドメイン名を解決することができます。

未認可クライアントの IPv4 の HTTP/HTTPS パケットは、スイッチの CPU にルーティングされます。エンドユーザーがネットワークアクセスを要求すると、Webベース認証がポートで有効な場合は、要求されたページが表示される前にログインページが表示されます。ユーザーはユーザー名およびパスワードを入力する必要があります。これらは、EAPプロトコルを使用して RADIUS サーバーによって認証されます。認証が成功すると、ユーザーに通知されます。

この時点でユーザーのセッションが認証されます。セッションが使用されている間は、開いたままです。指定された時間内に使用されない場合、セッションは終了します。この時間間隔は「待機時間」と呼ばれ、システム管理者が設定します。セッションが期限切れになると、ユーザー名とパスワードが失われ、ゲストは新しいセッションを開始するためにそれらを再入力する必要があります。

非認証 VLAN とゲスト VLAN

非認証 VLAN とゲスト VLAN は、サプリカント デバイスまたはポートを認証および認可する必要のないサービスへのアクセスを提供します。

ゲスト VLAN は、未認可クライアントに割り当てられる VLAN です。ゲスト VLAN、および 802.1x 認証プロパティで非認証にする 1 つ以上の VLAN を設定できます。

非認証 VLAN は、認可済みデバイス/ポートと未認可デバイス/ポートの両方によるアクセスを許可する VLAN です。非認証 VLAN には次の特性があります。

- スタティック VLAN である必要があり、ゲスト VLAN またはデフォルト VLAN にはできません。
- メンバー ポートは、タグ付きメンバーとして手動で設定する必要があります。
- メンバー ポートは、トランク ポートまたは一般的なポートである必要があります。アクセス ポートは非認証 VLAN のメンバーにはできません。

ゲスト VLAN（設定されている場合）は次の特性を持つスタティック VLAN です。

- 既存のスタティック VLAN から手動で定義する必要があります。
- ゲスト VLAN を音声 VLAN または非認証 VLAN として使用することはできません。

ホスト モードとゲスト VLAN

ゲスト VLAN を使用する場合、ホスト モードは次のように機能します。

- シングルホストおよびマルチホストモード：未認可ポートに着信する、ゲスト VLAN からのトラフィックは、タグなしのものもタグ付きのものも、ゲスト VLAN を介してブリッジされます。他のすべてのトラフィックは拒否されます。認証されていない VLAN からのトラフィックは、VLAN を介してルーティングされます。
- レイヤ 2 のマルチセッションモード：未認可クライアントから着信する、非認証 VLAN に属していないトラフィックは、タグなしのものもタグ付きのものも、TCAM ルールを使用してゲスト VLAN に割り当てられ、ゲスト VLAN を介してブリッジされます。認証されていない VLAN からのタグ付きトラフィックは、VLAN を介してルーティングされます。

  このモードは、ポリシーベース VLAN と同じインターフェイスでは設定できません。
- レイヤ 3 のマルチセッションモード：このモードはゲスト VLAN をサポートしていません。

RADIUS VLAN 割り当てまたはダイナミック VLAN 割り当て

このオプションが [Port Authentication] ページで有効になっている場合、RADIUS サーバーは認可済みクライアントにVLANを割り当てることができます。これは、RADIUS割り当てVLAN、またはダイナミック VLAN 割り当て（DVA）と呼ばれます。このガイドでは「RADIUS 割り当て VLAN」という用語を使用しています。

ポートがマルチセッションモードで、RADIUS割り当てVLANが有効な場合、デバイスはこのポートを認証プロセス中に追加して、RADIUSサーバーによって割り当てられたVLANのタグなしメンバーとします。タグなしパケットが認証および許可済みのデバイスもしくはポートから発信されたものである場合、そのパケットは、割り当て済み VLAN に所属するものとして分類されます。

（注） 複数セッション モードでは、デバイスがレイヤ 2 システム モードの場合にのみ、RADIUS VLAN 割り当てがサポートされます。

DVA 対応ポートでデバイスの認証および認可を行う場合は、次の点に注意してください。

- RADIUSサーバーは、デバイスを認証し、デバイスにVLANを動的に割り当てる必要があります。[Port Authentication] ページで、[RADIUS VLAN Assignment] フィールドを [static] に設定できます。これにより、ホストをスタティック設定に基づいてブリッジすることが可能になります。
- tunnel-type (64) = VLAN (13)、tunnel-media-type (65) = 802 (6)、および tunnel-privategroup-id = VLAN ID のように RADIUS 属性を指定した RADIUS サーバーにより、DVA がサポートされる必要があります。

RADIUS 割り当て VLAN 機能が有効になっている場合、ホスト モードの動作は次のようになります。

- シングルホストおよびマルチホストモード：RADIUS 割り当て VLAN に属しているトラフィックは、タグなしのものもタグ付きのものも、この VLAN を介してブリッジされます。非認証 VLAN に属していないその他のすべてのトラフィックは破棄されます
- フルマルチセッションモード：クライアントから着信する、非認証 VLAN に属していないトラフィックは、タグなしのものもタグ付きのものも、TCAMルールを使用してRADIUS割り当て VLAN に割り当てられ、その VLAN を介してブリッジされます。
- レイヤ 3 システム モードの複数セッション モード

このモードは、RADIUS 割り当て VLAN をサポートしていません。

次の表に、認証方式とポートモードに応じたゲスト VLAN および RADIUS VLAN 割り当てのサポートを示します。

表 *6 : VLAN* および *RADIUS VLAN* 割り当て

認証方式	シングルホスト	マルチホスト	マルチセッション	
			L3 のデバイス	L2 のデバイス
802.1X	†	†	N/S	†
MAC	†	†	N/S	†
Web	N/S	N/S	N/S	N/S

凡例

†：ポートモードはゲスト VLAN および RADIUS VLAN 割り当てをサポートします

N/S：ポートモードは認証方法をサポートしません。

違反モード

シングルホストモードでは、認可済みポートで未認可ホストがインターフェイスにアクセスしようとしたときに実行するアクションを設定できます。これは、[ホストおよびセッション認証] ページで行います。

次のオプションを使用できます。

- restrict：MAC アドレスがサプリカント MAC アドレスではないステーションがインターフェイスへのアクセスを試みると、トラップが生成されます。トラップ間の最短時間は 1 秒です。これらのフレームは転送されますが、送信元アドレスは不明のままです。
- protect：サプリカントアドレスではない送信元アドレスを持つフレームは廃棄されます。
- shutdown：サプリカントアドレスではない送信元アドレスを持つフレームを拒否し、ポートを閉じます。

SNMP トラップを、設定可能な最小の時間間隔で送信するようにデバイスを設定することもできます。seconds を 0 にした場合、トラップは無効になります。最小時間を指定しない場合、制限モードではデフォルトで 1 秒に設定され、その他のモードでは 0 に設定されます。

待機時間

認証失敗情報交換後、ポート（シングルホストモードまたはマルチホストモード）またはクライアント（マルチセッションモード）は、待機時間中に認証を試行できません。シングルホストモードまたはマルチホストモードの場合、この期間はポートごとに定義され、マルチセッションモードの場合、この期間はクライアントごとに定義されます。待機時間の間、スイッチは認証要求を受け付けず、開始もしません。

802.1x ベース認証と Web ベース認証のみがこの期間の対象です。待機時間に入る前に許可されるログインの試行回数を指定することもできます。0 の値は、ログインの試行回数が無制限であることを示します。[Port Authentication] ページで、待機時間の長さとログインの最大試行回数を設定できます。

モードの動作

次の表に、さまざまな状況で認証トラフィックと非認証トラフィックがどのように処理されるかを示します。

	非認証 トラフィック				認証トラフィック			
	ゲスト **VLAN** あり		ゲスト **VLAN** なし		**RADIUS VLAN** あり		**RADIUS VLAN** なし	
	タグなし	タグ付き	タグなし	タグ付き	タグなし	タグ付き	タグなし	タグ付き
シングルホスト	フレームはゲスト VLAN に再マッピングされます	フレームはゲスト VLAN または非認証 VLAN に属していないかぎりドロップされます	フレームはドロップされます	フレームは非認証 VLAN に属していないかぎりドロップされます	フレームは RADIUS 割り当て VLAN に再マッピングされます	フレームは RADIUS VLAN または非認証 VLAN に属していないかぎりドロップされます	フレームはスタティック VLAN 設定に基づいてブリッジされます	フレームはスタティック VLAN 設定に基づいてブリッジされます
マルチホスト	フレームはゲスト VLAN に再マッピングされます	フレームはゲスト VLAN または非認証 VLAN に属していないかぎりドロップされます	フレームはドロップされます	フレームは非認証 VLAN に属していないかぎりドロップされます	フレームは RADIUS 割り当て VLAN に再マッピングされます	フレームは RADIUS VLAN または非認証 VLAN に属していないかぎりドロップされます	フレームはスタティック VLAN 設定に基づいてブリッジされます	フレームはスタティック VLAN 設定に基づいてブリッジされます
ライトマルチセッション	N/S	N/S	フレームはドロップされます	フレームは非認証 VLAN に属していないかぎりドロップされます	N/S	N/S	フレームはスタティック VLAN 設定に基づいてブリッジされます	フレームはスタティック VLAN 設定に基づいてブリッジされます

