アドミニストレーション ガイド

Cisco Sx350、SG350X、SG350XG、Sx550X、および SG550XG シリーズ マネージド スイッチ、ファームウェア リリース 2.3.5.x、バージョン 0.5

Table of Contents

目次

目次

目次

1

はじめに

ここでは、Web ベースの設定ユーティリティの概要について説明します。具体的な内容は次のとおりです。

- Web ベースの設定ユーティリティの開始
- Power over Ethernet（PoE）
- アウトオブバンド ポート
- USB ポート
- 基本表示モードと拡張表示モード
- クイック スタート デバイス設定
- インターフェイス命名規則
- ウィンドウ ナビゲーション
- 検索ファシリティ

Web ベースの設定ユーティリティの開始

ここでは、Web ベースのスイッチ設定ユーティリティの操作方法を説明します。

ポップアップ ブロッカを使用している場合は無効にしてください。

ブラウザについての制約事項

管理ステーションで複数の IPv6 インターフェイスを使用している場合、IPv6 リンクローカル アドレスではなく IPv6 グローバル アドレスを使用して、ブラウザからデバイスにアクセスしてください。

設定ユーティリティの起動

Web ベースの設定ユーティリティを起動するには、次のようにします。

ステップ 1 Web ブラウザを開きます。

ステップ 2 ブラウザのアドレス バーに、設定するデバイスの IP アドレスを入力し、**Enter** キーを押します。

注 デバイスが工場出荷時設定の IP アドレス 192.168.1.254 を使用している場合、システム LED が連続的に点滅します。デバイスが DHCP から割り当てられた IP アドレスや管理者が設定したスタティック IP アドレスを使用している場合は、システム LED は点灯した状態になります。

SG350XG と SG550XG では、デフォルトの IP アドレス 192.168.1.254 がデバイスの OOB ポートに設定されますが、他のデバイスでは、それがデフォルトの VLAN（Vlan 1）に設定されます。OOB ポートに設定されている IP アドレスを使用してデバイスにアクセスする場合、OOB ポートがお使いのネットワークか PC に接続されていることを確認してください。

ログイン

デフォルトのユーザ名/パスワードは、**cisco/cisco** です。デフォルトのユーザ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。

注 GUI の言語をあらかじめ選択していない場合、ログイン ページの言語は、ブラウザで要求されている言語とデバイスに設定されている言語により決定されます。たとえば、ブラウザで中国語が要求されており、中国語がデバイスにロードされている場合、ログイン ページの表示は自動的に中国語になります。中国語がデバイスにロードされていない場合、ログイン ページは英語で表示されます。

デバイスにロードされている言語には、言語と国のコードが指定されています（例：en-US、en-GB、ja-JP など）。ブラウザの要求に基づいてログイン ページを特定の言語で自動的に表示するには、ブラウザが要求する言語と国の両方のコードが、デバイスにロードされている言語のものと一致している必要があります。ブラウザの要求に言語コードしか含まれておらず国コードが含まれない場合（例：fr）、一致する言語コードを持つ最初の組み込み言語が選択されます（国コードのマッチングは行われません。例：fr_CA）。

デバイス設定ユーティリティにログインするには、次のようにします。

ステップ 1 ユーザ名とパスワードを入力します。パスワードは 64 文字までの ASCII 文字で作成できます。パスワード複雑度ルールについては、パスワード強度に説明されています。

ステップ 2 英語を使用しない場合は、[言語] ドロップダウン メニューから目的の言語を選択します。デバイスに新しい言語を追加したり、現在の言語を更新したりするには、「アプリケーション ヘッダー」にある言語メニューに関する説明をご覧ください。

ステップ 3 デフォルト ユーザ ID(**cisco**)とデフォルト パスワード(**cisco**)を使用して初めてログインする場合、またはパスワードの有効期限が切れている場合は、[パスワードの変更] ページが表示されます。追加情報については、「パスワードの有効期限」を参照してください。

ステップ 4 [パスワード強度] ページで [パスワードの複雑度の設定] を選択するかどうかを決定します。

ステップ 5 新しいパスワードを入力し、[適用] をクリックします。

ログインが成功すると、[はじめに] ページが表示されます。

間違ったユーザ名またはパスワードを入力すると、エラー メッセージが表示され、[ログイン] ページのままになります。

ログインのたびに [はじめに] ページが表示されないようにするには、[起動時にこのページを表示しない] を選択します。このオプションを選択すると、[はじめに] ページの代わりに [システムの要約] ページが開きます。

HTTP/HTTPS

[ログイン] をクリックして HTTP セッション(セキュア接続ではない)を開くか、または [セキュアな接続(HTTPS)] をクリックして HTTPS セッション(セキュア接続)を開きます。デフォルトの RSA キーを使用してログオンを承認するように求められ、HTTPS セッションが開きます。

注 [セキュアな接続(HTTPS)] ボタンをクリックする前にユーザ名やパスワードを入力する必要はありません。

HTTPS の設定方法については、SSL サーバをご覧ください。

パスワードの有効期限

次の場合、[新しいパスワード] ページが表示されます。

- デフォルトのユーザ名 **cisco** とパスワード **cisco** で初めてデバイスにアクセスするとき。このページで、工場出荷時のデフォルト パスワードを変更する必要があります。
- パスワードの有効期限が切れると、このページが開き、新しいパスワードを選択するように要求されます。

ログアウト

デフォルトで、アプリケーションは 10 分間非アクティブな状態が続くとログアウトされるようになっています。「アイドル セッション タイムアウトの定義」セクションに説明されている方法で、デフォルト値を変更できます。

注意 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していない場合、デバイスをリブートすると、最後にファイルが保存された後に加えられた変更はすべて削除されます。このセッション中に行った変更を保持するため、ログオフする前に、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に保存してください。

[保存] アプリケーション リンクの左側にある赤く点滅する X アイコンは、実行コンフィギュレーションの変更がまだスタートアップ コンフィギュレーション ファイルに保存されていないことを示しています。[コンフィギュレーションのコピー/保存] ページにある [保存アイコン点滅の無効化] ボタンをクリックすると、点滅を無効にできます。

デバイスが IP 電話などの接続済みデバイスを自動的に検出すると（「Smartport とは」を参照）、ポートがデバイスに合わせて設定されます。この設定コマンドは、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。その結果、特にユーザが設定を変更していない場合でも、ログイン時に [保存] アイコンが点滅し始めます。

[保存] をクリックすると、[コンフィギュレーションのコピー/保存] ページが表示されます。スタートアップ コンフィギュレーション ファイルに実行コンフィギュレーション ファイルをコピーして、保存します。この保存の後は、赤い X アイコンと [保存] アプリケーション リンクは表示されなくなります。

ログアウトするには、ページ右上隅の [ログアウト] をクリックします。システムがデバイスからログアウトされます。

タイムアウトが発生したり、意図的にログアウトしたりすると、メッセージが表示され、[ログイン] ページが開いて、ログアウト状態を示すメッセージが表示されます。ログインすると、アプリケーションは初期ページに戻ります。

表示される初期ページは、[はじめに] ページの [起動時にこのページを表示しない] オプションによって異なります。このオプションを選択していない場合、初期ページは、[はじめに] ページです。このオプションを選択している場合、初期ページは、[システムの要約] ページです。

Power over Ethernet（PoE）

PoE をサポートしているのは一部のデバイスだけです。PoE をサポートしているモデルは次のようにモデル番号の最後に P が付きます。SF350-48HP。

PoE フィールドは、すべての関連ページにその説明がありますが、PoE をサポートしているデバイス上でのみサポートされます。

アウトオブバンド ポート

注 OOB は、SG350XG デバイスと SG550XG デバイスでのみサポートされます。

このスイッチはアウトオブバンド（OOB）ポートをサポートしています。このポートは管理ネットワーク用に使用されます。アウトオブバンド ポートとインバンド ポートは同じ IP ルーティング テーブルを共有するため、インバンド インターフェイスとアウトオブバンド インターフェイス両方に同じサブネットを使用することはできません。

OOB ポートには、基本 MACアドレスやインバンド ポートのアドレスとは異なる MAC アドレスが割り当てられます。この MAC アドレスは、OOB ポート上のスイッチから送信されるすべてのフレーム（IP フレームを含む）内の送信元 MAC アドレスとして使用されます。

このポートに割り当てられる IP アドレスを、インバンド ポートにも同時に割り当てることはできません。また、OOB ポートに割り当てられる IP アドレスは、デバイスのインバンド インターフェイスに設定されているどの IP サブネットにも属することはできません。

デフォルトで、OOB ポートにはデフォルトの IP アドレス 192.168.1.254 が設定されています。このデフォルト IP アドレスは、他のアドレスがダイナミックまたはスタティックに割り当てられていない場合に使用されます。このサブネットは予約されており、インバンド インターフェイスに割り当てることはできません。

ブリッジング

OOB ポートとインバンド レイヤ 2 インターフェイス間のブリッジングはサポートされていません。OOB ポートは VLAN または LAG のメンバーにすることはできません。また、ブリッジのプロトコル（STP や GVRP など）は OOB ポート上で有効にすることはできません。

OOB ポートではタグなしトラフィックしかサポートされません。

ポート設定

次のイーサネット設定が OOB ポート上でサポートされます。

- 速度（10/100/1000）
- デュプレックス
- 自動ネゴシエーション

DHCP クライアント

DHCP クライアント（IPv4 と IPv6）は、デフォルトで、OOB ポートとデフォルト VLAN 上で有効になります。

OOB ポート上のスタティック ルート

スタティック ルートが OOB ポート上でサポートされます。

OOB ポート上の IPv4 アドレス

OOB ポート上では、1 つの IPv4 アドレスしか定義できません。

デフォルトのスタティック IP アドレスは OOB 上でしか設定されません。

IP アプリケーション

以下を除く Telnet や SSH などのすべての IP アプリケーションが OOB ポート上でサポートされます。

- ARP プロキシ
- ルーティング プロトコル
- リレー アプリケーション（DHCP、DHCPv6、および UDP）

QoS と ACL

QoS と ACL は OOB ポート上でサポートされません（そのため、DOS 攻撃防御などの TCAM ベースの機能もすべてサポートされません）。

管理 ACL のみがサポートされます。

スタック サポート

OOB ポート名は、必ず、マスター ユニットの物理 OOB ポートにマップされます。スレーブの物理 OOB ポートは機能しないため、ネイバー デバイスまたは PC に接続されてもリンクを確立しません。

USB ポート

USB ポートは、外部ストレージ（disk-on-key）デバイスの接続に使用できます。このポートは、コンフィギュレーション、SYSLOG、およびイメージ ファイルを保持できます。スタック内では、マスターの USB ポートだけがアクティブになります。USB ポートは FAT32 ファイル システムを完全にサポートし、NTFS ファイル システムを部分的に（読み取りのみ）サポートします。

相対パスと完全修飾パスの両方を使用できます。

システムは、GUI 経由の USB ポート上の次のユーザ アクションをサポートします。

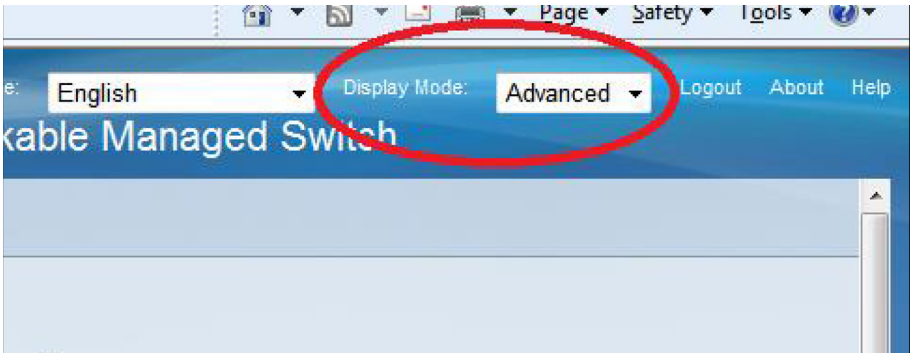
- USB コンテンツの表示
- USB 経由のファイルのコピー（TFTP を使用した場合と同じ）
- USB ファイルの内容の削除、名前の変更、および表示

基本表示モードと拡張表示モード

製品はさまざまな機能をサポートしているため、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割されています。

- [基本]:コンフィギュレーション オプションの基本サブセットが使用可能です。コンフィギュレーション オプションのいずれかが不足している場合は、デバイス ヘッダーで [拡張] モードを選択します。
- [拡張]:コンフィギュレーション オプションがすべて使用可能です。

下の図のように、モード間を移動します。



ユーザが基本から拡張に切り替えると、ブラウザでページがリロードされます。ただし、リロード後は、ユーザ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、ブラウザでページがリロードされます。ページが基本モードでも存在する場合は、ユーザが同じページに留まります。ページが基本モードでは存在しない場合は、ブラウザでユーザが使用していたフォルダの最初のページがロードされます。フォルダが存在しない場合は、[はじめに] ページが表示されます。

