



Cisco Catalyst C1300X バージョン 4.10.0.xx アドミニストレーションガイド

最終更新：2026 年 4 月 16 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 \(1 ページ\)](#)
- [Cisco Catalyst C1300x スwitchの機能 \(2 ページ\)](#)
- [前面パネル \(3 ページ\)](#)
- [ラックへのスイッチのマウント \(7 ページ\)](#)
- [スイッチの壁面への取り付け \(8 ページ\)](#)
- [前面パネルスイッチ \(9 ページ\)](#)
- [スイッチの設定 \(10 ページ\)](#)
- [工場出荷時設定の復元 \(13 ページ\)](#)
- [ナビゲーション \(13 ページ\)](#)

はじめに

Cisco Catalyst C1300x スタッキングスイッチを選択していただき、ありがとうございます。これらのスイッチは、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
 - Chrome
 - 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。

Cisco Catalyst C1300x スイッチの機能

Cisco® Catalyst 1300x シリーズ スイッチは、中小企業やブランチオフィス向けに設計されたエンタープライズクラスの固定型マネージド ギガビット イーサネット レイヤ 3 スイッチです。シンプルかつ回数変更可能でセキュアなスイッチであり、配線用ボックス外での導入環境に最適です。Catalyst 1300x シリーズはカスタマイズされた Linux OS ソフトウェア上で動作し、直感的なダッシュボードによりネットワークのセットアップが簡素化され、高度な機能によってデジタルトランスフォーメーションが促進される一方、広範なセキュリティによってビジネスクリティカルなトランザクションが保護されます。

Cisco Catalyst 1300X シリーズ スイッチには、最大 10 個の 60W Universal Power over Ethernet (UPoE) ポートをサポートする選択モデルが含まれます。この拡張機能により、フル機能の Wi-Fi 7 アクセスポイントなどの負荷の大きいデバイスに、単一のイーサネットケーブルを使用して直接電力を供給できます。Catalyst 1300X シリーズは、ポートあたり最大 60 ワットを供給することにより、追加の電源なしで最新のワイヤレスおよび IoT テクノロジーを簡単かつ高

いコスト効率で導入できます。これにより、ネットワークのセットアップが簡素化され、高度なビジネスアプリケーションの増加する電力要件に対応できます。

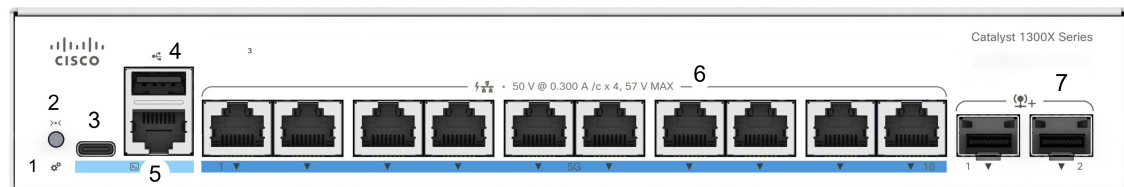
製品の特長

- コマンドライン インターフェイス（CLI）および/または直感的な Web UI 管理オプション。
- 接続されたデバイスの 802.1X サポートによるセキュリティ、Web ベース認証の一貫したインターフェイスにより、あらゆる種類のホストデバイスおよびオペレーティングシステムが認証されます。よって、IEE 802.1X クライアントを各エンドポイントに導入する必要がなく、複雑さが解消されます。
- 真のスタック機能を備えており、スタック内のすべてのスイッチを単一の IP アドレスを持つ 1 つの装置として設定、管理、および監視できます。
- 奥行 13 インチ（33 cm）未満のコンパクトなファンレスモデルが用意されており、小売店、オープンプランのオフィス、教室などの屋外配線クローゼットの設置など、柔軟な導入が可能です。
- ポートでのトラフィック量をモニターし、使われていない時間帯の電力を最適化することでエネルギー消費を抑える Energy Efficient Ethernet（IEE 802.3af）規格に対応しています。
- Bluetooth、Simple Network Management Protocol（SNMP）、USB-C コンソールへのアクセスを介した無線でのデバイス管理をサポートします。

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 Catalyst 1300X シリーズ モデル



1	コンソール	2	LED
3	USB タイプ C	4	USB タイプ A
5	RJ 45 ポート	6	10/100/1000 ポート
7	SFP ポート		



(注) Catalyst 1300X 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。

1. RJ-45 コネクタと USB-C 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 USB-C の方が優先されます）。

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ーのシリアルポートに接続するか USB-C 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：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。

- 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。



(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。

LED とリセット動作

デバイスには次のグローバル LED が装備されています。

表 1: システム LED

色	意味
オフ	スイッチに電源が入っていません。
緑色の点灯	スイッチは正常に動作しています。
緑色の点滅	CBD に接続されていない場合、点滅する緑色の LED は特定の情報（スタックユニット ID の表示、リセットボタンの押下時間など）を示します。
青色の点灯	デバイスの CBD エージェントはダッシュボードに接続されています。
青色の点滅	CBD に接続されている場合、点滅する青色の LED サポートは特定の情報（スタックユニット ID の表示、リセットボタンの押下時間など）を示します。
オレンジ色の点灯	スイッチに電力が供給されていますが、正常に動作していません。

色	意味
オレンジ色の点滅	ハードウェアまたはファームウェアの障害や構成ファイルのエラーを検出した場合、次の内容が含まれます。 • DRAM 読み取り/書き込みセルフテストの失敗 • フラッシュでのファームウェアヘッダー CEC チェック • 診断に失敗し、通常の動作に戻すことができない • ファン障害（専用ファン LED のないモデル） （オレンジ色の点滅頻度は、緑色の点滅よりも高い必要があります）。

表 2: イーサネットポートの LED

色	意味
オフ	リンクが確立されていないか、ポートが管理上の理由でシャットダウンされました。
緑色の点灯	リンクが確立されています
緑色に点滅	スイッチのアクティビティ。ポートがデータを送信または受信しています。
オレンジ色の点灯	PoE ポートがダウンリンクポートに電力を供給しています。
オレンジ色に点滅	ダウンリンクとアップリンクの両方のポートに対する、スイッチ内のポートの定義済み警告（エラー無効、STP ブロックなど）。

ポート LED ステータス

- ステータス 1：PD が接続され、PoE が電力を供給し、オレンジ色の LED が点灯していることを示します。
- ステータス 2：PD が起動し、リンクが確立され、オレンジ色の LED が消灯し、緑色の LED が点灯/点滅してリンクとトラフィックを確認しています。
- ステータス 3：スイッチで定義されたエラー（エラー無効など）が発生すると、緑色の LED が消灯し、オレンジ色の LED が点滅します。
- ステータス 4：スイッチがステータス 2 のときにリセットボタンを約 1 秒間押すと、オレンジ色の LED が 5 秒間点灯して PoE ステータスを示し、その後トラフィックステータスに戻ります（緑色の LED が点灯します）。

リセットボタンの動作

次に、定義された一連の時間にわたってリセットボタンが押された場合のさまざまなシナリオについて説明します。

1. リセットボタンを **1 秒未満** 押すと、ポートがデバイスに電力を供給しているときに、イーサネットポートの LED が 5 秒間オレンジ色に点灯します。
2. リセットボタンを **1 ～ 5 秒間** 押すと、システム LED は **緑色に点灯** し続けます。リセットボタンを離すと、スイッチはリロードされず、アクションは実行されません。
3. リセットボタンを **6 ～ 10 秒間** 押すと、システム LED は **ゆっくりと緑色に点滅** します。リセットボタンを離すと、スイッチは工場出荷時のデフォルト設定を使用せずにリロードされます。
4. リセットボタンを **11 ～ 15 秒間** 押すと、システム LED は **緑色に点灯** します。リセットボタンを離すと、スイッチはリロードされず、アクションは実行されません。
5. リセットボタンを **16 ～ 20 秒間** 押すと、システム LED は **緑色にすばやく点滅** します。リセットボタンを離すと、スイッチは工場出荷時のデフォルト設定にリロードされます。
6. リセットボタンを **20 秒以上** 押すと、システム LED は **緑色に点灯** します。リセットボタンを離すと、スイッチはリロードされず、アクションは実行されません。

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。

手順

- ステップ 1** スwitch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。

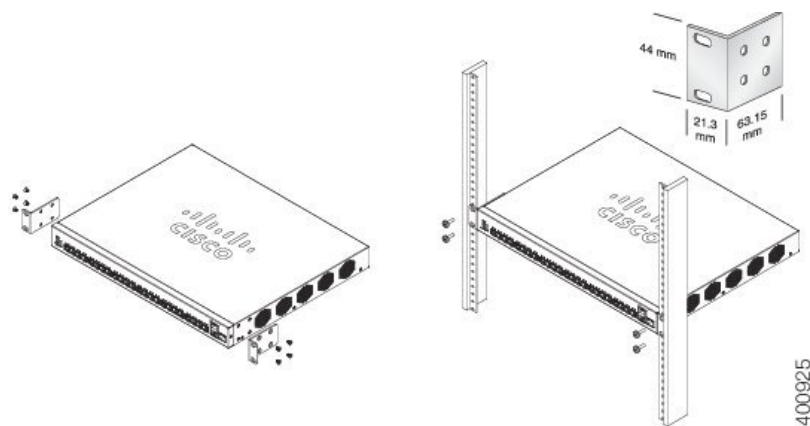


- (注) マウントブラケットは、24 および 48 ポートスイッチにのみ付属しています。88/10/16 ポートスイッチには、マウントブラケットは付属していません。マウントブラケットのパーツ RCKMNT-CMPCT-1K= を購入することを推奨します。

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。



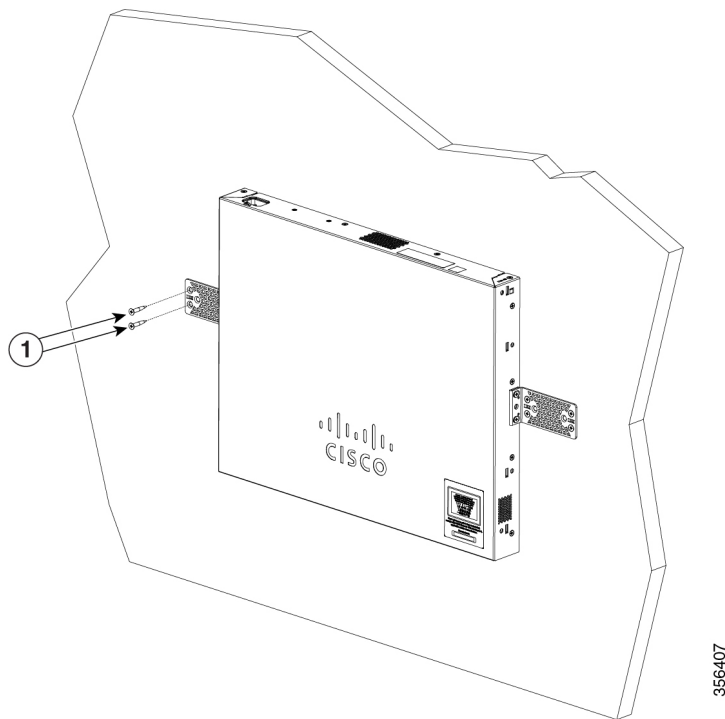
- 注意** 前面パネルを上に向けた状態で、スイッチを壁面に設置しないでください。スイッチを壁面に取り付ける場合は、エアフローを妨げないようにするため、またケーブルを扱いやすくするため、安全上の規定に従ってスイッチの前面パネルを下または横に向けてください。

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。

手順

- ステップ 1** スwitch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Switch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Switchを取り付けます。Switch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Switchの壁面への取り付け

24 ポートSwitchの壁面への取り付け



前面パネルスイッチ

Catalyst 1300X シリーズ Switch どちらも最大 8 台のSwitchに対応する前面パネルスタックを備えており、スタック全体のSwitchを単一の IP アドレスを持つ 1 つの装置として設定、管理、およびトラブルシューティングできます。どちらのシリーズもネットワーク管理と拡張性を簡素化しますが、Catalyst 1300X シリーズはスタッキング帯域幅を増やすことでこのエクスペリエンスを強化します。この帯域幅の増加により、スタックSwitch間のデータ転送が速くなります。これにより、優れたネットワークパフォーマンスが保証され、ネットワークの成長に伴うより要求の厳しいビジネスアプリケーションをサポートできるようになります。

このスタック機能により、管理プレーンの他にユニファイドデータおよびコントロールプレーンが提供されます。これにより、装置スタックが、スタックメンバーのすべてのポートを構成する1つのエンティティとして動作するため、柔軟性、拡張性、使いやすさが実現します。この機能により、肥大化するネットワーク環境における複雑さを劇的に軽減し、ネットワークアプリケーションの復元力と可用性を向上させます。また、前面パネルスタック機能では、Cross-Stack Quality of Service (QoS)、VLAN、リンク集約 (LAG)、およびポートミラーリングなどの機能（クラスタ化されたスイッチではサポートできない）により、その他のコストも節減され、管理面においてもメリットがもたらされます。

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。

手順

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、デフォルト設定からユーザー名とパスワードを変更してください。ネットワークの保護を強化するには、ログイン情報の変更が必要です。新しいパスワードは、パスワードの複雑性ルールに従う必要があります。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。

(注)

パスワードを作成する前に、[ログイン設定 \(349 ページ\)](#) 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。

[Getting Started] 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。

(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。

手順

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、[Reset] ボタンを 5 ～ 10 秒間押し続けます。
- 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 [Reset] ボタンを 15 ～ 20 秒間押し続けます。

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、WEBGUI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](#) (15 ページ)

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] : すべての設定オプションを使用できます。

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 (71 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 (375 ページ)
デバイス IP アドレスの変更	IPv4インターフェイス (255 ページ)
VLAN の作成	VLAN 設定 (177 ページ)
ポートの設定	ポート設定 (147 ページ)

デバイス ステータス

システム概要	システム概要 (33 ページ)
Port 統計	インターフェイス (37 ページ)
RMON 統計	統計情報 (56 ページ)
ログの表示	RAMメモリ (66 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 (75 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 (91 ページ)
デバイス設定のバックアップ	ファイル操作 (94 ページ)
MAC ベースの ACL の作成	MACベースACL (435 ページ)
IP ベースの ACL の作成	IPv4 ベース ACL (438 ページ)
QoS の設定	QoSプロパティ (451 ページ)
SPAN の設定	SPAN および RSPAN (44 ページ)

その他のリソース

Cisco Business ダッシュボードのマストヘッドまたは **CBD** アイコンをクリックすると、[Cisco Business ダッシュボード](#)の Web ページに移動します。このページで、ソフトウェアをダウンロードしたり、解説ビデオを視聴したり、オンラインチャットを使用して質問したりできます。

[Getting Started] ページには、シスコ Web ページの詳細情報に移動するための 4 つのホットリンクが用意されています。[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。

[Virtual Assistant] をクリックすると、質問できる仮想アシスタントに移動します。[CBD] をクリックすると、アプリケーションにアクセスできる Cisco Business Dashboard Web 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 \(17 ページ\)](#)

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、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。 • Refresh Time • リフレッシュなし • 1 分 • System Health • [Fan Status] : 1つのファンに障害が発生し、冗長ファンによってバックアップされている場合は黄色。ファンの動作時は緑色、ファンの動作不良時は赤色。 • Thermometer Status • 適正温度：緑色（温度計の目盛り：ほぼ 0）。 • 警告発生温度：黄色（温度計の目盛：半分）。 • 危険温度：赤色（温度計の目盛り：最大）。
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。 • [System Description] : デバイスの説明を表示します。 • [Host Name] : システム設定 (69 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。 • [System Location] (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。 • [System Contact] (設定されている場合) : 担当者の名前を入力します。 • [Total Available Power] (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（86 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（66 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トで、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 (150 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。 • [スタックアクティ (Stack Active)]：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イ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イ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。



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 \(25 ページ\)](#)
- [VLAN設定ウィザード \(27 ページ\)](#)
- [ACL 設定ウィザード \(28 ページ\)](#)

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。

手順

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 [Next] をクリックし、[General Information] の下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。
- [System Contact] : 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。
 - [User Defined] : 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 3 [Next] をクリックします。

ステップ 4 [IP Settings] タブのフィールドに入力します。

- [インターフェイス (Interface)] : IP インターフェイスについて、次のオプションのいずれかを選択します。
 - [ユニット (Unit)] : ドロップダウンメニューからユニットを選択します。
 - [ポート (Port)] : ドロップダウンメニューからポート番号を選択します。
 - [LAG] : LAG を入力します。
 - [VLAN] : VLAN を入力します。
 - ループバック
 - なし
- [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。
- [DHCP] を選択した場合は、以下を完了します。
 - [DNS Server] : DNS サーバーの IP アドレスを入力します。
- [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 5 [Next] をクリックします。

ステップ 6 [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 7 [Next] をクリックします。

ステップ 8 [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。

- [Manual Settings] : 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 9 [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 10 [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。

手順

- 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。

手順

- 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** [Next] をクリックします。
- ステップ 3** [ACL Configuration] タブで、ドロップダウンメニューから設定する ACL を選択します。それから、次のフィールドを入力します。
- [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** [Next] をクリックします。
- ステップ 5** 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。
 - [Permit Traffic] : ACE 条件に一致するパケットを転送します。
 - [Deny Traffic] : 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 6** MAC ベースの ACL の場合には、次のフィールドを入力します。

送信元 MAC 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。
Destination MAC Address	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）。
Destination MAC Wildcard Mask	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。
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。

ステップ 7 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	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。 • [Any (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。

Source IP Wildcard Mask	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。
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。

ステップ 8 [Next] をクリックします。

ステップ 9 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 10 [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。
 - [Physical interfaces only] : 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。
 - [VLANs only] : 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。変更が正常に適用されたことを示すメッセージが表示されます。

(注)

変更が正常に行われない場合は、「DoS 防御がポート単位モードで有効になっている場合は、ACL/ポリシーマップをインターフェイスにバインドできません。」というポップアップメッセージが表示されます。



第 5 章

検索

この章の内容は、次のとおりです。

- [検索](#) (31 ページ)

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。



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 (33 ページ)
- CPU 使用率 (35 ページ)
- ポート使用率 (36 ページ)
- インターフェイス (37 ページ)
- Etherlike (38 ページ)
- GVRP (39 ページ)
- 802.1X EAP (40 ページ)
- ACL (41 ページ)
- ハードウェアリソース使用率 (42 ページ)
- 健全性と電力 (43 ページ)
- SPAN および RSPAN (44 ページ)
- 診断 (47 ページ)
- オンボード パケット キャプチャ (52 ページ)
- RMON (55 ページ)
- sFlow (62 ページ)
- ログの表示 (65 ページ)

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。以下の設定を編集するには、[Edit] をクリックし、[システム設定 \(69 ページ\)](#) に移動してこの値を入力します。

- [System Description] : システムの説明。
- [System Location] : デバイスの物理的な場所。
- [System Contact] : 担当者の名前。
- [Host Name] : デバイスの名前。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。
- [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）。
- [System Uptime] : 最後のリブートから経過した時間。
- [Current Time] : 現在のシステム時刻。
- [Base MAC Address] : デバイスの MAC アドレス。
- [Jumbo Frames] : 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 \(147 ページ\)](#) 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、アクティ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 \(161 ページ\)](#) 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。
- [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。
- [Total PoE Power Allocated (W)] : 接続されている PoE デバイスに割り当てられている合計 PoE 電力。
- [PoE Power Mode] : 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。
- [Serial Number] : シリアル番号。
- [Product ID VID] : ポート番号とバージョン ID。

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。

手順

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。

手順

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 Utilization] : 発信パケットによって使用された帯域幅の量。
- [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、[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。

- [TX使用率 (TX Utilization)] : オンにすると、TX 使用率データが表示されます。
- [RX使用率 (RX Utilization)] : オンにすると、RX 使用率データが表示されます。
- [Time Span] : 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。

インターフェイス

[Interface] 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。

手順

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。

- [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。
- [Refresh Rate] : 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。

- [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。
- [Unicast Packets] : 受信された正常なユニキャスト パケット数。
- [Multicast Packets] : 受信された正常なマルチキャスト パケット数。
- [Broadcast Packets] : 受信された正常なブロードキャスト パケット数。
- [Packets with Errors] : 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。

- [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。
- [Unicast Packets] : 送信された正常なユニキャスト パケット数。

- [Multicast Packets] : 送信された正常なマルチキャスト パケット数。
- [Broadcast Packets] : 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。

手順

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] : 受信したフレームの数。
- [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。

手順

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

Invalid Protocol ID	無効なプロトコル ID エラー。

Invalid Attribute Type	無効な属性 ID エラー。
Invalid Attribute Value	無効な属性値エラー。
Invalid Attribute Length	無効な属性長エラー。
Invalid Event	無効なイベント。

ステップ 3 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。

ステップ 4 データを更新するには、ツールバーの [Refresh] をクリックします。

ステップ 5 すべてのインターフェイス統計を表示するには、[View 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。

手順

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	ポートで受信した EAPOL 通知フレーム。
受信済みEAPOL Announcement要求フレーム	ポートで受信した 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サブリカントフレーム	ポートで送信した EAPOL EAP サブリカントフレーム。
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 [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。

ステップ 5 カウンタを更新するには、[Refresh] をクリックします。

ステップ 6 [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。

手順

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。

- [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。

[Hardware Resources Table] には、次のフィールドが表示されます。

- IP エントリ
 - [In Use] : IP ルールで使用されている TCAM エントリ数。
 - [Maximum] : 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 (IPv6 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 マッピング
 - [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。
- [Maximum] : ACL および QoS ルールで使用可能な TCAM エントリの数。

健全性と電力

[Health and Power] ページは、すべての関連デバイスの温度ステータス、電源ステータス、およびファンステータスをモニターします。デバイス上のファンは、モデルによって異なります。[Health and Power] ページにアクセスするには、[Status and Statistics] > [Health and Power] の順に移動します。

次のセクションが表示されます。

電力の削減

- [Current Green Ethernet and Port Power Savings] : 現在のすべてのポートでの節電量。
- [Cumulative Green Ethernet and Port Power Savings] : デバイスの電源が投入された以降の、すべてのポートでの累積節電量。
- [Projected Annual Green Ethernet and Port Power Savings] : 1 週間におけるデバイスでの予測節電量。この値は、前週に発生した節減量に基づいて計算されます。
- [現在のPoE電力節約] (PoE SKU にのみ使用可能) : PD が接続されているポートで、時間範囲機能のために PoE が動作しないことにより節約された PoE 電力の現在量。
- [累積PoE電力節約] (PoE SKU にのみ使用可能) : デバイスの電源がオンになって以降、PD が接続されているポートで、時間範囲機能のために PoE が動作しないことにより節約された PoE 電力の累積量。
- [予測年間PoE電力節約] (PoE SKU にのみ使用可能) : デバイスの電源がオンになって以降、PD が接続されているポートで、時間範囲機能のために PoE が動作しないことにより節約される PoE 電力の年間予想量。予測は、前週の節減量に基づきます。

正常性テーブル*

- [Fan Status] : ファンが利用できない ([N/A]) か、利用可能で正常に動作している ([OK]) か、動作していない ([Failure]) が表示されます。
- [Redundant Fan Status] : ファンの冗長ステータスが表示されます。
 - [N/A] : 冗長ファンがその特定のモデルに適していません。
 - 準備完了 (Ready) : 冗長ファンは動作可能ですが、必要ではありません。
 - アクティブ (Active) : メイン ファンの 1 台が動作していないため、このファンを交換します。



(注) 冗長ファンステータスは、特定の SKU でのみサポートされています。

- [Sensor Status] : センサーが機能している ([OK]) か、機能していない ([Failure]) かが表示されます。
- [Temperature] : 次のいずれかのオプションが表示されます。
 - OK : 温度が警告しきい値未満です。
 - 警告 (Warning) : 温度が警告しきい値と重大しきい値の間です。
 - 重大 (Critical) : 温度が重大しきい値を超えています。
 - [N/A] : 利用できません。

Dying Gasp

Dying Gasp 機能は、デバイスで予期しない電力損失が発生していることを監視システムに警告するメカニズムを提供します。電源喪失イベントが発生すると、ハードウェアコンデンサがデバイスのシャットダウンを短時間遅らせます。この間に、デバイスは構成済みの Syslog サーバーまたは SNMP 通知受信者を介して Dying Gasp メッセージを送信します。

- Dying Gasp メッセージは、Syslog サーバーおよび SNMP サーバーで構成され、使用して送信されます。
- [Dying Gasp via Syslog] : 有効にする場合にオンにします。このコントロールを有効にすると、構成された syslog サーバー経由で Dying Gasp メッセージを送信できるようになります。
- [Dying Gasp via SNMP] : 有効にする場合にオンにします。このコントロールを有効にすると、構成された SNMP 通知受信者経由で Dying Gasp メッセージを送信できるようになります。
- [Primary Dying Gasp Method] : Dying Gasp が syslog と SNMP の両方で有効になっている場合、このコントロールは、Dying Gasp メッセージを送信するときにどちらの方式を優先するかを選択します。このコントロールは、[Dying Gasp via Syslog] コントロールと [Dying Gasp via SNMP] コントロールの両方がオンの場合にのみ有効になります。

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witch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 \(177 ページ\)](#) 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。

手順

-
- ステップ 1** [Status and Statistics] > [SPAN & RSPAN] > [RSPAN VLAN] の順にクリックして、以前に定義した 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。
-

セッション宛先

モニタ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。

手順

-
- ステップ 1** [ステータスと統計情報 (Status and Statistics)] > [SPANとRSPAN (SPAN & RSPAN)] > [セッション宛先 (Session Destinations)] をクリックします。
- ステップ 2** [Session Destinations Table] で、[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。
 - [Destination Type] : 次のいずれかのオプションを選択します。
 - [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)。
 - [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)。
 - [ポート (Port)] : ドロップダウンリストからポートを選択します。
 - [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。
-

セッション送信元

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。

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。

手順

ステップ 1 [ステータスと統計情報 (Status and Statistics)] > [SPANとRSPAN (SPAN & RSPAN)] > [セッションの送信元 (Session Sources)] をクリックします。

ステップ 2 [Session Source Table] で、[Add] をクリックします。

ステップ 3 セッションID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

[Copper Test] 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（167 ページ）](#)）を参照）。
- （任意）EEE の無効化（[プロパティ（167 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。

手順

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 [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。
- [Test Results] : 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。
 - [Open Cable] : ケーブルが一方側にしか接続されていません。
 - [Short Cable] : ケーブルにショートが発生しています。

- [Unknown Test Result] : エラーが発生しています。
- [Distance to Fault] : 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）。

- [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。
- チャンネル (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 チャンネル。
- [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。

- CWDM-SFP-1490
- CWDM-SFP-1510
- CWDM-SFP-1550
- CWDM-SFP-1570
- CWDM-SFP-1590
- 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。

- SFP-10G-ER
- SFP-10G-ER-S
- SFP-10G-BXD-I
- SFP-10G-BXU-I
- 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。

- SFP-H10GB-CU1-5M
- SFP-H10GB-CU2M
- SFP-H10GB-CU2-5M
- SFP-H10GB-ACU10M
- SFP-10G-AOC1M
- SFP-10G-AOC3M
- SFP-10G-AOC5M
- SFP-10G-AOC7M
- SFP-10G-AOC10M
- Cisco SFP-H10G-CU1M
- Cisco SFP-H10G-CU3M
- Cisco SFP-H10G-CU5M
- Cisco SFP-10/25G-CSR-S
- Cisco SFP-10/25G-LR-S
- Cisco SFP-10/25G-LR-I
- Cisco SFP-10/25G-BXD-I

- Cisco SFP-10/25G-BXU-I
- Cisco SFP-25G-ER-I
- Cisco SFP-25G-SR-S
- Cisco SFP-25G-AOC2M
- Cisco SFP-25G-AOC10M

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
- [Transmitter Fault] : 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。
- [Loss of Signal] : 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。
- [Data Ready] : 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。

手順

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。

オンボード パケット キャプチャ

オンボード パケット キャプチャ (OPC) は、デバイスの障害対応機能を強化します。スイッチの CPU によって送受信されるパケットをキャプチャする機能を提供します。パケットキャプチャはその後、ローカルストレージに保存され、オフライン分析用にエクスポートされます。キャプチャパラメータを定義し、キャプチャをアクティブ化するために使用されるエンティティは、キャプチャポイントと呼ばれます。デバイスは、最大4つのキャプチャポイントとキャプチャされたパケット用のバッファとして最大 20 メガバイトをサポートします。