	非認証 トラフィック				認証トラフィック			
	ゲスト VLAN あり		ゲスト VLAN なし		RADIUS VLAN あり		RADIUS VLAN なし	
	タグなし	タグ付き	タグなし	タグ付き	タグなし	タグ付き	タグなし	タグ付き
フル マルチセッション	フレームはゲスト VLAN に再マッピングされます	フレームは非認証 VLAN に属していないかぎりゲスト VLAN に再マッピングされます	フレームはドロップされます	フレームは非認証 VLAN に属していないかぎりドロップされます	フレームは RADIUS 割り当て VLAN に再マッピングされます	フレームは非認証 VLAN に属していないかぎり RADIUS VLAN に再マッピングされます	フレームはスタティック VLAN 設定に基づいてブリッジされます	フレームはスタティック VLAN 設定に基づいてブリッジされます

DHCPv4 のタイプと相互作用

DHCPv4 スヌーピング

DHCP スヌーピングは、誤った DHCP 応答パケットの受信を防ぎ、DHCP アドレスをログに記録するセキュリティ機能です。これは、デバイスのポートを信頼できるまたは信頼できないに分類することによって実現されます。

信頼できるポートは、DHCP サーバーに接続していて、DHCP アドレスの割り当てが許可されているポートです。信頼できるポートで受信した DHCP メッセージは、デバイスをパススルーできます。DHCP アドレスの割り当てが許可されていないポートは、信頼できないポートと呼ばれます。ポートを信頼できると宣言するまで、デフォルトでは信頼できないと見なされます。

DHCPv4 リレー

DHCP リレーは、DHCP サーバに DHCP パケットをリレーします。

レイヤ 2 およびレイヤ 3 における DHCPv4

レイヤ 2 システムモードで、デバイスは、DHCP リレーが有効になっている VLAN から受け取った DHCP メッセージをリレーします。レイヤ 3 システムモードで、デバイスは、IP アドレスのない VLAN から受け取った DHCP シグナルも送信できます。IP アドレスのない VLAN で DHCP リレーを有効にすると、Option 82 が自動的に挿入されます。この挿入は単一の VLAN で行われ、Option 82 のグローバル管理状態には影響しません。

透過型 DHCP リレー

外部 DHCP リレーエージェントが使用される透過型 DHCP リレーの場合は、次の手順を実行します。

- DHCP スヌーピングを有効にします。
- Option 82 の挿入を有効にします。
- DHCP リレーを無効にします。

通常の DHCP リレーの場合は、次の手順を実行します。

- DHCP リレーを有効にします。
- Option 82 の挿入を有効にする必要はありません。

Option 82

Option 82（DHCP リレーエージェント情報オプション）は、ポートおよびエージェント情報を中央 DHCP サーバーに渡して、割り当てられた IP アドレスがネットワークに物理的に接続されている場所を識別します。

Option 82 の主な目的は、DHCP サーバーが IP アドレスを受け取る最適な IP サブネット（ネットワークプール）を決定できるようにすることです。

デバイス上では、以下のオプション 82 設定が利用可能です。

- [DHCP Insertion]：Option 82 情報を持たないパケットに Option 82 情報を追加します。
- [DHCP Pass through]：信頼できないポートからの Option 82 情報を含む DHCP パケットを転送または拒否します。信頼できるポートでは、Option 82 情報が含まれている DHCP パケットは常に転送されます。

DHCP リレー、DHCP スヌーピング、および Option 82 モジュールによるパケットフローを次の表に示します。

発生する可能性のあるさまざまなシナリオがあります。

- DHCP クライアントと DHCP サーバーの両方が同じ VLAN にある。このシナリオでは、一般的なブリッジは、DHCP クライアントと DHCP サーバーの間で DHCP メッセージを渡します。
- DHCP クライアントと DHCP サーバーの両方が異なる VLAN にある。この場合、DHCP リレーのみが、DHCP クライアントと DHCP サーバーの間の DHCP メッセージのブロードキャストを実行可能であり、実際にそれを実行します。正規のルータがユニキャスト DHCP パケットを送信するため、IP アドレスのない VLAN 上で DHCP リレーが有効である場合、またはデバイスがルータ（レイヤ 2）でない場合には、外部ルータが必要になります。

DHCP リレーによってのみ、DHCP サーバーに DHCP メッセージが転送されます。

DHCPv4 スヌーピング、DHCPv4 リレーおよび Option 82 間の相互作用

次の表に、DHCP スヌーピング、DHCP リレー、および Option 82 のさまざまな組み合わせを使用した場合のデバイスの動作について説明します。DHCP スヌーピングが有効になっておらず、DHCP リレーが有効になっているときの DHCP 要求パケットの処理方法について以下で説明します。

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着
Option 82 の挿入が無効	Option 82 なしでパケットが送信されます	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 ブリッジを挿入：Option 82 が挿入されない	リレー：パケットを破棄 ブリッジ：元の Option 82 と一緒にパケットが送信されます
Option 82 の挿入が有効	リレー：Option 82 と一緒に送信 ブリッジ：Option 82 は送信されません	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 と一緒に送信 ブリッジ：Option 82 は送信されません	リレー：パケットを破棄 ブリッジ：元の Option 82 と一緒にパケットが送信されます

DHCP スヌーピングと DHCP リレーの両方が有効になっているときの DHCP 要求パケットの処理方法について以下で説明します。

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着
Option 82 の挿入が無効	Option 82 なしでパケットが送信されます	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 を挿入 ブリッジ：Option 82 を挿入しない	リレー：パケットを破棄 ブリッジ：元の Option 82 と一緒にパケットが送信されます

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
Option 82 の挿入が有効	リレー：Option 82 と一緒に送信 ブリッジ：Option 82 を追加 （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場合のように動作します）	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 と一緒に送信 ブリッジ：Option 82 を追加 （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場合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 Option 82 と一緒にパケットが送信されます

次に、DHCP スヌーピングが無効になっているときの DHCP リレーパケットの処理方法について説明します

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着
Option 82 の挿入が無効	Option 82 なしでパケットが送信されます	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 を破棄 ブリッジ：Option 82 なしでパケットが送信されます	リレー： 1. 応答の発信元がデバイスの場合、パケットは Option 82 なしで送信 2. 応答の発信元がデバイスではない場合、パケットは破棄されます。 ブリッジ：元の Option 82 と一緒にパケットが送信されます

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
Option 82 の挿入が有効	Option 82 なしでパケットが送信されます	リレー：Option 82 なしのパケットを送信 ブリッジ：Option 82 と一緒にパケットが送信されます	リレー：Option 82 を破棄 ブリッジ：Option 82 なしでパケットが送信されます	リレー：Option 82 なしのパケットを送信 ブリッジ：Option 82 ありのパケットを送信

次に、DHCP スヌーピングと DHCP リレーの両方が有効になっているときの DHCP 応答パケットの処理方法について説明します。

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着
Option 82 の挿入が無効	Option 82 なしでパケットが送信されます	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 を破棄 ブリッジ：Option 82 なしでパケットが送信されます	リレー： 1. 応答の発信元がデバイスの場合、パケットは Option 82 なしで送信 2. 応答の発信元がデバイスではない場合、パケットは破棄されます。 ブリッジ：元の Option 82 と一緒にパケットが送信されます
Option 82 の挿入が有効	Option 82 なしでパケットが送信されます	Option 82 なしでパケットが送信されます	リレー：Option 82 を破棄 ブリッジ：Option 82 なしでパケットが送信されます	Option 82 なしでパケットが送信されます

IPv6 管理インターフェイス

IPv6（インターネット プロトコル バージョン 6）は、パケット交換インターネット操作用のネットワーク層プロトコルです。IPv6は、最も幅広く使用されているインターネットプロトコルである IPv4 に代わるものとして作成されました。アドレスサイズが 32 ビットから 128 ビットに増加するため、IPv6 では IP を割り当てる際の柔軟性が増します。FE80::9C00:876A:130B または FE80:0000:0000:0000:0000:9C00:876A:130B は省略形の例で、一連のゼロは省略して「::」に置き換えることができます。

IPv4 しか使用できないネットワーク上で他の IPv6 ノードに接続するには、途中でマッピングする技術が必要です。このトンネリング技術を使用すれば、IPv6にしか対応していないホストでも IPv4 サービスに接続でき、孤立した 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またいで IPv6 ノードに接続できます。

ISATAP または手動メカニズムがトンネリングに使用されます（「IPv6 トンネル」を参照）。IPv4 ネットワークは仮想 IPv6 ローカルリンクとして扱われ、トンネリングを経由して、各 IPv4 アドレスからリンクローカル IPv6 アドレスへのマッピングが行われます。IPv6 Ethertype は、デバイスが IPv6 フレームを認識するために使用されます。

DoS防御

サービス妨害（DoS）攻撃は、デバイスをユーザーがアクセスできない状態にしようとするハッカーの行為です。

DoS 攻撃では、デバイスが外部の通信要求でオーバーロード状態になり、正当なトラフィックに応答できないようになります。

この攻撃では通常、デバイスの CPU がオーバーロードになります。

Secure Core Technology（SCT）

このデバイスは、DoS 攻撃に抵抗する方法の 1 つとして SCT を採用しています。デバイスの SCT はデフォルトで有効になっていて、無効にすることはできません。シスコデバイスは、エンドユーザー（TCP）トラフィックに加えて、管理トラフィック、プロトコルトラフィック、およびスヌーピングトラフィックを処理します。SCT を使用することで、デバイスは、受信するトラフィック量に関係なく、管理およびプロトコルトラフィックを受信して処理できます。これは、CPU に対する TCP トラフィックを制限することで実現されます。

他の機能との相互作用はありません。

DoS 攻撃の種類

DoS 攻撃には、次の種類のパケットやその他の戦略が関係している可能性があります

- TCP SYN Packets：このパケットには不正な送信者アドレスが含まれていることがよくあります。各パケットは接続要求として扱われ、TCP/SYN-ACK パケット（確認応答）を送り返して、送信者アドレスからのパケット（ACKパケットへの応答）を待機することで、サーバーでハーフオープン接続が生じる原因となります。しかし、送信者アドレスは正し