拡張コンフィギュレーションが存在し、ページが基本モードでロードされる場合は、ページ レベルのメッセージがユーザに表示されます(たとえば、2 台の RADIUS サーバが設定されていても、基本モードでは 1 台のサーバしか表示できません。また、802.1X 認証に時間範囲が設定されていても、基本モードでは時間範囲を表示できません)。

モードを切り替えると、ページ上で行われたすべての設定(適用なし)が削除されます。

クイック スタート デバイス設定

クイック初期セットアップは、「VLAN 設定ウィザード」で説明されている設定ウィザードを使用するか、[はじめに] ページのリンクを使用して次のように実行できます。

カテゴリ	リンク名 (ページ上)	リンク ページ
初期セットアップ	スタックの管理	各種管理: スタック管理
	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
	デバイス IP アドレスの変更	IPv4 インターフェイス
	VLAN の作成	VLAN 設定
	ポート設定	ポート設定
デバイス ステータス	システム サマリー	システムの要約
	ポート統計情報	インターフェイス
	RMON 統計情報	統計情報
	ログの表示	RAM メモリ
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
	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
	デバイス コンフィギュレーションのバックアップ	ファイル操作
	MAC ベース ACL の作成	MAC ベース ACL の作成
	IP ベース ACL の作成	IPv4 ベース ACL の作成
	QoS の設定	QoS プロパティ
	SPANの設定	スイッチド ポート アナライザ (SPAN および RSPAN)

[はじめに] ページには、シスコの Web ページに移動する 2 つのホット リンクが用意されています。[サポート] リンクをクリックすると、デバイスの製品サポート ページに移動します。[フォーラム] 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。

インターフェイス命名規則

GUI 内で、インターフェイスは次の要素を連結して表示されます。

- **インターフェイスのタイプ:** 次のタイプのインターフェイスは、さまざまなタイプのデバイスに存在します。
  - **ファスト イーサネット（10/100 ビット）**:**FE** と表示されます。350 ファミリでのみサポートされます。
  - **ギガビット イーサネット ポート（10/100/1000 ビット）**:**GE** と表示されます。350 ファミリでのみサポートされます。
  - **10 ギガビット イーサネット ポート（1000/10,000 Mbps）**:**XG** と表示されます。
  - **アウトオブバンド ポート**:**OOB** と表示されます。
  - **LAG（ポート チャネル）**:**LAG** と表示されます。
  - **VLAN**:**VLAN** と表示されます。
  - **トンネル**:**Tunnel** と表示されます。
- **ユニット番号**: スタック内のユニット番号。ユニット番号とインターフェイス番号の組み合わせによってポートが識別されます。たとえば、GE1/0/4 はスタックの最初のユニットのポート番号 4 です。
- **スロット番号**: スロット番号は常に 0 です。
- **インターフェイス番号:** ポート、LAG、トンネル、または VLAN ID。

ウィンドウ ナビゲーション

ここでは、Web ベースのスイッチ設定ユーティリティの機能を説明します。

アプリケーション ヘッダー

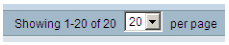
各ページにアプリケーション ヘッダーが表示されます。次のアプリケーション リンクが含まれています。

アプリケーション リンク名	説明
	[保存] アプリケーション リンクの左側にある赤く点滅する X アイコンは、実行コンフィギュレーションの変更がまだスタートアップ コンフィギュレーション ファイルに保存されていないことを示しています。赤い X アイコンの点滅は、[コンフィギュレーションのコピー/保存] ページで無効にできます。 [コンフィギュレーションのコピー/保存] ページを表示するには、[保存] をクリックします。デバイスのスタートアップ コンフィギュレーション ファイル タイプに実行コンフィギュレーション ファイルをコピーして、保存します。この保存の後は、赤い X アイコンと [保存] アプリケーション リンクは表示されなくなります。デバイスをリブートすると、スタートアップ コンフィギュレーション ファイル タイプが実行コンフィギュレーションにコピーされ、実行コンフィギュレーション内のデータに従ってデバイス パラメータが設定されます。
[ユーザ名]	デバイスにログインしているユーザの名前が表示されます。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)。

アプリケーション リンク名	説明
[言語メニュー]	このメニューには、次のオプションがあります。 • [言語の選択]: メニューに表示される言語の中から 1 つ選択します。この言語は、Web ベースの設定ユーティリティの言語になります。 • [言語のダウンロード]:デバイスに新しい言語を追加します。 • [言語の削除]:デバイスの第 2 言語を削除します。第 1 言語(英語)は削除できません。 注 言語ファイルをアップグレードするには、[ファームウェア/言語のアップグレード/バックアップ] ページを使用します。
[ログアウト]	クリックすると、Web ベースのスイッチ設定ユーティリティからログアウトします。
[バージョン情報]	クリックすると、デバイス名とデバイスのバージョン番号が表示されます。
[ヘルプ]	クリックすると、オンライン ヘルプが表示されます。
	重大度のレベルが [重要] より高い SYSLOG メッセージが記録されると、SYSLOG アラート ステータス アイコンが表示されます。[RAM メモリ] ページを開くには、このアイコンをクリックします。このページにアクセスした後は、SYSLOG アラート ステータス アイコンは表示されなくなります。アクティブな SYSLOG メッセージがない場合にこのページを表示するには、[ステータスと統計情報] > [ログの表示] > [RAM メモリ] の順にクリックします。

管理ボタン

システムのさまざまなページに表示され、よく使用されるボタンを次の表に示します。

ボタン名	説明
	プルダウン メニューを使用して、ページごとにエントリ数を設定します。
	必須フィールドを示します。
[追加]	クリックすると、関連する [追加] ページが表示され、テーブルにエントリを追加できます。情報を入力し、[適用] をクリックして、実行コンフィギュレーションに保存します。[閉じる] をクリックし、メインページに戻ります。[コンフィギュレーションのコピー/保存] ページを表示して、デバイスのスタートアップ コンフィギュレーション 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には、[保存] をクリックします。
[適用]	クリックすると、変更がデバイスの実行コンフィギュレーションに適用されます。デバイスを再起動すると、実行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 ファイル タイプか別のファイル タイプに保存していない限り、失われます。[コンフィギュレーションのコピー/保存] ページを表示して、デバイスのスタートアップ コンフィギュレーション 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には、[保存] をクリックします。
[キャンセル]	クリックすると、ページ上で行われた変更がリセットされます。
[クリア]	ページ上の情報をクリアします。
[フィルタのクリア]	クリックすると、表示される情報を選択するためのフィルタがクリアされます。
[すべてのインターフェイスカウンタのクリア]	クリックすると、すべてのインターフェイスの統計情報カウンタがクリアされます。
[インターフェイスカウンタのクリア]	クリックすると、選択したインターフェイスの統計情報カウンタがクリアされます。
[ログのクリア]	ログ ファイルをクリアします。

ボタン名	説明
[テーブルのクリア]	テーブル エントリをクリアします。
[閉じる]	メインページに戻ります。実行コンフィギュレーションに適用されていない変更があった場合、メッセージが表示されます。
[設定のコピー]	テーブルには、通常、コンフィギュレーション設定を含む 1 つ以上のエントリが含まれます。各エントリを個別に変更するのではなく、次のように、1 つのエントリを変更し、そのエントリを選択して複数のエントリにコピーすることができます。 1. コピーするエントリを選択します。[設定のコピー] をクリックすると、ポップアップが表示されます。 2. [コ1。ピー先] フィールドに宛先エントリ番号を入力します。 3. 変更を保存するには、[適用] をクリックします。メインページに戻るには、[閉じる] をクリックします。
[削除]	テーブルのエントリを選択して [削除] をクリックすると、そのエントリが削除されます。
[詳細]	クリック..すると、選択したエントリに関連付けられている詳細が表示されます。
[編集]	エントリを選択し、[編集] をクリックします。[編集] ページが表示され、エントリを変更できます。 1. [適用] をクリックし、実行コンフィギュレーションに変更を保存します。 2. [閉じる] をクリックし、メインページに戻ります。
[実行]	クエリ フィルタリング条件を入力し、[実行] をクリックします。ページに結果が表示されます。
[更新]	[更新] をクリックすると、カウンタ値が更新されます。
[テスト]	[テスト] をクリックすると、関連するテストが実行されます。
[デフォルトの復元]	工場出荷時のデフォルトを復元する場合に、[デフォルトに戻す] をクリックします。

検索ファシリティ

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、関連するページへのリンクだけでなく、関連するヘルプページへのリンクも表示されます。

検索機能にアクセスするには、キーワードを入力して、虫めがねアイコンをクリックします。キーワードのCDP を検索した結果の例を以下に示します。

基本モードでは、拡張モードのページへのリンクが表示されますが、使用することはできません。

2

ダッシュボード

ダッシュボードは 8 個の四角形の集合で、初めは空ですが、さまざまなタイプの情報を入力できます

使用可能なモジュールから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。

ダッシュボードを読み込むと、ダッシュボードに選択したモジュールがグリッドの所定の場所に読み込まれます。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定期的に更新されます。モジュールによっては、この間隔を設定することができます。

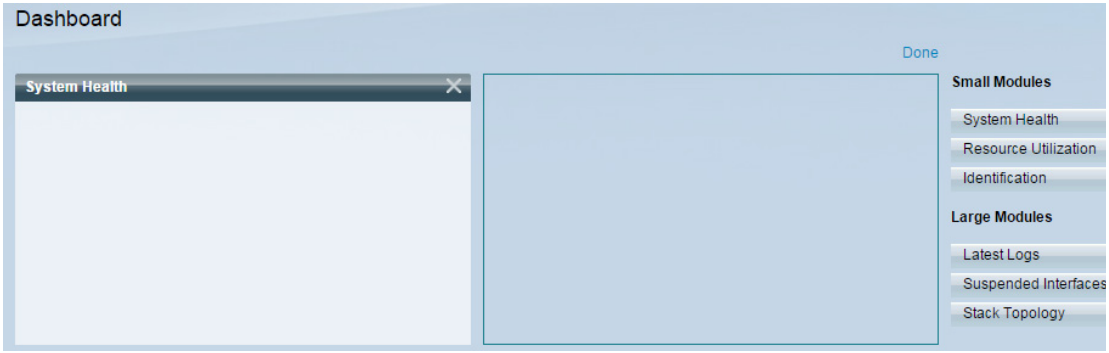
この章では以下のトピックを取り上げます。

- グリッド管理
- システム ヘルス
- リソース使用率
- 識別
- ポート使用率
- PoE 使用率
- 最新のログ
- 一時停止されたインターフェイス
- スタック トポロジ
- トラフィック エラー

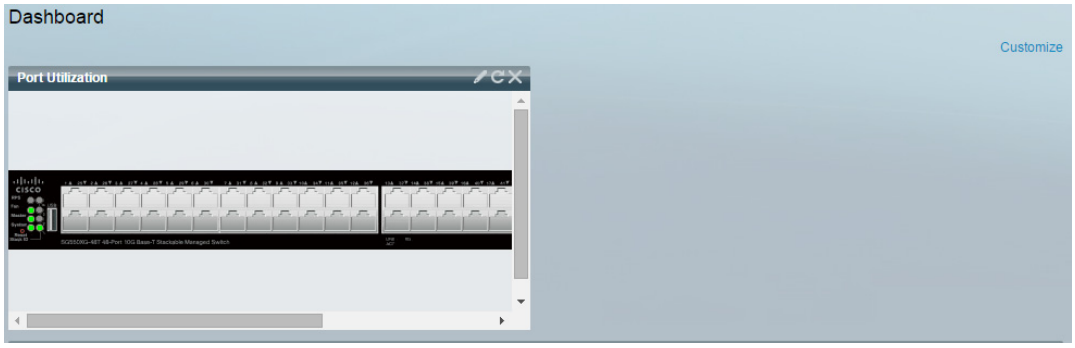
グリッド管理

ダッシュボードは複数のモジュールで構成されますが、同時に表示できるのは 1 つのモジュールのサブセットだけです。

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（下図参照（下のスクリーン キャプチャでは 2 つの四角形だけ表示））。