キャプチャバッファをローカルフラッシュまたはUSB上のファイルにエクスポートするには、[Buffer File Operation] を選択します。

1. [Crash Capture Destination] は、デバイスがクラッシュした場合にキャプチャファイルをエクスポートするために使用される設定です。このシナリオでは、ユーザーはファイルを手動でエクスポートできません。したがって、エクスポート先を手動で定義する必要があります。ファイルを保存する宛先デバイスを選択します。

- [Flash] : ファイルをデバイスのフラッシュに保存します。
- [USB] : デバイスに接続されている USB ストレージデバイスにファイルを保存します。



(注) この場合、キャプチャファイルの名前は自動的に設定され、キャプチャの日時が表示されます。

キャプチャポイント設定



(注) この設定は、[Advanced Mode] でのみ使用できます。

キャプチャポイントを定義してアクティブにするには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Onboard Packet Capture] > [Capture Point Settings] の順に移動します。

ステップ 2 [Add] をクリックしてキャプチャポイントを追加し、以下を設定します。

- [Capture Point Name] : キャプチャポイントの名前。
- [Buffer Mode] : キャプチャモードを次のいずれかに定義します。
 - [Linear] : キャプチャバッファがいっぱいになると、キャプチャが終了します。
 - [Circular] : バッファがいっぱいになると、キャプチャが終了し、バッファの先頭にあるパケットが書き換えられます。
- [Buffer Size (MB)] : キャプチャバッファのサイズを MB 単位で定義します。すべてのキャプチャポイントのバッファは 20 MB を超えることはできません。
- [Interface] : コントロールプレーン (CPU) インターフェイスのみがサポートされます。
- [Capture Direction] : キャプチャするトラフィックの方向を定義します (インバウンドトラフィックとアウトバウンドトラフィックの両方 ([both])、インバウンドトラフィックのみ ([in])、またはアウトバウンドトラフィックのみ ([out]))。

ステップ 3 [Apply] をクリックします。

ステップ 4 キャプチャポイントを編集または削除するには、キャプチャポイントを選択し、[Edit] または [Delete] をクリックします。

ステップ 5 キャプチャポイントをアクティブにするには、テーブルからキャプチャポイントの1つを選択し、[Operations] をクリックします。[Capture Point Operation] フィールドで、[Activate] を選択し、[Apply] をクリックします。[Capture Point Settings] テーブルのキャプチャポイントの状態が [Active] に設定されます。

ステップ 6 アクティブなキャプチャポイントを非アクティブにするには、アクティブなキャプチャポイントを選択し、[Operations] をクリックします。[Capture Point Operation] フィールドで、[Deactivate] を選択し、[Apply] をクリックします。[Capture Point Settings] テーブルのキャプチャポイントの状態が [Inactive] に設定されます。

バッファファイル操作



(注) この設定は、[Advanced Mode] でのみ使用できます。

キャプチャされたパケットは、メモリバッファに保存されます。さらにデバッグするためにパケットを不揮発性メモリにコピーするには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Onboard Packet Capture] > [Buffer File Operation] の順に移動します。

ステップ 2 キャプチャ中にデバイスがクラッシュした場合、パケットは自動的に不揮発性メモリに保存されます。クラッシュレポートを保存する接続先デバイスを選択します。

- [Flash] : ファイルをデバイスのフラッシュに保存します。（デフォルト）
- [USB] : デバイスに接続されている USB ストレージデバイスにファイルを保存します。

ステップ 3 [Apply] をクリックして、[Crash Capture Destination] の設定を保存します。

ステップ 4 キャプチャポイントバッファの 1 つを手動でエクスポートするには、画面の [Export Capture] セクションに移動し、次のように設定します。

- [Capture Point Name] : エクスポートするキャプチャポイントを選択します。
- [Capture File Name] : エクスポートするファイルの名前を定義します。
- [Export Destination] : ファイルを保存する宛先デバイスを選択します。
 - [Flash] : ファイルをデバイスのフラッシュに保存します。
 - [USB] : デバイスに接続されている USB ストレージデバイスにファイルを保存します。

ファイルは、選択に基づいてフラッシュまたは USB にエクスポートできます。

ステップ 5 キャプチャポイントファイルをエクスポートするには、[Export] をクリックします。

バッファ統計



(注) この設定は、[Advanced Mode] でのみ使用できます。

キャプチャバッファ統計情報を表示するには、次の手順を実行します。

手順

ステップ 1 [Status and Statistics] > [Onboard Packet Capture] > [Buffer Statistics] の順に移動します。

ステップ 2 [Capture Point Name] フィールドで、ドロップダウンリストからキャプチャバッファを選択して統計情報を表示します。

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

- リフレッシュなし
- 15秒
- 30 秒
- 60 秒

ステップ 4 次の統計情報が表示されます。

- [Buffer State] : アクティブまたは非アクティブ
- [Buffer Mode] : 線形または円形
- [Buffer Size (KB)] : バッファのサイズ (キロバイト単位)
- [Captured Packets] : キャプチャされたパケットの数
- [Buffer Used (KB)] : 使用されている実際のバッファサイズ。
- [Packet Capture Rate per Second] : キャプチャされたトラフィックの 1 秒あたりのパケットレート。
- [Packets Dropped] : キャプチャセッション中にドロップされたパケットの数。

ステップ 5 情報を手動で更新するには、[Refresh] をクリックします。

ステップ 6 バッファをクリアするには、[Clear Buffer] をクリックします。

RMON

リモート ネットワーク モニタリング (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

[Statistics] 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。

手順

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。
Broadcast Packets Received	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。
Multicast Packets Received	受信した良好なマルチキャストパケット数。
CRC & Align Errors	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）。
Fragments	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。
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。
Frames of 1024 Bytes or More	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 テーブルビューまたはグラフィックビューでカウンタを管理するには、次の手順を実行します。

- データをクリアするには、[Clear Interface Counters] をクリックします。
- データをリフレッシュするには、[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。
- [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。

[History] 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。

手順

ステップ 1 [Status and Statistics] > [RMON] > [History] 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。

- [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 [History Control Table] 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。

ステップ 6 [History Entry No.] ドロップダウン メニューから表示するサンプルのエントリ番号を選択します。

選択したサンプルに関するフィールドが表示されます。

- [Owner] : 履歴テーブルエントリの所有者。
- [Sample No.] : このサンプルから取得された統計情報。
- [Drop Events] : サンプリング中にネットワークリソース不足によりドロップされたパケット数。これは、正確なドロップされたパケット数ではなく、ドロップされたパケットが検出された回数を表しています。
- [Bytes Received] : 受信したオクテット数。不良パケットと FCS オクテットが含まれますが、フレーミングビットは含まれません。
- [Packets Received] : 不良パケット、マルチキャストパケット、ブロードキャストパケットを含む受信済みパケット数。
- [Broadcast Packets] : 正常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含まれません。
- [Multicast Packets] : 受信した正常なマルチキャストパケット数。
- [CRC Align Errors] : 発生した CRC とアラインメントエラー数。

- [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 オクテット超過)。
- [Fragments] : 受信したフラグメント数 (64 オクテット未満のパケット) 。フレーミングビットは含まれませんが、FCS オクテットは含まれます。
- [Jabbers] : 2000 オクテットを超える受信したパケット合計数。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。
- [Collisions] : 受信したコリジョン数。
- [Utilization] : インターフェイスが処理できる、最大トラフィックと比較した現在のインターフェイストラフィックの割合。

ステップ 7 [履歴制御テーブル] をクリックして履歴制御テーブルを表示します。

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。

手順

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] : 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。
- [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。
- [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。
 - [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。

- [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。
- [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。
- [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。
- [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 [Event Log Table] をクリックして、発生してログに書き込まれたアラームのログを表示します。

次のデータが表示されます。

- [Event Entry No.] : イベントのエントリ番号
- [Log No.] : イベントのログ番号
- [Log Time] : イベントログの時間
- [Description] : イベントログの説明。

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。

手順

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。

- [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。

Alarm Entry	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。
Counter Name	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。 • [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。 • [Rising Alarm] : 上昇値が上昇しきい値アラームをトリガーします。 • [Falling Alarm] : 下降値が下限しきい値アラームをトリガーします。 • [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。
Interval	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受信機

sFlow 受信機は、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 受信機のパラメータを設定するには、次の手順を実行します。

手順

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送信元インターフェイス（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 受信機（sFlow アナライザ）を追加するには、[追加（Add）] をクリックして、[受信機インデックス（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 次を設定します。

- [Server Definition] : [By IP address] または [By name] のいずれかで sFlow サーバを指定するかを選択します。

[Server 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 Address Type] : 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。
 - [Global] : 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] : 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 次を設定します。

- [Server IP Address/Name] : サーバーの IP アドレスまたは名前を入力します。どちらでも構いません。
- [Port] : SYSLOG メッセージが送信されるポート。
- [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 既存の sFlow 受信機を編集するには、**編集アイコン**をクリックし、以下の手順を実行します。

- [受信機指定方法 (Receiver Definition)] : sflow 受信機を [IP アドレス別 (By IP address)] に指定するか [名前別 (By name)] に指定するかを選択します。
- [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 Address Type] : 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。
 - [Global] : 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] : 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)。
- [受信機のIPアドレス/名前 (Receiver IP Address/Name)] : 受信機の IP アドレスまたは名前を入力します。
- [ポート (Port)] : ポート番号を入力します (範囲 1 ~ 65535、デフォルト : 6343)
- [最大データグラムサイズ (Maximum Datagram Size)] : データグラムサイズをバイト単位で入力します (範囲 : 1 ~ 2147483647、デフォルト : 1400)

ステップ7 [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、ポートを受信機に関連付ける必要があります。sFlow ポートは、[sFlow受信機 \(62 ページ\)](#) ページで受信機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。

手順

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。

- [Interface] : 情報の収集元となるユニット/ポートを選択します。
- [(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。

(注)

[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。インターフェイスには、最大 3 つのサンプリングレート値を設定できます。サンプリングレートは、インターフェイスで設定されているときにカウントされます。複数のインターフェイスで、3 つの許容レートうちの特定のサンプリングレートを設定できます。インターフェイスで 4 番目のレートを設定しようとすると、拒否されます。

- [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受信機 \(62 ページ\)](#) 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。
- [(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受信機 \(62 ページ\)](#) 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。

手順

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] : サンプルングされたパケットの数。
- [Datagrams Sent to Receiver] : 送信された sFlow サンプルングパケットの数。

ステップ 3 すべてのポートの sFlow 統計をクリアするには、[Clear All Interface Counters] または [Clear Interface Counters] をクリックします。

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

[RAMMemory] 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。

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。

- [Alert Icon Blinking] : 無効と有効を切り替えます。
- [Pop-Up Syslog Notifications] : 前述したようにポップアップ SYSLOG の受信を有効にします。
- [Current Logging Threshold] : 生成されるロ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。

- [ログインデックス (Log Index)] : ログ ID。
- [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（86 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 (69 ページ)
- IOS 設定の変換 (70 ページ)
- コンソール設定 (71 ページ)
- スタック管理 (71 ページ)
- Bluetooth 設定 (72 ページ)
- ユーザ アカウント (75 ページ)
- アイドルセッションタイムアウト (76 ページ)
- 時刻設定 (77 ページ)
- システム ログ (86 ページ)
- ファイル管理 (90 ページ)
- Cisco Business ダッシュボードの設定 (102 ページ)
- プラグアンドプレイ (PNP) (106 ページ)
- リブート (113 ページ)
- ハードウェアリソース (114 ページ)
- ディスカバリ - Bonjour (115 ページ)
- ディスカバリ - LLDP (116 ページ)
- ディスカバリ - CDP (134 ページ)
- デバイスの特定 (143 ページ)
- ping (144 ページ)
- traceroute (145 ページ)

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。

手順

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。

- [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。
- [System Contact] : 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] : 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。
 - [User Defined] : 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。

カスタムバナー設定

以下のバナーを設定できます。

- [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。
- [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] をクリックして新しい設定を保存します。

IOS 設定の変換

IOS 変換ツールは、Catalyst 1000 構成ファイルを Catalyst 1200/Catalyst 1300 シリーズの構成ファイルに変換します。これにより、Catalyst 1000 デバイスから Catalyst 1200/1300 シリーズのデバイスへのネットワークの移行が容易になります。

設定プロセスを開始するには、以下を実行します。

1. [管理 (Administration)] > [IOS構成の変換 (IoS Configuration Conversion)] の順にクリックします。
2. [実行 (Go)] をクリックします。 <https://cisco.com/go/iosconversiontool> にリダイレクトされます。

ログインして従来の Catalyst スイッチ構成ファイルをアップロードし、Catalyst 1200/1300 構成に変換します。

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 および 115200 のいずれかの速度に設定できます。コンソールポートのボーレートを設定するには、以下の手順を実行します。

コンソールのボーレートを設定するには、以下の手順を実行します。



(注) C1300x シリーズは、コンソールのボーレートの自動検出をサポートしていません。

手順

ステップ 1 [各種管理 (Administration)] > [コンソール設定 (Console Settings)] の順にクリックします。

ステップ 2 ドロップダウンリストから、ビット単位のコンソールポートのボーレート (デフォルトは 115200) 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) C1300X スイッチは、他のすべての C1300X スイッチとスタックできますが、スタッキング対応の C1300 スイッチとスタックできません。

スタックを管理するには、次の手順を実行します。

手順

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

- [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] : 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。

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。

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。

- [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スタック接続速度 (Unit x Stack Connection Speed)] : スタッキング インターフェイスの現在の速度を示します (サポートされる値は 10G または 25G で、読み取り専用です)。
- [リセット後のユニットxスタック接続速度 (Unit x Stack Connection Speed After Reset)] : ユーザーが設定でき、10G と 25G もサポートします。

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。

Bluetooth 設定

Bluetooth を使用すると、デバイスはワイヤレス接続し、短距離で相互に通信できます。これは、多くのアプリケーションで使用されている、便利で用途が広く、信頼性の高いテクノロジーです。

Bluetooth のサポートは、Bluetooth (BT) ドングルをデバイスの USB ポートに接続することによって実現されます。デバイスは、サポートされている BT ドングルがデバイスの USB ポートに挿入されたことを自動的に検出し、BT 操作を可能にする Bluetooth サポートを提供します。デバイス管理インターフェイスの Bluetooth インターフェイスにより、ユーザーは関連する Bluetooth 設定を適用できます。CLI およびテキスト構成ファイルでは、Bluetooth インターフェイスは「interface bluetooth 0」と表されます。BT ドングルが USB ポートに挿入されていない場合、BT インターフェイスを構成できます。

サポートされている Dongle のリスト：

- BT-D-400 Bluetooth 4.0 アダプタ (Kinivo 社製)
- Bluetooth 4.0 USB アダプタ (ASUS 社製)
- Bluetooth 4.0 USB アダプタ (Insignia 社製)
- Philips 4.0 Bluetooth アダプタ
- Lenovo LX1815 Bluetooth 5.0 USB アダプタ
- Lenovo LX1812 Bluetooth 4.0 USB アダプタ

スタックでは、BT ドングルの検出と操作はスタックアクティブユニットでのみサポートされます。デバイスは、USB ポートに挿入されている単一の USB デバイスの検出をサポートします。つまり、デバイスは、同じ USB インターフェイス上の複数の USB ドングルまたは USB ドングル + メモリスティックをサポートしません。

通知 syslog メッセージには、次のように、BT ドングルの検出と取り外しが成功したことが示されます。

- Dongle の挿入：「Bluetooth Dongle が USB ポートに挿入されました (Bluetooth Dongle inserted into USB port)」
- Dongle の取り外し：「Bluetooth Dongle が USB ポートから削除されました (Bluetooth Dongle removed from USB port)」

Bluetooth 設定を行うには、次の手順を実行します。

手順

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

ステップ 2 次の設定を行います。

Bluetooth サービス

デバイスで Bluetooth サービスを有効にする場合は、[Enable] をオンにします。デフォルトは有効です。

PIN	次の中から選択します。 • [Encrypted] : 暗号化された PIN を入力します • [Plaintext] : プレーンテキストの PIN (4 桁) を入力します デフォルトの PIN は 9999 です
Bluetooth デバイス名	デバイスが Bluetooth 経由で自身をアドバタイズするための文字列。次の中から選択します。 • [Switch Host Name] (デフォルト) • [User Defined] : ユーザー定義の名前を入力します (最大 20 文字)
BT インターフェイスの説明	Bluetooth インターフェイスの説明を入力します。 (0 ~ 64 文字)
BT IP インターフェイス	Bluetooth インターフェイスを介してデバイスを管理するために使用される IP インターフェイス。次の中から選択します。 • [None] : Bluetooth インターフェイスで IP アドレスが構成されません。 • [User Defined] : Bluetooth インターフェイスで IP アドレスとマスクを構成します。 (注) [BT IP Address] フィールドと [BT IP Mask] フィールドは両方とも、BT IP インターフェイスの前の項目に関連付けられていて、ユーザーが [BT IP Interface] で [User Defined] を選択した場合にのみアクティブになります。
BT IP アドレス	Bluetooth インターフェイスの IP アドレスを入力します。
BT IP マスク	IP アドレスの IP マスク/プレフィックス長。このコントロールは、IP インターフェイスがユーザー定義の場合にのみ有効です。次の中から選択します。 • Network Mask • Prefix Length
ドングルあり	ドングルが存在する場合に表示されます。

状態	Bluetooth 接続の状態を表示します。利用可能な状態は次のとおりです。 • [Not Ready]（ dongle が挿入されていない） • [Discoverable]（ dongle が挿入されていて検出可能） • [Connected]（Bluetooth パートナーに接続済み） • [Disabled]（Bluetooth インターフェイスが無効になっている）
コネクテッドデバイス名	接続されている Bluetooth デバイスの表示名。このフィールドは、スイッチとリモート Bluetooth デバイス間で Bluetooth 接続が確立されている場合にのみ表示されます。

ステップ 3 [Apply] をクリックして設定を保存します。

ステップ 4 [Display Sensitive Data as Plaintext] を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。

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。

手順

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]：現在のパスワードを入力します。（このフィールドは編集モードでのみ表示されます。）

- [Suggest Password] : クリックするとパスワードを自動生成します。次に、[Copy to Clipboard] をクリックしてパスワードをコピーし、このアカウントのパスワードを使用する場合は [Yes] をクリックします。
- [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 \(349 ページ\)](#) 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。

- [Confirm Password] : パスワードを再度入力します。
- [Password Strength Meter] : 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。

手順

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

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。

手順

ステップ 1 システム時刻を表示するには、[Administration] > [Time Settings] > [System Time] をクリックします。

次のように表示されます。

- [Actual Time (From SNTP Server)] : 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サーバーの種類。

ステップ 2 次のパラメータを入力します。

- [Clock Source Settings] : 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サーバーから取得されます。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 \(83 ページ\)](#) 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。

- [Manual Settings] : 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。
- [Date] : システムの日付を入力します。

- [Local Time] : システムの時刻を入力します。

(注)

[Main Clock Source (SNTP Servers)] が選択されている場合、これらの設定は無効になります。

- [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。
 - [Time Zone Offset] : 協定世界時 (UCT) 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 UCT +1、ニューヨークのタイムゾーン オフセットは UCT - 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。
- [Daylight Savings Settings] : 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] : UCT 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。
 - [Daylight Savings Type] : 次のいずれかをクリックします。
 - [USA] : 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。
 - [European] : 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。
 - [By dates] : 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。
 - [Recurring] : DST を毎年同じ日付に発生させます。
 - [By Dates] 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。
 - [From] : DST が開始する日付と時刻。
 - [To] : DST が終了する日付と時刻。

ステップ 3 [Recurring] 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。

- [From] : 毎年 DST が開始する日付。
 - [Day] : 毎年 DST が開始する曜日。

- [Week] : 毎年 DST が開始する月の週。
- [Month] : 毎年 DST が開始する月。
- [Time] : 毎年 DST が開始する時刻。
- [To] : 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。
 - [Day] : 毎年 DST が終了する曜日。
 - [Week] : 毎年 DST が終了する月の週。
 - [Month] : 毎年 DST が終了する月。
 - [Time] : 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、サテライト受信機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、デバイス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 \(78 ページ\)](#) 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。

手順

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	[Enable] 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 (注) このオプションは、 [Advanced Mode] でのみ 使用できます。	ドロップダウンリストから 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 (注) このオプションは、 [Advanced Mode] でのみ 使用できます。	ドロップダウンリストから 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。

(注)

ユーザーが独自の SNTP サーバーを追加しない場合に限り使用できるデフォルトの SNTP サーバーが複数あります。デフォルトの SNTP サーバーまたはユーザーが追加した SNTP サーバーを削除するには、サーバーを選択し、削除アイコンを押します。

このページでは、ユニキャスト SNTP サーバごとに次の情報が表示されます。

- [SNTP Server] : SNTP サーバーの IP アドレス。ストラタム レベルに応じて、優先サーバまたはホスト名が選択されます。
- [Poll Interval] : ポーリングが有効か無効かを示します。
- [Authentication Key ID] : SNTP サーバとデバイス間の通信に使用するキー ID。
- [Stratum Level] : 参照クロックからの距離を数値で示します。ポーリング間隔が有効になっていない限り、SNTP サーバーをプライマリサーバー (ストラタムレベル 1) にすることはできません。
- [Status] : SNTP サーバーのステータス。設定可能な値は次のとおりです。
 - [Up] : SNTP サーバーは現在正常に動作しています
 - [Down] : SNTP サーバーは現在使用できません。
 - [Unknown] : SNTP サーバのステータスは不明です。
 - [In Process] : SNTP サーバーへの接続は現在処理中です。
- [Last Response] : SNTP サーバから最後に応答を受信した日時。
- [Offset] : ローカル クロックに対するサーバクロックの概算オフセット (ミリ秒単位)。ホストは、RFC 2030 に記述されているアルゴリズムを使用してこのオフセットの値を決定します。
- [Delay] : サーバクロックとローカル クロック間のネットワーク パス全体での、ローカル クロックに対するサーバクロックの概算ラウンドトリップ遅延 (ミリ秒単位)。ホストは、RFC 2030 に記述されているアルゴリズムを使用してこの遅延の値を決定します。

- [Source] : SNTP サーバの定義方法。たとえば、手動や DHCPv6 サーバからなど。
- [Interface] : パケットを受信するインターフェイス。

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 Address Type	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、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。 • [Global] : 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	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。
ポーリング間隔	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 クライアントマルチキャスト/エニーキャストを機能させるには、メインクロックソース (SNTP サーバー) [システム時刻 \(78 ページ\)](#) 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。

手順

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有効にするものを選択します。

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、[Enable] をオンにします。
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、[Enable] をオンにします。
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、[Enable] をオンにします。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、[Enable] をオンにします。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 (ポート、LAG、または VLAN) を選択し、ドロップダウンメニューからオプションを選択して構成します。

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。

手順

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

ステップ 2 [Enable] をオンにすると、デバイスと SNTP サーバー間の SNTP セッションの SNTP 認証が有効になります。

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。

- [Authentication Key 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] : 次のオプションから選択します。
 - [User Defined (Encrypted)] : 認証に使用するキーを暗号化形式で入力します。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。
 - [User Defined (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 (最大 8 文字)。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] : デバイスが、この認証キーを使って、SNTP サーバーからのみ同期情報を受信できるようにする場合にオンにします。

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。

ステップ 7 SNTP 認証キーを削除するには、目的の認証キー ID のチェックボックスをオンにして、[Delete] アイコンをクリックします。

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。

Time Range



(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。

手順

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。

繰り返し時間範囲



(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。

手順

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。

- [Recurring Starting Time] : 時間範囲の開始点とする曜日と時刻を入力します。
- [Recurring Ending Time] : 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

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（66 ページ）](#)と[フラッシュメモリ（66 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。

手順

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。

Logging	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 Aggregator	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。
Max. Aggregation Time	SYSLOG メッセージが集約される間隔を入力します。

Originator Identifier (注) このオプションは、 [Advanced Mode] でのみ 使用できます。	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。 • [None] : SYSLOG メッセージに発生元識別子を含めません。 • [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。 • [User Defined] : SYSLOG メッセージに含まれる説明を入力します。
RAM Memory Logging	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。
Flash Memory Logging	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。

リモートログサーバー

[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。

手順

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。

Server Definition	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 Version	サポートする IP 形式を選択します。
IPv6 Address Type	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、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。 • [Global] : 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	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）。
Log Server IP Address/Name	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 ポート	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	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。

手順

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、[ファイル名（File Name）] フィールドにパスおよびファイル名を入力します。

TFTP (注) このオプションは、 [Advanced Mode] でのみ 使用できます。	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) (注) このオプションは、 [Advanced Mode] でのみ 使用できます。	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。 • [Global] : 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（ファームウェアの更新時に表示されます）	送信元の名前を入力します（0 ～ 62 文字を使用）
接続先（ファームウェアのバックアップ時に表示されます）	宛先を入力します（0 ～ 62 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。
ユーザー名	[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。 • [Global]：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（ファームウェアの更新時に表示されます）	送信元の名前を入力します（0 ～ 62 文字を使用）
接続先（ファームウェアのバックアップ時に表示されます）	宛先を入力します（0 ～ 62 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

手順

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] または [Source 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
- 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 については参照してファイルを見つけ、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。 • [Global] : 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 ~ 62 文字を使用)

機密データの処理	(注) このオプションは、SCPまたはTFTPのバックアップファイルモードの場合にのみ表示されます。 バックアップファイルに機密データを含める方法を、次のいずれかのオプションから選択します。 • 除外 (Exclude) : 機密データはバックアップに含めません。 • 暗号化 (Encrypt) : 暗号化された形式で機密データをバックアップに含めます。 • プレーン テキスト (Plaintext) : プレーン テキスト形式で機密データをバックアップに含めます。

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。
ユーザー名	[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。 • [Global] : 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 ～ 62 文字を使用)

ステップ 5 コピー方法として [HTTP/HTTPS] を選択した場合は、[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] をクリックして設定を保存します。

設定のバックアップ

設定ファイルのバックアップは、製品に障害が発生した場合のダウンタイムを最小限に抑えるために不可欠です。さらに、実稼働またはテスト機器で新しい設定をテストする前に、正常に動作することがわかっている設定ファイルをバックアップすることをお勧めします。設定の変更が期待どおりに機能していることを確認したら、必ず変更を適用し、新しいバックアップ設定ファイルを作成します。

スイッチの設定をバックアップおよび復元するために、デバイスの Web ベースのグラフィカル ユーザー インターフェイス (GUI) を使用できます。スイッチの設定をバックアップおよび復元する手順は次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	スイッチの Web ベースの GUI にログインします。	
ステップ 2	[Administration] > [File Management] > [File Operations] に移動します。	
ステップ 3	[Operation Type] で [Backup File] を選択します。	
ステップ 4	次に、[Source File Type] で [Running Configuration] を選択します。	

	コマンドまたはアクション	目的
ステップ 5	[Copy Method] については、次のいずれかのオプションを選択します。	• HTTP/HTTPS • USB • 内部フラッシュ
ステップ 6	次に、以下から [Sensitive Data Handling] オプションを選択します。	• Exclude • Encrypt • Plaintext
ステップ 7	[Apply] をクリックします。	

設定の復元

手順

	コマンドまたはアクション	目的
ステップ 1	スイッチの Web ベースの GUI にログインします。	
ステップ 2	[Administration] > [File Management] > [File Operations] に移動します。	
ステップ 3	[Operation Type] で [Update File] を選択します。	
ステップ 4	次に、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
ステップ 5	[Copy Method] については、次のいずれかのオプションを選択します。	• HTTP/HTTPS • USB • 内部フラッシュ
ステップ 6	次に、[File Name] セクションで [Browse] ボタンをクリックし、設定ファイルを探して選択します。	設定が実行コンフィギュレーションに直接適用された場合、スイッチは設定の変更をすぐに適用します。 設定がスタートアップコンフィギュレーションに適用されている場合は、スイッチをリブートして設定の変更を反映させる必要があります。 設定ファイルを復元すると、スイッチの現在の設定が上書きされることに注意してください。設定ファイルを復元する前に、現在の設定をバックアップし

	コマンドまたはアクション	目的
		て、バックアップ後に行われた変更が失われないようにしてください。

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。

手順

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。
- サイズ（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。

ステップ 5 [Refresh] アイコンをクリックしてデータを更新します。ファイルを削除する場合は、ファイルを選択して [Delete] アイコンをクリックします。