くないため、応答が受信されることはありません。このようなハーフオープン接続により、デバイスで使用可能な接続が一杯になり、正当な要求に応答できなくなります。

- [TCP SYN-FIN Packets]：新しい TCP 接続を確立するために SYN パケットが送られます。TCP FIN パケットは接続を終了するために使用されます。1 つのパケット内に SYN と FIN の両方のフラグが設定されることは決してありません。結果として、これらのパケットはデバイスへの攻撃を示している可能性があるため、ブロックする必要があります。
- Martian アドレス（Martian Addresses）：Martian アドレスは、IP プロトコルの観点からは不正なアドレスです。
- ICMP 攻撃：不適切な形式の ICMP パケットまたは膨大な数の ICMP パケットが攻撃の標的に送られると、システムクラッシュが発生する可能性があります。
- IP フラグメンテーション：重複する、サイズが大きすぎるペイロードを含む細切れの IP フラグメントをデバイスが受信します。このため、TCP/IP フラグメンテーションの再アセンブリコード内のバグが原因で、さまざまなオペレーティングシステムがクラッシュすることがあります。
- Stacheldraht ディストリビューション：攻撃者はハンドラに接続します。ハンドラはゾンビエージェントにコマンドを発行する侵害を受けたシステムで、それにより DoS 攻撃を可能にします。攻撃者は、ハンドラを介してエージェントを侵害します。自動ルーチンを使用して、攻撃対象のリモートホストで実行中のリモート接続を承認するプログラムの脆弱性をエクスプロイトします。各ハンドラは、最大 1,000 のエージェントを操ることができます。
- Invasor トロイの木馬：トロイの木馬により、攻撃者はゾンビエージェントをダウンロードできます（トロイの木馬にゾンビエージェントが含まれていることもあります）。攻撃者は、リモートホストからの接続をリッスンするプログラムの欠陥をエクスプロイトする自動化ツールを使用してシステムにアクセスすることもできます。このシナリオでは、Web サーバーとして機能するデバイスを主に問題にしています。
- Back Orifice トロイの木馬：これは、Back Orifice ソフトウェアを使用してトロイの木馬をインストールするトロイの木馬のバリエーションです。

DoS 攻撃に対する防御

サービス妨害（DoS）防御機能は、このような攻撃に対抗しているシステム管理者を次の方法で支援します。

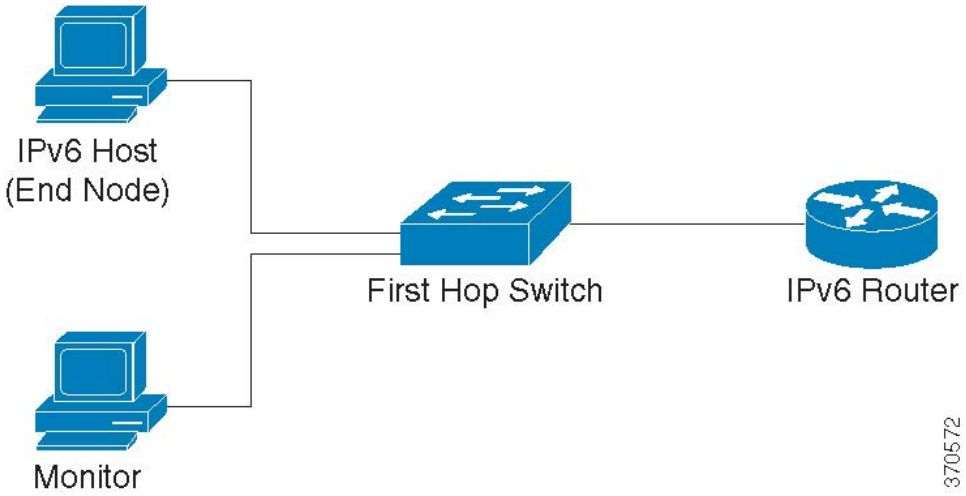
- TCP SYN 保護の有効化。この機能が有効になっている場合、SYN パケット攻撃の特定時にレポートが発行され、攻撃されたポートを一時的にシャットダウンできます。SYN 攻撃は、1 秒あたりの SYN パケットの数がユーザ設定のしきい値を超えた場合に特定されます。
- SYN-FIN パケットのブロック。
- 予約済み Martian アドレスを含むパケットのブロック。
- 特定のインターフェイスからの TCP 接続の防止およびパケットのレート制限。

- 特定の ICMP パケットのブロックの設定。
- 特定のインターフェイスからのフラグメント化された IP パケットの破棄。
- Stacheldraht ディストリビューション、Invasor トロイの木馬、および Back Orifice トロイの木馬からの攻撃の拒否。

IPv6 ファースト ホップ セキュリティ

IPv6 FHS は、IPv6 対応ネットワークでのリンク操作を保護するように設計された一連の機能です。これは、ネイバー探索プロトコルと DHCPv6 メッセージに基づいています。

この機能では、レイヤ2スイッチは（下に示すように）、複数の異なるルールに従って、ネイバー探索プロトコルメッセージ、DHCPv6メッセージ、およびユーザーデータのメッセージをフィルタ処理します。



IPv6 ファースト ホップ セキュリティの個別かつ独立したインスタンスは、その機能が有効になっている各 VLAN で実行されます。

表 7: 略語

名前	説明
CPA メッセージ	認証パス アドバタイズメント メッセージ
CPS メッセージ	認証パス請求メッセージ
DAD-NS メッセージ	重複アドレス検出ネイバー要請メッセージ
FCFS-SAVI	先入先出 - 発信元アドレス検証の改善
NA メッセージ	ネイバー アドバタイズメント メッセージ

名前	説明
NDP	ネイバー探索プロトコル
NS メッセージ	ネイバー要請メッセージ
RA メッセージ	ルータ アドバタイズメント メッセージ
RS メッセージ	ルータ要請メッセージ
SAVI	発信元アドレス検証の改善

IPv6 ファースト ホップ セキュリティのコンポーネント

IPv6 ファースト ホップ セキュリティには、次の機能があります。

- IPv6 ファースト ホップ セキュリティの共通機能
- RA ガード
- ND インスペクション
- ネイバー バインド整合性
- DHCPv6 ガード
- IPv6 ソース ガード

これらのコンポーネントは、VLAN で有効または無効にできます。

機能ごとに、VLAN default と port default という名前の 2 つの空の事前定義済みポリシーが存在します。最初のポリシーは、ユーザー定義ポリシーに接続されていない各 VLAN に接続され、2 番目のポリシーは、ユーザー定義ポリシーに接続されていない各インターフェイスと VLAN に接続されます。ユーザーはこれらのポリシーに明示的に接続できません。

IPv6 ファースト ホップ セキュリティのパイプ

IPv6 ファースト ホップ セキュリティが VLAN で有効になっている場合、スイッチは次のメッセージをトラップします。

- ルータ アドバタイズメント（RA）メッセージ
- ルータ要請（RS）メッセージ
- ネイバー アドバタイズメント（NA）メッセージ
- ネイバー要請（NS）メッセージ
- ICMPv6 リダイレクト メッセージ
- 認証パス アドバタイズメント（CPA）メッセージ
- 認証パス請求（CPS）メッセージ

- DHCPv6 メッセージ

トラップされた RA、CPA、および ICMPv6 リダイレクトメッセージは、RA ガード機能にルーティングされます。RA ガードはこれらのメッセージを検証し、不正なメッセージを破棄し、正当なメッセージを ND インスペクション機能に転送します。ND インスペクションはこれらのメッセージを検証し、不正なメッセージを破棄し、正当なメッセージを IPv6 ソースガード機能にルーティングします。

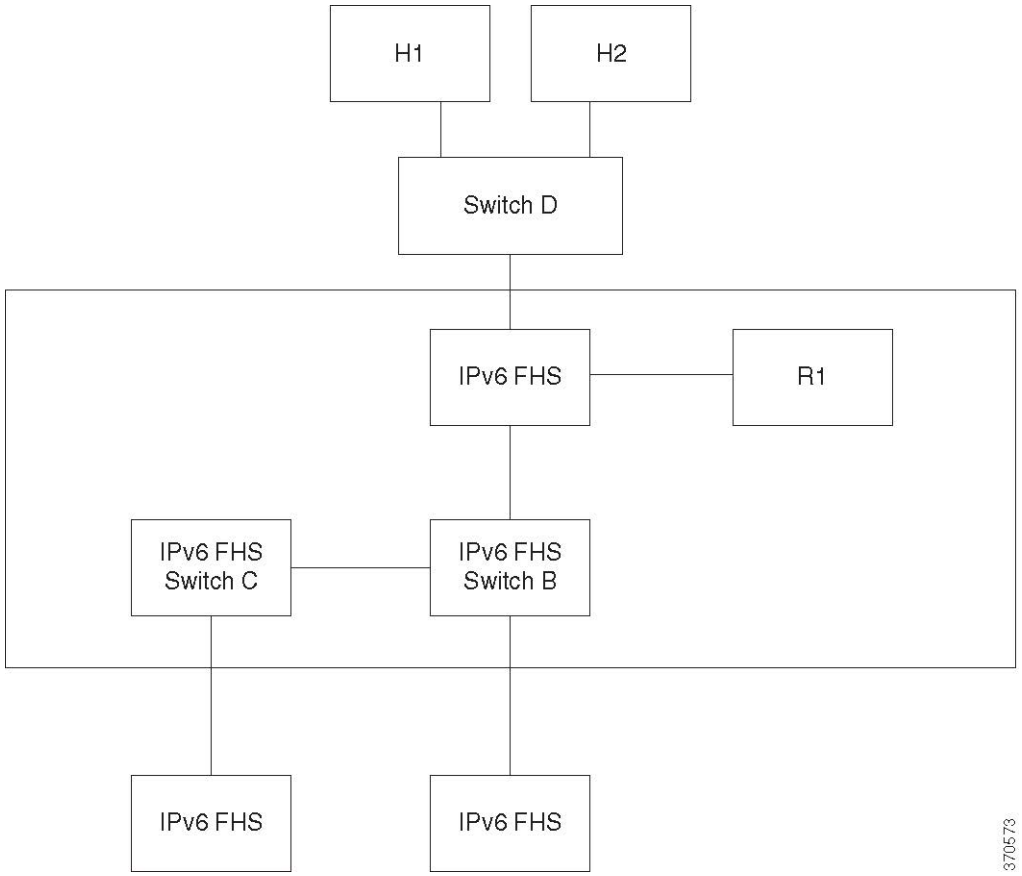
トラップされた DHCPv6 メッセージは、DHCPv6 ガード機能にルーティングされます。DHCPv6 ガードはこれらのメッセージを検証し、不正なメッセージを破棄し、正当なメッセージを IPv6 ソースガード機能に渡します。