現在非表示になっているモジュールを表示するには、ダッシュボードの右上にある [カスタマイズ] をクリックします（下図参照）。



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 ドロップして、グリッドにモジュールを追加します。

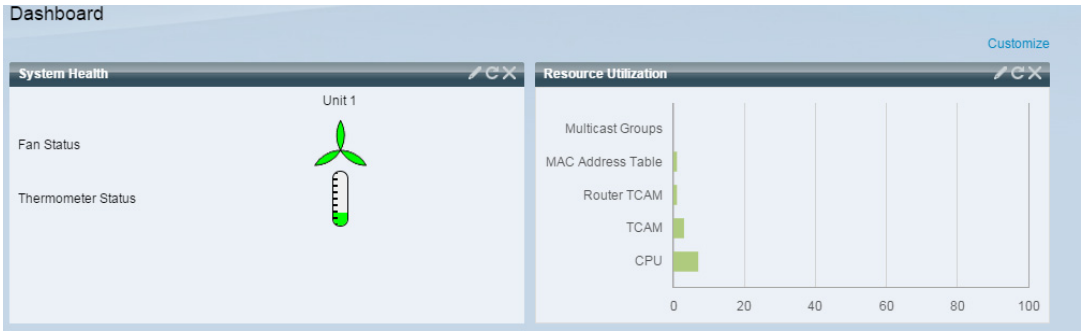
モジュールは次のグループに分かれています。

- **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、新しいモジュールが古いモジュールに置き換わります。

グリッド内のモジュールの配置を再調整するには、使用しているグリッド位置から別の位置へドラッグします。このモジュールは、未使用の場所にドロップすることも、同じサイズのモジュールによって使用されている場所にドロップすることもできます。選択した場所が使用済みの場合、モジュールの位置が入れ替わります。

右隅にある [完了] をクリックした場合にだけ、関連する情報がモジュールに読み込まれます(下図参照)。



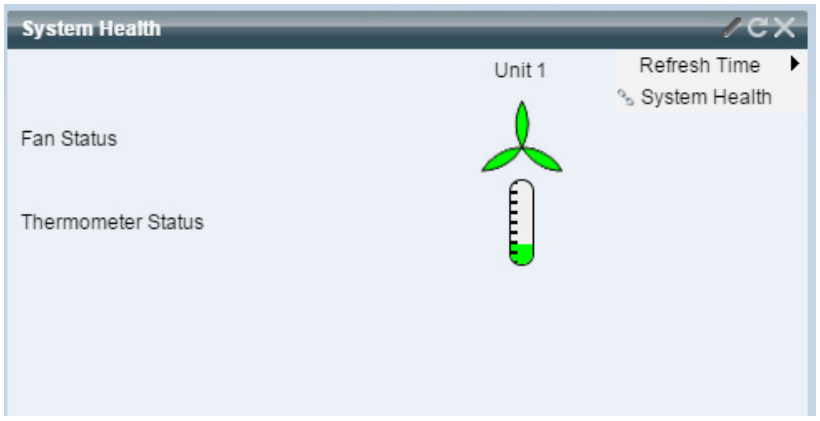
ダッシュボードに含まれる各モジュールのタイトル バーには、モジュールのタイトルと 3 つのボタンが表示されます。

これらのボタンの機能は次のとおりです。

- 鉛筆 :コンフィギュレーション 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。

システム ヘルス

このモジュールは、スタンドアロン デバイスまたはスタック内の各デバイスのデバイス温度(そのような情報が入手可能な場合)を表示します(下図参照)。



次のアイコンが表示されます。

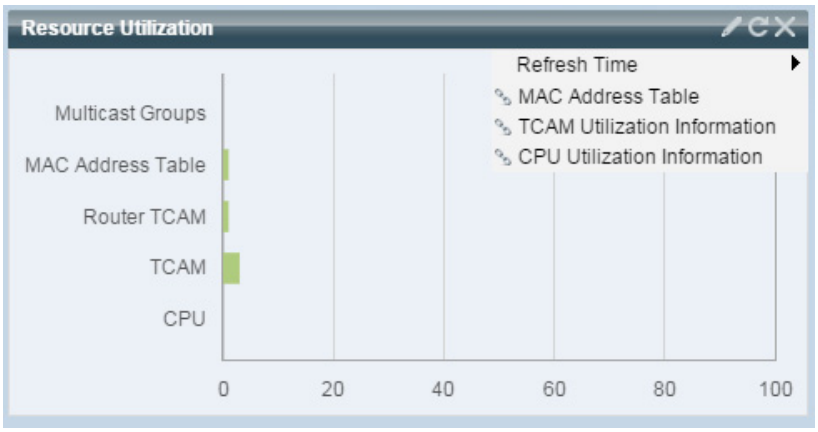
- [ファンステータス]:1 つのファンが故障し、冗長ファンでバックアップされている場合は黄色。ファンが動作中の場合は緑色。ファンが故障している場合は赤色。
- [温度計ステータス]
  - *適正温度*:緑色(温度計の目盛:ほぼ 0)。
  - *警告発生温度*:黄色(温度計の目盛:半分)。
  - *危険温度*:赤色(温度計の目盛:最大)。

次のコンフィギュレーション オプション(右上の鉛筆アイコン)が使用可能です。

- [リフレッシュ時間]:表示されたオプションのいずれかを選択します。
- [システムヘルス]:クリックすると [ヘルスと電力] ページが開きます。

リソース使用率

このモジュールには、さまざまなシステム リソースの利用状況がパーセント表示の横棒グラフ形式で表示されます、下図のように表示されます。



次のリソースを監視できます。

- [マルチキャストグループ]: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 アドレス テーブル]:使用中の MAC アドレス テーブルのパーセンテージ。
- [ルータ TCAM]:ルータ TCAM の使用率。

- [TCAM]:すべての非 IP TCAM エントリの使用率。
- [CPU]:CPU の使用率。

リソース使用率が 80 % を超えると、その横棒が赤色になります。

横棒上にカーソルをポイントすると、使用率の数値情報(使用済みリソース/最大使用可能リソース)を表すツールチップが表示されます。

次のコンフィギュレーション オプション(右隅)が使用可能です。

- [リフレッシュ時間]:表示されたオプションのいずれかを選択します。
- [マルチキャストグループ]:クリックすると [MAC グループ アドレス] が開きます。
- [MACアドレステーブル]:クリックすると [ダイナミック アドレス] が開きます。
- [TCAM 使用率情報]:クリックすると [TCAM 利用率] が開きます。
- [CPU 使用率情報]:クリックすると [CPU 利用率] が開きます。

識別

このモジュールには、デバイスとスタック(下図参照)に関する基本情報が表示されます。

次のフィールドが表示されます。

- [システムの説明]:デバイスの説明を表示します。
- [ホスト名]:[システム設定] ページで入力した情報かデフォルトの情報が使用されます。[開始ウィザード] で追加することもできます。

- [ファームウェア バージョン]:デバイス上で実行している現在のファームウェア バージョン。
- [MACアドレス(マスターユニット)]:ユニットの MAC アドレス。
- [シリアル番号(マスター ユニット)]:ユニットのシリアル番号。
- [システム ロケーション]:デバイスの物理的な場所を入力します。
- [システム コンタクト先]:連絡先の担当者名を入力します。
- [総有効電力]:デバイスに使用可能な電力量。
- [現在の電力消費量]:デバイスで消費される電力量。

次のコンフィギュレーション オプション(右隅)が使用可能です。

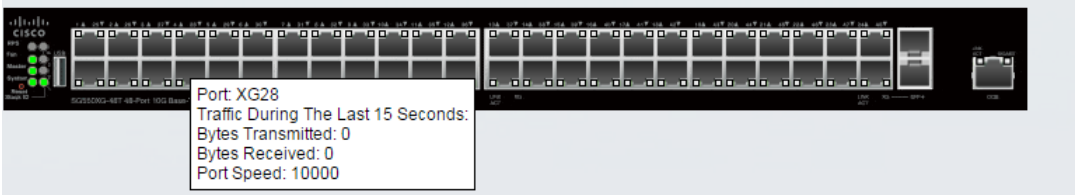
- [リフレッシュ時間]:表示されたオプションのいずれかを選択します。
- [システム設定]:クリックすると [システム設定] が開きます。
- [システムの要約]:クリックすると [システムの要約] が開きます。

ポート使用率

このモジュールには、デバイス上のポートがデバイス ビューまたはチャート ビューのどちらかで表示されます。ビューはコンフィギュレーション オプション(右上の鉛筆アイコン)で選択されます。

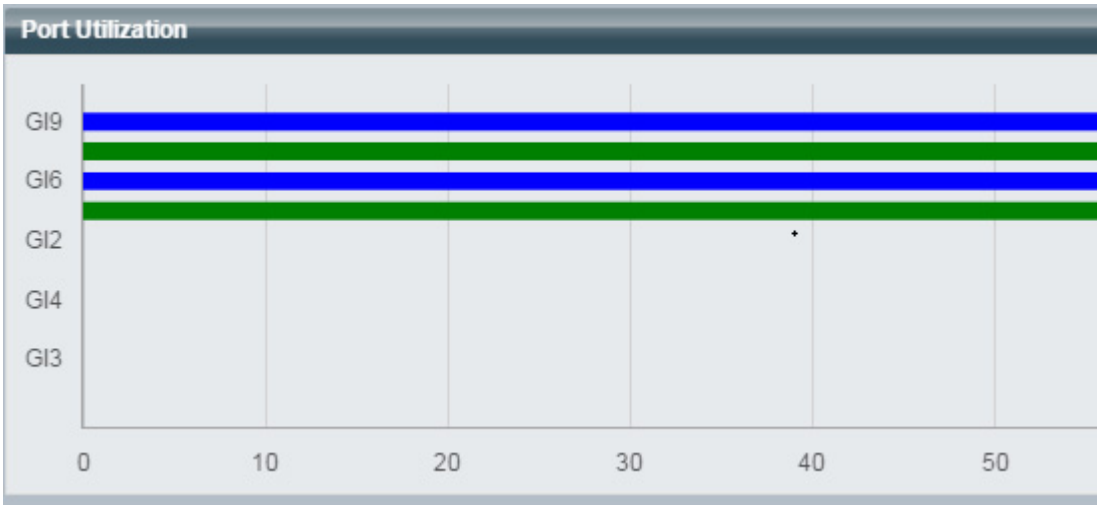
- **表示モード - デバイス ビュー**

  デバイスが表示されます。ポートにマウスを合わせるとそのポートに関する情報が表示されます。



- **表示モード - チャート ビュー**

  ポートのリストが表示されます。ポート使用率がバー形式で表示されます。



  ポートごとに、以下のポート使用率情報が表示されます。

  送信—%（緑色）

  受信—%（青色）

- [リフレッシュ時間]：表示されたオプションのいずれかを選択します。
- [インターフェイスの統計情報]：[ステータスと統計情報] > [インターフェイス] ページへのリンク。

PoE 使用率

このモジュールには、次の図のように、PoE の利用状況がグラフィック形式で表示されます。(下図参照)。

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 の値のダイヤルが付いた計器が表示されます。ダイヤル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、そのユニットの実際の 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。

追加のビューはコンフィギュレーション オプション(右上の鉛筆アイコン)で選択できます。

- [リフレッシュ時間]:表示されたオプションのいずれかを選択します。
- [PoE グローバル プロパティ]:[ポート管理] -> [PoE] -> [プロパティ] ページへのリンク。
- [PoE ポート設定]:[ポート管理] -> [PoE] -> [設定] ページへのリンク。

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表示されます（下図参照）。

次のコンフィギュレーション オプション（右隅）が使用可能です。

- [重大度しきい値]:「ログ設定」を参照。
- [リフレッシュ時間]: 表示されたオプションのいずれかを選択します。
- [ログの表示]: クリックすると [RAM メモリ] が開きます。

注　詳細については、「ログの表示」を参照してください。

一時停止されたインターフェイス

このモジュールには、中断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。ビューはコンフィギュレーション オプション（右上の鉛筆アイコン）で選択されます。

- **デバイス ビュー**

  このビューには、デバイスが表示されます。下図を参照してください。

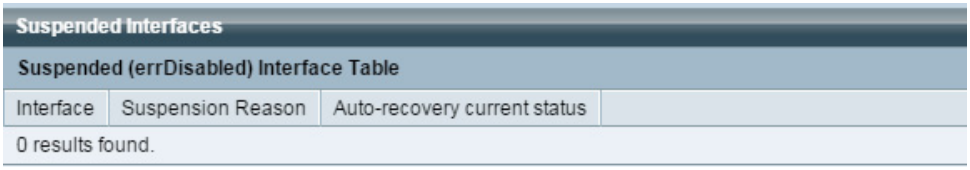
  ユニットどうしがスタック内で接続されている場合、ドロップダウン セレクタで、表示するデバイスを選択できます。デバイス内の中断されたポートすべてが赤色で表示されます。

中断されたポートにカーソルをポイントすると、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、ポートの LAG ID。
- 中断されている場合は、保留理由。

- **テーブル ビュー**

  テーブル ビューの場合、特定のスタック ユニットを選択する必要はありません。情報が表形式で表示されます（下図参照）。



  次のフィールドが表示されます。

  - [インターフェイス]: 中断されたポートまたは LAG
  - [保留理由]: インターフェイスが中断された理由
  - [現在のステータスの自動修復]: 中断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。