ステップ 6 [Apply] をクリックして設定を保存します。

DHCP 自動更新

DHCP 自動更新は、DHCP サーバーが DHCP クライアントに代わって DNS レコードを自動的に更新できる機能です。これにより、DNSA（フォワードルックアップ）およびPTR（逆引きルックアップ）レコードが IP アドレス割り当てと同期されたままになります。

仕組み：

1. DHCP クライアントが IP アドレスを要求すると、スイッチ（DHCP サーバーとして機能）が IP アドレスを割り当てます。
2. その後、スイッチは**ダイナミック DNS（DDNS）**プロトコルを使用して設定された DNS サーバーと通信します。
3. DNS サーバーは、クライアントのホスト名と IP アドレスでレコードを更新します。
4. フォワード（A）レコードと逆引き（PTR）レコードの両方を更新できます。

DHCP 自動更新をセットアップするには、次の手順を実行します。

手順

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、[Enable] に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 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 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	[Enable] チェックボックスをオンにすると、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 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 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。 • 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。 • [Global] : 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）。
前回の自動設定サーバーの IP アドレス	前回の自動設定サーバーの 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 ダッシュボードマネージャを使用して、Cisco Business スイッチ、Cisco Business Wireless、および Catalyst 1200、1300、および 1300X スイッチをモニターおよび管理できます。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、サポートされているすべてのシスコデバイスを設定およびモニターすることを可能にするアドオンです。

Cisco Business ダッシュボードを表示するには、[[Request a Demo](#)] をクリックします。

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。

手順

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。 プローブステータスが [Active] の場合、プローブステータス [Active] とともにプローブモードも次のように表示されます。 • [Active (Probe Managed)] : プローブはネットワーク検出を実行し、ダッシュボードに代わって各管理対象デバイスと直接通信します。 1つのネットワークでは、1つのProbeのみを有効にする必要があります。 • [Active (Direct Managed)] : 直接管理対象デバイスは、広範囲のネットワーク内にある他のデバイスを検出すると、ダッシュボードにそれらのデバイスを自動的に接続し、それらのデバイスを管理可能にします。必要に応じて、ダッシュボードで IP アドレス範囲を明示的に検索し、他の VLAN やサブネットにあるネットワークデバイスを検出することができます。 すべてのデバイスが直接管理をサポートしている場合は、直接管理ネットワークが推奨されます。
[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] (注) これらのロギングセクションはすべて、 [Advanced Mode] でのみ 使用できます。	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]、[Disconnected]、または [Unavailable]）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 Unavailable : CBD ダッシュボード接続が未設定、またはプローブが無効といった最も一般的な状態の場合、この切断メッセージが表示されます。
[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 Address/Name]	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。

[Connection Setup]	次のいずれかの接続設定を指定します。 • [Online with Web Browser] • [Offline with Access Key]
[Access Key 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。
[Access Key Secret]	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 [Apply] 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

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。これは、大規模でより複雑な環境について説明する場合にのみ適用されます。小規模なネットワークや一般的な小規模ビジネス環境では、PNP は必要ない可能性があります。

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

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](https://www.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。
version	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。

パラメータ	説明
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。
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。 <code>http://CBD IP address or domain name/ca/trustpool/CA_bundle_name</code> • TFTP サーバーを使用する場合は、次の URL 形式を使用します。<code>tftp://tftp server IP/CA_bundle_name</code>
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;Thhttp://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。

手順

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 トランスポート/設定の定義	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。 • [Default Settings] : 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。[Default Settings] オプションを選択すると、[PNP Transport] 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。
トランスポートプロトコル	トランスポートプロトコル（HTTP または HTTPS）を選択します。

TCP ポート	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 Version	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。 • [Link Local] : 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。 • [Global] : 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	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 アドレスまたは完全修飾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。 • [Default Settings] : 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。 • [Manual Settings] : 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。[Discovery Timeout] 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。

手順

[Administration] > [PNP] > [PNP Session] をクリックします。

次のフィールドが表示されます。

- [Administrative Status] : PNP が有効になっているかどうか。
- [Operational Status] : 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、[Discovery Wait]、[Discovery]、[Not Ready]、[Disabled]、[Session]、[Session Wait] です。
- [Transport Protocol] : PNP エージェント セッション情報を表示します。
- [TCP Port] : PNP セッションの TCP ポート。
- [Server IP Address] : 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)。
- [Remaining Timeout] : 残っているタイムアウトの値。



(注) [Resume] 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。

手順

ステップ 1 [Administration] > [Reboot] に移動します。

ステップ 2 リブートオプションを選択します。

- [Immediate] : すぐにリブートします。
- [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。
- [In] : デバイスが再起動するまでの日数、時間、分を入力します。経過可能な時間は、最大 24 日です。

- ステップ 3** (オプション) リブート時にスイッチを工場出荷時の設定にリセットするには、[Restore to Factory Defaults] をオンにします。
- ステップ 4** (オプション) 構成ファイルをクリアするには、[Clear Startup Configuration File] をオンにします。
- ステップ 5** [Reboot] をクリックして、アクションを確認します。
- ステップ 6** [Cancel Reboot] 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。
-

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。

手順

- ステップ 1** [Administration] > [Hardware Resources] 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 (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] : 値を入力します (範囲 0 ~ 32、デフォルト 12) 。
- [VLANマッピングの最大エントリ数 (Maximum VLAN—Mapping Entries)] : 次のいずれかを選択します。

- [デフォルトを使用 (Use Default)] : デフォルト値を使用します。
- [ユーザー定義 (User Defined)] : 値を入力します (範囲 0 ~ 512、デフォルト 13)。
- [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。

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、デバイスはディスカバリ - Bonjour 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。

手順

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

ステップ 2 [Enable] をオンにし、ディスカバリ - Bonjour 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 インターフェイス (ポート、LAG、または VLAN) を選択し、インターフェイスを構成します。

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、ディスカバリ - Bonjour 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。

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。

LLDP 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

[Properties] 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。

手順

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。

(注)

[Basic Mode] では LLDP ステータスのみが表示され、他のパラメータは [Advanced Mode] の場合にのみ表示されます。

LLDP Status	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 Frames Handling	[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 Advertise Interval	次のオプション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。

Topology Change SNMP Notification Interval	次のオプション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。
Hold Multiplier	次のオプション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。
Reinitializing Delay	次のオプションのいずれかを選択します。 • [Use Default] : デフォルトの時間を使用します。 • [User Defined] : 時間を入力します
Transmit Delay	次のオプションのいずれかを選択します。 • [Use Default] : デフォルトの時間を使用します。 • [User Defined] : 時間を入力します
Chassis ID Advertisement	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。 • [Host Name] : 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 Fast Start 機能の初期化時に 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 \(121 ページ\)](#) 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。

手順

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] または [Copy] 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 & Rx] : 送信も検出も行います。 • [Disable] : このポート上で LLDP を無効にします。
SNMP 通知	[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 Link Aggregation] : 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。 • [Manual Advertise] : アドバタイズする管理 IP アドレスを選択します。
IP Address	[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。

VLAN ID	アドバタイズする VLAN を選択します。
プロトコルID	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 ネットワークポリシー



(注) これは、[Advanced Mode] でのみ表示されます。

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 \(121 ページ\)](#) 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。

手順

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。

- [Network Policy Number] : 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。（範囲 0 ～ 4095）
- [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。
- [User Priority] : 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 Value] : 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。

手順

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

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。

- [Interface] : 設定するインターフェイスを選択します。
- [LLDP MED Status] : 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。

- [Location Coordinate] : LLDP を使用して送信する座標を入力します。
- [Location Civic Address] : 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。

ステップ 6 [LLDP Local Information Detail] をクリックして、LLDP ローカル情報を表示します。

LLDPポートステータス

[LLDP Port Status] 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。

手順

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

- [Chassis ID Subtype] : シャーシ ID のタイプ (例 : MAC アドレス) 。
- [Chassis 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) 。
- [Supported System Capabilities] : 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) 。
- [Enabled System Capabilities] : スイッチで有効になっている主要機能。
- [Port ID Subtype] : 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

- [Interface] : ポート ID。
- [LLDP Status] : 有効または無効。
- [LLDP MED Status] : 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。

- [# of neighbors] : 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、次のようになります。

手順

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）。
- [Chassis 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）。
- [Supported System Capabilities] : 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）。
- [Enabled System Capabilities] : スイッチで有効になっている主要機能。
- [Port ID Subtype] : 表示されるポート ID のタイプ。
- [ポート ID] : ポートの ID。
- [Port Description] : 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ダプタイズ機能] : 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]

- [Aggregation Capability] : インターフェイスを集約できるかどうか。
- [Aggregation Status] : 現在、インターフェイスが集約されているかどうか。
- [Aggregation Port ID] : アダプ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] : アダプ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] : アダプタイズされている、ポートの電力クラス。
- [電源タイプ] : 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。

[Extended PSE Information]

- [PoE デバイスタイプ] : 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 Power Value] : ポートの電力の値。

[Inventory Information]

- [ハードウェアリビジョン] : 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。
- [シリアル番号] : 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。
- [Asset 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]

- [Application Type] : 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 Type] : 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）。
- [User Priority] : 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。

手順

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。

- [Port ID Subtype] : 表示されるポート ID のタイプ。
- [ポート ID] : ポートの ID。
- [システム名] : 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。
- [Port ID Subtype] : 表示されるポート ID のタイプ。
- [ポート ID] : ポートの ID。
- [Port Description] : 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、およびネットワーク 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]

- [アドレスサブタイプ] : 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ダプタイズ機能] : 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] : アダプ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] : アダプタイズされている、ポートの電力クラス。
- [電源タイプ] : 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] : ポートの電源の優先順位。
- [PD 要求電力値] : POD デバイスから要求された電力量。
- [PSE 割り当て電力値] : 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] : アダプタイズされている、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 デバイスタイプ] : 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 Power Value] : ポートの電力の値。
- [ハードウェアリビジョン] : 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。
- [シリアル番号] : 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。
- [Asset 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]

- [Application Type] : 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 Type] : 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）。
- [User Priority] : 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。

ステップ 4 [LLDP Neighbor Table] のデータをフィルタ処理するには、[Filter] をオンにして、ドロップダウンリストからローカルポートを選択します。次に、[Go] をクリックして、選択したポートを表示します。

ステップ 5 [LLDP Neighbor Table] からポートを削除するには、ポートを選択して削除アイコンをクリックします。

LLDP の統計情報

[LLDP Statistics] 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。

手順

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。

- [Interface] : 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。
 - [Unrecognized] : 受信した TLV のうち、認識されなかった TLV の数。
- [Neighbor's Information Deletion Count] : これは、スペースが不足しているためにスイッチで追加できなかった有効な LLDP ネイバーの数を指します。このカウントは、スイッチでのネイバー検出アクティビティに関するインサイトを提供する LLDP 統計の一部です。

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。

手順

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。

- [Interface] : 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。
- [Status] : 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。

- [Interface] : 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。
- [LLDP Mandatory TLVs]
 - [Size (Bytes)] : 必須 TLV の合計バイト数。
 - [Status] : 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どうか、または過負荷状態であったかどうかを示されます。
- [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どうか、または過負荷状態であったかどうかを示されます。
- [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どうか、または過負荷状態であったかどうかを示されます。
- [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どうか、または過負荷状態であったかが示されます。
 - [802.1 TLV]
 - [Size (Bytes)] : LLDP MED 802.1 TLV パケットの合計バイト サイズ。
 - [Status] : LLDP MED 802.1 TLV パケットが送信されたかどうか、または過負荷状態であったかが示されます。
 - [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どうか、または過負荷状態であったかが示されます。
 - [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どうか、または過負荷状態であったかが示されます。
 - [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どうか、または過負荷状態であったかが示されます。
 - Total
 - [Total (Bytes)] : 各パケットの LLDP 情報の合計バイト数。
 - [Available Bytes Left] : 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 プロパティを設定するには、次の手順を実行します。

手順

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。

(注)

[Basic Mode] では CDP ステータスのみが表示され、他のパラメータは [Advanced Mode] の場合にのみ表示されます。

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 • [Flooding] : 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 (198 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。 • [Mac Address] : デバイスの MAC アドレスをデバイス ID として使用します。 • [Serial Number] : デバイスのシリアル番号をデバイス ID として使用します。 • [Hostname] : デバイスのホスト名をデバイス ID として使用します。
送信元インターフェイス	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。
インターフェイス	[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ダプ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、CDP 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。

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。

手順

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。

- [Entry No.] : CDP エントリ。
 - [Interface] : CDP エントリに使用されるインターフェイス。
 - [CDP Status] : ポートに対する CDP 発行オプション。
 - [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。
 - [No. of Neighbors] : 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。
- [Copy Settings] : 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。
 - [Edit] : 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（138 ページ）](#) に移動します。
 - [CDP Neighbor Information Details] : [CDP ネイバー情報（140 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ダプ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ダプ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ダプ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



(注) インターフェイスがダウン状態の場合、CDP の状態を除くすべての設定は使用できません。

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

手順

[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 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 でアダプタイズされるデバイス ID のタイプ。 • [Device ID] : デバイス ID TLV でアダプタイズされるデバイス ID。

System Name TLV	[System Name TLV] : デバイスのシステム名。
Address 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]	[Port ID] : ポート TLV でアドバタイズされるポートの ID。
Capabilities TLV	[Capabilities] : ポート TLV でアドバタイズされる機能。
Version TLV	[Version] : 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。
Platform TLV	[Platform] : 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。
Native VLAN TLV	[Native VLAN TLV] : ネイティブ VLAN TLV でアドバタイズされるネイティブ VLAN ID。
Full/Half Duplex 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。 • [Appliance 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	• [Request 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。
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。 • [Spare Pair Detection/Classification Required] : 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。

手順

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

ステップ 2 新しいインスタンスを開始するには、[Clear Table] をクリックして、CDP ネイバー情報テーブルの以前のデータをクリアします。

ステップ 3 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。[Clear Filter] 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。
System Name	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。
Advertisement Version	CDP プロトコルのバージョン。
Time to Live (sec)	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。
Platform	ネイバーのプラットフォーム TLV からの情報。
Neighbor Interface	ネイバーの発信インターフェイス。

ステップ 4 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。
System Name	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。
Advertisement Version	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。
Platform	ネイバーのプラットフォーム TLV からの情報。
Neighbor Interface	ネイバーの発信インターフェイス。
Native VLAN	ネイバーのネイティブ VLAN。
Application	ネイバーのアプリケーション。
Duplex	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。
Version	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。
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。 • [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 予備ペア動作状態 (PD Spare Pair Operational State)] : 4 ペア能力が有効か無効かを示します。



(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。

手順

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。

[Packets Received/Packets Transmitted] :

- [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。

- [Total] : 受信または送信した CDP パケットの合計数。
[CDP Error Statistics]
- [Illegal Checksum] : 無効なチェックサム値とともに受信したパケットの数。
- [Other Errors] : 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。

手順

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。
- [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。
- [UnitID] : 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。

手順

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
Host Definition	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 Version	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。
Destination IPv6 Address Type	次のオプションのいずれかを選択します。 • [Link Local] : 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。 • [Global] : 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。

オプション	説明
Link Local Interface	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。
Destination IP Address/Name	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。
Number of Pings (注) この設定は、[Advanced Mode] ビューでのみ使用できます。	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。
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。

- [Number of Sent Packets] : ping で送信されたパケットの数
- [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
- [Minimum Round Trip Time] : パケットが戻った最短の時間
- [Maximum Round Trip Time] : パケットが戻った最長の時間
- [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。

手順

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。

- [Host Definition] : ホストがその IP アドレスまたは名前で識別されるかどうかを選択します。
- [IPバージョン (IP Version)] : [バージョン6 (Version 6)] または [バージョン4 (Version 4)] のオプションから選択し、ホストの識別方法を決定します。
- [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] : 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。

- [Index] : ホップ数が表示されます。
 - [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 \(147 ページ\)](#)
- [エラー回復設定 \(150 ページ\)](#)
- [ループバック検出設定 \(152 ページ\)](#)
- [リンク集約 \(152 ページ\)](#)
- [UDLD \(156 ページ\)](#)
- [PoE \(160 ページ\)](#)
- [グリーンイーサネット \(167 ページ\)](#)

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。

手順

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 \(94 ページ\)](#) 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) [Interface] と [Port Description] は、メイン ページの [ポート] 列に表示されます。
Port Type	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、2500M (タイプ: 銅)、10G の各値をサポートします。 • [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。
Operational Status	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。
Link Status SNMP Traps	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。
Time Range	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。
Time Range Name	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] をクリックします。
Operational Time Range State	[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。
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、ポートはその伝送速度、デュプレックスモードを、ポートリンクパートナーにアドバタイズできます。

Operational Auto Negotiation	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。
Administrative Port Speed	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。
管理デュプレックスモード	• [フル (Full)] : インターフェイスがスイッチとクライアント間で同時に両方向にデータを送信できるようにします。
運用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。
自動アダプタイズメント	自動ネゴシエーションが有効な場合に、アダプ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。 • [Max Capability] : すべてのポート速度と両方のデュプレックスモード。 • [1000全二重 (1000 Full)] : 1000 Mbps の速度で全二重モード。 • [10全二重 (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全二重 (100 Full)] : 100 Mbps の速度で全二重モード。
運用アダプタイズメント	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。
Preference Mode	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。
Neighbor Advertisement	ネイバーデバイスによってアダプタイズされた機能が表示されます。
フロー制御	ポートで 802.3x フロー制御を有効化または無効化します (全二重モードの場合のみ)。

[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。
Operational MDI/MDIX	現在の MDI/MDIX 設定が表示されます。
Protected Port	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（154 ページ） を参照してください。
Member in LAG	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。

手順

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。
- **Automatic ErrDisable Recovery**
 - **[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。
 - **[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、リンクフラップ防止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。

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、次の手順を実行します。

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

アクティブ化されていないインターフェイスのリストと、その **[Suspension Reason]** が **[Suspended (errDisabled) Interface Table]** に表示されます。

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。

手順

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。（範囲 5 ～ 60、デフォルト 30）。

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せん)。その後、[LACP] ボタンが編集に使用できるようになります。
- [Dynamic] : 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。

手順

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 Address] : 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 Name] : 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。
- [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。

手順

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 Type	この LAG を構成しているポートのタイプが表示されます。
Description	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。
Link Status SNMP Traps	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。
Time Range	ポートを [Up] 状態にする時間範囲を有効にする場合に [Enable] をオンにします。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

オプション	説明
	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。
Time Range Name	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。
Operational Status	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。
Operational Time 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。
Administrative Auto Negotiation	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 が伝送速度をパートナーにアダプタイズすることを可能にします。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）。
Administrative Speed	LAG 内のポートの速度を表示します。
Administrative Advertisement	すべての LAG 速度と両方のデュプレックスモードを有効にするには、[Max Capability] をオンにします。LAG によってアダプタイズされる機能を選択します。
Administrative Flow Control	LAG で [Flow Control] を [Enable] または [Disable] に設定します。
Protected LAG	保護された LAG を有効にするには、チェックボックスをオンにします。
Operational Auto Negotiation	自動ネゴシエーション設定が表示されます。
Operational LAG Speed	LAG の現在の速度が表示されます。
Operational Advertisement	管理アダプ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 の機能をアダプタイズします。[Administrative Advertisement] フィールドで指定された値を使用できます。
Operational Flow Control	現在のフロー制御の設定が表示されます。

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。

手順

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、[Edit] をクリックします。

ステップ 4 [Edit LACP Settings] 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。

- [Port] : 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 Port Priority] : 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。

手順

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。

手順

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。

- [Interface] : 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。
- [UDLD State] : 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。
 - [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。

表示されるフィールドをフィルタリングするには、[Filter] にチェックマークを付け、[Interface Name equals to] に値を入力して [Go] 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。
- [Neighbor Information] :
 - [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。
 - [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デバイスとは、ネットワークトラフィックの中断、物理ネットワークの更新、またはネットワークインフラストラクチャの変更を行うことなく、既存のカップパーケーブルを介して、接続先の AFAIK PD（受電装置）に電力を供給する給電側機器（PSE）です。

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。

デバイスは 2 つのタイプの PoE ポートをサポートします。

- 802.3AT ポート：最大 30 ワットの電力を供給できます
- 802.3BT タイプ 3 ポート：最大 60 ワットの電力を供給できます

PoE ポートのタイプは SKU によって異なります。SKU には両方のタイプの PoE ポートがある場合があります。

PoE は次の各段階で実装されます。

- 検出：カップ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、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。

手順

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。

- [Power Mode] : 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。

- [Traps] : トラップを有効にするには、[Enable] をオンにします。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。
- [Power Trap Threshold] : 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。

デバイスの次の PoE 電源情報が表示されます。

- [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。
- [Allocated power] : PoE ポートに現在割り当てられている電力量。割り当て済み電力は、各 PoE ポートに割り当てられた電力を合計して計算されます。ポートが CDP または LLDP を使用して PD との電力割り当てをネゴシエートした場合、ポートの電力割り当ては CDP または LLDP ネゴシエーションの結果に基づきます。ポートが CDP または LLDP を使用した電力割り当てのネゴシエートを行わなかった場合、ポートに割り当てられる電力は PD の消費電力と等しくなります。
- [Available Power] : 公称電力から消費電力量を引いた値。

(注)

- LLDP ネゴシエーションに基づく電力割り当ては、ネゴシエートされた電力値よりも高くなる場合があります。
 - CDP ネゴシエーションに基づく電力割り当ては、ネゴシエートされた電力値と等しくなります。
 - ポートごとに割り当てられる電力（消費電力値と異なる場合）は、PoE 設定表の「電力」列の括弧内に表示されます。
-
- [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 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

永続的な PoE 機能（Always On PoE と呼ばれます）は、スイッチのステータスに対する PoE 動作の依存性を最小限に抑えます。この機能が導入される前は、再起動や致命的なエラーなどのスイッチ操作で中断が発生すると、デバイスが回復を完了するまで、PoE 動作も中断されました。

永続的な PoE を使用すると、reload コマンドまたは GUI の再起動機能によって実行されるようなウォームリブートでは、現在の状態での PoE の動作が中断されることはありません。

[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。

手順

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。

(注)

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。

- [Administrative Power Allocation (mW)] : 割り当て可能な電力量を入力します。
- [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。
- [Status] : ポートのステータスと失敗の理由を示します。802.3BT Type 3 をサポートする PoE ポートでは、Alt A と Alt B のペアに対してステータスが表示されます。

- [PoE Standard] : サポートされている PoE のタイプを表示します (例 : 802.3BT Type 3 PoE) 。
- [Interface] : 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。
- [Alt A Status] : PD が 30 W のポートに接続されていない場合は [None] または [Other] と表示されます。
- [Alt B Status] : PD が 60 W のポートに接続されていない場合は [None] または [Other] と表示されます。
- [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。
- [管理電力割り当て (mW)] : 割り当てることができる電力量を入力します。
- [クラス (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。802.3BT Type 3 をサポートする PoE ポートでは、Alt A と Alt B の両方のペアに対して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。
- [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。

- [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] : クラスの制限だけでなく、ポートの制限も考慮して、受電デバイス (PD) によって使用される実際の電力を指します。
- [クラス (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。802.3BT Type 3 をサポートする PoE ポートでは、Alt A と Alt B の両方のペアに対してクラスが表示されます。

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 \(161 ページ\)](#) 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。

手順

ステップ 1 [Port Management] > [PoE] > [PoE Settings-Class Limit] 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] : サポートされている PoE のタイプを表示します (例 : 802.3AT、802.3BT Type 3 PoE) 。
- [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。
- [Status] : ポートのステータスと失敗の理由を示します。802.3BT Type 3 をサポートする PoE ポートでは、Alt A と Alt B のペアに対してステータスが表示されます。

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。

- [Interface] : 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。
- [Status] : 802.3BT Type 3 をサポートする PoE ポートで、Alt A と Alt B の両方のペアに対してクラスが表示されます。
- [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。

(注)

次の 2 つの設定は、BT 標準規格に準拠するポートでのみサポートされます。

- [Auto Class Mode] : インターフェイスで 802.3BT 自動クラスを有効にする場合はオンにします。
- [Initiate Auto Class Process] : インターフェイスで自動クラスプロセスを開始する場合はオンにします。

(注)

[自動クラスプロセスの開始 (Initiate Auto Class Process)] コントロールは、ユーザーがインターフェイス上の [自動クラスモード (Auto Class Mode)] 設定をオンにして設定を適用した場合にのみアクティブになります。

- [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。802.3BT Type 3 をサポートする PoE ポートでは、Alt A と Alt B の両方のペアに対して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
5	45.0 ワット
6	60.0 ワット
802.3BT タイプ 3 クラス 5	45.0 ワット
802.3BT タイプ 3 クラス 6	60.0 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 [PowerLimit] 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。
- [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。

手順

- ステップ 1 [ポート管理 (Port Management)] > [PoE] > [統計 (Statistics)] をクリックします。
- ステップ 2 [Interface] を選択します。ユニットの選択はスタックブル デバイスでのみ表示されます。インターフェイスを選択すると画面がリロードされ、選択したインターフェイスの情報が表示されます。
- ステップ 3 [リフレッシュレート (Refresh Rate)] を選択します。オプションボタン ([更新なし (No refresh)]、[15 秒 (15 sec)]、[30 秒 (30 sec)]、[60 秒 (60 sec)]) を選択すると、画面の更新頻度がただちに更新されます。
- 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

- [過負荷 (Overload)] : 検出された過負荷状態の数
- [拒否 (Denied)] : 検出された拒否状態の数。
- [未検出 (Absent)] : 検出された未検出状態の数。
- [無効な署名カウンタ (Invalid Signature Counter)] : 検出された無効な署名状態の数。

(注)

802.3BT 標準規格をサポートするポートの場合、Alt A ペアと Alt B ペアのカウンタが別々に表示されます。

- ステップ 5 [Clear Event Counters] をクリックして、イベントカウンタをクリアします。
- ステップ 6 [View All Interfaces Statistics] をクリックして、すべてのインターフェイスに関する統計情報を表形式で表示します。
- ステップ 7 [View Interface History Graph] をクリックして、インターフェイス履歴グラフを表示します。

ステップ 8 データをリフレッシュするには、[Refresh] をクリックします。

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 RJ45 ポートでのみサポートされます。このモードはデフォルトでは無効になっています。

前述のグリーンイーサネット機能の他に、802.3az Energy Efficient Ethernet (EEE) もあります。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。

手順

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。

- [Short Reach] : 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 \(167 ページ\)](#) 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 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。

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。

手順

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。

(注)

一部のフィールドは、いくつかの SKU に関して表示されない場合があります。

- [Port] : ポート番号。
- [Energy Detect] : エネルギー検出機能に関するポートの状態。
 - [Administrative] : エネルギー検出が有効かどうかが表示されます。
 - [Operational] : エネルギー検出がローカルポートで現在動作しているかどうかが表示されます。これは、有効化されたかどうか（管理ステータス）、ローカルポートで有効化されたかどうか、およびローカルポートで稼働状態にあるかどうかを示す機能です。
 - [Reason] : エネルギー検出が有効にされているのに動作していない理由が表示されます。
- [Short Reach] : 短距離機能に関するポートの状態。
 - [Administrative] : 短距離機能が有効かどうかが表示されます。
 - [Operational] : 短距離機能がローカルポートで現在動作しているかどうかが表示されます。これは、有効化されたかどうか（管理ステータス）、ローカルポートで有効化されたかどうか、およびローカルポートで稼働状態にあるかどうかを示す機能です。
 - [Reason] : 短距離機能が有効にされているのに動作していない理由が表示されます。
 - [Cable Length] : ケーブルの長さ。
- [802.3 Energy Efficient Ethernet (EEE)] : EEE 機能に関するポートの状態です。
 - [Administrative] : EEE が有効だったかどうかが表示されます。
 - [Operational] : EEE がローカルポートで現在動作しているかどうかが表示されます。これは、有効化されたかどうか（管理ステータス）、ローカルポートで有効化されたかどうか、およびローカルポートで稼働状態にあるかどうかを示す機能です。
 - [LLDP Administrative] : LLDP 経由の EEE カウンタのアドバタイズが有効であったかどうかが表示されます。
 - [LLDP Operational] : LLDP 経由の EEE カウンタのアドバタイズが現在動作しているかどうかが表示されます。
 - [EEE Support on Remote] : EEE がリンクパラメーターでサポートされているかどうかが表示されます。EEE は、ローカルとリモート両方のリンクパートナーでサポートされている必要があります。