トラップされたデータメッセージは、IPv6 ソースガード機能にルーティングされます。ネイバーバインドテーブルを使用して、IPv6 ソースガードは受信メッセージ（トラップされたデータメッセージ、ND インスペクションからの NDP メッセージ、および DHCPv6 ガードからの DHCPv6 メッセージ）を検証し、不正なメッセージをドロップし、正当なメッセージを転送します。ネイバーバインド整合性では、受信メッセージ（NDP および DHCPv6 メッセージ）からネイバーを取得し、それらをネイバーバインドテーブルに保存します。

静的エントリは手動で追加することもできます。アドレスを学習したら、NBI 機能はフレームを転送します。ND インスペクション機能は、トラップされた RS、CPS NS および NA メッセージも受信します。ND インスペクションはこれらのメッセージを検証し、不正なメッセージを破棄し、正当なメッセージを IPv6 ソースガード機能に転送します。

IPv6 ファースト ホップ セキュリティの境界

IPv6 ファースト ホップ セキュリティ スイッチは、境界を形成することで、信頼できるエリアを信頼できないエリアから分離することができます。境界内のすべてのスイッチは IPv6 ファーストホップセキュリティをサポートし、境界内のホストとルータは信頼できるデバイスです。たとえば、下の図のスイッチ B とスイッチ C は、保護されたエリア内の内部リンクです。



ネイバーバインドポリシー設定画面の device-role コマンドで、境界を指定します。各 IPv6 ファースト ホップ セキュリティ スイッチは、エッジによって分割されたネイバーをバインドします。この方法により、バインドエントリは IPv6 ファースト ホップ セキュリティ デバイスに分散されて、境界を形成します。その後、IPv6 ファースト ホップ セキュリティ デバイスは、各デバイスですべてのアドレスのバインドを設定せずに、境界の内部にバインド整合性を提供できます。

ルータ アドバタイズメント ガード

ルータ アドバタイズメント（RA）ガードは、トラップされた RA メッセージを処理する最初の FHS 機能です。RA ガードは、次の機能をサポートしています。

- 受信した RA、CPA、および ICMPv6 リダイレクト メッセージのフィルタリング。RA ガードは、ロールがルータではないインターフェイスで受信された RA および CPA メッセージを破棄します。
- 受信した RA メッセージの検証。RA ガードは、インターフェイスに接続されている RA ガードポリシーに基づくフィルタリングを使用して RA メッセージを検証します。

メッセージが検証に合格しないと、ドロップされます。FHS 共通コンポーネントのロギング パケット ドロップ設定が有効になっている場合は、レートが制限された SYSLOG メッセージが送信されます。

ネイバー探索インスペクション

ネイバー探索（ND）インスペクションは、次の機能をサポートしています。

- 受信したネイバー探索プロトコルメッセージの検証
- 出力フィルタリング

メッセージ検証

インターフェイスに接続されている ND インスペクションポリシーに基づいて、ND インスペクションはネイバー探索プロトコルメッセージを検証します。[ND Inspection Settings] ページで、このポリシーを定義できます。

メッセージがポリシーで定義されている検証に合格しない場合、メッセージはドロップされ、代わりにレート制限 SYSLOG メッセージが送信されます。

出力フィルタリング

ND インスペクションは、ホスト インターフェイスとして設定されているインターフェイスでの RS および CPS メッセージの転送をブロックします。

ネイバー バインド整合性

ネイバー バインド（NB）整合性では、ネイバーのバインドが確立されます。NB 整合性の個別かつ独立したインスタンスは、その機能が有効になっている各 VLAN で実行されます。

アドバタイズされた IPv6 プレフィックスの学習

NB 整合性は、RA メッセージでアドバタイズされた IPv6 プレフィックスを学習し、ネイバー プレフィックス テーブルに保存します。プレフィックスは、割り当てられたグローバル IPv6 アドレスの検証に使用されます。デフォルトでは、この検証は無効になっています。これを有効にすると、アドレスは [Neighbor Binding Settings] ページのプレフィックスと照らし合わせて検証されます。アドレス検証に使用されるスタティックプレフィックスは、[Neighbor Prefix Table] ページで追加できます。

グローバル IPv6 アドレスの検証

NB 整合性は、次の検証を実行します。

- NS または NA メッセージのターゲット アドレスがグローバル IPv6 アドレスの場合は、RA プレフィックス テーブルで定義されているプレフィックスのいずれかに属している必要があります。

- DHCPv6 サーバーから提供されたグローバル IPv6 アドレスは、IPv6 プレフィックスリストで定義されているプレフィックスのいずれかに属している必要があります。

メッセージが検証に合格しない場合、メッセージはドロップされ、レート制限 SYSLOG メッセージが送信されます。

ネイバー バインド テーブルのオーバーフロー

新しいエントリを作成する空き領域がない場合は、エントリは作成されず、SYSLOGメッセージが送信されます。

ネイバーのバインドの確立

IPv6 ファースト ホップ セキュリティ スイッチは、次のメソッドを使用してバインド情報を検出および記録できます。

- NBI-NDP メソッド：スヌープされたネイバー探索プロトコル メッセージから IPv6 アドレスを学習
- NBI-DHCP メソッド：スヌープされた DHCPv6 メッセージから IPv6 アドレスを学習
- NBI 手動メソッド：手動設定を使用

IPv6アドレスは、ホストのネットワーク接続のリンク層プロパティにバインドされます。このプロパティは「バインドアンカー」と呼ばれ、ホストの接続に使用されるインターフェイス識別子（if Index）とホストの MAC アドレスで構成されています。

IPv6 ファースト ホップ セキュリティ スイッチは、境界インターフェイスのみでバインドを確立します。バインド情報は、ネイバーバインドテーブルに保存されます

NBI-NDP メソッド

使用される NBI-NDP メソッドは、RFC6620 で指定されている FCFS-SAVI メソッドに基づいていますが、次の違いがあります。

- リンク ローカル IPv6 アドレスのバインドのみをサポートする FCFS SAVI とは異なり、NBI-NDP はさらにグローバル IPv6 アドレスのバインドをサポートします。
- NBI-NDP は、NDP メッセージから学習した IPv6 アドレスのみを対象とした IPv6 アドレスバインドをサポートします。データ メッセージの発信元アドレス検証は、IPv6 ソースアドレス ガードによって提供されます。
- NBI-NDP では、アドレス所有権の証明は先着順の原則に基づいています。特定の発信元アドレスを要求する最初のホストが、さらに通知があるまでそのアドレスの所有者になります。ホストの変更は承認されないため、新しいプロトコルを必要とせずにアドレスの所有権を確認する方法を見つける必要があります。このため、NDP メッセージから IPv6 アドレスを最初に学習するたびに、スイッチはアドレスをインターフェイスにバインドします。この IPv6 アドレスを含む以降の NDP メッセージを、同じバインド アンカーに照らし合わせてチェックすることで、発信元が送信元 IP アドレスを所有していることを確認できます。

IPv6 ホストが L2 ドメインにローミングするか、またはその MAC アドレスを変更した場合は、このルールの例外が発生します。この状況では、ホストは引き続き IP アドレスの所有者ですが、関連付けられているバインドアンカーが変更された可能性があります。この状況に対処するために、NBI-NDP は、以前のバインド インターフェイスに DAD-NS メッセージを送信することにより、ホストに引き続き到達可能かどうかを検証します。以前に記録されたバインド アンカーでホストに到達できない場合、NBI-NDP は新しいアンカーが有効であると見なし、バインドアンカーを変更します。以前に記録されたバインドアンカーを使用してホストに引き続き到達可能な場合、バインドインターフェイスは変更されません。

ネイバーバインドテーブルのサイズを減らすために、NBI-NDP は境界インターフェイスのみでバインドを確立し（「IPv6 ファースト ホップ セキュリティの境界」を参照）、NS および NA メッセージを使用して、内部インターフェイス経由でバインド情報を配布します。NBI-NDP ローカル バインドを作成する前に、デバイスは関連するアドレスを照会する DAD-NS メッセージを送信します。あるホストが NA メッセージでそのメッセージに応答した場合、DAD-NS メッセージを送信したデバイスは、そのアドレスのバインドが別のデバイスに存在すると推測し、そのアドレスのローカル バインドを作成しません。DAD-NS メッセージへの応答として NA メッセージを受信しなかった場合、ローカルデバイスは、そのアドレスのバインドが他のデバイスに存在しないと推測し、そのアドレスのローカル バインドを作成します。