次のコンフィギュレーション オプション（右隅）が使用可能です。

- [表示モード]:[デバイスビュー] または [テーブルビュー] のどちらかを選択します。
- [リフレッシュ時間]: 表示されたオプションのいずれかを選択します。
- [エラー復旧設定]: クリックすると [エラー回復設定] が開きます。

スタック トポロジ

注 スタック構成は、デバイスの SG350 ファミリ（Sx350 を除く）と SG550 ファミリでのみサポートされます。

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、[スタック管理] 画面の [スタックトポロジビュー] セクションと同じです。下図のように表示されます。

次のフィールドが表示されます。

- [スタックトポロジ]: チェーンまたはリングのどちらか（スタック トポロジのタイプを参照）。
- [スタックマスター]: スタックのマスター ユニットとして機能しているユニットの番号。

モジュール内のユニットにカーソルをポイントすると、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カーソルをポイントすると、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。

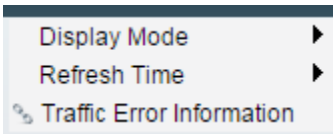
次のコンフィギュレーション オプション（右隅）が使用可能です。

- [スタック管理]: クリックすると [スタック管理] が開きます。

トラフィック エラー

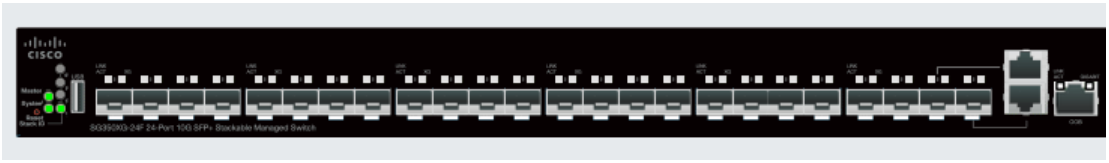
このモジュールには、RMON 統計情報に関してカウントされたさまざまなタイプのエラー パケットの数が表示されます。ビューはコンフィギュレーション オプション（右上の鉛筆アイコン）で選択されます。

鉛筆アイコンから次を選択できます。



- **表示モード - デバイス ビュー**

  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（下図参照）。



  スタッキング モードの場合、ドロップダウン セレクタで、表示するデバイスを選択できます。デバイス内の中断されたポートすべてが赤色で表示されます。

  中断されたポートにカーソルをポイントすると、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、ポートの LAG ID。
  - 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。

- **表示モード - テーブル ビュー**

  - *インターフェイス*: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。

- [リフレッシュ時間]:いずれかのリフレッシュレートを選択します。
- [トラフィックエラー情報]:リンクをクリックすると、[統計情報] ページが開きます。

3

設定ウィザード

ここでは、次の設定ウィザードについて説明します。

具体的な内容は、次のとおりです。

- 開始ウィザード
- VLAN 設定ウィザード
- ACL ウィザード

開始ウィザード

このウィザードは、デバイスの初期設定を支援します。

ステップ 1 [設定ウィザード] > [開始ウィザード] の順にクリックします。

ステップ 2 [ウィザードを起動] をクリックしてから、[次へ] をクリックします。

ステップ 3 次のフィールドを入力します。

- [システム ロケーション]:デバイスの物理的な場所を入力します。
- [システム コンタクト先]:連絡先の担当者名を入力します。
- [ホスト名]:このデバイスのホスト名を選択します。これは CLI コマンドのプロンプトで使用されます。
  - [デフォルトを使用]:これらのスイッチのデフォルト ホスト名(システム名)は、switch123456 で、123456 は 16 進数のデバイス MAC アドレスの下位 3 バイトになります。
  - [ユーザ定義]:ホスト名を入力します。文字、数字、およびハイフンのみ使用できます。ホスト名の開始または終了はハイフンにできません。その他の記号、句読点、ブランクも使用できません(RFC1033、1034、1035 の規定により)。

ステップ 4 [次へ] をクリックします。

ステップ 5 次のフィールドを入力します。

- [インターフェイス]:システムの IP インターフェイスを選択します。
- [送信元IPインターフェイス]:次のいずれかのオプションを選択します。
  - [DHCP]:デバイスが DHCP サーバから IP アドレスを受信する場合に選択します。
  - [スタティック]: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。

[送信元 IP インターフェイス] として [スタティック] を選択した場合は、次のフィールドに値を入力します。

- [IPアドレス]:インターフェイスの IP アドレス。
- [ネットワークマスク]:このアドレスの IP マスク。
- [管理デフォルトゲートウェイ]:デフォルト ゲートウェイの IP アドレスを入力します。
- [DNSサーバ]:DNS サーバの IP アドレスを入力します。

ステップ 6 [次へ] をクリックします。

ステップ 7 次のフィールドを入力します。

- [ユーザ名]:1 ～ 20 文字の新しいユーザ名を入力します。UTF-8 文字は使用できません。
- [パスワード]:パスワードを入力します(UTF-8 文字は使用できません)。パスワードの強度と複雑度が定義されている場合、ユーザ パスワードは、パスワード強度で設定されたポリシーに従う必要があります。
- [パスワードの確認]:パスワードを再び入力します。
- [パスワード強度]:パスワードの強度が表示されます。パスワードの強度と複雑度に関するポリシーは、[パスワード強度] ページで設定します。
- [現在のユーザ名とパスワードを維持する]:現在のユーザ名とパスワードを維持する場合に選択します。

ステップ 8 [次へ] をクリックします。

ステップ 9 次のフィールドを入力します。

- [クロックソース]:次のいずれかのオプションを選択します。
  - [手動設定]:デバイス システム時刻を入力する場合に選択します。これを選択した場合、[日付] と [時刻] を入力します。

- [デフォルトSNTPサーバ]:デフォルト SNTP サーバを使用する場合に選択します。

注 デフォルト SNTP サーバは名前で定義されるため、DNS を設定して動作可能にする必要があります(DNS サーバを設定して到達可能にする)。これは、[DNS 設定] で行います。

- [手動SNTPサーバ]:SNTP サーバの IP アドレスを入力する場合に選択します。

ステップ 10 [次へ] をクリックして、入力したコンフィギュレーションの概要を表示します。

ステップ 11 [適用] をクリックして、構成データを保存します。

VLAN 設定ウィザード

このウィザードは、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。最初のステップは、トランク ポート モード(タグ付きとタグなしのトランク ポートを設定する)が対象で、その後で、アクセス ポート モードを設定します。

ステップ 1 [設定ウィザード] > [VLAN設定ウィザード] の順にクリックします。

ステップ 2 [ウィザードを起動] をクリックしてから、[次へ] 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(グラフ表示内の必要なポートをクリックすることによって)。すでにトランク ポートとして設定されているポートが事前に選択されます。

ステップ 4 [次へ] をクリックします。

ステップ 5 次のフィールドを入力します。

- [VLAN ID]:設定する VLAN を選択します。既存の VLAN または**新しい VLAN** を選択できます。
- [新しいVLAN ID]:新しい VLAN の VLAN ID を入力します。
- [VLAN名]: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(グラフ表示内の必要なポートをクリックすることによって)。このステップで選択されなかったトランク ポートは、VLAN のタグ付きメンバーになります。

ステップ 7 [次へ] をクリックします。

ステップ 8 VLAN のアクセス ポートに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(グラフ表示内の必要なポートをクリックすることによって)。

ステップ 9 [次へ] をクリックして、入力した情報の概要を表示します。

ステップ 10 [適用] をクリックします。

ACL ウィザード

新しい ACL を作成するには、次のようにします。

ステップ 1 [設定ウィザード] > [ACLウィザード] の順にクリックします。

ステップ 2 [次へ] をクリックします。

ステップ 3 次のフィールドを入力します。

- [ACL名]:新しい ACL の名前を入力します。
- [ACLタイプ]:ACL のタイプを選択します。[IPv4] または [MAC]。

ステップ 4 [次へ] をクリックします。

ステップ 5 次のフィールドを入力します。

- [一致したときのアクション]:オプションのいずれかを選択します。
  - [トラフィックの許可]:ACE 条件に一致するパケットを転送します。
  - [トラフィックの拒否]:ACE 条件に一致するパケットをドロップします。
  - [インターフェイスのシャットダウン]:ACE 条件に一致するパケットをドロップし、パケットが受信されたポートを無効にします。このポートは、[エラー回復設定] ページから再アクティブ化できます。

ステップ 6 MAC ベース ACL の場合は、次のフィールドに値を入力します。

- [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 [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。

- [送信元MAC値]:送信元 MAC アドレスの照合に使用する MAC アドレスを入力します。必要に応じて、マスクも入力します。
- [送信元MACワイルドカードマスク]:MAC アドレスの範囲を定義するためのマスクを入力します。
- [宛先 MAC アドレス]:すべての宛先アドレスを許可する場合は [任意] を選択します。宛先アドレスを入力するか宛先アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先MAC値]:宛先 MAC アドレスの照合に使用する MAC アドレスを入力します。必要に応じて、マスクも入力します。
- [宛先 MAC ワイルドカード マスク]:MAC アドレスの範囲を定義するためのマスクを入力します。このマスクは、サブネット マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、**1** に設定したビットの値はマスクせず、**0** に指定したビットの値はマスクします。

  注 0000 0000 0000 0000 0000 0000 1111 1111 というマスクを例に説明します。0 になっているビットの一致は照合され、1 になっているビットの一致は照合されません。1 を 10 進数の整数に変換し、4 つずつの 0 をまとめて 0 として記述する必要があります。この例では、1111 1111 = 255 で、マスクは 0.0.0.255 と記述されます。

- [時間範囲名]:[時間範囲] 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。このフィールドは、[時間範囲] が事前に定義されている場合にのみ表示されます。

ステップ 7 IPv4 ベース ACL の場合は、次のフィールドに値を入力します。

- [プロトコル]:特定のプロトコルに基づく ACL を作成するための次のオプションのいずれかを選択します。
  - [任意(IP)]:すべての IP プロトコル パケットを受け入れます。
  - [TCP]:伝送制御プロトコル パケットを受け入れます。
  - [UDP]:ユーザ 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用の送信元ポート]:ドロップダウン リストからポートを選択します。
- [TCP/UDP用の宛先ポート]: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 [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [送信元 IP 値]:送信元 IP アドレスの照合に使用する IP アドレスを入力します。
- [送信元 IP ワイルドカード マスク]:IP アドレスの範囲を定義するためのマスクを入力します。このマスクは、サブネット マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、1 に設定したビットの値はマスクせず、0 に指定したビットの値はマスクします。
- [宛先IPアドレス]:すべての送信元アドレスを許可する場合は [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先IP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。
- [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 マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、1 に設定したビットの値はマスクせず、0 に指定したビットの値はマスクします。
- [時間範囲名]:[時間範囲] 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。このフィールドは、[時間範囲] が事前に定義されている場合にのみ表示されます。

ステップ 8 [次へ] 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。別のルールを追加するには、[このACLに別のルールを追加する] をクリックします。

ステップ 10 [次へ] をクリックして、ACL バインディング情報を入力します。

- [バインディングタイプ]:ACL をバインドするための次のオプションのいずれかを選択します。
  - [物理インターフェイスのみ]:ACL をポートにバインドします。この場合は、ACL をバインドするポートをクリックします。
  - [VLANのみ]:ACL を VLAN にバインドします。[ACLをバインドするVLANのリストの入力] 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。

[適用] をクリックします。

4

ステータスと統計情報

ここでは、デバイスの統計情報を表示する方法について説明します。

具体的な内容は、次のとおりです。

- システムの要約
- CPU 利用率
- インターフェイス
- Etherlike
- ポート使用率
- GVRP
- 802.1X EAP
- ACL
- TCAM 利用率
- ヘルスと電力
- スイッチド ポート アナライザ（SPAN および RSPAN）
- 診断
- RMON
- sFlow
- ログの表示

システムの要約

[システムの要約] ページには、デバイスのグラフ、デバイスの状態、ハードウェア情報、ファームウェア バージョン情報、一般的な PoE ステータスなどが表示されます。

システム情報を表示するには、[ステータスと統計情報] > [システムの要約] の順にクリックします。

システム情報

- [システムの説明]:システムの説明。
- [システム ロケーション]:デバイスの物理的な場所。この値を入力するには、[編集] をクリックし、[システム設定] ページに移動します。
- [システムコンタクト先]:コンタクト先の担当者名。この値を入力するには、[編集] をクリックし、[システム設定] ページに移動します。
- [ホスト名]:デバイスの名前。この値を入力するには、[編集] をクリックし、[システム設定] ページに移動します。デフォルトでは、デバイスのホスト名は、switch という単語と、デバイス MAC アドレスの下位 3 バイト（16 進数値の右側 6 桁）を連結したものになります。
- [システムオブジェクト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のベンダー ID（SNMP で使用される）。
- [システム稼動時間]:最後の再起動から経過した時間。
- [現在時刻]:現在のシステム時刻。
- [基本 MAC アドレス]:デバイスの MAC アドレス。スタック内に複数のユニットが存在する場合、マスター ユニットの基本 MAC アドレスが表示されます。
- [ジャンボフレーム]:ジャンボ フレームのサポート状態。このサポートは、[ポート設定] ページで有効または無効にできます。