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 インターフェイスを選択し、各オプションの [Enable] をオンにして、ポートで利用できるオプションを構成します。

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](#) (171 ページ)
- [Smartport タイプ設定](#) (172 ページ)
- [Smartport インターフェイス設定](#) (173 ページ)

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。

Smartport 機能を設定するには、次の手順を実行します。

手順

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

ステップ 2 テレフォニー OUI が有効か無効かを表示します。Auto Smartport とテレフォニー OUI を同時に使用することはできません。

ステップ 3 次の項目を設定します。*

- [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。

(注)

*この設定は基本モードでのみ使用できます。

- [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 4 [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



(注) この設定は、[Advanced Mode] でのみ使用できます。

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。

手順

-
- 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。
- [Port Type] : Smartport タイプを選択します。
 - [Macro Name] : 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 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



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

[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。

手順

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。
- [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。
- [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。タイプが [不明 (Unknown)] のインターフェイスを選択して、[診断の表示 (Show Diagnostics)] 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。
- [Unknown] 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。

- [Interface] : ポートまたは LAG を選択します。
- [Smartport Type] : 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 Application] : [Smartport Application] 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。
- [Persistent Status] : 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。
- [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 \(177 ページ\)](#)
- [インターフェイスの設定 \(179 ページ\)](#)
- [VLANへのポート \(181 ページ\)](#)
- [ポートVLANメンバシップ \(183 ページ\)](#)
- [VLAN 変換 \(184 ページ\)](#)
- [プライベートVLAN設定 \(191 ページ\)](#)
- [GVRP設定 \(191 ページ\)](#)
- [VLAN グループ \(192 ページ\)](#)
- [Voice VLAN \(197 ページ\)](#)
- [自動監視 VLAN \(204 ページ\)](#)
- [アクセスポートマルチキャストTV VLAN \(206 ページ\)](#)
- [カスタマーポートマルチキャストTV VLAN \(208 ページ\)](#)

VLAN 設定

VLANを作成すると、スイッチ上に個別のブロードキャストドメインを作成できます。ブロードキャストドメインは、ルータなどのレイヤ3デバイスを介して、互いに通信できます。VLANは主に、物理的な場所に関係なく、ホスト間のグループを形成するために使用されます。VLANはホスト間で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を確立する最も一般的な理由の1つは、音声用とデータ用に別のVLANを作成するためです。これにより、両方のタイプのパケットが送信されます。

VLAN の作成または構成

スイッチでVLANを作成または構成するには、次の手順を実行します。

手順

-
- 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。
- 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オンにします。
 - [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オンにします。
- (注)
VLAN テーブルには、VLAN の作成方法を示す [Originators] という用語が表示されます。
- 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。
-

レイヤ3スイッチング

レイヤ3スイッチは、スイッチとルータの機能を組み合わせたものです。IP ルーティング インテリジェンスが組み込まれていて、ルータとして機能するほか、同じサブネットまたは仮想 LAN 上にあるデバイスをすばやくリンクするためのスイッチとして機能します。着信パケットを検査し、送信元アドレスと宛先アドレスに応じてルーティングを決定し、ルーティングプロトコルを処理できます。レイヤ3スイッチは、次のようにスイッチとルータの両方として機能します。

デバイスをレイヤ3スイッチとしてセットアップするには、次の手順に従います。

手順

-
- ステップ1** [VLAN Management]>[VLAN Settings] をクリックします。
- ステップ2** [Add] をクリックします。
- ステップ3** VLAN ID と VLAN 名を入力します。
- ステップ4** [Apply] をクリックして、VLAN を作成します。
- ステップ5** 次に、[IPv4 Configuration]>[IPv4 Interface] に移動します。
- ステップ6** [Enable] をオンにして、IPv4 ルーティングを有効にします。これにより、すべてのレイヤ3 インターフェイス間のルーティングが可能になり、ある VLAN からのトラフィックを別の VLAN に転送できるようになります。

ステップ7 [Apply] をクリックして、すべてのレイヤ3 インターフェイス間のルーティングを有効にします。これにより、ある VLAN からのトラフィックを別の VLAN に転送できるようになります。

インターフェイスの設定

VLAN が構成されている物理ネットワークポートまたはボンドに接続されている仮想インターフェイスは、VLAN インターフェイスと呼ばれます。VLAN インターフェイスは、ルーティングされるトラフィックに正しい VLAN ID を自動的に割り当てるために使用されます。

VLAN 関連のパラメータは、[VLAN Interface Settings] ページに表示され、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。

手順

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

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。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3 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4 次のフィールドに値を入力します。

Interface	[Port/LAG] を選択し、ポートを選択または入力します。
Switchport Mode	レイヤ 2 またはレイヤ 3 を選択します。

Interface VLAN Mode	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。 • [Access]：インターフェイスは、1つのVLAN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。 • [Trunk]：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規格で定義されているすべての機能をサポートします。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。 • [Customer]：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設定する場合に選択します。
EtherTypeタギング	S-VLAN タグ用の [Ethertype tagging] 方式を選択します。 • Dot1q-8100 • Dot1ad-88a8 • 9100（旧非標準 QinQ イーサタイプ） • 9200（非標準 QinQ イーサタイプ）

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。 • [Admit Tagged Only] : 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。 • [Admit Untagged Only] : 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。
Ingress Filtering	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。インターフェイスがプライベート VLAN モードでない場合、[None] が選択されます。
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。

ステップ 5 [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方法で表示されます。これらを使用して、VLAN にメンバーを含めたり、VLAN からメンバーを除外したりできます。デフォルトの VLAN メンバーシップが禁止されている場合、ポートに対して他の VLAN メンバーシップは許可されません。そのポートに内部 VID として 4095 が割り当てられます。

エンドノード間のパスでパケットを転送するには、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。

2 つの VLAN 対応デバイス間に仲介する VLAN 対応デバイスがない場合、それらのタグなしポートメンバーシップは、同じ VLAN に属している必要があります。2 つのデバイス間にあるポートが、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、それらのポート

の PVID が一致する必要があります。これがないと、トラフィックが 1 つの VLAN から別の VLAN にリークする可能性があります。

VLAN 対応や VLAN 非対応のその他のネットワークデバイスは、VLAN タグ付きフレームを通過させることができます。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必要がある場合、最後の VLAN 対応デバイスが、宛先 VLAN のタグなしフレームをエンドノードに転送する必要があります。

特定の VLAN 内のポートを表示および構成するには、[VLANへのポート (Port to VLAN)] ページを使用して、以下の手順に従います。

手順

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、[インターフェイスの設定（179 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。
 - [Tagged] : インターフェイスは、VLAN のタグ付きメンバーになります。
 - [Untagged] : インターフェイスは、VLAN のタグなしメンバーになります。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 TV 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

アクセスレイヤスイッチで VLAN が使用可能になった場合、エンドユーザーはそれに参加できる必要があります。その結果、[Port VLAN Membership] ページには、デバイスのすべてのポートとともに、各ポートが所属する VLAN が表示されます。

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。

手順

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。

- [Interface] : ポート /LAG ID。
- [Mode] : [インターフェイスの設定（179 ページ）](#) で選択されたインターフェイス VLAN モード。
- [Administrative VLANs] : 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。
- [Operational VLANs] : 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] ボタンをクリックします。

ステップ 4 次のフィールドに値を入力します。

- [Interface] : ポートまたは LAG を選択します。
- [Current VLAN Mode] : [インターフェイスの設定（179 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 [Apply] をクリックします。

ステップ 6 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。

- [Interface] : ポートまたは LAG を選択します。
- [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。

VLAN 変換

VLAN 変換では、入力タグを別のタグに置き換えたり、出力でその逆を行ったりします。これは、一連の VLAN 変換ルールを構成するためにインターフェイスで使用されます。これらの

ルールが適用されると、そのインターフェイスの着信および発信パケットの VLAN-ID は、変換ルールからの適切な VLAN-ID にマッピングされます。この構成は、フレームの VLAN 識別子をインターフェイスで変更する必要がある場合に役立ちます。

ワンツーワンの VLAN トンネリング

VLAN トンネリングは、QinQ/Nested VLAN/カスタマーモード VLAN 機能を拡張する機能です。この機能は、サービスプロバイダーが単一の VLAN を使用して複数の VLAN を所有しているお客様をサポートできるようにします。カスタマー VLAN ID を保護しながら、複数のカスタマー VLAN でトラフィックを分離します。サービスプロバイダー エッジスイッチのトンネルポートに着信するパケット（適切な VLAN ID ですでに 802.1Q タグ付けされている）は、カスタマーに一意である VLAN ID を含む 802.1Q タグの別のレイヤでカプセル化されます。元々のカスタマーの 802.1Q タグは、カプセル化されたパケットの中に維持されます。したがって、サービスプロバイダーインフラストラクチャに着信するパケットは二重にタグ付けされます。

この機能は、スイッチがネットワーク経由でトラフィックを転送するために、通常の 802.1Q タグ（カスタマー VLAN/C-VLAN）に加えてサービスタグ（S-VLAN）と呼ばれる第 2 の ID タグが追加されるため、「ダブルタギング」または QinQ と呼ばれます。カスタマーネットワークがプロバイダーエッジスイッチに接続されるインターフェイスであるエッジインターフェイスでは、C-VLAN が S-VLAN にマッピングされ、オリジナルの C-VLAN タグがペイロードの一部として維持されます。タグなしフレームは除去されます。

フレームの最初の C-VLAN-ID は、非エッジのタグ付きインターフェイスを介して配信されるときに、S-VLAN タグの別のレイヤにマッピングされます。その結果、非エッジのインターフェイスを持つフレームでブロードキャストされるパケットには、外部 S-VLAN タグと内部 C-VLAN タグの 2 つのタグが付けられます。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経由で転送されている間は、サービス VLAN タグがそのまま保持されます。フレームが出力デバイスのエッジインターフェイスから送信されるときに S-VLAN タグが除去されます。タグのないフレームはドロップされます。

VLAN トンネリング機能では、基本的な QinQ/Nested VLAN 実装に加えて、個別のコマンドセットを使用して次の機能が提供されます。

- エッジインターフェイスごとに、S-VLAN を分離するためのさまざまな C-VLAN のマッピングを複数提供
- エッジインターフェイスで受信された特定の C-VLAN に対してドロップアクションの設定が可能
- S-VLAN に明確にマッピングされていない C-VLAN に対してアクションの設定が可能（ドロップまたは特定の S-VLAN へのマッピング）
- グローバルまたは NNI インターフェイス（ネットワーク ノードインターフェイス - バックボーンポート）ごとに、S-VLAN タグの EtherType が設定可能以前の QinQ の実装では、S-VLAN タグには EtherType 0x8100 のみがサポートされていました。

インターフェイスでデバイスを S-VLAN として設定するまえに、ユーザ指定の S-VLAN を作成しておく必要があります。この VLAN が存在しない場合、コマンドは失敗します。

IPv4/IPv6 転送と、VLAN トンネリングは同時には使用できません。つまり、IPv4 転送または IPv6 転送のいずれかが有効になっている場合、インターフェイスを VLAN トンネリング モードに設定することはできません。また、任意のインターフェイスを VLAN トンネリング モードに設定すると、そのデバイスで IPv4 転送および IPv6 転送を有効にすることはできません。

次の機能も、VLAN トンネリング機能と同時には使用できません。

- 自動音声 VLAN
- Auto Smartport
- 音声 VLAN

エッジインターフェイスを含む VLAN では、IPv4 と IPv6 のインターフェイスを定義することができません。

VLAN 変換

エッジインターフェイスを含む VLAN では、次のレイヤ 2 の機能はサポートされません。

- IGMP/MLD スヌーピング
- DHCP スヌーピング
- IPv6 ファースト ホップ セキュリティ

エッジインターフェイス (UNI - ユーザ ネットワーク インターフェイス) では、次のプロトコルを有効にすることができません。

- STP
- GVRP

エッジインターフェイス (UNI - ユーザ ネットワーク インターフェイス) では、次の機能はサポートされません。

- RADIUS VLAN 割り当て
- 802.1x VLAN
- SPAN/RSPAN : ネットワーク キーワードを使用する宛先ポート、またはネットワーク キーワードまたはリフレクタ ポートを使用するリフレクタ ポート宛先ポートとして。

インターフェイスで VLAN トンネリングを適用するには、ルータの TCAM ルールを使用する必要があります。ルータに十分な TCAM 用リソースがない場合、コマンドは失敗します。ユーザーは、[Administration] > [Routing Resources] 経由で、VLAN トンネリング (およびマッピング) 用のルータ TCAM リソース割り当てを追加および削除できます (システムの再起動が必要)。

元の QinQ 実装 (顧客モードに関連するコマンド) もまた、新しい VLAN トンネリング実装で維持されています。顧客ポートモードは、VLAN マッピング トンネル ポート モードにおいては特殊なケースであり、TCAM リソースの割り当てを必要としません。

レイヤ2制御プロトコル（L2CP）のBPDUトンネリング

デフォルトでは、下記MACアドレス宛ての入力L2PDUは、VLANトンネルエッジポートでドロップされます（処理されません）。

- 01:80:C2:00:00:00-01:80:C2:00:00:FF（ただし、処理が行われてドロップされないLACPフレーム（宛先MAC 01:80:C2:00:00:02）は除きます）
- 01:00:0C:00:00:00-01:00:0C:FF:FF:FF

VLANトンネル設定の一部として、ドロップと転送のどちらを実施するか定義して、レイヤ2制御プロトコルPDU（CDP、LLDP、VTP、STP）をカプセル化することができます。これをL2CPトンネリングと呼びます。この機能では、特定のタグなしレイヤ2プロトコルフレームをプロバイダネットワークで転送できるトンネルが作成されます（タグ付きフレームはドロップされます）。この機能は、VLANマッピングインターフェイスで設定します。L2CPトンネリング機能は、プロバイダネットワーク内のそれぞれ異なった側にある2つのカスタマーサイトを接続する際に有用です。この機能により、2つのサイト間で、ISPクラウドを介したサポート対象プロトコルのパケットの転送が可能になります。

そのようなフレームをトンネリングするには、PDUをプロバイダネットワークで転送する際にVLAN ID（第2のタグ）として使用されるVLANを定義する必要があります。リモートカスタマーサイトでPDUが受信されると、外側のVLANが除去され、PDUは、リモートカスタマーネットワークにおいて、そのネットワークからの発信データと同様の処理を施されます。この機能では、インターフェイスごとのL2CPトンネル転送が可能になることに加え、カプセル化に使用するS-VLANを割り当てたり、このトラフィック用の事前定義済みCoSを割り当てたり、インターフェイスによって転送されるL2CP PDUのレートを制限したりすることもできます。

ワンツーワンのVLANマッピング

VLANトンネリングに加えて、デバイスはVLANワンツーワンマッピングをサポートします。VLANワンツーワンマッピングでは、エッジインターフェイス（カスタマーネットワークがプロバイダーエッジスイッチに接続されるインターフェイス）上で、C-VLANがS-VLANにマッピングされ、オリジナルのC-VLANタグが指定されたS-VLANに置き換えられます。タグなしフレームは除去されます。フレームが非エッジのタグ付きインターフェイス上で送信される場合、単一のVLANタグ、つまり、指定されたS-VLANのタグが付けられます。トラフィックがサービスプロバイダーのインフラストラクチャネットワーク経由でルーティングされている間は、サービスVLANタグが保持されます。フレームがエッジインターフェイスに送信されるたびに、出力デバイスのS-VLANタグがC-VLANタグに置き換えられます。ワンツーワンVLANマッピングモードでは、インターフェイスは出力タグ付きインターフェイスとして定義されるマッピングを持つすべてのS-VLANに属します。インターフェイスのPVIDは4095に設定されます。

VLAN マッピング

バックボーンネットワークは、同じVLAN内の2つのレイヤ2ユーザーネットワークを接続できます。2つのユーザーネットワークは、ユーザー間のレイヤ2接続を確保し、レイヤ2プロトコルを均一に展開するために、シームレスに相互運用する必要があります。ただし、パッ

クボーンネットワークとユーザーネットワークの VLAN プランが異なるため、バックボーンネットワークはユーザーネットワークからの VLAN パケットを直接送信できません。この問題を解決するには、VLAN マッピングを構成します。ユーザーネットワークからの VLAN パケットがバックボーンネットワークに入ると、バックボーンネットワークのエッジデバイスはカスタマー VLAN (C-VLAN) ID をサービス VLAN (S-VLAN ID) に変更します。

パケットが送信された後、デバイスは VLAN ID の変更を元に戻します。これにより、2 つのユーザーネットワークがシームレスに通信できます。

VLAN マッピングを設定するには、次の手順を実行します。

手順

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。
 - [Tunnel Mapping] : 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。
- [One to One Translation] : このオプションは、[Mapping Type] の選択時に [one-to-one] 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。
- [Tunnel Mapping] : このオプションは、[Mapping Type] の選択時に [Tunnel Mapping] 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] または [Outer VLAN ID] を選択します。[Outer VLAN ID] を選択した場合は、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

各種のレイヤ2プロトコルは、トポロジを拡張し、ローカルサイトとリモートサイトの両方を組み込むために、サービスプロバイダー ネットワークを通して接続された各サイトの顧客が使用する必要があります。すべての VLAN は、サービスプロバイダー ネットワーク上のローカルサイトとリモートサイトを含む適切なスパンニングツリーを確立する必要があり、STPは正しく機能する必要があります。近くにあるシスコの機器は、ローカルサイトとリモートサイトの両方から Cisco Discovery Protocol (CDP) によって検出される必要があります。VTPに参加している顧客ネットワークのすべてのサイトでは、VLAN トランッキングプロトコル (VTP) を利用して矛盾しない VLAN 設定を提供する必要があります。

プロトコルトンネリングが有効の場合、インバウンド側のサービスプロバイダースイッチは、レイヤ2プロトコルパケットを特別な MAC アドレスを使用してカプセル化し、サービスプロバイダーネットワーク経由で送信します。このパケットはネットワークのコアスイッチでは処理されずに通常のパケットとして転送されます。CDP、STP、VTP のレイヤ2プロトコルデータユニット (PDU) は、サービスプロバイダーネットワークを通過し、サービスプロバイダーネットワークのアウトバウンド側の顧客スイッチに配信されます。

VLAN 変換トンネルエッジポートで受信される L2CPDU の処理を設定するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [VLAN Translation] > [Protocol Handling] の順にクリックします。

各種のレイヤ2プロトコルは、トポロジを拡張し、ローカルサイトとリモートサイトの両方を組み込むために、サービスプロバイダー ネットワークを通して接続された各サイトの顧客が使用する必要があります。すべての VLAN は、サービスプロバイダー ネットワーク上のローカルサイトとリモートサイトを含む適切なスパンニングツリーを確立する必要があり、STP は正しく機能する必要があります。近くにあるシスコの機器は、ローカルサイトとリモートサイトの両方から Cisco Discovery Protocol (CDP) によって検出される必要があります。VTPに参加している顧客ネットワークのすべてのサイトでは、VLAN トランッキングプロトコル (VTP) を利用して矛盾しない VLAN 設定を提供する必要があります。

(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 [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 1 つ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 つまたは複数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 次のフィールドを入力します。

- [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。
 - [None] : 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] : 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 を選択します。
- [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選択します。
 - [User defined] : しきい値を 8～256 Kbps に設定する場合に選択します（デフォルトは 32 Kbps）。
- [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

スイッチ上のポートを互いに分離するために、プライベート VLAN は VLAN のイーサネットブロードキャストドメインをサブドメインに分割します。プリンシパル VLAN と 1 つ以上のサブ VLAN がサブドメインを構成します。プライベート VLAN ドメインにあるすべての VLAN によって、プライマリ VLAN が共有されます。あるサブドメインは、セカンダリ VLAN ID を使用して別のサブドメインと区別できます。

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内の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、タグなしのトラフィックかプライオリティタグ付きのトラフィックを受信して、タグなしのトラフィックを送信することを目的としています。

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。

手順

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

Generic VLAN Registration Protocol (GVRP) は、大規模なネットワーク内で VLAN を制御できるようにする標準ベースのプロトコルです。GVRP は IEEE 802.1Q 仕様に準拠しています。IEEE 802.1Q 仕様は、ネットワーク トランク インターコネクト上でフレームに VLAN 構成デー

タをタグ付けする方法を定義しています。これにより、ネットワークデバイスは VLAN 構成情報を他のデバイスとその場で交換できます。

GVRP は、各ポート上だけでなくグローバルに有効化する必要があります。オンにすると、GVRP によって GARP パケットデータ単位 (GPDU) が送受信されます。定義済みであってもまだ非アクティブな VLAN の情報は伝達されません。伝達するには、VLAN が少なくとも 1 つのポートでアクティブになっている必要があります。デフォルトでは、GVRP はグローバルでも、ポートでも無効になっています。

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。

手順

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。

- [Interface] : 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、タグ付きまたはタグなしの VLAN の論理グループです。VLAN がタグ付けされている場合、その VLAN との間で送受信される各パケットには VLAN ID が含まれます。ネットワークトラフィックには、タグ付きパケットとタグなしパケットの両方を含めることができます。パケットに VLAN タグがない場合、パケットはタグなし VLAN に送信されます。

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。この場合、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できます。また、それぞれが独自の MAC アドレスのセットを持つ複数の MAC ベースの VLAN グループを定義することもできます。特定のポートや LAG をこれらの MAC ベースグループ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 MAC アドレス範囲を含めることはできません。

デバイスの MAC アドレスに基づいてパケットを転送するには、MAC アドレスのグループを作成し、VLAN にマッピングする必要があります。最大 256 個の MAC アドレス（ホストまたは範囲）を構成し、1 つまたは複数の MAC ベースの VLAN グループにマッピングできます。

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。

手順

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。

手順

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。

手順

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 ([インターフェイスの設定 \(179 ページ\)](#) 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。

手順

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。

手順

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 次のフィールドに入力します。

- [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。

手順

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、IP フォンからの IP 音声トラフィックをアクセスポートで伝送できます。IP フォンがスイッチに接続されると、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) 値として 5 (どちらの値もデフォルトの設定値) を使用して、音声トラフィックを送信します。データ伝送が均質性に欠ける場合、IP フォンの音質が劣化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。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するため、QoS は分類およびスケジューリングを使用します。

音声 VLAN は、LLDP-MED ネットワークルールを使用して CoS/802.1p 設定や DSCP 設定を伝達できます。アプライアンスが LLDP-MED パケットを送信する場合、LLDP-MED はデフォルトでは音声 QoS オプションを使用して応答するように設定されます。MED をサポートするデバイスが送信する音声トラフィックは、LLDP-MED 応答で受け取ったものと同じ CoS/802.1p パラメータおよび DSCP パラメータを使用する必要があります。ユーザーは、独自のネットワーク設定を使用したり、音声 VLAN と LLDP-MED の間の自動更新を無効にしたりできます。OUI モードで使用する場合、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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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。

手順

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。

(注)

Auto Smartport とテレフォニー OUI を同時に使用することはできません。CoS/802.1p および DSCP の値は、LLDP MED ネットワークポリシーと自動音声 VLAN に対してのみ使用されます。

ステップ 2 次の [Administrative Status] フィールドに値を入力します。

- [Voice 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 [Auto Voice VLAN Activation] 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] : LLDAP-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 LLDAP-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。

- [Dynamic Voice 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。
 - [Enable Auto Voice VLAN] : 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。
 - [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
 - [Auto Voice VLAN Activation] : 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。
 - [Immediate] : 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。
 - [By external Voice VLAN trigger] : 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の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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

自動音声 VLAN は音声 VLAN の維持を行います。音声 VLAN ポート メンバーシップを維持するには Auto Smartport に依存します。自動音声 VLAN は、動作時に次の機能を実行します。

アクティブにすると、自動音声 VLAN は次のタスクを実行します。

- 直接接続されたネイバーデバイスからの CDP アドバタイズメントで、音声 VLAN の情報を検索します。

- 複数のネイバースイッチやルータ（Cisco Unified Communications（UC）デバイスなど）がそれぞれの音声 VLAN をアドバタイズしている場合、MAC アドレスが最も小さいデバイスからの音声 VLAN が使用されます。

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) [Source Type] が [Inactive] 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。

手順

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 [Operational Status] 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。
- [Voice 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。
- [Root Switch MAC Address] : 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。
- [Voice VLAN ID Change Time] : 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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

Voice over Internet Protocol (VoIP) 機器からのトラフィックが、IP 電話、VoIP エンドポイント、音声システムなどの音声デバイスで構成される特定の VLAN に割り当てられている場合、

音声仮想ローカルエリアネットワーク（VLAN）が使用されます。スイッチでは、ポートメンバーを検出して音声 VLAN に自動的に追加し、設定された Quality of Service（QoS）を音声 VLAN からのパケットに割り当てます。音声デバイスが別々の音声 VLAN 内にある場合、音声デバイス間で通信を行うには IP ルータが必要です。

組織固有識別子（OUI）を使用して、特定の製造者の Media Access Control（MAC）アドレスを OUI テーブルに追加できます。MAC アドレスの最初の 3 バイトには製造者 ID が含まれ、最後の 3 バイトには一意のステーション ID が含まれています。OUI がテーブルに追加されると、IP 電話が OUI テーブルにリストされている場合、音声 VLAN ポートのポートで特定の IP 電話から受信した音声は音声 VLAN に転送されます。

受信したパケットの送信元 MAC アドレスは、スイッチによってチェックされ、音声パケットであるかどうか判断されます。VoIP トラフィックの送信元 MAC アドレスには、事前構成済みの OUI プレフィックスが含まれています。特定の製造者の MAC アドレスと説明を OUI テーブルに手動で入力できます。OUI がリストされている特定の IP 電話から音声 VLAN ポートで受信したすべてのトラフィックは、音声 VLAN にルーティングされます。

テレフォニー OUI を設定したり、新しい音声 VLAN OUI を追加したりするには、次の手順を実行します。

手順

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。

- [Telephony OUI Operational Status] : 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。
- [Remark CoS/802.1p] : 出トラフィックをリマークするかどうかを選択します。
- [Auto Membership Aging Time] : 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。

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。次のメッセージを含むポップアップが表示されます。「ユーザー定義の OUI がすべて消去されます。続行しますか? (All User-defined OUIs will be erased. Do you want to continue?)」[OK] をクリックします。

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。

- [Telephony OUI] : 新しい OUI を入力します。
- [Description] : 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。

テレフォニー OUI インターフェイス



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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せん。

- [All] : 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。

手順

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。

- [Interface] : ポートまたは LAG インターフェイスを選択します。
- [Telephony OUI VLAN Membership] : 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。
- [音声 VLAN QoS モード (Voice VLAN QoS Mode)] (メイン ページの [テレフォニー OUI QoS モード (Telephony 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。
- [Telephony Source MAC Address] : 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。

自動監視 VLAN

多くの場合、カメラや監視機器などの監視デバイス間のネットワーク通信には、より高い優先順位を与える必要があり、組織内の監視インフラストラクチャを構成するさまざまなデバイスが相互に到達可能であることが重要です。通常、ネットワーク管理者は、すべての監視デバイスが同じ VLAN に接続されていることを確認し、この優先度の高いトラフィックを許可するようにこの VLAN とそのインターフェイスを設定する必要があります。

自動監視 VLAN (ASV) 機能は、ネットワーク上の監視デバイスを検出して VLAN に割り当て、それらのトラフィックの優先順位を設定することにより、このセットアップを自動化します。

ASV の一般設定



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

ユーザーは、OUI と MAC アドレスのリストを作成して、ネットワーク上の監視トラフィックを定義します。この機能が有効になっているインターフェイス上で、OUI または MAC アドレスのいずれかに送信元が一致するトラフィックは、監視トラフィックと見なされます。MAC と OUI の任意の組み合わせで、監視トラフィックに最大 32 の送信元を定義できます。

ASV の構成

この機能をアクティブにする場合、ユーザーは既存の静的 VLAN を選択して ASV VLAN として指定する必要があります。次に、ユーザーは、この VLAN のトラフィックの CoS と、VLAN メンバーシップのエージングタイムを設定します。最後に、監視トラフィックを受信すると予想されるインターフェイスで ASV 機能をアクティブにする必要があります。

ASV の一般的な設定を行うには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Auto-Surveillance VLA] > [ASV General Settings] をクリックします。

ステップ 2 ドロップダウンメニューから、自動監視 VLAN の ID を選択します。この設定は、ASV VLAN ID を選択するために使用されます。[None] を選択すると、機能は無効になります。