NBI-NDP は、ライフタイム タイマーをサポートしています。タイマーの値は、[Neighbor Binding Settings] ページで設定できます。このタイマーは、バインドされた IPv6 アドレスが確認されるたびに再起動されます。タイマーが期限切れになった場合、デバイスは短い間隔で最大 2 つの DAD-NS メッセージを送信してネイバーを検証します。

NBI-DHCP メソッド

NBI-NDP メソッドは、SAVI Solution for DHCP（draft-ietf-savi-dhcp-15、2012 年 9 月 11 日）で指定されている SAVI-DHCP メソッドに基づいています。

NBI-NDP と同様に、NBI-DHCP は、拡張性のために境界バインドを提供します。NBI-DHCP メソッドと NBI-FCFS メソッドには、次の違いがあります。NBIDHCP は DHCPv6 メッセージで発表された状態に従います。そのため、NS/NA メッセージで状態を配布する必要はありません。

NB 整合性ポリシー

他の IPv6 ファースト ホップ セキュリティ機能の動作と同じように、インターフェイスでの NB 整合性の動作は、インターフェイスに接続されている NB 整合性ポリシーで指定されます。これらのポリシーは、[Neighbor Binding Settings] ページで設定されます

DHCPv6 ガード

DHCPv6 ガードでは、トラップされた DHCPv6 メッセージが処理されます。DHCPv6 ガードは、次の機能をサポートしています。

- 受信したDHCPv6メッセージのフィルタリング。DHCPガードは、ロールがクライアントであるインターフェイスで受信されたDHCPv6メッセージを破棄します。インターフェイスロールは [DHCP Guard Settings] ページで設定されます。
- 受信したDHCPv6メッセージの検証。DHCPv6ガードは、インターフェイスに接続されている DHCPv6 ガード ポリシーに基づくフィルタリングを使用して DHCPv6 メッセージを検証します。

メッセージが検証に合格しないと、ドロップされます。FHS 共通コンポーネントのロギング パケット ドロップ設定が有効になっている場合は、レートが制限された SYSLOG メッセージが送信されます。

IPv6 ソース ガード

ネイバー バインド整合性（NB 整合性）が有効になっている場合、IPv6 ソース ガードは、有効になっているかどうかに関係なく、NDP および DHCPv6 のメッセージの送信元 IPv6 アドレスを検証します。NB整合性とIPv6ソース ガードがどちらも有効になっている場合、IPv6ソース ガードはTCAM を設定して、どの IPv6 データ フレームを転送、ドロップ、または CPU にトラップする必要があるかを指定し、トラップされた IPv6 データ メッセージの送信元 IPv6 アドレスを検証します。NB整合性が有効になっていない場合、IPv6 ソース ガードは有効になっているかどうかに関係なくアクティブ化されません。

TCAM に新しいルールを追加する空き領域がない場合、TCAM オーバーフローカウンタが増加し、インターフェイス識別子、ホストのMACアドレス、およびホストのIPv6アドレスが含まれるレート制限SYSLOGメッセージが送信されます。IPv6 ソース ガードは、ネイバー バインドテーブルを使用して、受信したIPv6メッセージの送信元アドレスを検証します。ただし、検証なしで渡される次のメッセージを除きます。

- RS メッセージ（送信元 IPv6 アドレスが未指定の IPv6 アドレスに等しい場合）。
- NS メッセージ（送信元 IPv6 アドレスが未指定の IPv6 アドレスに等しい場合）。
- NA メッセージ（送信元 IPv6 アドレスがターゲット アドレスに等しい場合）。

IPv6 ソース ガードは、送信元 IPv6 アドレスが未指定の IPv6 アドレスに等しい他のすべてのIPv6メッセージをドロップします。IPv6 ソース ガードは、境界に属する信頼できないインターフェイスのみで実行されます。

IPv6 ソース ガードは、次の場合に入力 IPv6 メッセージをドロップします。

- ネイバー バインド テーブルに IPv6 アドレスが含まれていない場合。
- ネイバー バインド テーブルに IPv6 アドレスが含まれているが、別のインターフェイスにバインドされている場合。

IPv6 ソースガードは、不明な送信元 IPv6 アドレスの DAD_NS メッセージを送信することにより、ネイバーリカバリプロセスを開始します

-

攻撃からの保護

この項では、IPv6 ファースト ホップ セキュリティで提供される攻撃からの保護について説明します

IPv6 ルータ スプーフィングに対する保護

IPv6 ホストは、受信した RA メッセージを次の目的で使用できます。

- IPv6 ルータの検出
- ステートレス アドレスの設定

悪意のあるホストは、RA メッセージを送信して、自身を IPv6 ルータとしてアドバタイズし、ステートレス アドレス設定用の偽造プレフィックスを提供する可能性があります。RA ガードは、IPv6 ルータを接続できないすべてのインターフェイス用のホスト インターフェイスとしてインターフェイス ロールを設定することにより、このような攻撃からの保護を実現します。

IPv6 アドレス解決スプーフィングに対する保護

悪意のあるホストは、NA メッセージを送信して、特定の IPv6 アドレスを持つ IPv6 ホストとして自身をアドバタイズする可能性があります。NB 整合性は、次の方法でこのような攻撃からの保護を提供します。

- 特定の IPv6 アドレスが未知の場合は、内部インターフェイスのみにネイバー要請（NS）メッセージが転送されます。
- 特定の IPv6 アドレスが既知の場合は、IPv6 アドレスがバインドされているインターフェイスにのみ NS メッセージが転送されます。
- ネイバー アドバタイズメント（NA）メッセージは、ターゲット IPv6 アドレスが別のインターフェイスにバインドされている場合はドロップされます。

IPv6 重複アドレス検出スプーフィングに対する保護

IPv6 ホストは、特別な NS メッセージ（重複アドレス検出ネイバー要請（DAD_NS）メッセージ）を送信することによって、割り当てられている各 IPv6 アドレスに対して重複アドレス検出を実行する必要があります。

悪意のあるホストは、DAD_NS メッセージに対する応答を送信して、特定の IPv6 アドレスを持つ IPv6 ホストとして自身をアドバタイズする可能性があります。NB 整合性は、次の方法でこのような攻撃からの保護を提供します。

- 特定の IPv6 アドレスが未知の場合は、内部インターフェイスにのみ DAD_NS メッセージが転送されます
- 特定の IPv6 アドレスが既知の場合は、IPv6 アドレスがバインドされているインターフェイスにのみ DAD_NS メッセージが転送されます。
- NA メッセージは、ターゲット IPv6 アドレスが別のインターフェイスにバインドされている場合はドロップされます。

DHCPv6 サーバ スプーフィングに対する保護

IPv6 ホストは、DHCPv6 プロトコルを次の目的で使用できます。

- ステートレス情報の設定
- ステートレス アドレスの設定

NBD キャッシュ スプーフィングに対する保護

IPv6 ルータは、IPv6 アドレスをラスト ホップ ルーティング用の MAC アドレスにマップするネイバー探索プロトコル（NDP）キャッシュをサポートしています。悪意のあるホストは、ラスト ホップ転送用に異なる宛先 IPv6 アドレスを含む IPv6 メッセージを送信して、NBD キャッシュのオーバーフローを引き起こす可能性があります。

NDP 実装の組み込みのメカニズムでは、ネイバー探索キャッシュ内で許容される不完全状態のエントリの数が制限されます。これにより、ハッカーによるテーブルのフラッディングに対する保護が実現されます。

セキュア センシティブ データ管理

セキュアセンシティブデータ（SSD）は、パスワードやキーなどのデバイス上の機密データの保護を可能にするアーキテクチャです。パスワード、暗号化、アクセス制御、およびユーザー認証を使用して、機関で機密データを管理するための安全なアプローチを作成します。

この機能は、構成ファイルを保護し、構成プロセスを保護し、SSD ゼロタッチ自動構成を容易にするように拡張されています。

SD は、ユーザー資格情報および SSD ルールに基づき暗号化された機密データや機密データへのプレーンテキストでのアクセスの許可/拒否、機密データを含むコンフィギュレーション ファイルの改ざんからの保護により、デバイスの機密データ（パスワードやキーなど）を保護します。

さらに、SSD では、機密情報を含むコンフィギュレーション ファイルをセキュアにバックアップおよび共有することができます。

ユーザーは機密データに必要な保護のレベルを、プレーンテキストの機密データを保護しないレベルから、デフォルトパスフレーズに基づく暗号化による最小限の保護、ユーザー定義のパスフレーズに基づく暗号化による強力な保護まで、選択できます。

認証され承認されたユーザーのみに機密データへの読み取り権限が付与され、これは SSD の規制に従って行われます。ユーザー認証プロセスを通じて、デバイスはユーザーに対する管理アクセスを認証および承認します。SSD を使用しているかどうかにかかわらず、管理者は、ローカル認証データベースを使用して認証プロセスの安全性を確保したり、ユーザー認証プロセスで使用される外部認証サーバーへの通信の安全性を確保したりすることが推奨されます。

要約すると、SSD は、SSD 規則、SSD 属性、およびユーザー認証を使用して、デバイス上の機密データを保護します。また、デバイスの SSD 規則、SSD 特性、ユーザー認証構成はすべて、SSD が保護する重要なデータです。

SSD 管理

SSD管理は、機密データをどのように処理および保護するかを指示する一連のセットアップパラメータで構成されます。SSD 構成パラメータは、SSD によって保護される機密情報です。