  注 ジャンボ フレームを動作させるには、有効にした後、デバイスを再起動する必要があります。

ソフトウェア情報

- [ファームウェア バージョン(アクティブ イメージ)]:アクティブ イメージのファームウェア バージョン番号。

  注 スタックでは、マスターのバージョンに基づいてファームウェア バージョン番号が表示されます。

- [ファームウェアのMD5チェックサム(アクティブイメージ)]:アクティブ 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)]:非アクティブ 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、マスター 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)]:非アクティブ イメージの MD5 チェックサム。

  注 次の 3 つのフィールドは、デバイス上の言語ごとに 1 回ずつ計 2 回表示される可能性があります。
- [ロケール]:第 1 言語のロケール。(常に英語に設定されています)。
- [言語バージョン]:第 1 言語または英語の言語パッケージ バージョン。
- [言語の MD5 チェックサム]:言語ファイルの MD5 チェックサム。

TCP/UDP サービスのステータス

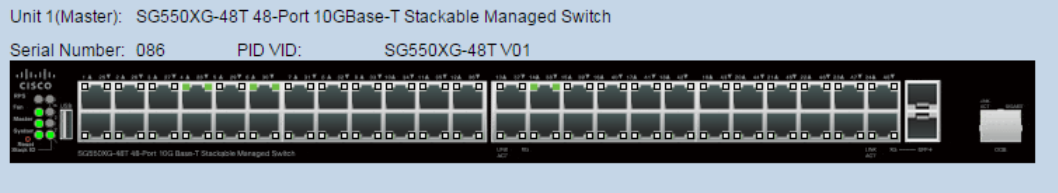
次のフィールドをリセットするには、[編集] をクリックして [TCP/UDP サービス] ページを開きます。

- [HTTPサービス]:HTTP の状態(有効または無効)。
- [HTTPS サービス]:HTTPS の状態(有効または無効)。
- [SNMP サービス]:SNMP の状態(有効または無効)。
- [Telnetサービス]:Telnet の状態(有効または無効)。
- [SSHサービス]:SSH の状態(有効または無効)。

マスターユニットの PoE 電源情報(デバイス サポート PoE)

- [マスターユニットのPoE電源情報]:[詳細] をクリックすると、[PoE のプロパティ] ページに直接リンクします。このページには、ユニットごとの PoE 電源情報が表示されます。
- [最大有効PoE電力(W)]:スイッチにより給電可能な最大電力。
- [PoE電力消費合計(W)]:接続されている PoE デバイスに給電された合計 PoE 電力。
- [PoE 電源モード]:ポート制限またはクラス制限。

下の図のように、マスター ユニットがグラフィカルに表示されます。



ポート上にカーソルを移動する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。

- **ユニットID**
- [シリアル番号]:シリアル番号。
- [PID VID]:ポート番号とバージョン ID。

CPU 利用率

デバイスの CPU は、管理インターフェイスを処理するエンドユーザ トラフィックに加えて、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

トラフィックが過剰に発生すると CPU に負荷がかかり、デバイスの通常の動作に支障をきたす場合があります。デバイスは、セキュア コア テクノロジー(SCT)機能を使用することにより、受信したトラフィックの合計量に関係なく、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。デバイスでは SCT はデフォルトで有効になっており、無効にできません。

他の機能との干渉は発生しません。

CPU 利用率を表示するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [CPU利用率] の順にクリックします。

[CPU 入力レート] フィールドには、CPU に対する 1 秒あたりの入力フレーム レートが表示されます。

ウィンドウに、デバイス上の CPU 使用率を示すグラフが表示されます。X 軸はサンプル番号、Y 軸は利用率になります。

ステップ 2 [CPU利用率] チェックボックスがオンになっていることを確認します。

ステップ 3 統計情報が更新されるまでの**リフレッシュ レート**（秒単位の時間）を選択します。指定した間隔で新しいサンプルが作成されます。

デバイス上の CPU 使用率を示すグラフを含むウィンドウが表示されます。

インターフェイス

[インターフェイス] ページには、トラフィック統計情報がポート別に表示されます。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、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、次のようにします。

ステップ 1 [ステータスと統計情報] > [インターフェイス] の順にクリックします。

ステップ 2 パラメータを入力します。

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

[受信統計情報] には、着信パケットについての情報が表示されます。

- [合計バイト(オクテット)]: 受信されたオクテット数。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。
- [ユニキャストパケット]: 受信された正常なユニキャスト パケット数。

- [マルチキャストパケット]:受信済みの正常なマルチキャスト パケット数。
- [ブロードキャストパケット]:受信済みの正常なブロードキャスト パケット数。
- [エラーがあるパケット]:受信済みのエラーのあるパケット数。

[送信統計情報] には、送信パケットについての情報が表示されます。

- [合計バイト(オクテット)]:送信されたオクテット数。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。
- [ユニキャストパケット]:送信済みの正常なユニキャスト パケット数。
- [マルチキャストパケット]:送信済みの正常なマルチキャスト パケット数。
- [ブロードキャストパケット]:送信済みの正常なブロードキャスト パケット数。

ステップ 3 テーブル ビューまたはグラフィック ビューに統計情報カウンタを表示するには、次のようにします。

- テーブル ビューにすべてのポートを表示するには、[すべてのインターフェイス統計情報の表示] 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、[インターフェイス履歴グラフの表示] をクリックします。このビューでは、表示する結果の [期間] と表示する統計情報のタイプを選択できます。たとえば、[過去5分間] と [ユニキャストパケット] を選択した場合は、過去 5 分間に受信されたユニキャスト パケットの数が表示されます。

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。このページには、トラフィックを中断する可能性のある物理レイヤ(レイヤ 1)のエラーについての詳細な情報が表示されます。

Etherlike 統計を表示したり、リフレッシュ レートを設定したりするには、次のようにします。

ステップ 1 [ステータスと統計情報] > [Etherlike] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インターフェイス]: イーサネット統計情報を表示する特定のインターフェイスを選択します。
- [リフレッシュ レート]: Etherlike 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。

選択したインターフェイスのフィールドが表示されます。

注 次のフィールドのいずれかにエラーの数(0 以外)が表示された場合は、[最終更新] 時刻が表示されます。

- [フレームチェックシーケンス(FCS)エラー]: Cyclic Redundancy Check(CRC; 巡回冗長検査)に失敗した受信フレーム数。
- [単一コリジョン フレーム]: 単一コリジョンに含まれるが、正常に送信できたフレーム数。
- [レイトコリジョン]: データの最初の 512 ビットの後に検出されたコリジョン。
- [過剰コリジョン]: 過剰コリジョンが原因で拒否された送信回数。
- [オーバーサイズパケット]: 2000 オクテットを超える受信パケット。
- [内部MAC受信エラー]: 受信側のエラーにより拒否されたフレーム。
- [受信済みポーズフレーム]: 受信されたフロー制御ポーズ フレーム。このフィールドは、XG ポートに対してのみサポートされます。ポート速度が 1 G の場合は、受信済みポーズ フレーム カウンタが作動しません。
- [送信済みポーズフレーム]: 選択されたインターフェイスから送信されたフロー制御ポーズ フレーム。

ステップ 3 テーブル ビューに統計情報カウンタを表示するには、[すべてのインターフェイス統計情報の表示] をクリックしてすべてのポートをテーブル ビューに表示します。

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、次のようにします。

ステップ 1 [ステータスと統計情報] > [ポート使用率] の順にクリックします。

ステップ 2 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示す [リフレッシュレート] 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。

- [インターフェイス]: ポートの名前。
- [Tx使用率]: 発信パケットに使用される帯域幅の量。
- [Rx使用率]: 着信パケットに使用される帯域幅の量。

ポート上の一定期間の使用率推移のグラフを表示するには、ポートを選択して、[インターフェイス履歴グラフの表示] をクリックします。さらに、次のフィールドが表示されます。

- [期間]: 時間の単位を選択します。グラフには、この時間の単位にわたるポート使用率が表示されます。

GVRP

[GVRP] ページには、ポートとの間で送受信された GARP VLAN 登録プロトコル（GVRP）フレームに関する情報が表示されます。GVRP は、スイッチ上での VLAN 情報の自動コンフィギュレーション用の規格ベースのレイヤ 2 ネットワーク プロトコルです。これは、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、そのポートで GVRP がグローバルに有効になっている場合にのみ表示されます。[GVRP 設定] ページを参照してください。

GVRP 統計を表示したり、リフレッシュ レートを設定したりするには、次のようにします。

ステップ 1 [ステータスと統計情報] > [GVRP] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インターフェイス]:GVRP 統計情報を表示する特定のインターフェイスを選択します。
- [リフレッシュレート]:GVRP ページがリフレッシュされるまでの時間を選択します。

[アトリビュート(カウンタ)] には、さまざまなパケット タイプのカウンタがインターフェイス別に表示されます。これらは、[受信済み] パケットと [送信済み] パケットに関して表示されます。

- [Join Empty]:受信または送信された GVRP の Join Empty パケット数。
- [Empty]:受信または送信された GVRP の Empty パケット数。
- [Leave Empty]:受信または送信された GVRP の Leave Empty パケット数。
- [Join In]:受信または送信された GVRP の Join In パケット数。
- [Leave In]:受信または送信された GVRP の Leave In パケット数。
- [Leave All]:受信または送信された GVRP の Leave All パケット数。

[GVRPエラー統計情報] セクションには、GVRP エラー カウンタが表示されます。

- [無効なプロトコルID]:無効なプロトコル ID エラー。
- [無効なアトリビュートタイプ]:無効なアトリビュート ID エラー。
- [無効なアトリビュート値]:無効なアトリビュート値エラー。
- [無効なアトリビュート長]:無効なアトリビュート長エラー。
- [無効なイベント]:無効なイベント。

ステップ 3 統計情報カウンタをクリアするには、[すべてのインターフェイス統計情報の表示] をクリックしてすべてのポートを 1 つのページに表示します。

802.1X EAP

[802.1x EAP] ページには、送信または受信された Extensible Authentication Protocol（EAP; 拡張認証プロトコル）フレームについての情報が表示されます。802.1X 機能を設定するには、[プロパティ] ページ（[セキュリティ] > [802.1x]）を参照してください。

EAP 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、次のようにします。

ステップ 1 [ステータスと統計情報] > [802.1x EAP] の順にクリックします。

ステップ 2 統計情報を取得するためにポーリングする**インターフェイス**を選択します。

ステップ 3 EAP 統計情報がリフレッシュされるまでの時間を示す**リフレッシュ レート**を選択します。

選択したインターフェイスに対する値が表示されます。

- [受信済み EAPOL EAP フレーム]: ポートで受信された有効な EAPOL フレーム。
- [受信済み EAPOL 開始フレーム]: ポートで受信された有効な 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 通知フレーム]: ポートで受信された EAPOL 通知フレーム。
- [受信済み EAPOL 通知要求フレーム]: ポートで受信された EAPOL 通知要求フレーム。
- [受信済み EAPOL 無効フレーム]: ポートで受信された EAPOL 無効フレーム。
- [受信済み EAPOL EAP パケット長エラー フレーム]: このポートで受信された、パケット本体の長さが無効な EAPOL フレーム。
- [受信済み未認識 CKN を含む MKPDU フレーム]: このポートで受信された、未認識 CKN を含む EAP フレーム。
- [受信済み MKPDU 無効フレーム]: ポートで受信された MKPDU 無効フレーム。
- [最終EAPOLフレームバージョン]: 一番新しく受信した EAPOL フレームに関連付けられていたプロトコル バージョン番号。
- [最終EAPOLフレーム送信元]: 一番新しく受信した EAPOL フレームに関連付けられていた送信元 MAC アドレス。

- [送信済み EAPOL EAP サプリカント フレーム]:ポートで送信された EAPOL EAP サプリカント フレーム。
- [送信済み EAPOL 開始フレーム]:ポートで送信された EAPOL 開始フレーム。
- [送信済み EAPOL ログオフ フレーム]:ポートで送信された EAPOL ログオフ フレーム。
- [送信済み EAPOL 通知フレーム]:ポートで送信された EAPOL 通知フレーム。
- [送信済み EAPOL 通知要求フレーム]:ポートで送信された EAPOL 通知要求フレーム。
- [送信済み EAPOL EAP オーセンティケータ フレーム]:ポートで送信された EAP オーセンティケータ フレーム。
- [送信済み CKN を含まない EAPOL MKA フレーム]:ポートで送信された CKN を含まない MKA フレーム。