- ステップ3** CoSを入力します。この設定は、ASVの監視トラフィックに適用されるサービスクラス（CoS）を選択するために使用されます。指定できる値の範囲は0～7です。デフォルトは5です。
- ステップ4** [Membership Aging Time] には、日、時間、分を入力します（範囲：1分～30日、デフォルトは1日）。この設定は、ASVメンバーシップのエージングタイムを構成するために使用されます。このエージングタイム内にインターフェイスで監視トラフィックが受信されない場合、そのインターフェイスはASVから削除されます。
- ステップ5** [Add] をクリックして監視トラフィック送信元を追加し、以下を構成します。
- [Source Type] : 次のいずれかを選択します。
 - OUI Prefix
 - MAC Address
 - [Source] : 送信元を入力します。このフィールドの検証とヒントは、選択した送信元タイプに基づいて変わります。タイプが [OUI Prefix] の場合、値はユニキャスト MAC アドレスの3オクテットのプレフィックスである必要があります。

タイプが [MAC Address] の場合、値はユニキャスト MAC アドレスである必要があり、ヒントは表示されません。
 - [説明 (Description)] : 送信元の説明を入力します。
- ステップ6** [Apply] をクリックして設定を保存します。

ASV インターフェイス設定



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

ユーザーは、選択したインターフェイスで自動監視機能をアクティブにします。この機能は、一般またはアクセス VLAN モードのポートまたは LAG でアクティブにできます。

ASVが有効になっているインターフェイスで監視トラフィックが検出されると、このトラフィックはASVにルーティングされます。一般 VLAN モードのインターフェイスでは、各監視トラフィックは、ACLおよびQoSルールと共有されるリソーステーブルのエントリを消費します。このテーブルの消費されたエントリの数を表示するには、[Hardware Resource Utilization] ページに移動します。

ASV インターフェイス設定を行うには、次の手順を実行します。

手順

- ステップ1** [VLAN Management] > [Auto-Surveillance VLAN] > [ASV Interface Settings] をクリックします。
- ステップ2** インターフェイスタイプとしてポートまたはLAGを選択し、[Go] をクリックします。

ステップ3 ASV インターフェイス設定を編集するには、[Edit] をクリックします。

ステップ4 次にインターフェイス（ポートまたはLAG）を選択します。

ステップ5 [Enable] をオンにして、自動監視 VLAN メンバーシップを有効にします。

ステップ6 [Apply] をクリックして設定を保存します。

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）ではないサブスクリバに対して、サブスクリバ 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リバは、同じマルチキャストVLANID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VLANIDのメンバーとして静的に設定されます。

サブスクリバが（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（「[インターフェイスの設定（179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、サブスクリ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（[インターフェイスの設定（179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 \(177ページ\)](#)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。

手順

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が割り当てられている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]：グループ範囲のマルチキャストアドレスの数を指定します。
 - [By range]：[Multicast Group Start]フィールドのアドレスよりも大きい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では、同じデータVLAN上に存在しない（レイヤ2隔離）のサブスクライバへのマルチキャスト伝送が可能で、その際、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する必要はありません。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。

手順

-
- 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** [Multicast 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リイバに対してプロビジョニングされ、サブスクリイバはレイヤ 2 での分離が維持されます。

各サブスクリイバには、CPE MUX ボックスがあります。MUX には、サブスクリイバのデバイス（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リ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。

サブスクリイバからサービス 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。

サブスクリ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リイバの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リバ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。

- サブスクリバイバの 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、サブスクリバ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

CPE VLAN のマルチキャスト TV VLAN へのマッピング

サブスクリバイバの VLAN で CPE MUX をサポートするには、サブスクリバイバに、複数のビデオ プロバイダー（各々が異なる外部 VLAN に割り当てられたもの）が必要となることがあります。CPE マルチキャスト VLAN（内部）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。

手順

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（「[インターフェイスの設定（179 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、以下の手順を実行します。

手順

-
- 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** [Multicast 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

スパンニングツリー

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 \(211 ページ\)](#)
- [STP インターフェイス設定 \(213 ページ\)](#)
- [RSTP インターフェイス設定 \(215 ページ\)](#)
- [MSTP \(218 ページ\)](#)
- [PVST \(224 ページ\)](#)

STP 状態およびグローバル設定

スパン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。

手順

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

スパンニングツリー状態	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、スパン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ン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ン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

優先順位	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 (213 ページ) を参照してください。

指定ルート

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。

ルートポート	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。
ルートパスコスト	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。

手順

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。

インターフェイス	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。
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、スパン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 (211 ページ) で定義した設定を使用する場合に選択します。 • [Filtering] : インターフェイスでスパン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。 • [Flooding] : インターフェイスでスパン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。
パスコスト	[デフォルトを使用 (Use Default)] または [ユーザー定義 (User Defined)] を選択し、1 ~ 200000000 の範囲を入力して、ルートパスコストへのポートの寄与を設定します。
優先順位	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。

ポート状態	このポートの現在の STP 状態が表示されます。 • [Disabled] : このポートに対して STP は現在無効になっています。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。 • [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。
代表ブリッジ 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。
速度	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。

手順

ステップ 1 [Spanning Tree]> [RSTP Interface Settings] をクリックします。

ステップ 2 エントリ番号を選択し、[Activate Protocol Migration] をクリックします。

(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のみ使用可能となります。プロトコル移行のアクティブ化により、まだ STP を使用しているリンクパートナーが存在しているかどうか、また、存在する場合は RSTP または MSTP のどちらに移行したかが判明します。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 3 既存のインターフェイスの設定を編集する場合は、インターフェイスを選択して [編集 (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。

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。
Point to Point Administrative Status	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。
Point to Point Operational Status	[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。

Role	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。
Mode	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。
Fast Link Operational Status	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 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。

MSTP



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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ン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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

グローバル MSTP は、VLAN グループごとに個別のスパンニング ツリーを設定し、各スパンニング 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 \(219 ページ\)](#) 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。

手順

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。

- [Region Name] : MSTP リージョン名を定義します。これはデフォルトではスイッチのベース MAC アドレスです。
- [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。
- [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 Master] : アクティブリージョンを表示します。

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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

[MSTP Instance Settings] 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。



(注) VLAN から MSTP インスタンスへの設定が行われていない限り、この画面のすべてのオプションは空白になります。

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。

手順

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。

- [MSTP 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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

[MSTP Interface Settings] 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。

手順

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。

- [Instance equals to] : 設定する MSTP インスタンスを選択します。
- [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
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。
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。 • [Discarding] : 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。 • [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。 • [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。 • [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。 • [Boundary] : 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 (213 ページ) で確認できます。
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。 • [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。 • [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。

オプション	説明
	• [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。 • [Backup] : インターフェイスは、スパン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。 • [Disable] : インターフェイスは、スパンニングツリーに参加しません。 • [Boundary] : 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 (213 ページ) で確認できます。
Mode	現在のインターフェイス スパンニング 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。
Type	ポートの MST タイプが表示されます。 • [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。 • [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。
Designated Port 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。
Remain Hops	次の宛先までの残りのホップ数が表示されます。
Forward Transitions	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



(注) この設定は、[Advanced Mode] でのみ使用できます。

[VLAN to MSTP Instance] ページでは、各 VLAN をマルチ スパンニング 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。

手順

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、[Add] をクリックします。MSTP インスタンスの VLAN を編集するには、[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。

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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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 向けに個別のスパンニング 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。最大 126 の PVST インスタンスがサポートされます。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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

PVST VLAN 設定を定義するには、次の手順を実行します。

手順

ステップ 1 [Spanning Tree] > [PVST] > [PVST VLAN Settings] の順にクリックします。

[PVST VLAN Settings] 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 (Copy Settings)] 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 (Edit)] 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。

- [Priority] : PVST VLAN STP のプライオリティ値。
- [Address] : VLAN のアドレスこのオプションはメニューテーブルには表示されますが、[Edit] メニューには表示されません。これは、スイッチのベース MAC アドレスを使用して自動的に生成されます。
- [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）。
- [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。
- [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。

ステップ3 [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。

ステップ4 [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。
- [ルートプライオリティ（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。
- [ルートパスコスト（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。
- [ルートブリッジID（Root Bridge ID）] : この VLAN のルートブリッジ ID。
- [ブリッジID（Bridge ID）] : このデバイスと VLAN のブリッジ ID。
- [トポロジ変更回数（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。
- [最後のトポロジ変更（Last Topology Change）] : トポロジが最後に変更された日時の詳細。

PVSTインターフェイスの設定



(注) この設定は、[詳細モード（Advanced Mode）] ビューでのみ表示されます。

[PVST Interface Settings] 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。

手順

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
インターフェイス	インターフェイス名。
優先順位	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。 • [Listening] : 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。 • [Learning] : 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。 • [Forwarding] : 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。 • [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。 • [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。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
	• [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。 • [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。
代表ブリッジ 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。
代表コスト	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ーワ ルディングステートに変更された回数が表示されます。

PVST不整合ポート



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

[PVST Inconsistent Ports] 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。

手順

[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。
 - [Inconsistency] : 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 \(229 ページ\)](#)
- [ダイナミックアドレス設定 \(230 ページ\)](#)
- [ダイナミック アドレス \(230 ページ\)](#)
- [予約済みMACアドレス \(231 ページ\)](#)

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。

手順

ステップ 1 [MAC Address Tables] > [Static Addresses] の順にクリックします。

[Static Addresses] 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 Address] : 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。
- [Status] : 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。
 - [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。

- [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。
- [Delete on timeout] : 期限が切れると、アドレスは削除されます。
- [Secure] : 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。

手順

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。

手順

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 Address] : テーブルに対して照会する MAC アドレスを入力します。
- [Interface] : 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 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。

手順

ステップ 1 [MAC Address Tables] > [Reserved MAC Addresses] の順にクリックします。

ステップ 2 [Add] または [Edit] をクリックして値を変更します。

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。
- [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。
 - [All] : 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。
- [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。
 - [Discard] : 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。

予約済みMACアドレス



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](#) (233 ページ)
- [MACグループアドレス](#) (235 ページ)
- [IPマルチキャストグループアドレス](#) (237 ページ)
- [IPv4マルチキャストコンフィギュレーション](#) (238 ページ)
- [IPv6マルチキャストコンフィギュレーション](#) (244 ページ)
- [IGMP/MLDスヌーピングIPマルチキャストグループ](#) (250 ページ)
- [マルチキャスト ルータ ポート](#) (251 ページ)
- [不在転送](#) (252 ページ)
- [登録解除済みマルチキャスト](#) (253 ページ)

マルチキャストのプロパティ



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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ドされます。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。

手順

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。

Bridge Multicast Filtering Status	フィルタリングを有効にする場合に [Enable] を選択します。
VLAN ID	転送方式を設定する VLAN ID を選択します。

Forwarding Method for IPv6	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。
Forwarding Method for IPv4	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



(注) この設定は、[Advanced Mode] ビューでのみ表示されます。

[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。

手順

-
- 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 equals to] : 表示するグループの VLAN ID を設定します。
 - [MAC Group Address equals to] : 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 アドレスが含まれます。
- 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 Group Address] : 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 Group Address] : 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。
- [Static] : 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] : 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



(注) この設定は、[Advanced Mode] ビューでのみ表示されます。

[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。

手順

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 equals to] : 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 Version equals to] : IPv6 または IPv4 を選択します。
- [IP Multicast Group Address equals to] : 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。
- [Source IP Address equals to] : 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 Version] : IP アドレスのバージョンを選択します。
- [IP Multicast Group Address] : 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。
- [Source Specific] : 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。

- [Interface Type equals to] : 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。

- [Static] : 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。
- [Forbidden] : 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 \(233 ページ\)](#)) 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。

手順

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 \(233 ページ\)](#) 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。

オプション	説明
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。 • [Auto] : 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。

オプション	説明
	• [User Defined] : 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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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）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。

手順

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。

- [Interface Name] : IGMP スヌーピングが定義されるインターフェイス。
- [Router IGMP Version] : 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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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。

手順

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。

- [Interface Name] : IGMP スヌーピングが定義される VLAN。
- [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。

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) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

Internet Group Management Protocol (IGMP) は、IP ネットワーク上のホストおよびルータがマルチキャスト グループ メンバーシップを作成するために使用します。IGMP は Web のリソースに使用でき、ビデオやゲームのオンラインストリーミングなどのアプリケーションをサポートします。IGMP プロキシにより、デバイスは背後のクライアントに代わって IGMP メッセージを発行できます。

IGMP プロキシを有効にするには、次の手順を実行します。

手順

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 Multicast Routing	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。
Downstream Protection	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。
送信元固有マルチキャスト	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 Access List	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。 • [Default list] : 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。 • [Use global] : 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。 • [Disable] : 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。 • [Enable] : 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。
Outgoing Interfaces	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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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



(注) この設定は、[Advanced Mode] ビューでのみ表示されます。

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 \(233 ページ\)](#)) 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。

手順

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 \(233 ページ\)](#) 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
VLAN ID	ドロップダウンリストから VLAN ID を選択します。
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。

オプション	説明
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 MLD クエリを中継した後、マルチキャストクライアントから MLD 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。この機能を有効にすると、デバイスポートに送信される不要な MLD トラフィックをブロックするのにかかる時間が短縮されます。
最終メンバクエリ 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。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。
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 クエリア選出メカニズムが無効になっている場合、MLD スヌーピングクエリアは、有効化された後に一般クエリ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。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



- (注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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）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。

手順

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。

手順

ステップ1 [Multicast] > [IPv6 Multicast Configuration] > [MLD VLAN Settings] の順にクリックします。

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。
- [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)] : 定期的な一般的な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。

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) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。



(注) MLD プロキシは、[IPv6グローバルコンフィギュレーション \(291 ページ\)](#) 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。

手順

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、デバイスに必要なないダウンストリームのパケットを破棄します。
- [ソース固有マルチキャスト (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 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 \(306 ページ\)](#) 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。
- [Downstream Protection] : 次のいずれかのオプションを選択できます。
 - [Use global] : 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。
 - [Disable] : 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。
 - [Enable] : 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。
- [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。
- [Outgoing interface] : パケット転送時に使用されるインターフェイス。

- [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。
- [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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

[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たします。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。

手順

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。
- [Group Address] : 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。
- [Source Address] : 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。
- [Included Ports] : マルチキャスト ストリームの宛先ポートのリスト。

- [Excluded Ports] : 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。

手順

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 equals to] : ルータ ポートの VLAN ID を選択します。
- [IP Version equals to] : 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。
- [Interface Type equals to] : 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。

- [Static] : 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。
- [Dynamic] : (表示のみ) このポートは、IGMP/MLD クエリ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 \(250 ページ\)](#) を使用します。
- [Forbidden] : このポートで IGMP/MLD クエリ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 にフラッドされます。

[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 \(233 ページ\)](#) 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ドされます。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。

手順

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 equals to] : 表示するポート /LAG がメンバになっている VLAN の ID。
- [Interface Type equals to] : 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。

- [Static] : 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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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。

手順

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] を選択して、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。

- [Port/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。
 - [Forwarding] : 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。
 - [Filtering] : 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 \(255 ページ\)](#)
- [IPv4 スタティックルート \(257 ページ\)](#)
- [IPv4 転送テーブル \(258 ページ\)](#)
- [RIPv2 \(259 ページ\)](#)
- [アクセス リスト \(264 ページ\)](#)
- [ARP \(266 ページ\)](#)
- [ARP プロキシ \(267 ページ\)](#)
- [UDP リレー/IP ヘルパー \(268 ページ\)](#)
- [DHCP リレー \(269 ページ\)](#)
- [DHCP サーバ \(277 ページ\)](#)
- [OSPFv2 \(285 ページ\)](#)

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に対して設定できます。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 VLANID (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。

手順

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。

- [IPv4 Routing] : IPv4 ルーティングを有効にするには、[Enable] チェック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。
- [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。
 - [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] : 設定された IP アドレス マスク。
- [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。
 - [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。
 - [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。
 - [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 設定に関連付けられたインターフェイスとしてポート、LAG、VLAN、ループバックを選択し、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。

- [Dynamic IP Address] : IP アドレスを DHCP サーバーから受け取ります。
- [Static IP Address] : 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。
- *[DHCPによる自動設定 (Auto Configuration via DHCP)] : ステータス ([無効 (Disabled)] または [有効 (Enabled)]) が表示されます。

(注)

* これらは [Edit] ポップアップオプションにのみ表示されます。

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異なる IP アドレスを受信する可能性があります。

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。

手順

ステップ 1 [IPv4 Configuration] > [IPv4 Static Routes] をクリックします。

ステップ 2 [Add] をクリックして新しい IPv4 スタティックルートを追加するか、[Edit] をクリックして既存のルートを編集します。

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。

- [Metric] : 次のいずれかを選択します。
 - [Use Default] : デフォルトのメトリックを使用する場合に選択します。
 - [User Defined] : 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 スタティックルートテーブルが表示されます。上記のリストにない次のフィールドが表示されます。

- [Outgoing Interface] : このルートの送信インターフェイス。

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。

手順

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。

- [Destination IP Prefix] : 宛先 IP アドレスのプレフィックス。
- [Prefix Length] : 宛先 IP の IP ルート プレフィックス。
- [Route Type] : ルートがローカル、拒否、またはリモート ルートかどうか。
- [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。
 - [Default] : 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。
 - [Static] : 手動で作成されたルート。
 - [Dynamic] : 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。
 - [Directly Connected] : 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。
- [Metric] : このホップのコスト（より低い値が優先）。
- [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。
- [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。

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 モードで稼働します。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。

手順

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。
 - [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 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。
- [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、デフォルトルートとして機能します。
- [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。
- [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。
- [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。

- [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。

手順

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 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。
- [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。
- [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）。
- [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（260 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。
 - [Disable] : この RIP インターフェイス上でデフォルトルートを実アドバタイズしません。
 - [Enable] : この RIP インターフェイス上でデフォルトルートを実アドバタイズします。
- [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。
- [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。
 - [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。

- [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。
- [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 RIPv2 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 RIPv2 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 RIPv2 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 RIPv2 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 RIPv2 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。

手順

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 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。
- [Bad Packets Received] : IP インターフェイスで RIPv2 によって識別された不良パケットの数を指定します。
- [Bad Routes Received] : IP インターフェイスで RIPv2 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。
- [Update Sent] : IP インターフェイスで RIPv2 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。

手順

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。

- [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。
- [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。
- [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。
- [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。

手順

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。
 - [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 (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アドレスリスト

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。

手順

ステップ 1 [IPv4 Configuration] > [Access List] > [Source IPv4 Address List] の順にクリックします。

ステップ 2 アクセスリストにパラメータを追加するには、[Add] をクリックして、次のフィールドに入力します。

- [Access List Name] : 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。
 - [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 アドレスのマスクのタイプと値。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 (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。

手順

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 Entry Age Out] : 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。
- [Clear ARP Table Entries] : 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。
- [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 Address] : IP デバイスの IP アドレス。
- [MAC Address] : IP デバイスの MAC アドレス。
- [Status] : 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 Version] : 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、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 Address] : ローカル デバイスの IP アドレスを入力します。
- [MAC Address] : 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、パブリッシングとすることがあります。

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。

手順

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。

手順

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ドされます。

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 リレー

ここでは、Dynamic Host Configuration Protocol (DHCP) 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。

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。

手順

ステップ 1 [IPv4設定 (IPv4 Configuration)] > [DHCPスヌーピング/リレー (DHCP Snooping/Relay)] > [プロパティ (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 Snooping Status] : DHCP スヌーピングを有効にする場合に選択します。
- [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。
- [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。
- [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。[Add DHCP Server] 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 DHCP 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。

手順

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。

- [Option 82 Insertion] : [Enable] 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 [Circuit-ID Template] に入力します。デフォルトの回線 ID を使用する場合は [Use Default] を選択します。回線 ID を設定する場合は [User Defined] 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、[Preview] ボタンを使用します。

ステップ 3 [Remote-ID Template] 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)

[Total Sub-Option Payload] 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す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
\$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	
\$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\$	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。	64	該当なし	
\$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
\$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

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-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
\$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す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。

手順

- ステップ 1 [IPv4 設定 (IPv4 Configuration)] > [DHCP スヌーピング/リレー (DHCP Snooping/Relay)] > [インターフェイス設定 (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、[Add] 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 Relay)]、[DHCP スヌーピング (DHCP Snooping)]、または両方) を選択します。
- 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 \(276 ページ\)](#) 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。

手順

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спек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。

手順

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
 - [Active] : 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。
- Reason
 - No Problem

- No Resource
- No Snoop VLAN
- 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。
- [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。
 - [Dynamic] : エントリのリース時間は制限されています。
 - [Static] : エントリは静的に設定されています。
- [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。

手順

-
- 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。

- **[Remote Client]** : 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。

手順

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。
- [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。
 - [Network Mask] : プールのネットワーク マスクを確認し、入力します。
 - [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。
- [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。
- [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。
- [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。
 - [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。
 - [時間] : リースの時間数。時間数の値を追加するには、その前に日数値を指定する必要があります。
 - [分] : リースの分数。分数の値を追加するには、その前に日数値と時間数値を指定する必要があります。
- [Default Router IP Address (Option 3)] : 次から選択します。
 - Auto
 - Disable
 - [User Defined] : デフォルトルータの IP アドレスを入力します

- [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。
- [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 ネームサーバーを入力します。
- [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。
 - [Hybrid] : b ノードと p ノードのハイブリッドな組み合わせが使用されます。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。
 - [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。
 - [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。
 - [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。
- [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。
- [File Server Host Name (sname/Option 66)] : TFTP/SCP サーバの名前を入力します。
- [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かと仮定します。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。

手順

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。

- [Start IP Address] : 除外 IP アドレスの範囲の最初の 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するには、次の手順を実行します。

手順

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 Address/Client Identifier

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 Address	ホストに静的に割り当てられる IP アドレスを入力します。
Host Name	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。 • [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。 • [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。

Identifier Type	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。 • [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。
Default Router IP Address (Option 3)	次のオプション ([Auto]、[Disable]、[User Defined]) から、静的ホストのデフォルトルータを選択します。
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。
Domain Name (Option 15)	スタティックホストのドメイン名を入力します。
NetBIOS WINS Server IP Address (Option 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 Node Type (Option 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。 • [Hybrid] : b ノードと p ノードのハイブリッドな組み合わせが使用されます。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。 • [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。 • [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。 • [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。

File Server IP Address (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。
File Server Host Name (sname/Option 66)	TFTP/SCP サーバーの名前を入力します。
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 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 静的ホストの詳細を表示するには、[Static Host] テーブルから IP アドレスを選択し、[Details] タブをクリックします。

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。

手順

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 \(278 ページ\)](#) 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。

- [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。
- [Code] : DHCP オプション コードを入力します。
- [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。

- [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。
- [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。
- [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。
- [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。
- [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。

手順

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 Address/Client Identifier] : 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。
- [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。
- [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。

- [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。
 - [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。
 - [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 アドレスバインドを削除するには、[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。

OSPFv2

Open Shortest Path First (OSPF) は内部ゲートウェイ ルーティング プロトコルです。Open Shortest Path First (OSPF) 内部ゲートウェイ プロトコルを使用すると、ルータはリンクステートメッセージを交換し、ネットワーク情報を収集してノードの距離に基づいて最適なルーティングパスを決定します。相互接続されたルータが多数存在するネットワークでは、OSPF は RIP よりも効率的です。これは、OSPF は使用するリンク帯域幅が少なく、コンバージェンスが速いためです。



- (注) OSPFv2 は、デバイスで IP ルーティングが有効になっている場合にのみアクティブになります。[IPV4設定 (IPV4 Configuration)] で、IPv4 インターフェイスの IPv4 ルーティングが有効になっていることを確認してください。

Catalyst 1300X シリーズ スイッチの OSPF 機能の詳細については、『Catalyst 1300X [CLI Guide](#)』を参照してください。

OSPFv2 設定フロー

1. OSPF プロセスを作成し、ルータ ID を割り当てます。複数のプロセスを作成できます。以下の構成は、各プロセスに適用できます。
2. プロセスに 1 つ以上のエリアを追加します。各エリアで以下を行います。

1. デバイスのインターフェイスに設定されている IP アドレスからエリアネットワークにアクセスします。
2. エリアのタイプと設定を定義します。
3. ネットワークの設定を行います。

OSPFv2 プロセス

OSPFv2 は、個別のルーティングプロセスとして設定されているのではなく、インターフェイス上で有効になっています。つまり、OSPFv2 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のルーティングプロセスおよび関連する設定が自動的に作成されます。

手順

ステップ 1 [IPv4 の設定 (IPv4 Configuration)] > [OSPFv2] > [OSPFv2 プロセス (OSPFv2 Process)] の順にクリックして、OSPFv2 プロセステーブルを表示します。

ステップ 2 テーブルに表示されるフィールドは次のとおりです。

- [プロセス ID (Process ID)] : プロセス識別子。
- [ルータ ID (Router ID)] : プロセスに割り当てられたルータ ID。
- [管理ステータス (Administrative Status)] : プロセスの管理ステータス。
- [動作ステータス (Operational Status)] : プロセスの動作ステータス。

ステップ 3 新しい OSPFv2 プロセスを追加する場合はクリックします。

ステップ 4 OSPFv2 プロセスに対して以下を定義します。

- [プロセス ID (Process ID)] : OSPFv2 プロセスの ID を表す整数。

警告

実行中の OSPFv2 プロセスのルータ ID を変更すると、プロセスが自動的に再起動されます。

- [ルータ ID (Router ID)] : デフォルトのルータ ID (デバイスに設定されている最小 IPv4 アドレス) を使用するか、ルータ ID を手動で設定する (IPv4 形式) かを選択します。
- [シャットダウン (Shutdown)] : シャットダウン状態でプロセスを作成するには、シャットダウンを有効にするチェックボックスをオンにします。

(注)

これにより、ユーザーはトラフィックをアクティブ化せずにプロセス設定を構成できます。

ステップ 5 [適用 (Apply)] をクリックしてプロセスを作成します。

ステップ 6 [プロセスの再起動 (Restart Process)] をクリックして、OSPF v2 プロセスを再起動します。

ステップ 7 画面の上部にある [OSPFv2 エリアテーブル (OSPFv2 Area Table)] ボタンをクリックすると、[OSPFv2 エリア (OSPFv2 Area)] 画面にリダイレクトされます。

OSPFv2 エリア

OSPFv2 エリアテーブルは、IPv4 ネットワークの異なるエリア内のルーティング情報を整理および管理するために、OSPFv2 で使用されるデータ構造です。OSPFv2 は IPv4 向けに設計されたリンク ステート ルーティング プロトコルで、エリアを使用してルーティングを効率的に最適化および管理します。

OSPFv2 エリア テーブルを設定するには以下の手順を実行します。

手順

- ステップ 1** [IPv4 設定 (IPv4 Configuration)] > [OSPFv2] > [OSPFv2 エリアテーブル (OSPFv2 Area Table)] をクリックします。
- ステップ 2** このテーブルの情報は、各 OSPFv2 プロセス ID (フィルタボタン) ごとに表示されます。必要な OSPFv2 プロセスを選択し、[移動 (Go)] をクリックします。
- ステップ 3** テーブルに表示されるフィールドは次のとおりです。
- [エリア ID (Area ID)] : IPv4 フォーマットのエリア ID
 - [エリアタイプ (Area type)] : [バックボーン (Backbone)]、[通常 (Normal)]、[スタブ (Stub)]、[NSSA]
 - [ステータス (Status)] : エリアの管理ステータス (アップまたはダウン)
- ステップ 4** エントリを選択して [詳細 (Details)] をクリックすると、完全なエリア設定が表示されます。
- ステップ 5** 画面の上部にある [OSPFv2 プロセステーブル (OSPFv2 Process Table)] ボタンをクリックして [OSPFv2 プロセス (OSPFv2 Process)] 画面にリダイレクトするか、[OSPFv2 ネットワークテーブル (OSPFv2 Network Table)] ボタンを押して [OSPFv2 IPv4 ネットワーク (OSPFv2 IPv4 Network)] 画面にリダイレクトします。
- ステップ 6** [追加 (Add)] をクリックして、1 つ以上のエリアを作成します。次のフィールドを設定します。
- [プロセス ID (Process ID)] : ドロップダウンボックスから OSPFv2 プロセス ID を選択してください。このエリアは、選択されたプロセス ID と関連付けられます。
 - [エリア ID (Area ID)] : エリア ID を IPv4 形式で構成します。
 - [シャットダウン (Shutdown)] : エリアをシャットダウン状態で作成するには、有効にします。これにより、エリアを非アクティブ状態に保ちながらエリア設定を構成できます。
 - [エリアネットワーク (Area Networks)] : エリアに追加する 1 つ以上の IPv4 ネットワークを選択します。
 - [スタブ/NSSA エリア (Stub/NSSA Area)] : このエリアをスタブエリアまたは NSSA (Not So Stubby Area) として設定する場合に選択します。このオプションは、エリアがバックボーンエリアでない (エ