SSD 構成はすべて、適切な権限を持つ人だけがアクセスできる SSD ページから行います。

SSDルール

SSD規則により、管理チャネルのユーザーセッションに割り当てられる読み取りアクセス許可とデフォルトの読み取りモードが定義されます。SSD 規則が属するユーザーおよび SSD 管理チャネルは、独自のIDを提供します。同じユーザーだが異なるチャネルに対応する異なるSSD規則が存在することがあります。逆に、同じチャネルだが異なるユーザーに対応する異なる規則が存在することがあります。

読み取りアクセス許可は、次のような機密データを表示する方法を指定します。暗号化された形式のみ、プレーンテキスト形式のみ、暗号化された形式とプレーンテキスト形式の両方、または機密データへのアクセス許可なし。SSD規制は機密データとして分類されているため、保護されています。

デバイスでサポートできる SSD 規則は合計 32 個あります。デバイスにより、ユーザーアイデンティティ/クレデンシャルおよびユーザーの機密データへのアクセスで経由する管理チャネルのタイプに最も一致するSSD規則のSSD読み取りアクセス許可がユーザーに付与されます。

すべてのデバイスには、一連のデフォルト SSD 規則が含まれています。SSD 規則は、管理者がいつでも追加、削除、変更できます。

デフォルトの SSD ルール

デバイスは、次のファクトリー デフォルトの規則を保持しています。

ルール キー		規則アクション	
ユーザ	チャネル	読み取り権限	デフォルト読み取りモード
レベル 15	セキュア XML SNMP	Plaintext Only	Plaintext
レベル 15	セキュア	Both	Encrypted
レベル 15	非セキュア	Both	Encrypted
すべて（All）	非セキュア XML SNMP	Exclude	Exclude
すべて（All）	セキュア	Encrypted Only	Encrypted
すべて（All）	非セキュア	Encrypted Only	Encrypted

デフォルトの規則を変更することはできますが、削除することはできません。SSDデフォルト規則を変更した場合は、それらを復元できます。

セキュア シェル

セキュアシェル（SSH）は、SSH クライアント（デバイス）と SSH サーバー間でデータのセキュアな送信を可能にするネットワークプロトコルです。

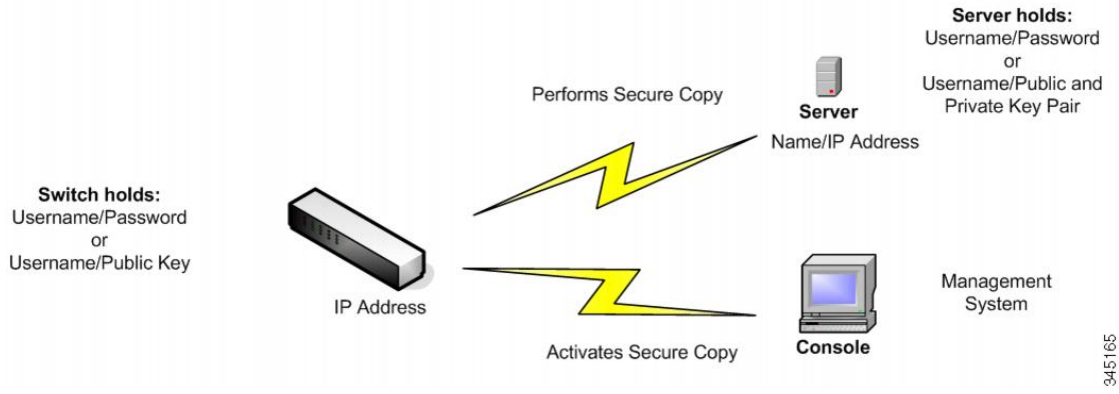
SSH クライアントは、中央の SSH サーバーに保持されているさまざまなシステムファイルを持つ1つ以上のスイッチで構成されるネットワークの管理を支援します。SSH プロトコルを使用してネットワークを通じて構成ファイルを転送するアプリケーションであるセキュアコピー（SCP）により、ユーザー名/パスワードなどの機密データが盗まれないことが保証されます。セキュアコピー（SCP）は、ファームウェア、ブートイメージ、設定ファイル、言語ファイル、およびログファイルを中央SCPサーバーからデバイスへ安全に転送するための方法です。

SSH に関しては、デバイスで実行されている SCP が SSH クライアント アプリケーションであり、SCP サーバが SSH サーバ アプリケーションとなります。

ファイルが TFTP または HTTP を介してダウンロードされる場合、データ転送は保護されません。ファイルがSCPを介してダウンロードされる場合、データはセキュアチャネル経由でSCPサーバーからデバイスへ送信されます。この安全なチャネルを作成するには、ユーザーがアクティビティを実行する権限を持っていることを確認するため、認証が必要です。この項目ではサーバーの操作について説明しませんが、認証情報は、デバイスと SSH サーバーの両方に、ユーザーが入力する必要があります。

次の図は、SCP 機能を利用できる一般的なネットワーク構成を示しています。

一般的なネットワーク構成



QoS

QoS（Quality of Service）は、さまざまなアプリケーション、データフロー、またはユーザーのパフォーマンスを保証するために、1 つまたは複数のタイプのトラフィックに他よりも高い優

先度を割り当てます。QoSでは、ネットワーク上に存在するさまざまな変数を調べることで、問題への対処方法が決定されます。

QoS が対処する問題

- 遅延：宛先ネットワークへの理想的なパフォーマンスを発揮できないルート。このような遅延により、VoIPなどの一部のアプリケーションでエラーが発生する可能性があります。
  - QoS を使用する最大の理由は、リアルタイム アプリケーション（RTA）への対応です。
- パケットのドロップ：バッファが一杯になり、パケットが時間内に処理されないと、それらのパケットがドロップされます。競合のあるリンクでは、QoSがトラフィックに優先度を割り当てるため、重要度の低いトラフィックのパケットがドロップされます。
- エラー：パケットはさまざまな理由で破損しますが、TCP を使用しているため、ACK を受信するまで再送信が継続され、再送信と遅延が発生します。
- ジッター：パケットが宛先に到達するパスは複数存在する可能性があり、最適パスが使用されない場合があります。この変動により、「ジッター」と呼ばれる遅延が発生します。ジッターは 30 ミリ秒未満にする必要があります。また、パケット損失は 1% 以下にする必要があります。
- 順不同配信：パケットはさまざまなパスを使用して宛先に到達するため、受信するアプリケーションでパケットの並べ替えに予期以上の時間がかかり、遅延やドロップが発生する場合があります。QoSは、予測可能性のレベルに関する要件を持つアプリケーションが、必要な帯域幅を受け取ることを保証します。

QoS のメカニズム

- 分類：QoS のクラス指向のメカニズムによってサポートされます。
- 輻輳管理：各インターフェイスのキューイングメカニズムでパケットの送信に優先順位を付けるために使用されます。
- ポリシング：パケットをドロップまたはマークダウンすることによってレート制限を適用するために使用されます。
- シェーピング：バッファを使用してパケットを遅延させることによってレート制限を適用するために使用されます。

QoS の一般パラメーターを設定を設定するには、次の手順に従います。

ステップ 1 [QoSプロパティ]ページで信頼モードを選択し、QoSを有効にします。次に、[インターフェイス設定]ページで、ポートに対する QoS を有効にします。

ステップ 2 [QoS プロパティ] ページで、各インターフェイスにデフォルトの CoS または DSCP プライオリティを割り当てます。

ステップ 3 [キュー] ページで、各出力キューに対してスケジュール方式（完全優先または WRR）と WRR 帯域割り当て率を設定します。

ステップ 4 [DSCP 値のキューへのマッピング] ページで、各 IP DSCP/TC 値に出力キューを割り当てます。デバイスが DSCP 信頼モードになっている場合、着信パケットは、その DSCP/TC 値に基づいて出力キューに格納されます。

ステップ 5 各 CoS/802.1p プライオリティに出力キューを割り当てます。デバイスが CoS/802.1 信頼モードになっている場合、すべての着信パケットは、パケットの CoS/802.1p プライオリティに基づいて出力キューに格納されます。この作業は [CoS/802.1p 値のキューへのマッピング] ページで行います。

ステップ 6 次のページで、帯域幅とレート制限を設定します。

a) [キューあたりの出力シェーピング] ページで、各キューに対する出力シェーピングを設定します。

b) [帯域幅] ページで、各ポートに対する入力レート制限と出力シェーピング レートを設定します。

QoS の機能とコンポーネント

QoS 機能は、ネットワークのパフォーマンスを最適化する目的で使用されます。

QoS を使用すると、次のことが可能です。

- 次の属性に基づいて着信パケットをトラフィック クラスに分類する。
  - デバイス設定
  - 入力インターフェイス
  - パケット内容
  - これらの属性の組み合わせ

QoS には、以下のことが含まれます。

- トラフィック分類：着信パケットのそれぞれを、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 フローに属するものとして分類します。分類は ACL（アクセス制御リスト）によって行われ、ACL の条件を満たすトラフィックだけが CoS または QoS 分類の対象になります。
- ソフトウェア キューへの割り当て：着信パケットが転送キューに割り当てられます。パケットは特定のキューに送信され、それらのパケットが属しているトラフィック クラスの機能として処理されます。
- その他のトラフィック クラス処理属性：QoS 機構が各種のクラス（帯域幅管理など）に適用されます。