ステップ 4 統計情報カウンタをクリアするには、次のようにします。

- すべてのインターフェイスのカウンタを表示するには、[すべてのインターフェイス統計情報の表示] をクリックします。
- すべてのインターフェイスのカウンタをクリアするには、[インターフェイス カウンタのクリア] をクリックします。

ACL

ACL ロギング機能が有効になっている場合、ACL ルールと一致するパケットに対して情報 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、次のようにします。

ステップ 1 [ステータスと統計情報] > [ACL] の順にクリックします。

ステップ 2 ページが更新されるまでの**リフレッシュ レート**(秒単位)を選択します。指定した間隔で新しいインターフェイスのグループが作成されます。

次の情報が表示されます。

- [グローバルトラップパケットカウンタ]:リソース不足が原因でグローバルにトラップされたパケットの数。

- [トラップ パケット – Port/LAG ベース]: 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。
- [トラップ パケット – VLAN ベース]: 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 統計情報カウンタを管理するには、[カウンタのクリア] 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クリアします。

TCAM 利用率

TCAM は ACL(アクセス コントロール リスト)やサービス品質(QoS)などのアプリケーションによって生成されたルールを保持しますが、ルータ TCAM は IP ルーティング用のルールとユーザ作成ルールを保持します。

一部のアプリケーションは、初回起動時にルールを割り振ります。さらに、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。

TCAM 利用率を表示するには、[ステータスと統計情報] > [TCAM利用率] をクリックします。

[TCAM利用率] ページは次のフィールドを表示します。

- [ユニット番号]: TCAM 利用率の表示対象となるスタック内のユニット。これは、デバイスがスタックの一部でない場合には表示されません。
- [ルーティングおよびマルチキャストルーティングの最大TCAMエントリ数]: ルーティングおよびマルチキャスト ルーティングに使用可能なルータ TCAM エントリの最大数。
- [IPv4 ルーティング]
  - [使用中]: IPv4 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 ルーティングに使用可能なルータ TCAM エントリの数。
- **IPv4 マルチキャスト ルーティング**
  - [使用中]: IPv4 マルチキャスト 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 マルチキャスト ルーティングに使用可能なルータ TCAM エントリの数。

- **IPv4ポリシーベースのルーティング**
  - [使用中]:IPv4 ポリシーベース 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 エントリの数。
- **IPv6ルーティング**
  - [使用中]:IPv6 マルチキャスト 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 マルチキャスト ルーティングに使用可能なルータ TCAM エントリの数。
- [IPv6 マルチキャスト ルーティング]:IPv6 ルーティングに使用されるルータ TCAM エントリの数。
  - [使用中]:IPv6 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 ルーティングに使用可能なルータ TCAM エントリの数。
- **IPv6ポリシーベースのルーティング**
  - [使用中]:IPv6 ポリシーベース 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 エントリの数。
- **VLAN マッピング**
  - [使用中]: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 エントリの数。
- [非IPルールの最大TCAMエントリ数]:非 IP ルールに使用可能な ルータ TCAM エントリの最大数。
- **非IPルール**
  - [使用中]:非 IP ルールで使用される TCAM エントリ数。
  - [最大]:非 IP ルールで使用可能な TCAM エントリ数。

さまざまなプロセス間での割り振りを変更する方法を表示するには、「ルーティング リソース」セクションを参照してください。

ヘルスと電力

[ヘルスと電力] 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します。モデルにより、デバイスのファンの個数は異なります。ファンがないモデルも存在します。

冗長電源

この機能は、SG550 シリーズでのみサポートされます。

RPS 2300 は AC 電源のバックアップです。これは、AC 電源が機能を停止した場合にデバイスに電力を供給するために使用されます。550 ファミリ上でのみサポートされます。

バックアップ電源に切り替える必要が生じた場合は、デバイスが処理を中断することなく、リブートせずに電源を切り替えます。デバイスは 1 秒ごとに RPS ステータスをポーリングし、RPS が電力を供給している場合は、RPS LED が点灯し、RPS がアクティブであれば、SYSLOG が生成されます。

メイン電源が復旧すると、デバイスが RPS に電力の供給を停止するように通知します。SYSLOG が生成されます。

RPS LED（デバイスの前面パネルに付いている）は現在の RPS ステータスを示します。

- 消灯：RPS が接続されていません。
- 緑（点灯）：RPS の準備ができています。
- オレンジ（点滅）：RPS がデバイスに電力を供給しています。
- オレンジ（点灯）：RPS は接続されていますが、他の 2 つのデバイスに電力を供給しています。この場合、RPS は、他の 2 つのデバイスに電力を供給しながら、現在のデバイスにも電力を供給することはできません。

ファン

デバイスによっては、その動作にファンが不可欠な場合があります。ファンがないと、デバイスの温度が高くなりすぎて自動的にシャットダウンします。ファンは可動部品のため、故障することがあります。システムには冗長ファンが取り付けられています。このファンは、システム ファンのいずれかが故障しない限り、作動しません。作動した場合は、冗長ファンがデバイスの環境モニタリングの一部になります。

冗長ファンは 1 日 1 分以上作動させることをお勧めします。

デバイスによっては、ハードウェアを過熱から保護するための温度センサーが備わっています。その場合、デバイスが過熱しクール ダウンする間に、デバイスは次のアクションを実行します。

イベント	アクション
最低 1 つの温度センサーが警告しきい値を超える	次の処理が生成されます。 • Syslog メッセージ • SNMP トラップ
最低 1 つの温度センサーが危険しきい値を超える	次の処理が生成されます。 • Syslog メッセージ • SNMP トラップ 次のアクションが実行されます。 • システム LED がオレンジ色に点灯します(ハードウェアがサポートしている場合)。 • ポートの無効化:危険温度を超えた状態が 2 分以上続くと、すべてのポートがシャットダウンします。 • (PoE をサポートするデバイスの場合)電力消費量を減らし、熱放出を抑えるために、PoE 回路が無効になります。
危険しきい値超過後のクール ダウン時間(すべてのセンサーが警告しきい値より 2 °C 以上低い値になるまで)。	すべてのセンサーが警告しきい値より 2 度低い値までクール ダウンすると、PHY が再び有効になり、すべてのポートが復旧します。 ファン ステータスが [OK] になると、ポートが有効になります。 (PoE をサポートするデバイスの場合)PoE 回路が有効になります。

[ヘルスと電力] フィールド

デバイスのヘルス パラメータを表示するには、[ステータスと統計情報] > [ヘルスと電力] の順にクリックします。

注 デバイスに関連するフィールドのみが表示されます。

このセクションには、Green Ethernet 機能や LED 無効化機能によって、またポートをダウンさせる（物理的にまたは時間範囲設定によって）ことによってデバイスで節約される電力が表示されます。

PoE 節約には、特定の時刻（通常は、PoE ネットワーク要素が使用されていないとき）にポートへの PoE をシャットダウンする PoE 時間範囲機能を使用することにより節約される電力の合計が表示されます。

次の情報が表示されます（フィールドの順序はデバイスによって異なる場合があります）。

省電力

- [現在の Green Ethernet およびポート電力節約]：現在、すべてのポートで節約されている電力量。
- [累積 Green Ethernet およびポート電力節約]：デバイスの電源がオンになって以降、すべてのポートで節約されている電力の累積量。
- [予測年間 Green Ethernet およびポート電力節約]：1 週間でデバイス上で節約される電力量の予想。この値は、前の週の節約量に基づいて計算されます。
- [現在の PoE 電力節約]：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]：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]：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。この予想は、前の週の節約量に基づきます。

（XG ファミリ以外のデバイスの場合）特定の時間範囲の電力オペレーションをスケジュールするには、ページ上の次の文章内の青色のリンクをクリックします。「電力節約は、[時間範囲] を使用して [データ] と [PoE] オペレーションをスケジュールすることにより、増加させることができます。」以下のページが表示されます。

- [時間範囲]：[各種管理] > [時間の設定] > [時間範囲] ページが表示されます。電力オペレーションの時間範囲を設定します。
- [データ]：[ポート管理] > [ポート設定] ページが表示されます。時間範囲を 1 つ以上のポートに関連付けます。
- [PoE]：[ポート管理] > [PoE] > [設定] ページが表示されます。時間範囲を 1 つ以上のポート上の PoE オペレーションに関連付けます。

デバイスがスタックの一部になっている場合は、[ヘルスと電力] ページに以下のフィールドが表示されます。

ヘルステーブル

- [ユニット番号]: スタック内のユニット番号が表示されます。
- [ファンステータス]: 次の値が使用できます。
  - [OK]: ファンが正常に動作している。
  - [障害]: 複数のファンが正しく動作していません。
  - [N/A]: ファンがその特定のモデルに適していません。
- [冗長ファンステータス]: 次の値が使用できます。
  - [準備完了]: 冗長ファンが動作可能ですが、必要ありません。
  - [アクティブ]: メイン ファンのいずれかが停止して、このファンが代わりに動作しています。
- [温度]: オプションは次のとおりです。
  - [OK]: 温度が警告しきい値未満の場合。
  - [警告]: 温度が警告しきい値と危険しきい値の間の場合。
  - [危険]: 温度が危険しきい値を超えている場合。
  - [N/A]: 該当なし。

  [メイン電源ステータス](以下のフィールドは、PD デバイスであるデバイスと RPS をサポートしているデバイスの場合に表示されます)
  - [メイン電源ステータス]: メイン電源に関して以下のいずれかが表示されます。

    [アクティブ]: 電源は使用中です。

    [障害]: メイン電源で障害が発生しました。
  - [メイン電源予算]: デバイスの PSE 処理のためにメイン電源から割り当てることが可能な電力量。

- [冗長電源ステータス]:バックアップ電源に関して以下のいずれかが表示されます。

  [アクティブ]:電源は使用中です。

  [使用可能]:冗長電源は接続されていますが、使用されていません。

  [使用不可]:冗長電源は接続されていますが、すでに電力を他のデバイスに供給しています。

  [切断]:冗長電源は接続されていません。

- [冗長電源予算]:デバイスの PSE 処理のためにバックアップ電源から割り当てることが可能な電力量。

[イーサネット経由電源ステータス] (最大 2 つの PD を使用できます)

- [PD ポート 1 ID]:PD ポート 1 のポート番号
- [PD ポート 1 ネゴシエーション モード]:ネゴシエーション モード (後述の定義を参照)。
- [PDポート1ステータス]:接続されているかどうか
- [PDポート1タイプ]:PD のタイプ
- [PDポート1予算]:デバイスの PSE 処理のために割り当てることが可能な最大電力量
- [PDポート2 ID]:PD ポート 2 のポート番号
- [PD ポート 2 ネゴシエーション モード]:ネゴシエーション モード (後述の定義を参照)。
- [PDポート2ステータス]:接続されているかどうか
- [PDポート2タイプ]:PD のタイプ
- [PDポート2予算]:デバイスの PSE 処理のために割り当てることが可能な最大電力量

デバイスがスタックの一部になっていない場合は、[ヘルスと電力] ページに以下のフィールドが表示されます。

- [ファンステータス]:次の値が使用できます。
  - [OK]:ファンが正常に動作している。
  - [障害]:ファンが正常に動作していません。
  - [N/A]:ファン ID が特定のモデルに適合していません。

- [冗長ファンステータス]:次の値が使用できます。
  - [準備完了]:冗長ファンが動作可能ですが、必要ありません。
  - [アクティブ]:メイン ファンのいずれかが停止して、このファンが代わりに動作しています。
  - [障害]:標準ファンが故障しており、冗長ファンが正常に動作していません。
- [温度]:オプションは次のとおりです。
  - [OK]:温度が警告しきい値未満の場合。
  - [警告]:温度が警告しきい値と危険しきい値の間の場合。
  - [危険]:温度が危険しきい値を超えている場合。
  - [N/A]:該当なし。

[電源ステータス](以下のフィールドは、PD デバイスであるデバイスと RPS をサポートしているデバイスの場合に表示されます)

- [電源ステータス]:次のようなオプションがあります。
  - [メイン]:次のいずれかの値が表示されます。

    [アクティブ]:電源は使用中です。

    [障害]:メイン電源で障害が発生しました。
  - [冗長]:冗長電源のステータスを提供します。次のいずれかが表示されます。

    [アクティブ]:冗長電源(RPS)が使用中です。

    [利用可能]:RPS は接続されていますが、使用されていません。

    [使用不可]:RPS は接続されていますが、電力を他のデバイスに供給しています。

    [未接続]:RPS が接続されていません。

    [あり]:RPS は接続されています。

イーサネット電源テーブル(スタック内のユニットの 1 つで PD ポートがサポートされている場合のみ表示されます)。次のフィールドが表示されます。

- [ポート名]:ポートの番号。
- [PD ステータス]:次の値のいずれかが表示されます。
  - [接続]:PD ポートが、電力を供給している PSE デバイスに接続されています。
  - [未接続]:PD ポートが PSE デバイスに接続されていません。