リア ID が 0.0.0.0 ではない) 場合にのみ使用できます。このオプションを選択した場合は、以下のフィールドの設定を続けます。

- [スタブ/NSSA (Stub/NSSA)] : このエリアがスタブエリアまたは NSSA のいずれであるかを選択します。
- [デフォルト サマリー ルート コスト (Default Summary Route Cost)] : スタブエリアまたは NSSA (Not-So-Stubby Area) に送信されるデフォルトサマリールートのコストを指定します。次のいずれかの利用可能なオプションを選択します。
 1. デフォルト : 1 の値
 2. ユーザー定義 : 範囲 : 1 ~ 16777214
- [ABRサマリーアドバタイズメント (ABR Summary Advertisement)] : エリア境界ルータ (ABR) がサマリーリンクアドバタイズメントをスタブエリアに送信できるようにします。
- トランスレータロールとトランスレータ安定性間隔は、エリアが NSSA として定義されている場合にのみ設定できます。
 - [トランスレータロール (Translator Role)] : NSSA 境界ルータがタイプ 7 LSA をタイプ 5 LSA に無条件に変換するかどうかを指定します。
 1. [常に (Always)] を選択すると、他の NSSA 境界ルータのトランスレータ状態に関係なく、常に NSSA 境界ルータがタイプ 7 LSA をタイプ 5 LSA に変換します。
 2. [候補 (Candidate)] を選択すると、NSSA 境界ルータが RFC 3101 のセクション 3.1 で説明されているトランスレータ選択プロセスに参加するように指定します。
 - [トランスレータ安定性間隔 (Translator Stability Interval)] : 選出されたトランスレーターが、もはや自身のサービスが不要であると判断した後も、翻訳業務を継続すべき秒数を指定します。デフォルト値は 40 秒です。
- [適用 (Apply)] をクリックしてエリアを作成します。

OSPFv2 IPv4 ネットワーク

OSPFv2 IPv4 エリアネットワークを表示、編集、または設定するには、以下の手順を実行します。

手順

ステップ 1 [IPv4 の設定 (IPv4 Configuration)] > [OSPFv2] > [OSPFv2 IPv4 ネットワーク (OSPFv2 IPv4 Networks)] の順にクリックして、OSPFv2 IPv4 ネットワークテーブルを表示します。このテーブルの情報は OSPFv2 プロ

セス ID ごとに表示され、必要に応じて [エリアID (Area ID)] も表示されます。必要な OSPFv2 プロセスと任意でエリア ID を選択し、[移動 (Go)] をクリックします。

ステップ 2 [OSPFv2 IPv4 ネットワークテーブル (OSPFv2 IPv4 Network Table)] には、以下のフィールドが表示されます。

- [OSPFv2 プロセス (OSPFv2 Process)] : このエントリの OSPF プロセス ID。
- [エリアID (Area ID)] : このエントリのエリアID。
- [コスト (Cost)] : この OSPFv2 ネットワーク インターフェイスに関連付けられているコスト。
- [ステータス (Status)] : この OSPFv2 ネットワーク インターフェイスのステータス。

ステップ 3 OSPFv2 IPV4 エリアネットワークテーブルを編集するには、テーブルから OSPFv2 プロセスを選択して [編集 (Edit)] アイコンをクリックし、以下を設定します。

- 設定するプロセス ID、エリア ID、およびエリアネットワークを選択します。
- インターフェイスコストを構成します。デフォルトのコストを選択するか、ユーザー定義コスト（範囲 1 ～ 65535）を選択します。パスコストは、 $10^{10}/\text{ifSpeed}$ の式を使用して計算されます。
- [シャットダウン (Shutdown)] : 必要に応じて、OSPFv2 ネットワークを管理上のダウン状態に設定できます。

ステップ 4 設定を適用するには、[適用 (Apply)] をクリックして設定を適用します。



第 15 章

IPv6 設定



(注) IPv6 設定およびこの章に記載されているすべてのセクションは、[Advanced Mode] でのみ使用できます。

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 \(291 ページ\)](#)
- [IPv6 インターフェイス \(293 ページ\)](#)
- [IPv6 トンネル \(295 ページ\)](#)
- [IPv6 アドレス \(297 ページ\)](#)
- [IPv6 ルータ設定 \(298 ページ\)](#)
- [IPv6 デフォルトルータリスト \(302 ページ\)](#)
- [IPv6 ネイバー \(303 ページ\)](#)
- [IPv6 プレフィックス リスト \(305 ページ\)](#)
- [IPv6 アクセス リスト \(306 ページ\)](#)
- [IPv6 ルート \(307 ページ\)](#)
- [DHCPv6 リレー \(309 ページ\)](#)
- [OSPFv3 \(310 ページ\)](#)

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 FE80:0000:0000:0000:9C00:876A: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。

手順

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] : [Enable] 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 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 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 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 Client Settings
 - [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。
 - [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。
 - [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 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 ではアドレス長が 32 ビットから 128 ビットに拡張されたので、IP アドレス割り当ての柔軟性が大幅に向上しています。IPv6 アドレスは、4 桁の 16 進数のグループ 8 個で記述します (たとえば、FE80:0000:0000:0000:9C00:876A:130B)。

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。



(注) トンネルインターフェイスは、[IPv6 トンネル \(295 ページ\)](#) で作成します

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。

手順

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 Link Local Default Zone] : デフォルトゾーンを定義する機能を有効にする場合は [Enable] を選択します。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 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は、次のフィールドとともに表示されます。

- [Tunnel Type] : [N/A]、[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 Interface] : 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）を有効にする場合は [Enable] を選択します。
- [Rapid Commit] : アドレス割り当てとその他の設定で 2 つのメッセージ交換の使用を有効にする場合は [Enable] を選択します。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。
- [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から受信されない場合、ここに入力した値が使用されません。[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 Address Auto Configuration] : ネイバーによって送信されるルータアドバタイズメントからの自動アドレス設定を有効にする場合は [Enable] を選択します。
- [Number of DAD Attempts] : 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。
- [Send ICMPv6 Messages] : 宛先到達不能メッセージを生成します。
- [MLD Version] : IPv6 MLD バージョンを選択します。
- [IPv6 Redirects] : ICMP IPv6 リダイレクトメッセージの送信を有効にする場合は [Enable] を選択します。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** 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 10** 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。
- ステップ 11** [Apply] をクリックして設定を保存します。
- ステップ 12** [Restart] を押して、DHCPv6 サーバーから受信されるステートレス情報の更新を開始します。
-

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は、ホストマッピングテーブルで ISATAP ホスト名とアドレス間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。

手順

ステップ 1 [IPv6 Configuration] > [IPv6 Tunnel] をクリックします。

ステップ 2 ISATAP パラメータを入力します。

- [送信要求間隔]：アクティブ化された ISATAP ルータが検出されない場合に、ISATAP ルータに送信要求メッセージを送信する間隔（秒数）を入力します。この間隔は、[Default Value] または [User Defined] のいずれかの間隔です。

- [ロバストネス]：対ルータ送信要求クエリーの送信間隔を計算する際に使用されます。数値が大きいほど、クエリー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 3 [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。

- [トンネル番号]：トンネルの番号を選択します。
- [Tunnel Type]：トンネルタイプを選択します。[Manual]、6 ～ 4、[ISATAP] から選択します。
- [トンネル状態]（メインページの [状態]）：トンネルを有効にする場合に選択します。このトンネルが後にシャットダウンされる場合、そのことがこのフィールドに示されます。
- [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に変更があった場合にトラップを生成する機能を有効にする場合に選択します。特定のポートでそのようなトラップを受け取ることに関心がない場合（例えば JSP で必要になるのはインフラストラクチャに接続されているポートのトラップのみであり、ユーザーの装置に接続されているポートのトラップは不要）、この機能を無効にすることができます。
- [送信元]（メインページの [送信元のタイプ]）：次のオプションのいずれかが表示されます。
 - [自動]：トンネルインターフェイスで送信されるパケットの送信元アドレスとして設定済みのすべての IPv4 インターフェイスの中から、最小の IPv4 アドレスが自動選択されます。その最小の IPv4 アドレスがインターフェイスから削除された場合（完全削除または別のインターフェイスに移動）、その次に最小となる IPv4 アドレスがローカル IPv4 アドレスとして選択されます。
 - [IPv4 Address]：トンネルの送信元アドレスとして使用されるインターフェイスの IPv4 アドレスを入力します。
 - [インターフェイス]：トンネルの送信元アドレスとして使用される IPv4 アドレスに対応するインターフェイスを選択します。
メインページに [送信元アドレス] という名前の列が表示されます。これは、上記選択に基づいて選択された実際の IP アドレスを表します。
- [宛先]：（手動トンネルの場合のみ）トンネルの宛先アドレスを指定するために、以下のオプションのうちの 1 つを選択します。
 - [ホスト名]：リモートホストの DNS 名。
 - [IPv4 アドレス]：リモートホストの IPv4 アドレス。
- [ISATAPルータ名]：（ISATAP トンネルの場合のみ）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ため、以下のオプションのうちの 1 つを選択します。
 - [Use Default]：これは常に ISATAP です。

- [User Defined] : ルータのドメイン名を入力します。

ステップ 5 [適用 (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。

ステップ 6 ISATAP トンネルを編集または削除するには、[Edit] または [Delete] アイコンをクリックします。

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。

手順

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。

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 Interface	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 Address Type	追加する IPv6 アドレスのタイプを選択します。 • [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] : 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。 • [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)

オプション	説明
	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。3 ～ 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。
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 部を識別する場合は [Enable] 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。

IPv6 アドレステーブルには、設定不可能な次のフィールドも表示されます。

オプション	説明
アドレスソース	アドレスソースタイプのいずれか（DHCP、システム、スタティック）が表示されます。
DAD ステータス	[重複アクセス検出（Duplicate Access Detection）] がアクティブかどうかと DAD 状態が表示されます。トンネルタイプのインターフェイスの場合、この列は表示されません。
優先ライフタイム	優先ライフタイムのエントリが表示されます。
有効なライフタイム	有効なライフタイムのエントリが表示されます。
期限切れ時間	有効期限が表示されます。

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。

手順

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
Interface	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。
Suppress Router Advertisement	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。
Router Preference	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。
Include Advertisement Interval Option	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。
Hop Limit	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。
Managed Address Configuration Flag	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。
Other Stateful Configuration Flag	[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

オプション	説明
	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。
Neighbor Solicitation Retransmissions Interval	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。
Maximum Router Advertisement Interval	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。
Minimum Router Advertisement Interval	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。
Router Advertisement Lifetime	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。

手順

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。または、インターフェイスを編集する場合は、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** 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。
Valid Lifetime	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。 • [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。
Preferred Lifetime	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。 • [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。
Auto Configuration	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。
Prefix Status	次のオプションのいずれかを選択します。 • [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

オプション	説明
	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）。 • [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。 • [Offlink] : 指定されたプレフィックスをオフリンクとして設定します。プレフィックスは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、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、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。

手順

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。

- [Outgoing Interface] : 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。
- [Default Router IPv6 Address] : デフォルト ルータのリンク ローカル IP アドレス。
- [Type] : デフォルト ルータのタイプ。
 - [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。
 - [Dynamic] : 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。
- 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

これは 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。

手順

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 Address] : 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 Address] : 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。
- [Router]：ネイバーがルータかどうかを指定します ([Yes]、[No]、または [N/A])。

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。

手順

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。
 - [Create new list]：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。

手順

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、[Go] 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。
 - [Use existing list] : 既存のアクセス リストを選択します。
 - [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。
 - [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。
- [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 サブネット上になり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。
- [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。
- [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。
- 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。
- [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 Redirect)] : 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 (Router Advertisement)] : 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。

手順

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 サーバのリストを設定するには、次の手順を実行します。

手順

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 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 サーバのアドレスを入力します。
- [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。

手順

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。
- [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 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。

OSPFv3



(注) OSPFv3 は Advanced モードでのみ使用できます。

Open Shortest Path First バージョン 3 (OSPFv3) は、IPv6 ネットワークをサポートするように設計された内部ゲートウェイ ルーティング プロトコルです。OSPFv2 と同様に、OSPFv3 を使用すると、ルータはリンクステート情報を交換し、リンクメトリックに基づいて最も効率的なルーティングパスを計算できます。しかし、OSPFv3 は IPv6 の構造と要件に対応するための機能強化が導入されています。複雑で大規模な IPv6 環境において、OSPFv3 は効率的なルート収

束と帯域幅の使用量削減を実現し、従来のルーティングプロトコルに代わる堅牢な選択肢となります。



- (注) OSPFv3 は、デバイスで IPv6 ルーティングが有効になっている場合にのみアクティブになります ([IPv6 設定 (IPv6 Configuration)] > [IPv6 グローバル設定-IPv6 ルーティング (IPv6 Global Configuration - Ipv6 Routing)] を有効に設定)。

Catalyst 1300X シリーズ スイッチの OSPF 機能の詳細については、『[Catalyst 1300X CLI Guide](#)』を参照してください。

OSPFv3 設定フロー

1. OSPFv3 プロセスを作成し、ルータ ID を割り当てます。複数のプロセスを作成できます。以下の構成は、各プロセスに適用できます。
2. プロセスに 1 つ以上のエリアを追加します。エリアごとに、エリアのタイプと設定を定義します。
3. エリアネットワーク設定を構成します。

OSPFv3 Process

OSPFv3 は、個別のルーティングプロセスとして設定されているのではなく、インターフェイス上で有効になっています。つまり、OSPFv3 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のルーティングプロセスおよび関連する設定が自動的に作成されます。OSPFv3 では、ルーティングプロセスの初期化、ルータ ID の定義、パッシブインターフェイスの設定など、[OSPFv2](#) と同じ基本プロセスが使用されます。

手順

ステップ 1 [IPv6 の設定 (IPv6 Configuration)]、[OSPFv3]、[OSPFv3 プロセス (OSPFv3 Process)] の順にクリックして、OSPFv3 プロセステーブルを表示します。

ステップ 2 テーブルに表示されるフィールドは次のとおりです。

- [プロセス ID (Process ID)] : プロセス識別子。
- [ルータ ID (Router ID)] : プロセスに割り当てられたルータ ID。

警告

実行中の OSPFv3 プロセスのルータ ID を変更すると、プロセスが自動的に再起動されます。

- [管理ステータス (Administrative Status)] : プロセスの管理ステータス。
- [動作ステータス (Operational Status)] : プロセスの動作ステータス。

ステップ 3 新しい OSPFv3 プロセスを追加する場合はクリックします。

ステップ 4 OSPFv3 プロセスに対して以下を定義します。

- [プロセスID (Process ID)] : OSPFv3 プロセスの ID を表す整数。
- [ルータID (Router ID)] : デフォルトのルータ ID (デバイスに設定されている最小 IPv4 アドレス) を使用するか、ルータ ID を手動で設定する (IPv4 形式) かを選択します。
- [シャットダウン (Shutdown)] : シャットダウン状態でプロセスを作成するには、シャットダウンを有効にするチェックボックスをオンにします。

(注)

これにより、ユーザーはトラフィックをアクティブ化せずにプロセス設定を構成できます。

ステップ 5 [適用 (Apply)] をクリックしてプロセスを作成します。

ステップ 6 プロセスを再起動するには、テーブル内の 1 つ以上のエントリを選択して、再起動ボタンを押します。これによりリセットされ、このプロセスの OSPF アクティビティが開始されます。

ステップ 7 画面の上部にある [OSPFv3エリア (OSPFv3 Area)] ボタンをクリックすると、[OSPFv3エリア (OSPFv3 Area)] 画面にリダイレクトされます。

ステップ 8 [プロセスの再起動 (Restart Process)] をクリックして、OSPFv3 プロセスを再起動します。

OSPFv3 エリアテーブル

OSPFv3 エリアテーブルは、IPv6 ネットワークの異なるエリア内のルーティング情報を整理および管理するために、OSPFv3 で使用されるデータ構造です。OSPFv3 は IPv6 向けに設計されたリンク ステートルーティングプロトコルで、エリアを使用してルーティングを効率的に最適化および管理します。

OSPFv3 エリア テーブルを設定するには以下の手順を実行します。

手順

ステップ 1 [IPv6設定 (IPv6 Configuration)] > [OSPFv3] > [OSPFv3エリアテーブル (OSPFv3 Area Table)] をクリックします。

ステップ 2 このテーブルの情報は、各 OSPFv3 プロセス ID (フィルタボタン) ごとに表示されます。必要な OSPFv3 プロセスを選択し、[移動 (Go)] をクリックします。

ステップ 3 テーブルに表示されるフィールドは次のとおりです。

- [エリアID (Area ID)] : IPv4 フォーマットのエリア ID
- [エリアタイプ (Area type)] : [バックボーン (Backbone)]、[通常 (Normal)]、[スタブ (Stub)]、[NSSA]
- [ステータス (Status)] : エリアの管理ステータス (アップまたはダウン)

ステップ 4 エントリの選択時に [詳細 (Details)] をクリックすると、完全なエリア設定が表示されます (テーブルに表示されるものに加えて、[エリアネットワーク (Area Networks)] および [スタブ/NSSA エリア (Stub/NSSA Area)] の設定: [デフォルト サマリー ルート コスト (Default Summary Route Cost)]、[ABR サマリー アドバタイズメント (ABR Summary Advertisement)]、[トランスレータ ロール (Translator Role)]、[トランスレータ 安定性 間隔 (Translator Stability Interval)])。

ステップ 5 画面の上部にある [OSPFv3 プロセス テーブル (OSPFv3 Process Table)] ボタンをクリックして [OSPFv3 プロセス (OSPFv3 Process)] 画面にリダイレクトするか、[OSPFv3 ネットワーク テーブル (OSPFv3 Network Table)] ボタンを押して [OSPFv3 IPv6 ネットワーク (OSPFv3 IPv6 Network)] 画面にリダイレクトします。

ステップ 6 [追加 (Add)] をクリックして、1 つ以上のエリアを作成します。次のフィールドを設定します。

- [プロセス ID (Process ID)] : ドロップダウンボックスから OSPFv3 プロセス ID を選択します。エリアは選択したプロセス ID に関連づけられます。

- [エリア ID (Area ID)] : エリア ID を IPv4 形式で構成します。

(注)

エリア ID 0 がバックボーンエリアとして定義されています。

- [シャットダウン (Shutdown)] : エリアをシャットダウン状態で作成するには、有効にします。これにより、エリアを非アクティブ状態に保ちながらエリア設定を構成できます。

- [IPv6 エリア ネットワーク (Area Networks)] : エリアに追加する 1 つ以上の IPv6 ネットワークを選択します。

(注)

IPv6 対応のインターフェイスのみが表示されます。

1. 設定するインターフェイスのタイプを選択します (unit : 物理インターフェイスの場合は [LAG] または [VLAN]) 。

2. インターフェイスのタイプを選択した後、左側のリストボックスから右側のリストボックスに移動して、必要なインターフェイスを追加します。

3. 必要に応じて、LAG インターフェイスと VLAN インターフェイスに対してこのアクションを繰り返します。

- 上記のステップで選択したインターフェイスが表示されます。

1. [選択されたインターフェイス (Selected Interfaces)] : エリアに追加するために選択された物理インターフェイス。

2. [選択された VLAN (Selected VLANs)] : エリアに追加するために選択された VLAN。

3. [選択された LAG (Selected LAGs)] : エリアに追加するために選択された LAG。

(注)

選択されたインターフェイスフィールドには、左側のリストボックスから右側のリストボックスに移動されたインターフェイスが表示されます。適用ボタンを押すまで、新しいインターフェイスは追加されません。

- [スタブ/NSSAエリア (Stub/NSSA Area)] : このエリアをスタブエリアまたは NSSA (Not So Stubby Area) として設定する場合に選択します。このオプションは、エリアがバックボーンエリアでない (エリア ID が 0.0.0.0 ではない) 場合にのみ使用できます。このオプションを選択した場合は、以下のフィールドの設定を続けます。
- [スタブ/NSSA (Stub/NSSA)] : このエリアがスタブエリアまたは NSSA のいずれであるかを選択します。
- [デフォルト サマリー ルート コスト (Default Summary Route Cost)] : スタブエリアまたは NSSA (Not-So-Stubby Area) に送信されるデフォルトサマリールートのコストを指定します。次のいずれかの利用可能なオプションを選択します。
 1. デフォルト : 1 の値
 2. ユーザー定義 : 範囲 : 1 ~ 16777214
- [ABRサマリーアドバタイズメント (ABR Summary Advertisement)] : エリア境界ルータ (ABR) がサマリー リンク アドバタイズメントをスタブエリアに送信できるようにします。
- トランスレータロールとトランスレータ安定性間隔は、エリアが NSSA として定義されている場合にのみ設定できます。
 - [トランスレータロール (Translator Role)] : NSSA 境界ルータがタイプ 7 LSA をタイプ 5 LSA に無条件に変換するかどうかを指定します。
 1. [常に (Always)] を選択すると、他の NSSA 境界ルータのトランスレータ状態に関係なく、常に NSSA 境界ルータがタイプ 7 LSA をタイプ 5 LSA に変換します。
 2. [候補 (Candidate)] を選択すると、NSSA 境界ルータが RFC 3101 のセクション 3.1 で説明されているトランスレータ選択プロセスに参加するように指定します。
 - [トランスレータ安定性間隔 (Translator Stability Interval)] : 選出されたトランスレーターが、もはや自身のサービスが不要であると判断した後も、翻訳業務を継続すべき秒数を指定します。デフォルト値は 40 秒です。
- [適用 (Apply)] をクリックしてエリアを作成します。

OSPFv3 IPv6 エリアネットワーク

OSPFv3 IPv6 エリアネットワークを表示、編集、または設定するには、以下の手順を実行します。

手順

-
- ステップ 1** [IPv6の設定 (IPv6 Configuration)] > [OSPFv3] > [OSPFv3 IPv6エリアネットワーク (OSPFv3 IPv6 Area Networks)] をクリックして、OSPFv3 IPv6 ネットワークテーブルを表示します。このテーブルの情報は OSPFv3 プロセス ID ごとに表示され、必要に応じて [エリアID (Area ID)] も表示されます。必要な OSPFv3 プロセスと任意でエリア ID を選択し、[移動 (Go)] をクリックします。
- ステップ 2** [OSPFv3 IPv6 ネットワークテーブル (OSPFv3 IPv6 Network Table)] には、以下のフィールドが表示されます。
- [OSPFv3 プロセス (OSPFv2 Process)] : このエントリの OSPF プロセス ID。
 - [エリアID (Area ID)] : このエントリのエリアID。
 - [IPv6 インターフェイス (Ipv6 Interface)] : このエントリの IPv6 インターフェイス。
 - [コスト (Cost)] : この OSPFv3 IPv6 インターフェイスに関連付けられているコスト。
 - [ステータス (Status)] : この OSPFv3 IPv6 インターフェイスのステータス。
- ステップ 3** OSPFv3 IPV6 エリアネットワークテーブルを編集するには、テーブルから OSPFv3 プロセスを選択して [編集 (Edit)] アイコンをクリックし、以下を設定します。
- 設定するプロセス ID、エリア ID、およびエリアネットワークを選択します。
 - インターフェイスコストを構成します。デフォルトのコストを選択するか、ユーザー定義コスト（範囲 1 ～ 65535）を選択します。パスコストは、 $10^{10} / \text{ifSpeed}$ の式を使用して計算されます。
 - [シャットダウン (Shutdown)] : 必要に応じて、OSPFv3 ネットワークを管理上のダウン状態に設定できます。
 - 設定を適用するには、[適用 (Apply)] をクリックして設定を適用します。
- ステップ 4** [OSPFv3 エリアテーブル (OSPFv3 Area Table)] ナビゲーションボタンをクリックすると、[OSPFv3 エリアテーブル (OSPFv3 Area Table)] ページにページがリダイレクトされます。
-



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 \(317 ページ\)](#)
- [ドメインネームシステム \(320 ページ\)](#)
- [IPDT \(324 ページ\)](#)

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は、デバイスが、パケットをルーティングする前に、それらのパケットをルート マップに照合するプロセスです。ルート マップは、どのパケットが次にどのデバイスにルーティングされるかを決定します。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。

手順

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 [追加 (Add)] をクリックしてルートマップを追加するか、[編集 (Edit)] をクリックして既存のルートマップを編集し、次のパラメータを設定します。

- 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。

手順

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。

手順

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 [Policy Based Routes] テーブルの上部に、[Filter] セクションが表示されます。次の手順で [Filter] を使用して以前に定義したポリシーベースのルートをフィルタ処理します。

- [Apply a Filter] : ドロップダウンメニューから目的のフィルタ条件と演算子を選択し、テキストフィールドに値を入力してから、[Go] をクリックします。
- [Clear the Filter] : フィルタを削除してすべてのエントリを表示するには、[Clear Filter] をクリックします。

ステップ 3 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、デバイスで使用するデフォルト 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。

手順

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 = $2 * (\text{ポーリング再試行回数} + 1) * \text{ポーリング タイムアウト}$
 - 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 Address Type] : 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、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。

- [Global] : 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 \(320 ページ\)](#) 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) : デバイスで利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。

手順

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。

ホスト マッピング テーブルには以下のフィールドが表示されます。

- ホスト名 (Host Name) : ユーザ定義のホスト名または完全修飾名。
- [IP Address] : ホスト IP アドレス。
- IP バージョン (IP Version) : ホストの IP アドレスの IP バージョン。
- タイプ (Type) : キャッシュに格納するのがダイナミック エントリまたはスタティック エントリか。
- 状態 (Status) : ホストへのアクセス試行の結果が表示されます。
 - [OK] : 試行成功。
 - [ネガティブ キャッシュ] : 試行失敗。再試行しないでください。
 - [応答なし] : 応答はありませんが、将来システムによる再試行が可能です。
- TTL (秒) (TTL (Sec)) : これがダイナミック エントリの場合は、キャッシュ内での存続時間。
- 残存 TTL (秒) (Remaining TTL (Sec)) : これがダイナミック エントリの場合は、キャッシュ内での残りの存続時間。

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 Address Type] : 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、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。

- [Global] : 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。

IPDT

一部のネットワーキング アプリケーション (802.1x ベースのダイナミック ACL など) では、インターフェイスまたは VLAN に接続されているホストの IP アドレス (または MAC から IP へのマッピング) を認識する必要があります。IP デバイストラッキング (IPDT) は、この機能を提供します。

IPDT は、スイッチに接続されているホストの IP アドレスをホスト MAC アドレスにマッピングできるアプリケーションです。IPDT は、ホストから送信された特定の packets をスヌーピングすることでこれを実現します。IPDT アプリケーションは、パケットの実際のスヌーピングには関与しません。実際のスヌーピングは、ARP スヌーピングや DHCP スヌーピングなどの既存のアプリケーションによって実行されます。IPDT は、IP から MAC へのマッピングデータベースの作成と維持のみを行います。

IP から MAC へのマッピングを必要とするアプリケーションは、IPDT クライアントとして認識しています。

IPDT は、エントリが追加、変更、または削除されると、IPDT クライアントを更新します。IPDT クライアントは、ホストの IP アドレスの IPDT をポーリングすることもできます。

IP デバイストラッキングは、次の 2 つの方法のいずれかでインターフェイスで有効になります。

- インターフェイスの 802.1x 管理ポート制御設定が [Auto] に設定されている。
- ユーザーがインターフェイスの [Maximum host] 値を変更する。

IP デバイス トラッキング マッピング

[IP Device Tracking (IPDT) Mapping] テーブルには、IP デバイストラッキング機能によって学習されたホストの IP から MAC へのマッピングが表示されます。IPDT トラッキングマッピングを表示するには、次の手順を実行します。

手順

ステップ 1 [General IP Configuration] > [IPDT] > [IP Device Tracking Mapping] の順に選択します。

ステップ 2 [IP Device Tracking Mapping] テーブルの [Filter] セクションで、インターフェイスを選択し、[Go] をクリックします。