QoS モード

選択されている QoS モードは、システム内のすべてのインターフェイスに適用されます。

- 基本モード：サービス クラス（CoS）。

同じクラスのトラフィックはすべて、同じように処理されます。具体的には、着信フレーム内で示されている QoS 値に基づいて、出力ポート上の出力キューを決定するという 1 つの QoS アクションが実行されます。この QoS 値は、レイヤ 2 においては VLAN Priority Tag（VPT）802.1p 値となり、レイヤ 3 においては、IPv4 の場合は Differentiated Service Code Point（DSCP）値、IPv6 の場合はトラフィック クラス（TC）値となります。デバイスが基本モードで動作している場合、外部デバイス上で割り当てられたこの QoS 値が信頼されます。外部デバイス上で割り当てられた、パケットの QoS 値によって、そのパケットのトラフィック クラスと QoS が決定されます。

- 拡張モード：フローごとのサービス品質（QoS）。

  拡張モードの場合、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 マップはフローのトラフィックの種類を定義し、1 つ以上の ACL が含まれています。ACL に合致するパケットは、フローに属します。
  - ポリサーは、設定されている QoS をフローに適用します。フローの QoS 設定に含められるのは、出力キュー、DSCP または CoS/802.1p 値、およびアウト オブ プロファイル（超過）トラフィックに対するアクションです。

- 無効モード：このモードでは、すべてのトラフィックが単一のベスト エフォート キューにマッピングされるため、特に優先されるトラフィックのタイプはありません。

アクティブになるのは一度に 1 つのモードだけです。システムが QoS 拡張モードで動作するように設定されているときには、QoS 基本モードの設定値はアクティブになりません。その逆も同じです。

モードが変更されると、次のことが発生します。

- QoS 拡張モードからその他のモードに変更される場合、ポリシー プロファイル定義とクラス マップが削除されます。インターフェイスに直接適用されている ACL は、適用された状態のままになります。
- QoS 基本モードから拡張モードに変更される場合、基本モードでの QoS 信頼モードの設定は保持されません。
- QoS が無効にされた場合、シェーパーとキューの設定（WRR/SP 帯域幅の設定）はデフォルト値にリセットされます。

その他のすべてのユーザ設定は、そのまま維持されます。

SNMP

SNMP は、マネージャとエージェント間の通信のメッセージ フォーマットを提供するアプリケーションレイヤプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および管理情報ベース（MIB）で構成されます。SNMP マネージャは、CiscoWorks などのネットワーク管理システム（NMS）に統合できます。エージェントおよび MIB は、スイッチ

に常駐します。スイッチにSNMPを設定するには、マネージャとエージェントの関係を定義します。

SNMPは、通常、ルータの管理に関連付けられていますが、さまざまなタイプのデバイスの管理に使用できることを理解することが重要です。スイッチはSNMPエージェントとして機能し、SNMPv1、v2、v3をサポートします。

SNMPエージェントはMIB変数を格納し、SNMPマネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイスパラメータやネットワークデータの保存場所であるMIBから値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態をSNMPマネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MACアドレス追跡、TCP接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

SNMP バージョン

インターネット技術標準化委員会（IETF）は、SNMPを含むインターネットトラフィックを制御する標準プロトコルの定義を担当しています。IETFは、IPレルムに存在する多くのプロトコルの仕様であるRequests for Comments（RFC）を公開しています。これらのドキュメントは、まず、標準化提案として標準化過程に入り、次に、ドラフトステータスに移行します。最終ドラフトが最終的に承認されると、そのRFCに標準ステータスが与えられますが、完全に承認された標準は一般に思われているほど多くありません。他にも「歴史的」と「実験的」という2つの標準化過程の分類があり、それぞれ、「より新しいRFCによって置き換えられたドキュメント」と「まだ標準になるには準備不足であるドキュメント」が含まれます。次のリストには、現在のすべてのSNMPバージョンとそれぞれのIETFステータスが含まれています。

- SNMPバージョン1（SNMPv1）は、SNMPプロトコルの最初のバージョンです。これはRFC 1157で定義されており、歴史的IETF標準です。SNMPv1のセキュリティの基盤であるコミュニティストリングは、単なるパスワード（プレーンテキストストリング）にすぎません。この文字列を認識するすべてのSNMPベースアプリケーションに、デバイスの管理情報へのアクセスが許可されます。SNMPv1には基本として3つのコミュニティ（読み取り専用、読み取り/書き込み、トラップ）があります。SNMPv1は歴史的標準ですが、今でも多くのベンダーがサポートする主要なSNMP実装であることに注意してください。
- SNMPバージョン2（SNMPv2）は、多くの場合、コミュニティストリングベースのSNMPv2と呼ばれます。
- SNMPバージョン3（SNMPv3）は、最新バージョンのSNMPです。ネットワーク管理上の主な役割はセキュリティです。管理対象エンティティ間の強力な認証およびプライベート通信のサポートが追加されています。

システムへのアクセスを制御するには、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、コミュニティストリングおよびそのアクセス権限で構成されます。適切な権限および正しい操作を持つコミュニティを指定するSNMPメッセージにのみ、システムは応答します。

SNMPエージェントは、デバイスの管理に使用される変数のリストを維持します。これらの変数は、管理情報ベース（MIB）で定義されます。

表 *8 : SNMP* のバージョンとセキュリティ レベル

バージョン	レベル	認証	暗号化
SNMPv1	noAuthNoPriv	コミュニティストリング	未対応
SNMPv2C	noAuthNoPriv	コミュニティストリング	未対応
SNMPv3	noAuthNoPriv	Username	未対応
SNMPv3	authNoPriv	Message Digest 5（MD5）またはSecure Hash Algorithm（SHA）	なし
SNMPv3	authPriv（暗号化ソフトウェアイメージが必要）	MD5 または SHA	データ暗号規格（DES）またはAdvanced Encryption Standard（AES）

（注） その他のバージョンにはセキュリティの脆弱性があるため、SNMPv3を使用することをお勧めします。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリートポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS がスイッチにアクセスするには、NMS のコミュニティ ストリング定義が、スイッチ上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致していなければなりません。

コミュニティ ストリングの属性は、次のいずれかです。

- Read-Only（RO）：許可された管理ステーションに、コミュニティ ストリングを除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- Read-Write（RW）：許可された管理ステーションに、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ ストリングに対するアクセスは許可しません。
- クラスタを作成すると、コマンド スイッチがメンバ スイッチと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドスイッチ上で最初に設定された RW および RO コミュニティストリングにメンバスイッチ番号（*@esN*、*N* はスイッチ番号）を追加し、これらのストリングをメンバスイッチに伝播します。

サポートされている MIB

Management Information Base（MIB）は定義の集合であり、これらによって管理対象デバイス内の管理対象オブジェクトのプロパティが定義されます。サポート対象 MIB の一覧を表示するには、次の URL に移動し、Cisco MIBS として列挙されたダウンロード エリアに移動します：

http://www.cisco.com/cisco/software/navigator.html

SNMP を介したスイッチポートモードの設定

スイッチで SNMP を介してスイッチポートモードを設定するには、次の手順を実行します。

ステップ 1 コンソールポート経由でスイッチに接続し、スイッチを工場出荷時のデフォルトにリセットします。

ステップ 2 SNMP を有効にして、読み取りおよび書き込み権限のコミュニティ名を設定します。

ステップ 3 任意の MIB ブラウザ（MG-Soft など）で、vlanPortModeState を選択して右クリックします。

ステップ 4 次に、[Set] を選択します。

ステップ 5 [Select Table Instance(s)] が表示されます。このテーブルには、インターフェイス ID に対応するインスタンス ID と、スイッチポートに対応する [Value] 列の値が含まれます。

例：

インスタンス 1 は GigabitEthernet 1/0/1 インターフェイスに対応します。

例：

インスタンス 3 は GigabitEthernet 1/0/3 インターフェイスに対応します。

[Value] は、インターフェイスのスイッチポートモードがアクセスされていることを示します。

全般モード	10	プライベート - VLAN プロミスキャスモード	13
アクセス モード	11	プライベート - VLAN ホストモード	14
トランク モード	12	カスタマー	15

ステップ 6 [Instance 3] を選択し、GigabitEthernet 1/0/3 インターフェイスのスイッチポートモードを [General] に変更します。

ステップ 7 次に、トランクモードについて手順を繰り返します。

SNMP を介した VLAN の作成または追加

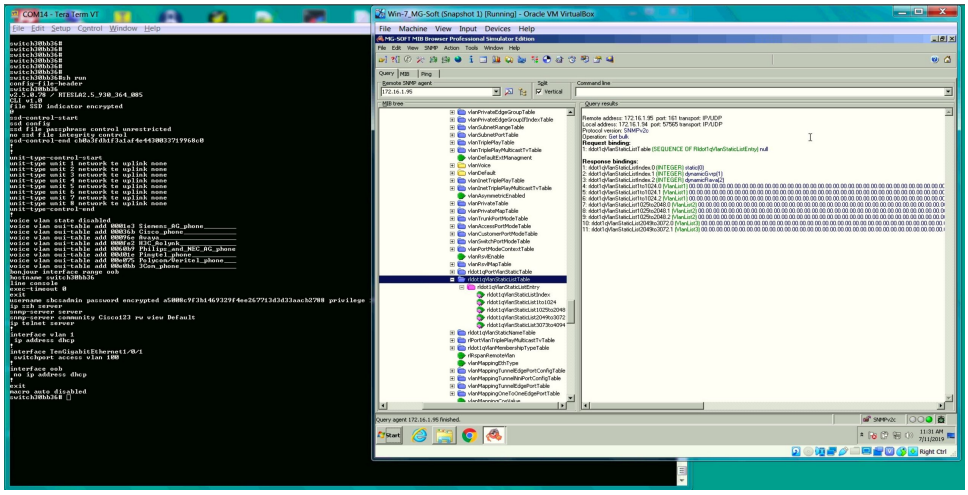
スイッチで VLAN を作成または追加するには、次の手順を実行します。

ステップ 1 コンソールポート経由でスイッチに接続し、スイッチを工場出荷時のデフォルトにリセットします。

ステップ 2 SNMP を有効にして、読み取りおよび書き込み権限のコミュニティ名を設定します。

ステップ 3 show run コマンドを実行します。

ステップ 4 任意の MIB ブラウザ（この例では MG-Soft）で、rldot1qVlanStaticListTable MIB コンテナを選択し、Get Bulk 操作を実行します。