- [ネゴシエーション モード]:次の値のいずれか。
  - [自動]:CDP または LLDP ネゴシエーションが電力レベルの決定に使用されます。
  - [802.3AF の強制]:両側で AF 電力標準を使用します。
  - [802.3AT の強制]:両側で AT 電力標準を使用します。
  - [60W の強制]:両側で 60W の電力を使用します。
- [電力予算]:実際にポートに割り当てられた電力量。

スイッチド ポート アナライザ(SPAN および RSPAN)

ポート ミラーリングやポート モニタリングとも呼ばれる SPAN 機能は、ネットワーク アナライザで分析されるネットワーク トラフィックを選択します。ネットワーク アナライザは、Cisco SwitchProbe デバイスにすることも、その他のリモート モニタリング(RMON)プローブにすることもできます。

ネットワーク デバイスでは、ポート ミラーリングにより、1 つのデバイス ポート、複数のデバイス ポート、または VLAN 全体で受信されるネットワーク パケットのコピーが、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されます。この機能は、通常、侵入検知システムなど、ネットワーク トラフィックのモニタリングを必要とする場合に使用されます。モニタリング ポートに接続されたネットワーク アナライザはデータ パケットを処理します。

デバイスは、セッションあたり最大 8 つのインターフェイスをミラーリングできます。

ネットワーク ポートが受信し、ミラーリング対象の VLAN に割り当てられているパケットは、そのパケットが最終的にトラップまたは破棄される場合であっても、アナライザ ポートにミラーリングされます。送信(Tx)ミラーリング機能がアクティブな場合、デバイスから送信されるパケットはミラーリングされます。

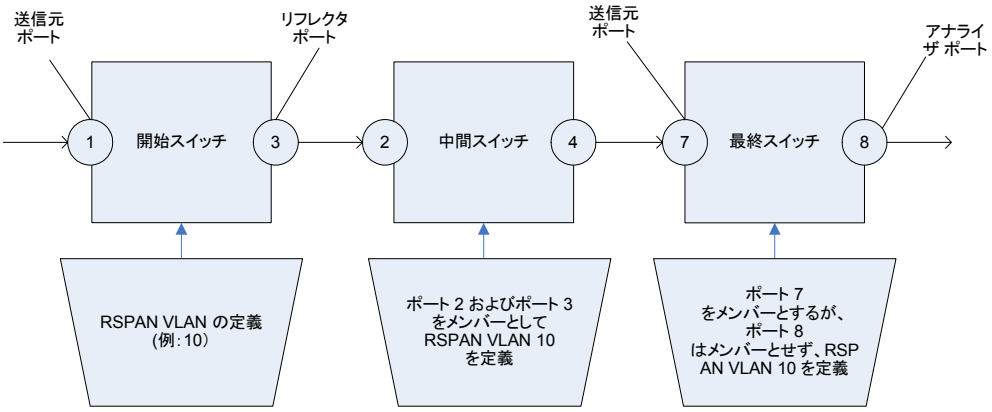
ミラーリングにより、送信元ポートからのトラフィックがすべてアナライザ(宛先)ポートで受信されるというわけではありません。アナライザ ポートがサポートできる以上のデータが送信された場合、一部のデータが失われる可能性があります。

VLAN ミラーリングは、手動で作成されていない VLAN についてはアクティブにできません。たとえば、VLAN 23 が GVRP によって作成された場合は、ポート ミラーリングがその上で動作しません。

リモート SPAN

RSPAN は、ネットワーク全体で複数のスイッチのモニタリングを有効にし、リモート スイッチ上でアナライザ ポートを定義可能にすることで、SPAN を拡張します。図 1 に示すように、開始(送信元)および最終(宛先)スイッチに加えて、トラフィックが流れる中間スイッチを定義できます。

図 1　RSPAN スイッチの導入:



各 RSPAN セッションのトラフィックは、参加しているすべてのスイッチでその RSPAN セッション専用のユーザ指定 RSPAN VLAN を通じて伝送されます。トラフィックは、開始デバイス上の送信元インターフェイスからリフレクタ ポート経由で RSPAN VLAN にコピーされ、中間スイッチ上のトランク ポートを通じて、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に転送されます。

リフレクタ ポートはパケットを RSPAN VLAN にコピーするメカニズムです。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上で設定する必要があります。

注　パケットが複数の送信元から同時に到着する場合は、RSPAN によってすべてのパケットが正確にコピーされるとは限りません。正確なモニタリングが必要な場合は、TCAM ベースのミラー ポリシーを使用してください。

RSPAN ワークフロー

次のワークフローは、開始、中間、および最終スイッチの設定方法を示します。

- 開始スイッチ
- 中間スイッチ
- 最終スイッチ

開始スイッチ

1. RSPAN VLAN を定義します。この RSPAN VLAN はすべてのスイッチで同じである必要があります。
2. 1 つ以上の送信元インターフェイスを定義します。これらはポートまたは VLAN にすることができます。RSPAN VLAN のメンバーで**ない**ことを確認します。
3. リフレクタ ポート(宛先、出力ポート)を定義し、RSPAN VLAN でないことを確認します。
4. 宛先タイプをリモート VLAN として定義します。
5. ネットワーク トラフィックを有効に設定します。

中間スイッチ

1. RSPAN VLAN を定義します。この RSPAN VLAN は開始、中間、および最終スイッチで同じである必要があります。
2. RSPAN VLAN のメンバーであるポートが少なくとも 2 つあることを確認します。トラフィックは RSPAN VLAN 経由でスイッチを通過します。

最終スイッチ

1. RSPAN VLAN を定義します。この RSPAN VLAN は開始、中間、および最終スイッチで同じである必要があります。
2. 中間スイッチに接続された送信元ポートが RSPAN VLAN のメンバーであることを確認します。
3. 送信元インターフェイスをリモート VLAN として定義します。
4. 宛先ポートを定義し、RSPAN VLAN に含まれていないことを確認します。
5. 宛先タイプをローカル インターフェイスとして定義します。

RSPAN VLAN

RSPAN VLAN は開始、中間、および最終デバイスで定義する必要があります。

VLAN を RSPAN VLAN として設定するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [SPANとRSPAN] > [RSPAN VLAN] の順にクリックします。

それまでに定義済みの RSPAN VLAN が表示されます。

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 [適用] をクリックします。

SPAN セッションの宛先

宛先ポートは開始および最終デバイスで設定する必要があります。開始デバイスの場合、これはリフレクタ ポートです。最終デバイスの場合、これはアナライザ ポートです。

宛先ポートを追加するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [SPAN と RSPAN] > [SPAN セッション宛先] の順にクリックします。

すでに定義されている宛先が表示されます。

ステップ 2 [追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [セッション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。
- [宛先タイプ]: 次のいずれかのオプションを選択します。
  - [ローカルインターフェイス]: 送信元ポートと同じデバイス上の宛先ポートです(SPAN に関連)。
  - [リモートVLAN]: 送信元ポートと異なるデバイス上の宛先ポートです(RSPAN に関連)。

  [宛先タイプ] が [リモートVLAN] である場合、次のフィールドを設定します。
  - [リフレクタポート]: 最初のデバイス上のターゲット ポートとして機能するユニット/ポート。

  [宛先タイプ] が [ローカルインターフェイス] である場合、次のフィールドを設定します。
  - [ポート]: デバイス上のアナライザ ポートとして機能するユニット/ポート。
- [ネットワークトラフィック]: モニタリングされるトラフィック以外のトラフィックがポート上で可能であることを有効にする場合に選択します。

ステップ 4 [適用] をクリックします。

SPAN セッションの送信元

開始および最終デバイス上に 1 つ以上の SPAN または RSPAN 送信元を設定する必要があります。

ミラーする送信元ポートを設定するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [SPAN と RSPAN] > [セッションの送信元] の順にクリックします。

ステップ 2 [追加] をクリックします。

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

ステップ 4 開始スイッチ上の SPAN または RSPAN に対して、トラフィックがモニタリングされるユニットおよびポートまたは VLAN（**送信元インターフェイス**）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 [モニタタイプ] 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および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 [適用] をクリックします。ミラーリング用の送信元インターフェイスが設定されます。

診断

ここでは、ポート ミラーリングの設定、ケーブル テストの実行、およびデバイス動作情報の表示について説明します。

具体的な内容は、次のとおりです。

- カッパー ポート テスト
- 光モジュール ステータス
- テクニカル サポート情報

カッパー ポート テスト

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

VCT によって、2 つのタイプのテストが実行されます。

- Time Domain Reflectometry（TDR; タイム ド メイン反射率計）テクノロジーは、ポートに取り付けられているカッパー ケーブルの品質と特性をテストします。長さ 140 m までのケーブルをテストできます。テスト結果は、[カッパー テスト] ページの [テスト結果] ブロックに表示されます。
- DSP ベース テストは、アクティブな XG リンクに対して実行され、ケーブルの長さを測定します。これらの結果は、[カッパー テスト] ページの [詳細情報] ブロックに表示されます。このテストはリンク速度が 10 G の場合にのみ実行できます。

カッパー ポート テスト実行時の前提条件

テストを実行する準備として、次のようにします。

- （必須）ショート リーチ モードの無効化（[プロパティ] ページを参照）
- （任意）EEE の無効化（[プロパティ] ページを参照）

ケーブル テスト（VCT）を実行する際には、CAT6a データ ケーブルをご使用ください。

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

注意 ポートはテスト時、停止状態となり、通信は中断されます。テスト後、ポートは稼動状態に戻ります。Web ベースのスイッチ設定ユーティリティ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、その間このデバイスと通信できなくなるので、推奨できません。

ポートに取り付けられているカッパー ケーブルをテストするには、次のようにします。

ステップ 1 [ステータスと統計情報] > [診断] > [カッパーテスト] の順にクリックします。

ステップ 2 テストを実行するユニットおよびポートを選択します。

ステップ 3 [カッパーテスト] をクリックします。

ステップ 4 メッセージが表示された場合、リンクが停止状態になることを了承する場合は [OK] をクリックし、テストを中止する場合は [キャンセル] をクリックします。

[テスト結果] ブロックに次のフィールドが表示されます。

- [最終更新]: ポートに対して最後のテストが実行された時刻。
- [テスト結果]: ケーブル テストの結果。選択項目は次のとおりです。
  - [OK]: ケーブルはテストに合格しました。
  - [ケーブルなし]: ケーブルがポートに接続されていません。
  - [開放ケーブル]: ケーブルの一方の側しか接続されていません。
  - [短絡ケーブル]: ケーブルにショートが発生しています。
  - [テスト結果不明]: エラーが発生しました。
- [障害個所までの距離]: 障害が検出されたケーブル位置からポートまでの距離。
- [動作ポート ステータス]: ポートの状態(アップまたはダウン)が表示されます。

[詳細情報] ブロックに次の情報が表示されます(ページを開くたびに情報が更新されます)。

- [ケーブル長]: 長さの目安を提供します。
- [ペア]: テスト中のケーブル ワイヤ ペア。
- [ステータス]: ワイヤ ペアのステータス。赤は障害が発生していることを示し、緑は正常な状態を示します。
- [チャネル]: ケーブル チャネル。ワイヤのタイプ(ストレート ケーブルまたはクロス ケーブル)を示します。
- [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

[光モジュールステータス] ページには、Small Form-factor Pluggable（SFP）トランシーバにより報告される動作状況が表示されます。

サポートされている GE SFP（1000 Mbps）トランシーバは次のとおりです。

- MGBBX1: 1000BASE-BX-20U SFP トランシーバ（シングルモード ファイバ対応、波長 1310 nm）は、最大 40 km までサポートします。
- MGBLH1: 1000BASE-LH SFP トランシーバ（シングルモード ファイバ対応、波長 1310 nm）は、最大 40 km までサポートします。
- MGBLX1: 1000BASE-LX SFP トランシーバ（シングルモード ファイバ対応、波長 1310 nm）は、最大 10 km までサポートします。
- MGBSX1:1000BASE-SX SFP トランシーバ（マルチモード ファイバ対応、波長 850 nm）は、最大 550 m までサポートします。
- MGBT1: 1000BASE-T SFP トランシーバ（カテゴリ 5 カッパー ワイヤ対応）は最大 100 m までサポートします。

サポートされている XG SFP+（10,000 Mbps）トランシーバは次のとおりです。

- Cisco SFP-10GSR
- Cisco SFP-10GLRM
- Cisco SFP-10GLR

サポートされている XG パッシブ ケーブル（Twinax/DAC）は次のとおりです。

- Cisco SFP-H10GCU1m
- Cisco SFP-H10GCU3m
- Cisco SFP-H10GCU5m

光テスト結果を表示するには、[ステータスと統計情報] > [診断] > [光モジュールステータス] 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。

- [ポート]：SFP が接続しているポート番号。
- [説明]：光トランシーバの説明。
- [シリアル番号]：光トランシーバのシリアル番号。
- [PID]：VLAN ID。