ステップ 3 各エントリの情報は次のとおりです。

- [IP Address] : ホストの IP アドレス。
- [MAC address] : ホストの MAC アドレス。
- [VLAN] : ホストがメンバーになっている VLAN。
- [Port] : ホストが接続されているインターフェイス。
- [Probe Interval] : デフォルトのプロブ間隔（エージングタイマー）は 30 秒です。
- [State] : エントリの状態。
 - [Active] : ホストはデバイスから送信されたプロブに応答しており、インターフェイスはアップ状態です。
 - [In-active] : エントリがアクティブ状態の間にインターフェイスがダウン状態に移行しました。
- [Source] : ホストの IP アドレスと MAC アドレスを学習するために IP デバイストラッキングで使用方法。サポートされる値は、ARP または DHCP です。

（注）

ホストがデバイスから送信されたプロブに応答しない場合、エントリはテーブルから削除されます。

ステップ 4 適用されたフィルタに関係なく、デバイストラッキングエントリをクリアするには、[Clear Table] をクリックします。

IP デバイストラッキング設定

IPDT の主な役割は、リンクされたホストの追跡（MAC-IP アドレスの関連付け）を維持することです。これを実現するために、デフォルトの 30 秒間隔でユニキャスト Address Resolution Protocol（ARP）プロブを送信します。これらのプロブは、リンクの反対側に接続されて

いるホストの MAC アドレスに送信され、レイヤ 2 (L2) をデフォルトの送信元として使用します。

IPDT トラッキング設定を行うには、次の手順を実行します。

手順

ステップ 1 [General IP Configuration] > [IPDT] > [IP Device Tracking Settings] の順に選択します。

ステップ 2 次のパラメータを設定します。

- [Default Probe Count] : デバイス トラッキング エントリが削除されるまでに送信されるプローブのデフォルト数。この値は、インターフェイスでプローブ数が定義されていない場合に使用されます。
- [Default Probe Interval] : デバイスによって送信されるプローブ間のデフォルトの間隔（秒単位）。この値は、インターフェイスでプローブ間隔が定義されていない場合に使用されます。
- [Probe Delay Interval] : リンクがアップ状態に移行してからプローブを送信するまでの待機時間（秒単位）。この設定は、プローブの送信が早すぎると、接続されたステーションの DHCP プロセスに影響する場合に役立ちます。
- [Auto Source IP Address Value] : IP アドレスが設定されていない VLAN インターフェイスによって送信されるプローブの送信元 IP アドレスとして使用する IP アドレス。
- [Auto Source IP Wildcard Mask]（自動送信元 IP アドレス値が設定されている場合にのみ設定に使用可能） : 自動送信元 IP アドレスに適用するマスク。送信元 IP アドレスのホスト部分のみがプローブ送信元アドレスに使用されます。
- [Total number of interfaces enabled (read-only)] : IP デバイストラッキングが有効になっているインターフェイスの数を示します。

ステップ 3 [Apply] をクリックして設定を適用します。

IP デバイストラッキング設定テーブルのフィールドの説明 :

- [Port] : デバイスポート
- [Administrative Status] : インターフェイス上の IP デバイストラッキング設定の状態。サポートされる値 :
 - [Enable] : ユーザーによってインターフェイスで IP デバイストラッキングが有効化されました。
 - [Disable] : ユーザーによってインターフェイスで IP デバイストラッキングが無効化されました。
 - [Auto]（デフォルト状態） : インターフェイスの [802.1x Administrative Port Control] 設定が [auto] に設定されている場合、インターフェイスで IP デバイストラッキングがアクティブになります。
- [Operational Status] : インターフェイス上の機能の動作ステータス。
- [Maximum Hosts] : このインターフェイスの IP デバイス トラッキング テーブルに追加できるホストの最大数。値 0 は、この機能がインターフェイスで無効になっていることを示します。有効な値の範囲は 1 ~ 65534 で、65535 は範囲外です。

- [Application] : インターフェイスで 802.1x が有効になっているかどうかを示します。これにより、[Administrative Status] が [Auto] の場合にインターフェイスで IP デバイストラッキングがアクティブになります。
- [Probe Count] : ホストエントリが IP デバイス トラッキング テーブルから削除される前に、このインターフェイスで送信されたプローブの数。「(Default)」の表示もある場合は、デフォルトのグローバルプローブカウント値がプローブカウント値に適用されたことを意味します。
- [Probe Interval] : このインターフェイスで送信されるプローブ間のデフォルトの間隔（秒単位）。「(Default)」の表示もある場合は、デフォルトのグローバルプローブ間隔値がプローブ間隔値に適用されたことを意味します。

ステップ 4 インターフェイスの設定を編集するには、テーブルでインターフェイスの行を選択し、[Edit] をクリックします。

ステップ 5 次に、以下の項目を設定します。

- [Interface] : 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。
- [Port] : ドロップダウンリストからポートを選択します。
- [IP Device Tracking Operational Status] : このインターフェイスの IP デバイストラッキング機能のステータスを表示します（読み取り専用フィールド）。
- [IP Device Tracking Administrative Status] : インターフェイスの管理ステータスを設定します。
 - [Auto]（デフォルト状態） : [802.1x Administrative Port Control] 設定が [auto] に設定されている場合にのみ、インターフェイスで IP デバイストラッキングがアクティブになります。
 - [Disable] : インターフェイスで IP デバイストラッキングが無効です。
 - [Enable] : インターフェイスで IP デバイストラッキングが有効です。
- [Maximum Hosts] : IP デバイス トラッキング テーブルに追加できるホストの最大数。この設定は、[IP Device Tracking Administrative Status] が有効に設定されている場合に必須です。
- [Probe Count] : ホストエントリが IP デバイス トラッキング テーブルから削除される前に、このインターフェイスで送信されたプローブの数。「(Default)」の表示もある場合は、デフォルトのグローバルプローブカウント値がプローブカウント値に適用されたことを意味します。
- [Probe Interval] : このインターフェイスで送信されるプローブ間のデフォルトの間隔（秒単位）。「(Default)」の表示もある場合は、デフォルトのグローバルプローブ間隔値がプローブ間隔値に適用されたことを意味します。



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。

- [FIPS プロパティ \(329 ページ\)](#)
- [TACACS+クライアント \(330 ページ\)](#)
- [RADIUS Client \(333 ページ\)](#)
- [RADIUS サーバ \(336 ページ\)](#)
- [ダイナミック承認サーバ \(344 ページ\)](#)
- [ログイン設定 \(349 ページ\)](#)
- [ログイン保護ステータス \(352 ページ\)](#)
- [キー管理 \(352 ページ\)](#)
- [管理アクセス方式 \(355 ページ\)](#)
- [管理アクセス認証 \(360 ページ\)](#)
- [セキュア センシティブ データ管理 \(361 ページ\)](#)
- [SSL Server \(365 ページ\)](#)
- [SSH サーバ \(368 ページ\)](#)
- [SSH クライアント \(371 ページ\)](#)
- [TCP/UDPサービス \(375 ページ\)](#)
- [ストーム制御 \(376 ページ\)](#)
- [ポートセキュリティ \(379 ページ\)](#)
- [802.1X 認証 \(381 ページ\)](#)
- [サービス拒絶防御 \(395 ページ\)](#)
- [IP ソース ガード \(402 ページ\)](#)
- [ARP インспекション \(405 ページ\)](#)
- [IPv6 ファースト ホップ セキュリティ \(408 ページ\)](#)
- [証明書の設定 \(429 ページ\)](#)

FIPS プロパティ

連邦情報処理標準 (FIPS) は、アメリカ国立標準技術研究所 (NIST) によって開発された、公に発表されている一連の標準規格です。これは、非軍事の米国政府機関や請負業者がコンピュー

ターシステムで使用することを目的としています。これらの標準規格は、情報技術およびサイバーセキュリティにおける共通の品質と相互運用性を保証します。

FIPS 140 は、暗号モジュールのセキュリティ要件に焦点を当てた、FIPS 標準規格の特定のシリーズです。これらのモジュールは、データの暗号化と復号化に使用されるハードウェアまたはソフトウェアコンポーネントです。FIPS 140 シリーズでは、これらの暗号モジュールが厳格なセキュリティ基準を満たし、機密情報を保護できることを保証します。

デバイスは、以下の管理インターフェイスでの FIPS 140-2 準拠をサポートしています。

- HTTPS サーバーおよびクライアント
- SSHv2 サーバーおよびクライアント
- SNMPv3

デバイスでは、以下の 2 つのモードがサポートされます。

- FIPS 準拠モード
- FIPS 非準拠モード

デフォルトでは、スイッチは FIPS 非準拠モードです。

FIPS を設定するには、次の手順を実行します。

手順

ステップ 1 [セキュリティ (Security)] > [全般 (General)] > [FIPS プロパティ (FIPS Properties)] の順にクリックします。

ステップ 2 [FIPS モード (FIPS Mode)] を選択し、デバイスで FIPS モードを有効にします。

ステップ 3 [適用 (Apply)] をクリックします。[FIPS モード変更の確認 (Confirm FIPS mode change)] という確認ウィンドウが表示されます。[OK] をクリックして操作を完了します。

(注)

重要：このアクションによってデバイスが自動的に再起動され、SSH キー、SSH サーバーキーのフィンガープリント、および HTTPS キーと証明書が削除されます。FIPS モードを変更する前に、デバイスの設定を保存することをお勧めします。

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。

手順

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tring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。
Timeout for Reply	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。
Source IPv4 Interface	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。
Source IPv6 Interface	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。TACACS+ サーバーを編集するには、TACACS+ サーバーを選択して [Edit] をクリックします。

ステップ 6 次に、パラメータを構成します。

オプション	説明
Server Definition	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 Version	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 Address Type	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。
Link Local Interface	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tring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。

オプション	説明
	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tringがない場合は、プレーンテキストモードでキースtring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。
Timeout for Reply	[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 サーバのパラメータ値を設定するには、次の手順を実行します。

手順

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 ポートアカウントリングに 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 アカウントリ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 アカウントリングと 802.1X ポートアカウントリングの両方に RADIUS サーバーが使用されることを指定します。
- なし (None) : RADIUS サーバがアカウントリングに使用されないことを指定します。

ステップ 3 アカウントリング期間の数値を入力します (範囲 : 1 ~ 65535、無効 : 0)

(注)

管理アクセス用の RADIUS アカウントリングを有効にできるのは、TACACS+ アカウントリングが無効になっている場合のみです。

ステップ 4 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)] : 応答のない RADIUS サーバーへのサービス要求がバイパスされるようになるまでのタイムインターバル (単位 : 分) を入力します。デッドタイムは、非応答 RADIUS サーバーがトランザクション要求によって省略される間のタイムインターバルを分単位で指定します (範囲 : 0 ~ 2000)。デフォルトのインターバルは 0 です (非応答 RADIUS サーバーは省略されません)。
- 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5 [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6 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7 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 Address Type] : 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、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。
 - [Global] : 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 (KeyString) : 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)] : 応答のない RADIUS サーバーへのサービス要求がバイパスされるようになるまでのタイムインターバル (単位: 分) を入力します。デッドタイムは、非応答 RADIUS サーバーがトランザクション要求によって省略される間のタイムインターバルを分単位で指定します (範囲: 0~2000)。デフォルトのインターバルは 0 です (非応答 RADIUS サーバーは省略されません)。
- [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せん。
 - [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。
- [メッセージ認証の強制 (Force Message Authenticator)] : メッセージ認証の強制を有効にするには、[有効 (Enable)] をオンにします。

ステップ 8 [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 9 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。

アカウントिंग: RADIUS サーバを使用したログインセッションのアカウントिंग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トング レポートを生成できるようになります。RADIUS サーバのアカウント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。

手順

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 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は [Enable] チェックボックスをオンにします。
- [RADIUS Authentication Failure Traps]：失敗したログインのトラップを生成する場合は [Enable] チェックボックスをオンにします。
- [RADIUS Authentication Success Traps]：成功したログインのトラップを生成する場合は [Enable] チェックボックスをオンにします。

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。

手順

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 [Add] をクリックして秘密鍵を追加するか、[Edit] をクリックして、秘密鍵テーブルの既存の秘密鍵を編集します。次に、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。
- [Key's MD5 Digest] : デフォルトでは定義されていません。これは、秘密鍵テーブルを編集する場合にのみ表示されます。
- 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] : 指定されたサーバに対して、デバイスは既存のデフォルトキースtringを使用して、RADIUS クライアントの認証を試行します。
 - [Keep current user defined key] : 既存のユーザー定義キーを保持する場合に選択します。
 - 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。

手順

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 RADIUS サーバーグループを追加するか、[Edit] をクリックして既存のグループを編集します。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。

手順

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] または [Edit] をクリックして、以下を設定します。

- [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's MD5] : パスワードの MD5 暗号化ハッシュが表示されます。
- [Password] : 次のいずれかのオプションを入力します。
 - [Keep current password] : 現在のパスワードを保持するには、このオプションを使用します。
 - 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tringがない場合は、プレーンテキストモードでキースtring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。

手順

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 RADIUS サーバ アカウンティング イベントをクリアするには、[Clear] をクリックします。

ステップ3 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。
 - [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。

手順

ステップ1 [Security] > [RADIUS Server] > [RADIUS Server Rejected Users] をクリックします。

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。

手順

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。

手順

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アカウンティング要求数	不明なアドレスからの着信アカウンティング要求の数。
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。

ダイナミック承認サーバー

次の手順を実行して、動的許可サービスの認証、許可、アカウンティング（AAA）サーバとしてデバイスを有効にします。認可変更（CoA）は RADIUS プロトコルの拡張であり、AAA または dot1x ユーザーセッションをダイナミックに変更できます。これには、ユーザーの切断およびユーザーセッションに適用される認可の変更のサポートが含まれます。

手順

ステップ 1 [Security] > [Dynamic Authorization Server] をクリックします。

ステップ 2 次の設定を行います。

設定	説明
サーバーキーの一致を強制する（Enforce Server Key Match）	サーバーキーの一致を強制するには、[有効（Enable）] をオンにします。この制御が無効になっている場合、デバイスと CoA クライアントで設定されたキーが一致しなくても、CoA クライアントとの RADIUS 交換は成功します。

設定	説明
受信時のタイムスタンプを強制する (Enforce Timestamp on Rx)	パケットオブディスコネクト (POD) 要求または認可変更 (CoA) の受信パケットのタイムスタンプを強制するには、[有効 (Enable)] をオンにします。これらのパケットにタイムスタンプが含まれていない場合、パケットは破棄されます。
Disable Port コマンドを処理する (Handle Disable Port Commands)	CoA disable port コマンドの処理を有効にするには、[有効 (Enable)] をオンにします。オフにすると、デバイスは、1 つ以上のホストセッションをホストする認証ポートを管理上シャットダウンする RADIUS サーバーの CoA disable port コマンドを無視します。
Bounce Port コマンドを処理する (Handle Bounce Port Commands)	CoA bounce port コマンドの処理を有効にするには、[有効 (Enable)] をオンにします。オフにすると、デバイスは、認証ポートでリンクフラップを引き起こす RADIUS サーバーの bounce port コマンドを無視します。これにより、このポートに接続されている 1 つ以上のホストからの DHCP 再ネゴシエーションが発生します。
デフォルトのサーバーキー MD5	デバイスと CoA クライアント間の共有キーを定義します。次のいずれかを選択します。 - なし - 既存のデフォルトキーを維持する - ユーザー定義(暗号化) - ユーザー定義(平文)
UDP Port	CoA 要求の UDP ポートを設定する値を入力します (範囲 0 ～ 59999、デフォルト : 1700) 。
ドメイン ストリッピング	CoA アプリケーションのユーザー名ドメインのオプションを設定します。以下のいずれかのオプションを選択します。 [None] : ドメインの削除なし [Left to Right] : この左から右キーワードは、左から右に向かって移動して最初に見つかったデリミタで文字列を終わらせます。 [Right to Left] : この右から左キーワードは、右から左に向かって移動して最初に見つかったデリミタで文字列を終わらせます

設定	説明
ドメインデリミタ	このデリミタフィールドは、ドメインデリミタを指定します。文字引数として次のいずれかのオプションを選択できます：@、/、\$、%、\、#、または-。

ステップ 3 [Client] テーブルは、特定の CoA クライアントの CoA クライアントごとの MD5 サーバーキーを定義します。クライアントごとのキーは、[Default Server Key MD5] 設定で定義されたキーを上書きします。特定の CoA クライアントに対してキーが定義されていない場合、クライアントは [Default Server Key MD5] を使用します。特定の CoA クライアントのキーを追加または編集するには、[追加 (Add)] または [編集 (Edit)] をクリックし、ポップアップウィンドウで次のように設定します。

- [IPアドレス (IP Address)] : CoA クライアントの IPv4 または IPv6 アドレス
- [MD5ダイジェスト (MD5 Digest)] : 未定義 (デフォルト)
- [Ignore NAS Identifiers] : チェックして有効にします。
- [Server Key] : 次のいずれかを選択します。
 - [Use default key] : この場合、デフォルトのサーバーキーが使用されます。
 - [現在のユーザー定義キーを保持 (Keep current user defined key)] : この場合、現在のユーザー定義キーを保持します。
 - [User Defined (Encrypted)] : 暗号化された形式でキーを入力します。
 - [User Defined (Plaintext)] : プレーンテキスト形式でキーを入力します。

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 次に、[Client Address] を選択し、[Counters] をクリックしてカウンタを表示します。次の表で、ポップアップに表示されるフィールドについて説明します。

フィールド	説明
IPアドレス	IP address
Average ACK response time	ミリ秒単位の平均 ACK 応答時間。

CoA カウンタ	説明
Requests	CoA クライアントから受信した要求をカウントします。
Transactions	CoA の完了トランザクションをカウントします。スイッチが CoA クライアントからの要求に 응답して ACK または NAK を送信すると、完了トランザクションが発生します。

CoA カウンタ	説明
再送信	受信した再送信された CoA 要求をカウントします。再送信された CoA 要求は、要求識別子が前の要求の識別子と同じである要求です。
Active Transactions	現在アクティブなトランザクション。アクティブなトランザクションとは、CoA クライアントからの要求を受信したが、ACK または NAK 応答がまだ送信されていないトランザクションです。ACK または NAK が送信されると、このカウンタはデクリメントされます。
ACX Responses	スイッチから送信された ACK 応答の数をカウントします。
NAK Responses	スイッチから送信された NAK 応答の数をカウントします。
Invalid Requests	スイッチが受信した無効な要求をカウントします。無効な要求は、次のいずれかです。 • 要求内のシークレットがデバイスに設定されているシークレットと一致しない要求。 • セッション識別子のない要求。 • サポートされていない属性を持つ要求。 • サポートされている属性が空の要求。 • event-timestamp が最新ではないため、または event-timestamp が必須で、受信した要求にこの属性が含まれていないために破棄された要求。 • Event-Timestamp 属性が最新ではないか、欠落している要求。 • ユーザー設定が原因でドロップされた「disable port」または「bounce port」コマンドで受信した要求。
Errors	エラーをカウントします。エラーは、リソースの問題が原因で要求を処理できない内部エラーであるか、CoA クライアントにシークレットが設定されていない場合に発生する可能性があります。
PoD カウンタ	説明
リクエスト (Requests)	切断パケット (PoD) の要求をカウントします。

トランザクション (Transactions)	Pod の完了トランザクションをカウントします。スイッチが PoD 切断からの要求に応答して ACK または NAK を送信すると、完了トランザクションが発生します。
再送信 (Retransmissions)	受信した再送信された PoD 切断要求をカウントします。
Active Transactions	現在アクティブなトランザクション。アクティブなトランザクションとは、PoD からの要求を受信したが、ACK または NAK 応答がまだ送信されていないトランザクションです。ACK または NAK が送信されると、このカウンタはデクリメントされます。
ACX Responses	スイッチから送信された ACK 応答の数をカウントします。
NAK Responses	スイッチから送信された NAK 応答の数をカウントします。
Invalid Requests	スイッチが受信した無効な要求をカウントします。無効な要求は、次のいずれかです。 • 要求内のシークレットがデバイスに設定されているシークレットと一致しない要求。 • セッション識別子のない要求。 • サポートされていない属性を持つ要求。 • サポートされている属性が空の要求。 • event-timestamp が最新ではないため、または event-timestamp が必須で、受信した要求にこの属性が含まれていないために破棄された要求。 • Event-Timestamp 属性が最新ではないか、欠落している要求。 • ユーザー設定が原因でドロップされた「disable port」または「bounce port」コマンドで受信した要求。
Errors	PoD プロセス中のエラーの数。

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。

手順

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

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
パスワードエージング	[Enable] をオンにし、パスワードエージングを有効にします。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、パスワードを変更できる警告メッセージが表示されます。ユーザーは警告を無視して、実際の有効期限まで既存のパスワードを引き続き使用できます。
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。
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：1 ～ 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、許可される最大繰り返し数は 3 です。
- 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、一般的なパスワードのリストと比較されます。[SecLists/パスワード共通のログイン情報](#) 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」の代わりに「\$」、「a」の代わりに「@」、「o」の代わりに「0」、「l」の代わりに「1」、「i」の代わりに「!」、「e」の代わりに「3」。禁止されているパスワードの例：「efg123!\$」、「abcd765%」、「kjl!\$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」、「catalyst」、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」の代わりに「\$」、「a」の代わりに「@」、「o」の代わりに「0」、「l」の代わりに「1」、「i」の代わりに「!」、「e」の代わりに「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。
- 既知のパスワードはパスワードとして使用できません

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。

手順

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）
静音時間 アクセスプロファイル (356 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。

[Login Protection Status] の設定を表示するには、[Security] > [Login Protection Status] の順に選択します。

- [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。
- [Login Failures in the Last 3600 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。

キーチェーン設定

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。

手順

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。

手順

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 (Encrypted)] : キーチェーン文字列の値。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。
- [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。このオプションを選択した場合は、下の [Start Date] と [Start Time] 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。
- [Send 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。デフォルトのオプションをオンにします。
 - [Always Valid] : キー識別子の存続期間に制限はありません。
 - [ユーザー定義 (User Defined)] : 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。
- [Start Date] : 送信ライフタイムが有効な最も早い日付を入力します。
- [開始時刻 (Start Time)] : [開始日 (Start Date)] において、送信ライフタイムが有効な最も早い時刻を入力します。
- [End Time] : 送信ライフタイムが有効な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] : 送信ライフタイムの有効期間が制限されません
 - [Duration] : 送信ライフタイムの有効期間が制限されます。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。
 - [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。

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 \(358 ページ\)](#) 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。

手順

- ステップ 1** [Security]>[Mgmt Access Method]>[Access Profiles] をクリックします。
- 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。
- ステップ 3** アクティブ アクセス プロファイル変更を確認するポップアップが表示されます。[OK] をクリックして変更を確定するか、[Cancel] をクリックして変更をキャンセルします。
- 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。

手順

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。

手順

-
- 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権限が RADIUS サーバによって付与されるようにするには、RADIUS サーバが RADIUS 属性「Service-Type 6」値「Administrative」を返す必要があります。
 - **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、デフォルトパストレーズに基づく暗号化による最小限の保護、ユーザ定義のパスト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す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。

手順

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。

手順

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ことを示します。

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。
- チャンネル (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。

手順

ステップ 1 [Security] > [SSL Server] > [SSL Server Authentication Settings] の順にクリックします。

SSL サーバ キー テーブルに証明書 1 と 2 の情報が表示されます。フィールドは、次のフィールドを除いて [Edit] ページで定義されています。

- 有効期間の開始日 (Valid From) : 証明書の有効期間の開始日を指定します。
- 有効期間の終了日 (Valid To) : 証明書の有効期間の終了日を指定します。
- 証明書の生成元 (Certificate Source) : 証明書の生成元、システム (自動生成) またはユーザ (ユーザ定義) を指定します。

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。

証明書要求の生成

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。

手順

ステップ 1 [Generate Certificate Request] をクリックします。

ステップ 2 次に、次のフィールドに入力します。

- [Certificate ID] : 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。
- [Common Name] : 証明書の名前を入力します。
- [Organization Unit] : 組織単位を入力します。
- [Organization Name] : 組織名を入力します。
- [Location] : 場所または市町村名を入力します。
- [State] : 州/都道府県を入力します。
- [Country] : 国の名前を入力します。
- [Certificate Request] : 証明書要求の開始が表示されます。
- * [期間 (Duration)] : 証明書が有効な日数が表示されます。(範囲は 30 ~ 1095 日、デフォルトは 730 日です。

(注)

[Duration] フィールドは、既存の証明書を編集しようとした場合にのみ表示されます。

ステップ 3 [Generate Certificate Request] 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 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 5 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。

- 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。

•

ステップ 6 [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 7 [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 8 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。

次のタスク

証明書チェーンの表示

デバイス証明書が CA ルート認証局ではなく中間 CA 認証局によって署名されている場合、ユーザーはデバイス証明書の署名に使用された中間証明書と、ルート証明書までのチェーン内の各証明書をインポートする必要があります。中間証明書は、[CA Certificate Settings] を使用してインポートできます。この証明書チェーンを表示するには、SSL サーバーキーテーブルから証明書 1 または 2 を選択し、[Certificate Chain] をクリックします。これにより、[証明書チェーン (Certificate Chain)] モーダルが開き、デバイス証明書とデバイス証明書チェーンの中間証明書部分が表示されます。

自己署名証明書の更新

自己署名証明書を更新するには、次の手順を実行します。

手順

ステップ 1 更新する証明書を選択して [Edit] をクリックします。

ステップ 2 次に、次のフィールドに入力します。

- [Certificate ID]：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。
- [Common Name]：証明書の名前を入力します。
- [Organization Unit]：組織単位を入力します。
- [Organization Name]：組織名を入力します。
- [Location]：場所または市町村名を入力します。

- [State] : 州/都道府県を入力します。
- [Country] : 国の名前を入力します。
- [Certificate Request] : 証明書要求の開始が表示されます。
- [Duration] : 証明書が有効な日数が表示されます。（範囲は 30 ～ 1095 日、デフォルトは 730 日です）

ステップ 3 [Generate] ボタンを押します。

SSH サーバ



(注) このセクションとそのサブセクションは、[Advanced Mode] でのみ使用できます。

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。

認証を有効にして、ユーザを追加します。

手順

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と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 [Enable] を選択します。
- [SSHセッションロギング (SSH Session Logging)] : [有効 (Enable)] を選択すると、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] : 公開キーを使用した SSH クライアントユーザーの認証を有効にする場合に [Enable] を選択します。
- [Automatic Login] : [SSH User Authentication by Public Key] 機能を有効にする場合に [Enable] を選択します。

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 サーバの SSH サーバ公開キー（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。ユーザは、SSH セッションで SSH サーバ認証を実行する場合に、このデバイスの SSH サーバ公開キー（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。

手順

ステップ 1 [Security] > [SSH Server] > [SSH Server Authentication] の順にクリックします。

[Fingerprint] セクションのキーごとに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。
 - [削除] : キーを削除できるようにします。
 - [Details] : 生成されたキーを表示できるようにします。[Details] ウィンドウでは、[Display Sensitive Data as Plaintext] をクリックすることもできます。これをクリックすると、キーが暗号化された形式ではなく、プレーンテキストで表示されます。キーがすでに平文で表示されている場合は、[機密データを暗号化して表示 (Display Sensitive Data as Encrypted)] をクリックしてテキストを暗号化形式で表示することができます。
 - [Apply] をクリックして設定を保存します。

SSH クライアント



(注) このセクションとそのサブセクションは、[Advanced Mode] でのみ使用できます。

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 サーバグループ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。

手順

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 [Global Configuration] で、[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。
- [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。
- [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 [Credentials] で、（どの方式が選択されている場合でも）[Username] を入力するか、またはデフォルトのユーザー名をそのまま使用します。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。
- [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] : 各 SSH サーバタイプの公開キーと秘密キー（暗号化）が表示されます。

（注）

公開/秘密キーは暗号化され、デバイスのメモリに保存されます。キーはデバイス コンフィギュレーション ファイルの一部であり、秘密キーは暗号化形式またはプレーン テキスト形式でユーザに表示できます。

SSH サーバ認証

SSH サーバ認証を有効にし、信頼できるサーバを定義するには、次の手順を実行します。

手順

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。
 - **[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サーバーのユーザーパスワードの変更

SSH クライアントサーバでパスワードを変更すると、リモート SSH サーバにのみ影響します。SSH サーバのパスワードを変更するには、次の手順を実行します。

手順

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。
 - **[Link Local]** : 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。

- [Global] : 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する必要があります。
- 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する必要があります。
- 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。

手順

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



(注) このセクションとそのサブセクションは、[Advanced Mode] でのみ使用できます。

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を受信した場合、こ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あります。

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。

手順

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。

手順

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] を選択します。使用可能なオプションは次のとおりです。