ステップ 5 上のスライドを参照して、VLAN を作成または追加します。

a) VLAN 2 ～ 14、16 を追加します。

b) [rldot1qVlanStaticList1to1024] を選択します。

c) [Set] 操作ウィンドウを開きます。

d) VLAN 値をオクテット形式 ”# 0x7F 0xFD で設定します。

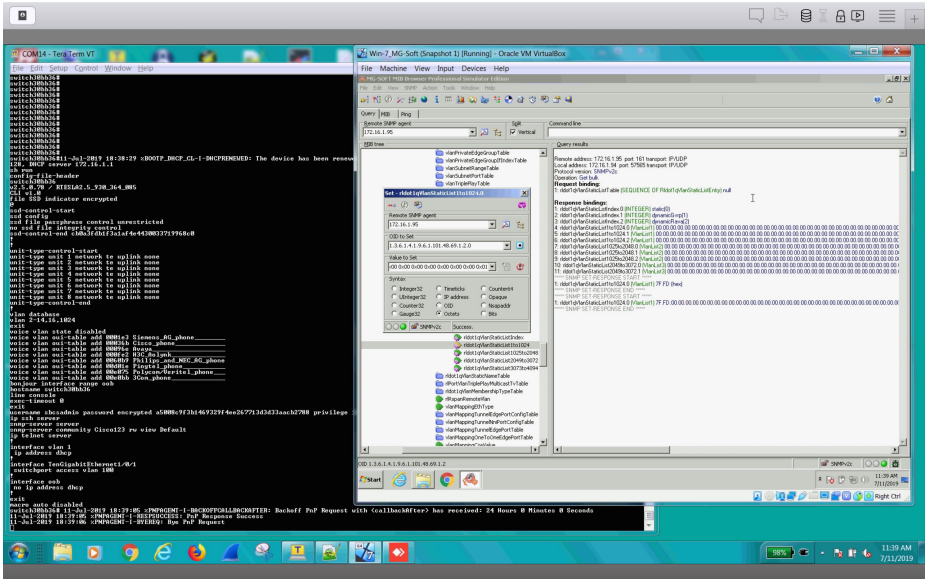
例：

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

オクテットビット：0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1

オクテット（16 進数）：7 F F D

ステップ 6 [Set] をクリックして VLAN を追加します。



ステップ 7 VLAN 1024 を追加する場合は、次の手順を実行します。

a) [Set] 操作ウィンドウを開いた状態で、[Value to Set] をクリックしてアイコンを更新します。このフィールドが “rldot1qVlanStaticList1to1024 で更新されます。

b) フィールド内を最後のオクテットまで右にスクロールして、1024 番目のビット値を 1 に設定します。

c) [Set] をクリックします。

4 つの分かりやすい VLAN のリストがあります。

- rldot1qVlanStaticList1to1024
- rldot1qVlanStaticList1025to2048
- rldot1qVlanStaticList2049to3072
- rldot1qVlanStaticList3073to4094

SNMP 経由の再起動リセット

スイッチを工場出荷時のデフォルト設定にリセットするには、次の手順を実行します。

ステップ 1 コンソールポート経由でスイッチに接続し、スイッチを工場出荷時のデフォルトにリセットします。

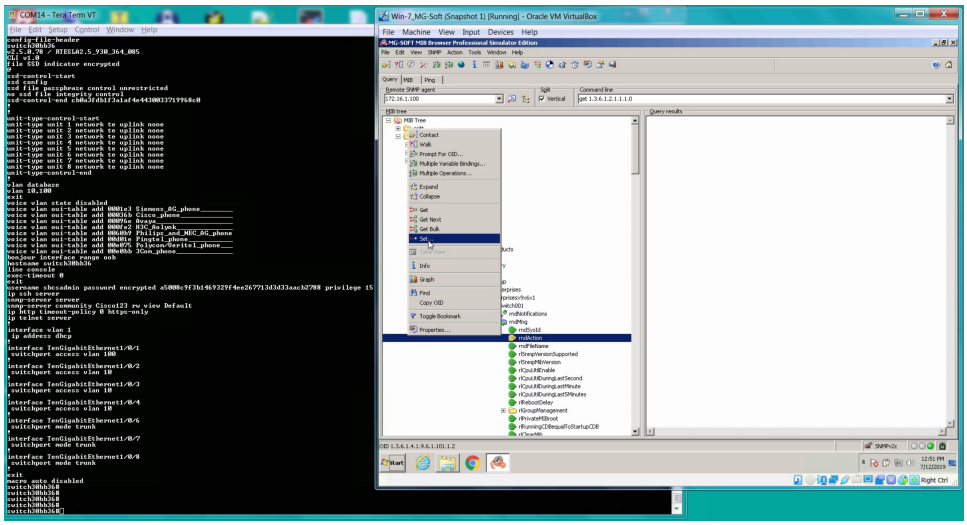
ステップ 2 SNMP を有効にして、読み取りおよび書き込み権限のコミュニティ名を設定します。

ステップ 3 設定を保存します。

ステップ 4 show コマンドを実行します。

ステップ 5 任意の MIB ブラウザ（この例では MG-Soft）で、rndAction MIB を選択します。

ステップ 6 右クリックし、[Set] を選択します。

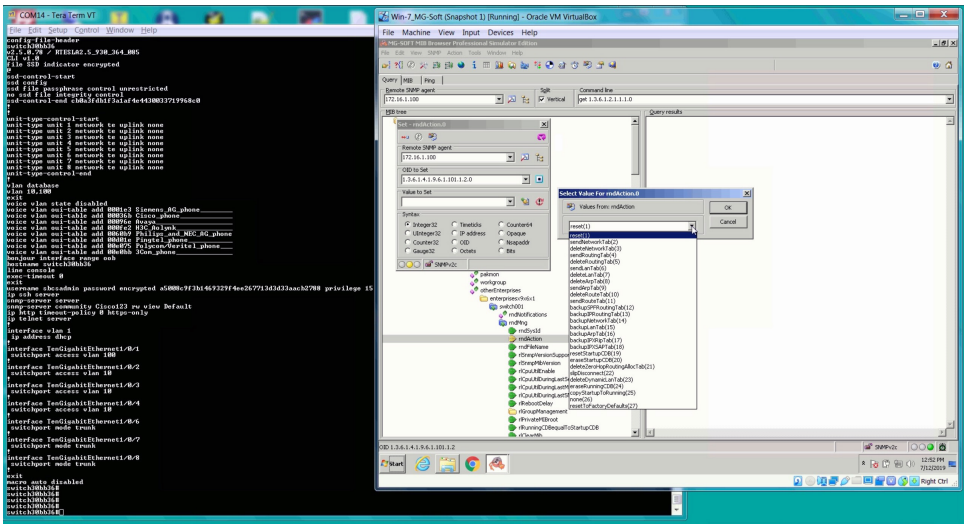


ステップ 7 [Value to Set] フィールドの横に 2 つのアイコンがあります。

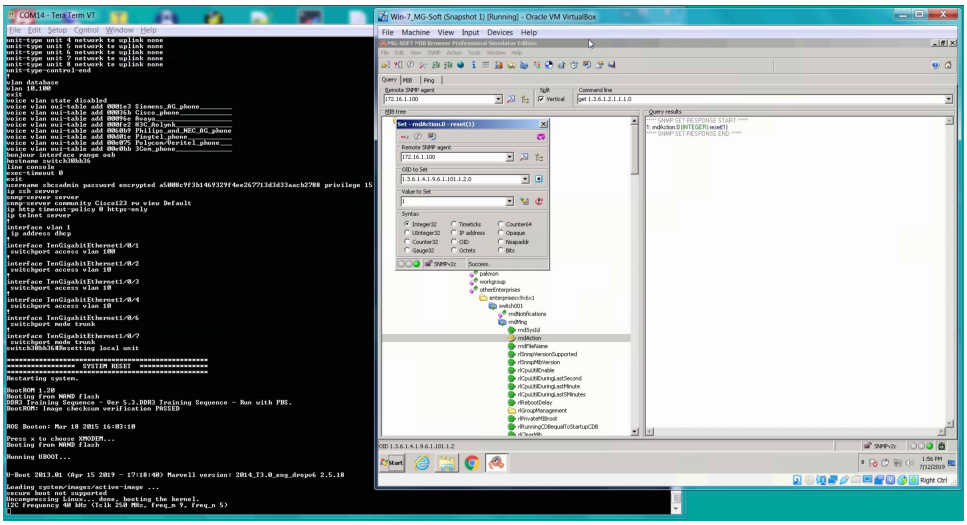
a) [Select From Value List] をクリックします。

b) ドロップダウンリストから [Reset] 選択し、[OK] をクリックします。

c) 次に、[Set] をクリックします。



d) スイッチの再起動後、ユーザー名とパスワードでログインし、[resetTo Factory Default(27)] を選択して手順を繰り返します。再起動後、新しいユーザー名とパスワードを作成する必要があります。



翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。