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 秒	統計情報は 30 秒ごとに更新されます。
60 秒	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	(マルチキャストストーム制御についてのみ) 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。

手順

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ブリカント
- オーセンティケーター
- 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/サブリカント、オーセンティケーター、または両方として使用できます。

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。

手順

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 サブ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。

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。

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。

手順

ステップ1 [Security] > [802.1X Authentication] > [Port Authentication] 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 インターフェイスを選択し、以下のパラメータを設定します。

オプション	説明
Interface	ユニットとポートを選択します。
Current Port Control	現在のポート許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。サブ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ブリカントになります。
Administrative Port Control	管理ポートの許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

オプション	説明
	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。
Control Direction	[Control Direction] によって、トラフィックの方向が決まります。以下のいずれかのオプションを選択します。 • [Both] : (デフォルト) スイッチポートはポートが 802.1X または MAC 認証バイパス (MAB) を介して許可されるまで、入力 (着信) トラフィックと出力 (発信) トラフィックの両方をブロックします。 • [Ingress-only] : スイッチポートは入力トラフィックのみをブロックしますが、出力トラフィックは限定的に許可します。
RADIUS VLAN Assignment	選択すると、選択したポート上でダイナミック VLAN 割り当てが有効になります。 • [Disable] : 機能が有効になっていません。 • [Reject] : RADIUS サーバーがサブリカントを許可したのにサブリカント VLAN を提供しなかった場合、そのサブリカントは拒否されます。 • [Static] : RADIUS サーバーがサブリカントを許可したのにサブリカント VLAN を提供しなかった場合、そのサブリカントは許可されます。
Guest VLAN	選択すると、未許可のポートにゲスト VLAN を使用できるようになります。
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、ポート上で 802.1x 認証が有効になります。
MAC-Based Authentication	選択すると、サブリカント 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 サーバのサブリカントのユーザ名とパスワードが、サブリカント 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、サブリカント MAC アドレスに基づく Web ベース認証が有効になります。

オプション	説明
Periodic Reauthentication	選択すると、[再認証期間（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。
Reauthenticate Period	秒単位で値を入力します。（範囲：300～4294967295、デフォルトは3600）
Reauthenticate Now	再認証するにはチェックボックスをオンにします。
Authenticator State	定義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、認証が指定した時間範囲に制限されます。
Time Range Name	[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。
Maximum WBA Login Attempts	Web ベース認証で許可されるログインの最大試行回数を入力します。[無制限（Infinite）] を選択して無制限にするか、[ユーザー定義（User Defined）] を選択して制限を設定します。
Maximum WBA Silence Period	[無制限（Infinite）] を選択して無制限にするか、[ユーザー定義（User Defined）] を選択して制限を設定します。[ユーザー定義（User Defined）] には、範囲（1～4294967295）を入力します。
Max Hosts	このインターフェイスで利用できる、許可されたホストの最大数を入力します。 [無制限（Infinite）] を選択して無制限にするか、[ユーザー定義（User Defined）] を選択して制限を設定します。[ユーザー定義（User Defined）] には、範囲（1～4294967295）を入力します。 （注） 値を 1 に設定すると、複数セッションモードの Web ベース認証に対して単一ホストモードがシミュレートされます。

オプション	説明
Quiet Period	待機期間の長さを秒単位で入力します。
Resending EAP	サブリカント（クライアント）からの、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）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を入力します（単位：秒）。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	送信される EAP 要求の最大数を入力します。定義された期間内に応答が受信されなかった（サブ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。（範囲：1 ～ 10、デフォルト：2）
EAP Max Retries	送信可能な EAP 再試行の最大数を入力します。（範囲：1 ～ 10、デフォルト：2）
EAP Timeout	タイムアウトが発生するまで EAP 応答を待機する最大時間を秒単位で入力します。
Supplicant Timeout	EAP 要求がサブリカントに再送信されるまでの経過時間を入力します（単位：秒）。
Server Timeout:	デバイスが認証サーバーに要求を再送信するまでの経過時間を入力します（単位：秒）。
Supplicant	選択して、デバイスを 802.1x サブリカントとして設定します。 (注) このオプションは、[Supplicant Credentials] でサブリカントが設定されていない場合は使用できません。
Credentials	このサブ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、サブ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	サブリカントが RADIUS サーバーから FAIL 応答を受信してから認証を再開するまで待機する期間を入力します。

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。

手順

ステップ 1 [Security]> [802.1X Authentication]> [Host and Session Authentication] 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 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。
 - [Multiple 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] : サブリカントの 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。

[Host and Session Authentication Table] の [Number of Violations] 列に違反数が表示されます。

サブリカントクレデンシャル



(注) この設定は、詳細モードで使用可能です。

802.1X オーセンティケーター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 サブリカントとして設定できます。このサブリカントは、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。サブ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 サブリカントとして設定されたインターフェイスで利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。

サブ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。

手順

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、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 5 [Display Sensitive Data as Plaintext] をクリックすると、サブリカントクレデンシャルがプレーンテキスト形式で表示されます。

MAC ベース認証設定



(注) この設定は、詳細モードで使用可能です。

MAC ベース認証は、802.1X のサブ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。

手順

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 ベースのサブ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 ベースのサブ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、サブリカント ユーザー名はサブリカント 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、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ブリカントの名前。
- [Port] : ポート番号。
- [Session Time (DD:HH:MM:SS)] : そのポートでサブリカントが認証および認可されていた時間の長さ。
- [Authentication Server] : RADIUS サーバー。
- [MAC アドレス] : サブリカントの MAC アドレスが表示されます。

ロック済みクライアント



(注) この設定は、詳細モードで使用可能です。

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。

手順

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



(注) この設定は、詳細モードで使用可能です。

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。

手順

- 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。エンドユーザー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 label 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] : 現在のロゴ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 label 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 label 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を示されます。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 label 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 label 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。

認証セッション



(注) この設定は、[Advanced Mode] でのみ使用できます。

インターフェイスで認証されたセッションの詳細を表示するには、次の手順を実行します。

手順

ステップ 1 [Security] > [802.1x Authentication] > [Authenticated Sessions] の順に選択します。

ステップ 2 [Authenticated Sessions] テーブルをフィルタリングするには、ドロップダウンメニューからユニットとインターフェイスを選択し、[Go] をクリックします。

ステップ 3 [Authenticated Sessions] テーブルには、インターフェイス上のすべての 802.1x 認証済みセッションに関する次のフィールドが表示されます。

- [Port] : 情報が表示されているポート ID。
- [User Name] : このセッションで認証に使用されるサブリカント名。
- [Mac Address] : サブリカントの MAC アドレスが表示されます。
- [Common Session ID] : このセッションを一意に識別するセッション ID。

ステップ 4 特定のセッションの詳細を表示するには、目的のセッションを選択して、[Details] をクリックします。ポップアップには、メインテーブルに表示されるフィールドに加えて、次のフィールドが表示されます。

- [Supplicant IP Address] : サブリカントの IP アドレス。
- [Reason] : 認証が失敗した理由。セッションステータスが [Unauthorized] に設定されている場合にのみ表示されます。
- [Host Authentication] : インターフェイスに設定されている認証モード。
- [Session Time] : このセッションがアクティブな時間。
- [Accounting Session ID] : アカウンティングセッションのセッション ID。
- [Tagging] : VLAN ID のモードをタグ付きまたはタグなしで表示します。
- [ACL Name 1] : このセッションでインターフェイスに適用される最初の ACL の名前。
- [ACL Type 1] : このセッションでインターフェイスに適用される ACL のタイプ。フィルタ ID (リダイレクトまたはダウンロード可能) を指定できます
- [Redirect URL] : このセッションに指定されたリダイレクト URL。このフィールドは、ACL タイプがリダイレクトの場合にのみ表示されます。

(注)

同じセッションで複数の ACL を適用できます。この場合、[ACL Name 2] ... [ACL Name 3] などの追加情報が表示されます。

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。

手順

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（35 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 \(397 ページ\)](#) 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 \(399 ページ\)](#) 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 \(400 ページ\)](#) 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 \(401 ページ\)](#) 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 \(401 ページ\)](#) 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 of 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。

手順

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 (PPS) (「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



(注) この設定は、詳細モードで使用可能です。

[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。

手順

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] リストに予約済みの 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



(注) この設定は、詳細モードで使用可能です。

[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。

手順

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



(注) この設定は、詳細モードで使用可能です。

[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。

手順

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 Address] : SYN レート保護をユーザー定義する対象の IP アドレスを入力するか、[All addresses] 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 Rate Limit] : 受信する SYN パケットの数 (PPS : 1 秒あたりのパケット数) 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



(注) この設定は、詳細モードで使用可能です。

[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。

手順

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



(注) この設定は、詳細モードで使用可能です。

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。

手順

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



（注） この設定とそのサブセクションは、詳細モードで使用できます。

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）。

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。

手順

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。

手順

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。

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 リレー \(269 ページ\)](#)」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。

手順

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、サブセットを選択し、関連する検索条件を入力してデータをフィルタ処理し、[Retry Now] をクリックします。

ARP インспекション



(注) この設定とそのサブセクションは、詳細モードで使用できます。

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 1A 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 1B 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。

手順

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 \(276 ページ\)](#) 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。

手順

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。

手順

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。

手順

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спекション VLAN 設定

VLAN 上の ARP インспек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。

手順

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спек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



(注) この設定とそのサブセクションは、詳細モードで使用できます。

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 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спек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：

手順

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。

- [Policy Name] : ユーザ定義のポリシー名を入力します。

- [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。
- [Inherited] : VLAN またはグローバル設定の値を使用します。
- [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\(VLAN\) \(422 ページ\)](#)」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\(ポート\) \(423 ページ\)](#)」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

IPv6 RA ガード機能を使用すると、ネットワーク デバイス プラットフォームに到着した不要または不正な RA ガードメッセージを、ネットワーク管理者がブロックまたは拒否できます。デバイスでは RA を使用して、リンクで自身をアナウンスします。IPv6 RA ガード機能は、それらの RA を調査して、承認されていないデバイスから送信された RA を除外します。

ホストモードでは、RA とルータリダイレクトメッセージはポート上ですべてブロックされます。RA ガード機能は、レイヤ 2 (L2) デバイスの構成データを、受信した RA フレーム内のデータと比較します。L2 デバイスは、RA フレームとルータリダイレクトフレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます

[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 :

手順

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 [RA Guard VLAN List] で、RA ガードが有効になっている VLAN を 1 つ以上入力します。

ステップ3 次に、以下の項目を設定します。

- [Minimum 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確認するかどうかを示します。次のいずれかを選択します。
 - [No Limit] : ホップカウント限度の下限の検証を無効にします。
 - [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。
- [Maximum 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確認するかどうかを示します。次のいずれかを選択します。
 - 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。
 - [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。
- [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。次のいずれかを選択します。
 - 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。
- [Other Configuration Flag] : このフィールドは、IPv6 RA ガードポリシー内での、アドバタイズされた他のコンフィギュレーションフラグの検証について指定します。次のいずれかを選択します。
 - 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。
- 最小ルータプリファレンス (Minimal Router Preference) : このフィールドは、RA ガードポリシーで、RA ガードポリシー内で 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指定します。次のいずれかを選択します。
 - 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。
 - 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。

- 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。
- 最大ルータ プリファレンス (Maximal Router Preference) : このフィールドは、RA ガードポリシーで、RA ガードポリシー内で 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指定します。次のいずれかを選択します。
 - 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。
 - 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。
 - 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。

ステップ 4 [RA Guard Policy Table] にポリシーを追加するには、[Add] をクリックして、以下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。
 - [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。
 - [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。
 - [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。
 - [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。
 - [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 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 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 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\(VLAN\) \(422 ページ\)](#)」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\(ポート\) \(423 ページ\)](#)」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：

手順

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、ポリシーがユーザー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。

- [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。
 - [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\(VLAN\) \(422 ページ\)](#)」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\(ポート\) \(423 ページ\)](#)」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：

手順

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。

- [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спек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спек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\(VLAN\) \(422 ページ\)](#) 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\(ポート\) \(423 ページ\)](#) 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：

手順

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、またはエントリ数に制限を設定しない場合は、[No Limit] を選択します。このポリシーに特別な値を設定するには、[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、またはエントリ数に制限を設定しない場合は、[No Limit] を選択します。このポリシーに特別な値を設定するには、[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、またはエントリ数に制限を設定しない場合は、[No Limit] を選択します。このポリシーに特別な値を設定するには、[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。 • 有効化 (Enable) : アドレスの検証を有効にします。 • 無効化 (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) (422 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) (423 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：

手順

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 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 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 5 次のフィールドに入力します。

- [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 6 [Apply] をクリックしてポリシーを接続します。

ステップ 7 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：

手順

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 ポリシーをフィルタ処理するには、[Filter] チェックボックスを選択し、ドロップダウンメニューから [Policy Type] を選択して、[Go] をクリックします。

ステップ 3 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 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。

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 :

手順

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 [Filter] をオンにしてフィルタをアクティブ化し、ドロップダウンリストからポリシータイプを選択します。次に、[Go] をクリックしてデータをフィルタリングします。

ステップ 3 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 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：

手順

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。

- [None] : 何もクリアしません。
- 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ました。
 - DHCP : DHCPv6 プロトコル メッセージから学習しました。
- [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。そのライフタイムは 1 秒未満であるため、その有効期限は表示されません。
 - 有効 (Valid) : ホストの IPv6 アドレスがバインドされました。
- 有効期限 (秒) (Expiry Time (Sec.)) : 確認されない場合、エントリが削除されるまでの残りの秒数。
- [TCAM Overflow] : [No] のマークが付けられたエントリは、TCAM オーバーフローが原因で TCAM に追加されなかったものです。

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。

- 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または LAG。
- [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：

手順

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、[テーブルをクリア (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。

- [None] : 何もクリアしません。
- 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] : プレフィックスが適用される 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。
- 有効期限 (秒) (Expiry Time (Sec)) : エントリが削除されるまでの残り時間。

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。

ステップ 5 次のフィールドを設定します。

- [VLAN ID] : プレフィックスが適用される VLAN ID を選択します。
- [IPv6 Prefix] : IPv6 プレフィックスを入力します。
- [Prefix length] : IPv6 プレフィックス長を入力します。

- [Autoconfig] : オンにすると、ステートレス構成の自動設定が有効になります。

FHS の状態

FHS 機能のグローバル設定を表示するには：

手順

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спекションの状態

現在のVLAN上のNDインспекション状態	現在の VLAN で ND インспекションが有効になっているかどうか。
Device Role	ND インспек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：

手順

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（ポートまたは LAG）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



(注) この設定とそのサブセクションは、詳細モードで使用できます。

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

また、証明書設定機能を使用して、デバイスの HTTPS サーバー証明書チェーンを作成する中間証明書をインポートできます。詳細については、[SSLサーバー認証設定（365 ページ）](#)を参照してください。



- (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。

- [証明書名 (Certificate name)] : 証明書を識別するために使用される文字列。
- [所有者 (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で追加したい場合、またはスイッチのユーザーが証明書を追加したい場合、デバイスの HTTPS サーバー証明書の署名に使用される中間証明書を含むスタティック証明書を追加できます。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。

- [証明書名 (Certificate name)] : 証明書を識別するために使用される文字列。
- [所有者 (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)。証明書をユーザーが追加した場合は「スタティック」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。

手順

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 Type] : 証明書のタイプとして、[root]（デフォルト）または[intermediate]（デバイスの HTTPS サーバー証明書チェーンの一部）を選択します。
- [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。
タイプ	これには、[signer]、[static]、または [dynamic] を選択できます。
CA Type	[Root]、[Intermediate]、または [N/A]（署名者証明書の場合）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。

オプション	説明
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)。
 - [CAタイプが次に等しい (CA Type equals to)] : CA タイプ (ルート) を入力し、[実行 (Go)] をクリックしてフィルタ処理します。
- フィルタをクリアするには、[フィルタのクリア (Clear Filter)] をクリックします。

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 証明書失効リスト

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。

手順

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）（0～160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2～40）。

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 \(435 ページ\)](#)
- [MAC ベースの ACE \(436 ページ\)](#)
- [IPv4 ベース ACL \(438 ページ\)](#)
- [IPv4 ベース ACE \(438 ページ\)](#)
- [IPv6 ベース ACL \(443 ページ\)](#)
- [IPv6 ベース ACE \(443 ページ\)](#)
- [ACL バインディング \(VLAN\) \(447 ページ\)](#)
- [ACL バインディング \(ポート\) \(448 ページ\)](#)
- [インターフェイス ACL ごとの IPv4 \(449 ページ\)](#)

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。

手順

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。設定を永続的に保存するには、[Save] アイコンをクリックします。

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。

手順

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。

オプション	説明
ACL Name	ACE が追加されている ACL の名前が表示されます。
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	一致時に実行され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。
Logging	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。
Time Range	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。
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。時間範囲は システム時刻の設定 セクションで定義します。

オプション	説明
Destination MAC Address	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。
Destination MAC Address Value	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）。
Destination MAC Wildcard Mask	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の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。
Source MAC Address Value	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。
VLAN ID	照合する 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 [含める (Include)] を選択します。
802.1p 値	VLAN 優先順位タグ (VPT) タグに追加する 802.1p 値を入力します。
802.1p マスク	VPT タグに適用するワイルドカードマスクを入力します。
イーサタイプ	照合するフレームのイーサタイプを入力します。

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。

手順

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。

手順

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 Name	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 (150 ページ) ページで再アクティブ化されます。
Logging	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。
Time Range	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。
Time Range Name	[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 (78 ページ) セクションでは、時間範囲について説明します。

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。

Source IP 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。
Source IP Address Value	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。
Source IP Wildcard Mask	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。
Destination IP Address	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。
Destination IP Address Value	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）。
Destination IP Wildcard Mask	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 ～ 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	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の数。
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



(注) この設定は、[詳細モード（Advanced Mode）] ビューでのみ表示されます。

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。

手順

ステップ 1 [Access Control] > [IPv6-Based ACL] 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 [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) この設定は、[詳細モード（Advanced Mode）] ビューでのみ表示されます。



(注) 各 IPv6 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 ACE を定義するには、次の手順を実行します。

手順

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 Name	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。 • [Shutdown] : ACE 基準に一致するパケットをドロップし、パケットの宛先ポートを無効にします。ポートは エラー回復設定 (150 ページ) ページで再アクティブ化されます。
Logging	ACL ルールと一致する ACL フローのログギングを有効にする場合に選択します。
Time Range	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。
Time Range Name	[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 (78 ページ) セクションでは、時間範囲について説明します。

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 • [リストから選択 (Select from list)] : 次のいずれかのオプションから選択します。 • [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。 • [Protocol ID to match] : 照合するプロトコルの ID を入力します。
Source IP Address	すべての送信元アドレスを許可する場合は[任意 (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[ユーザー定義 (User defined)]を選択します。
Source IP Address Value	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プレフィックス長	送信元 IP アドレスのプレフィックス長を入力します。
Destination IP Address	すべての宛先アドレスを許可する場合は[任意 (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[ユーザー定義 (User defined)]を選択します。
Destination IP Address Value	宛先 IP 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プレフィックス値	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。 • [リストから選択] : パケットを照合する 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	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。 • [リストから選択] : パケットを照合する 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。 (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 (Any)]を選択します。または[ユーザー定義 (User defined)]を選択して、ACL で受け入れる特定のフローラベル (範囲 : 0 ~ 1048575) 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	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、[任意] 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を選択します。 • [ICMP Type to Match]：フィルタリングに使用するメッセージタイプの数。
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せんが、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。

手順

ステップ 1 [Access Control] > [VLAN] をクリックします。

ステップ 2 VLAN を編集するには、VLAN を選択し、[Edit] をクリックします。

必要な VLAN が表示されない場合は、[追加 (Add)] をクリックして新しい VLAN を追加します。そして次のステップに進みます。

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 既存の VLAN をコピーするには、[Copy]（コピーアイコン）をクリックします。バインディングテーブルから VLAN を削除する場合は、[Delete] をクリックします。

ステップ 5 [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。

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。デフォルトアクションでは、ACL 内のルールを満たさないすべてのパケットが破棄されます（すべて拒否）。ACL のデフォルトアクションをオーバーライドし、対象のポートに [Permit Any] を設定することで該当のパケットを転送できます。

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。

手順

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])。

インターフェイス	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 のルールアクション ([いずれも拒否 (deny any)] または [いずれも許可 (permit any)])。

ステップ 4 インターフェイスを編集する場合は、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 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 6 [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。

インターフェイス ACL ごとの IPv4

ポートに適用された ACL および ACE の詳細を表示するには、次の手順を実行します。

手順

-
- ステップ 1** [Access Control] > [IPv4 per Interface ACL] の順にクリックし、必要なインターフェイスを選択します。
- ステップ 2** [Filter] セクションで、ドロップダウンメニューから [Interface] を選択し、[Go] をクリックします。選択したインターフェイスに応じて ACL が表示されます。
- ステップ 3** ACL は、選択したインターフェイスに応じて、[IPv4 per Interface ACL] テーブルに表示されます。デフォルト値は、最初のポートに基づいて入力されます。[Protocol]、[Source Port]、[Destination Port]、または [ICMP Type] の値が特定のプロトコル、アプリケーション、または ICMP にマッピングされている場合、列に表示される値はマッピングされた値であり、受信した数値ではありません。
- ステップ 4** [認証済みセッションテーブル (Authenticated Sessions Table)] ボタンをクリックして、[セキュリティ (Security)] > [802.1x 認証 (802.1x Authentication)] > [認証済みセッション (Authenticated Sessions)] の順に選択します。
-



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 \(451 ページ\)](#)
- [QoS 基本モード \(461 ページ\)](#)
- [QoS 拡張モード \(463 ページ\)](#)
- [QoS 統計情報 \(473 ページ\)](#)

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。

手順

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（サービスクラス）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。

手順

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。

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。

手順

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。802.1p プライオリティ値のキューへのマッピングがな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。

手順

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。

手順

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 (kbits/sec)] : 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。
[Committed Information Rate (CIR) (kbits/sec)]	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



(注) 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。

手順

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



(注) 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。

手順

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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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

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、または 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。

手順

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 TCP ポートを選択し、[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。[任意 (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、[ユーザー定義 (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



(注) 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。

手順

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。

グローバル設定



(注) [General] - [QoS Properties] QoS モードが [Advanced] に設定されている場合、このオプションは使用できません。

[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。

手順

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有効化して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。

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。

インターフェイスの設定

[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。

手順

- 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



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

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、関連するポリシーによって適用されます。ポリシーには、シングル ポリシーと集約ポリシーの 2 種類があります。それぞれのポリシーは、QoS 仕様により設定されます。シングル ポリシーは、そのポリシーの 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。集約ポリシーは、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。集約ポリシーは、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、すべてのポリシーに 2 つのしきい値が割り当てられます。1 目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 目目のしきい値に到達すると、ユーザ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。

手順

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 マッピング

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 \(451 ページ\)](#) 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。

手順

ステップ 1 [Quality of Service] > [QoS Advanced Mode] > [Out of Profile DSCP Mapping] をクリックします。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。

手順

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が選択します。

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。

手順

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 \(456 ページ\)](#) 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 \(456 ページ\)](#) 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 \(472 ページ\)](#) 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。

手順

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。

手順

- 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。
Class Map Name	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。

Action Type	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。
Police Type	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是集約ポリサーです。

ステップ 5 [Police Type] が [Aggregate] の場合は、[Aggregate Policer] を選択し、以下の QoS パラメータを入力します。

Ingress Committed Information Rate (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。
Ingress Committed Burst Size (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。

Exceed Action	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。

ステップ 6 [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。

手順

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 インターフェイス（ポートまたは LAG）を選択し、以下を構成します。

- [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 [Enable] を選択して出力ポリシーバインディングを有効化し、以下を構成します。

- [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



- (注) [General] - [\[QoS Properties\]](#) QoS モードが [Basic] に設定されている場合、このオプションは使用できません。

[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。

手順

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。

ステップ 5 [Delete] をクリックしてデータを削除するか、[Clear Counters] をクリックして、シングルポリサー統計テーブルからデータをクリアします。

集約ポリサー統計



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



(注) [General] - [QoS Properties] QoS モードが [Basic] に設定されている場合、このオプションは使用できません。

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。

手順

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。

手順

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 秒] : 統計情報は 30 秒ごとに更新されます。
- [60 秒] : 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 \(477 ページ\)](#)
- [SNMP ビュー \(479 ページ\)](#)
- [SNMP グループ \(480 ページ\)](#)
- [SNMP ユーザー \(482 ページ\)](#)
- [コミュニティ \(484 ページ\)](#)
- [トラップの設定 \(486 ページ\)](#)
- [通知受信者SNMPv1、2 \(486 ページ\)](#)
- [通知受信者SNMPv3 \(488 ページ\)](#)
- [通知フィルタ \(490 ページ\)](#)

エンジン ID



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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す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。

手順

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 アドレスを基にして生成されています。
- 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 アドレスとエンジン 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 Address Type]：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。
 - [Global]：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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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 \(480 ページ\)](#)) 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。

手順

ステップ 1 [SNMP]>[Views] をクリックします。

ステップ 2 [追加 (Add)] をクリックして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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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、各ユーザーが読み取りまたは書き込み可能な内容、および受け取る通知を制御する方法が提供されます。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 \(479 ページ\)](#) 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。

手順

ステップ 1 [SNMP] > [グループ (Groups)] の順にクリックします。

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)] : 選択したビューに対する管理アクセス権限は、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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

SNMPユーザは、ログインクレデンシヤル（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 \(477 ページ\)](#) 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 \(480 ページ\)](#) で定義します。

SNMP ユーザを表示し、新規で定義するには：

手順

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。

コミュニティ



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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：コミュニティのアクセス権限は、読み取り専用、読み取り/書き込み、SNMP 管理者のいずれかに設定できます。また、[SNMP ユーザー（482 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（480 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。

手順

ステップ 1 [SNMP] > [Communities] をクリックします。

ステップ 2 [追加 (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 Management Station	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 Version	[IPv4] または [IPv6] を選択します。

IPv6 Address Type	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。 • [Link Local] : 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。 • [Global] : 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。
IP Address	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。
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。 • [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。 [Read Only] : 管理アクセスは読み取り専用で制限されます。コミュニティに変更を加えることはできません。 [Read Write] : 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。 • [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。 • [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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

[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。

手順

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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

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処理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 \(490 ページ\)](#) 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：

手順

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。

- [Informs IPv4 Source Interface] : ドロップダウンから、IPv4 SNMP サーバーとの通信に使用するトラップメッセージ内で送信元 IPv4 アドレスとして使用するオプション ([Auto] または [VLAN1]) を選択します。
- [Traps IPv4 Source Interface] : ドロップダウンから、IPv4 SNMP サーバーとの通信に使用するトラップメッセージ内で送信元 IPv4 アドレスとして使用するオプション ([Auto] または [VLAN1]) を選択します。
- [Informs IPv6 Source Interface] : ドロップダウンから、IPv6 SNMP サーバーとの通信に使用する通知メッセージ内で送信元 IPv6 アドレスとして使用するオプション ([Auto] または [VLAN1]) を選択します。
- [Traps IPv6 Source Interface] : ドロップダウンから、IPv6 SNMP サーバーとの通信に使用するトラップメッセージ内で送信元 IPv6 アドレスとして使用するオプション ([Auto] または [VLAN1]) 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。

- [Server Definition] : 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 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。
 - [Link Local] : 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。
 - [Global] : 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。

- [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 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。
- [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。
- [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。
- [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。
- [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。
- [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] : トラップに含める情報を定義した SNMP フィルタ ([通知フィルタ \(490 ページ\)](#)) 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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

SNMPv3 で受信者を定義するには：

手順

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。

- [Server Definition] : 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 Address Type] : 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、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。
 - [Global] : 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] : 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) 。
- [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 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。
- [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
- [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。再試行回数 : 範囲 0 ~ 255、デフォルト 3
- [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。
- [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 Level] 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。
- [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



(注) この設定は、[詳細モード (Advanced Mode)] ビューでのみ表示されます。

[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。

手順

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。[オブジェクト ID ツリーフィルタ (Object Identifier Tree Filter)] には、設定された各フィルタのステータスが表示されます。

ステップ 2 [Add] をクリックして通知フィルタを追加するか、[Edit] をクリックして既存の通知フィルタを編集します。

ステップ 3 次のパラメータを入力または変更します。

- [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。
 - [Object ID] : [Include in filter] 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。

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。

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。