- [VID]:光トランシーバの ID。
- [温度]:SFP の動作温度(摂氏)。
- [電圧]:SFP の動作電圧。
- [電流]:SFP の電流消費量。
- [出力電力]:送出される光電力。
- [入力電力]:受け取る光電力。
- [トランスミッタ障害]:リモート SFP から報告される信号損失。値は [TRUE]、[FALSE]、および [N/S](信号なし)になります。
- [信号消失]:ローカル SFP から報告される信号損失。値は [TRUE] か [FALSE] になります。
- [データ レディ]:SFP が動作しています。値は [TRUE] か [FALSE] になります。

テクニカル サポート情報

このページでは、デバイス ステータスの詳細なログが提供されます。この情報は、テクニカル サポートがユーザの問題解決を支援する場合に非常に役に立ちます。その理由は、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です。

デバッグに役立つテクニカル サポート情報を表示するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [診断] > [テクニカルサポート情報] の順にクリックします。

ステップ 2 [生成] をクリックします。

さまざまな **show** CLI コマンドからの情報が表示されます。

注 このコマンドからの出力の生成にはしばらく時間がかかる場合があります。情報が生成されたら、[技術サポート データの選択] をクリックすることにより、画面上のテキスト ボックスからコピーすることができます。

RMON

RMON（リモート ネットワーキング モニタリング）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一定期間行い、トラップを SNMP マネージャに送信することによって、プロアクティブな対応をすることができます。ローカル SNMP エージェントは、実際のリアルタイムのカウンタを、事前定義されたしきい値と比較してアラームを生成するので、SNMP 中央管理プラットフォームでポーリングする必要がなくなります。ネットワークのベース ラインを基準とした相対幅を持つ適切なしきい値が設定されていれば、これはプロアクティブな管理において効果的なメカニズムとなります。

RMON を使用すると、SNMP マネージャがデバイスを頻繁にポーリングして情報を得る必要がなくなるため、マネージャとデバイス間のトラフィックを減らすことができますし、デバイスがイベント発生時にイベントを報告するため、マネージャがタイムリーなステータス レポートを取得できるようになります。

この機能により、次のアクションを実行できるようになります。

- 現在の統計情報（カウンタ値がクリアされたとき以降）を表示する。一定期間、これらのカウンタ値を収集して、収集データのテーブルを表示することもできます。収集された各セットは、[履歴] タブに 1 行で表示されます。
- 「特定のレイト コリジョン数に達した」など、カウンタ値に関して興味を引く変化を定義して（アラームを定義）、このイベントが発生したときに実行するアクションを定義する（ログ、トラップ、またはその両方）。

統計情報

[統計情報] ページには、パケット サイズについての詳細情報および物理レイヤ エラーについての情報が表示されます。表示される情報は、RMON 規格に基づいています。オーバー サイズ パケットは、次の基準を満たすイーサネット フレームとして定義されます。

- パケットの長さが MRU バイト サイズより長い。
- コリジョン イベントが検出されていない。
- レイト コリジョン イベントが検出されていない。
- 受信した (Rx) エラー イベントが検出されていない。
- 有効な CRC がパケットにある。

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には、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [統計情報] の順にクリックします。

ステップ 2 イーサネット統計情報を表示する**インターフェイス**を選択します。

ステップ 3 インターフェイス統計情報がリフレッシュされるまでの時間を示す**リフレッシュ レート**を選択します。

選択したインターフェイスに関する以下の統計情報が表示されます。

注 次のフィールドのいずれかにエラーの数(0 以外)が表示された場合は、[最終更新] 時刻が表示されます。

- [受信済みバイト]:受信されたオクテット数。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。
- [ドロップイベント]:ドロップされたパケット数。
- [受信済みパケット]:マルチキャスト パケットとブロードキャスト パケットを含む、受信済みの正常なパケット数。
- [受信済みブロードキャストパケット]:受信済みの正常なブロードキャスト パケット数。この数にはマルチキャスト パケットは含まれません。
- [受信済みマルチキャストパケット]:受信済みの正常なマルチキャスト パケット数。
- [CRC &アラインメントエラー]:発生した CRC とアラインメント エラー数。
- [アンダーサイズパケット]:受信済みアンダーサイズ パケット数(64 オクテット未満)。
- [オーバーサイズ パケット]:受信済みオーバーサイズ パケット数(2000 オクテット超過)。
- [フラグメント]:受信済みフラグメント(フレーミング ビットを含まず、FCS オクテットを含む、64 オクテット未満のパケット)の数。
- [ジャバー]:1632 オクテットを超える受信済みパケット数。この数にはフレーミング ビットは含まれず、FCS オクテットは含まれます。この FCS オクテットには、オクテットの整数(FCS エラー)を持つ不良 Frame Check Sequence(FCS;フレーム チェック シーケンス)、または非整数オクテット(アラインメント エラー)を持つ不良 FCS のいずれかが含まれます。ジャバー パケットは、次の基準を満たすイーサネット フレームとして定義されます。

- パケットのデータ長が MRU より長い。
- 無効な CRC がパケットにある。
- 受信した (Rx) エラー イベントが検出されていない。

- [コリジョン]:受信済みコリジョン数。ジャンボ フレームが有効である場合、ジャバー フレームのしきい値はジャンボ フレームの最大サイズまで引き上げられます。
- [64 バイト フレーム]:送信または受信された 64 バイトを格納するフレーム数。
- [65 ～ 127 バイト フレーム]:送信または受信された 65 ～ 127 バイトを格納するフレーム数。
- [128 ～ 255 バイト フレーム]:送信または受信された 128 ～ 255 バイトを格納するフレーム数。
- [256 ～ 511 バイト フレーム]:送信または受信された 256 ～ 511 バイトを格納するフレーム数。
- [512 ～ 1023 バイト フレーム]:送信または受信された 512 ～ 1023 バイトを格納するフレーム数。
- [1024 バイト以上のフレーム]:送信または受信された 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。

ステップ 4 テーブル ビューまたはグラフィック ビューにカウンタを表示するには、次のようにします。

- テーブル ビューにすべてのポートを表示するには、[すべてのインターフェイス統計情報の表示] 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、[グラフィックビュー] をクリックします。このビューでは、表示する結果の [期間] と表示する統計情報のタイプを選択できます。

RMON の履歴

RMON 機能を使用すると、インターフェイスごとに統計情報をモニタできます。

[履歴] ページでは、サンプリング頻度、保存するサンプル数、およびデータ収集元ポートを定義できます。

データは、サンプリングされてから保存され、[履歴テーブル] をクリックして表示できる [履歴テーブル] ページに表示されます。

RMON 制御情報を入力するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [履歴] の順にクリックします。このページに表示されるフィールドは、下にある [RMON履歴の追加] ページで定義されます。このページにあり、[追加] ページで定義されていないフィールドは次のものだけです。

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

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [新規履歴エントリ]:新しい [履歴] テーブル エントリ番号が表示されます。
- [送信元インターフェイス]: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。
- [最大保持サンプル数]:保存されるサンプル数を入力します。
- [サンプリング間隔]:ポートからサンプルが収集された秒数を入力します。フィールド範囲は 1 ～ 3600 です。
- [オーナー]:RMON 情報を要求した RMON ステーションまたはユーザを入力します。

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

ステップ 5 実際の統計情報を表示するには、[履歴テーブル](下に説明)をクリックします。

RMON 統計情報テーブル

[履歴] ページには、インターフェイス固有の統計情報ネットワーク サンプリングが表示されます。サンプルは、上で説明されている [履歴制御テーブル] で構成されています。

RMON 履歴統計情報を表示するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [履歴] の順にクリックします。

ステップ 2 [履歴テーブル] をクリックします。

ステップ 3 [履歴エントリ番号] ドロップ ダウン メニューから、オプションでサンプルのエントリ番号を選択して表示します。

選択したサンプルのフィールドが表示されます。

- [オーナー]:履歴テーブル エントリのオーナー。
- [サンプル番号]:統計情報はこのサンプルから取得されます。
- [ドロップイベント]: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、ドロップ パケットが検出された回数を表します。ただしドロップされたパケットの正確な数を表さない場合があります。
- [受信済みバイト]:受信されたオクテット数。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。
- [受信済みパケット]: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。
- [ブロードキャストパケット]:正常なブロードキャスト パケット数。この数にはマルチキャスト パケットは含まれません。
- [マルチキャストパケット]:受信済みの正常なマルチキャスト パケット数。
- [CRCアラインメントエラー]:発生した CRC とアラインメント エラー数。
- [アンダーサイズパケット]:受信済みアンダーサイズ パケット数(64 オクテット未満)。
- [オーバーサイズ パケット]:受信済みオーバーサイズ パケット数(2000 オクテット超過)。
- [フラグメント]:受信済みフラグメント(フレーミング ビットを含まず、FCS オクテットを含む、64 オクテット未満のパケット)の数。
- [ジャバー]:2000 オクテットを超える受信済みパケット合計数。この数にはフレーミング ビットは含まれず、FCS オクテットは含まれます。この FCS オクテットには、オクテットの整数(FCS エラー)を持つ不良 Frame Check Sequence (FCS; フレーム チェック シーケンス)、または非整数オクテット(アラインメント エラー)を持つ不良 FCS のいずれかが含まれます。
- [コリジョン]:受信済みコリジョン数。
- [利用率]: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。

RMON イベント制御

アラームをトリガーするオカレンスや、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されます。

- [イベント] ページ:アラームがトリガーされたときに発生するアクションを設定します。これは、ログとトラップのどのような組み合わせでも構いません。
- [アラーム] ページ:アラームをトリガーするオカレンスを設定します。

RMON イベントを定義するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [イベント] の順にクリックします。

このページには、事前に定義されたイベントが表示されます。

このページのフィールドは、[時間] フィールドを除き、[RMONイベントの追加] ダイアログボックスによって定義されます。

- [時間]:イベントの時刻を表示します。(これは、親ウィンドウの読み取り専用テーブルであり、定義できません。)

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [イベントエントリ]:新しいエントリのイベント エントリ インデックス番号が表示されます。
- [コミュニティ]:トラップが送信されるときに含める SNMP コミュニティ ストリングを入力します(任意)。トラップがネットワーク管理ステーションに届くようにするには、[通知受信者] ページを使用してコミュニティを定義する必要があることに注意してください。
- [説明]:イベントの名前を入力します。この名前は、アラームをイベントに付加する場合に [RMON アラームの追加] ページで使用されます。
- [通知タイプ]:このイベントの結果のアクションのタイプを選択します。次の値から選択します。
  - [なし]:アラームの発生時に行われるアクションはありません。
  - [ログ(イベントログテーブル)]:アラームの発生時、イベント ログ テーブルにログ エントリを追加します。
  - [トラップ(SNMPマネージャとSyslogサーバ)]:アラームの発生時、リモート ログ サーバにトラップを送信します。

- [ログとトラップ]:アラームの発生時、イベント ログ テーブルにログ エントリを追加し、リモート ログ サーバにトラップを送信します。

- [オーナー]: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 [適用] をクリックします。RMON イベントは、実行コンフィギュレーション ファイルに保存されます。

ステップ 5 [イベントログテーブル] 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(以下の説明を参照)。

RMON イベント ログ

[イベント] ページには、発生したイベント(アクション)のログが表示されます。次の 2 つのイベントのタイプがログに書き込まれます:ログまたはログとトラップ。イベントがアラームにバインドされ([RMON アラーム] ページを参照)、アラーム条件が発生した場合に、そのイベントのアクションが実行されます。

ステップ 1 [ステータスと統計情報] > [RMON] > [イベント] の順にクリックします。

ステップ 2 [イベントログテーブル] をクリックします。

イベントを表示する特定のインターフェイスをフィルタで選択できます。

このページには次のフィールドが表示されます。

- [イベントエントリ番号]:イベントのログ エントリ番号。
- [ログ番号]:ログ番号(イベント内)。
- [ログ時刻]:ログ エントリが入力された時刻。
- [説明]:アラームをトリガーしたイベントの説明。

RMON アラーム

RMON アラームは、エージェントが保守するカウンタまたはその他の SNMP オブジェクト カウンタに対して例外イベントを生成するために、しきい値とサンプリング間隔を設定するためのメカニズムを備えています。アラームには、上昇しきい値と下降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、対になっている下降しきい値を超えるまでは、上昇イベントは生成されません。下降アラームが実行された後、上昇しきい値を超えると次のアラームが実行されます。

1 つ以上のアラームが 1 つのイベントにバインドされます。イベントは、アラームの発生時に実行するアクションを示します。

アラーム カウンタは、絶対値またはカウンタ値の変化（デルタ）のいずれかで監視できます。

RMON アラームを入力するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [RMON] > [アラーム] の順にクリックします。

すでに定義されているアラームがすべて表示されます。フィールドについては、下記の [RMONアラームの追加] ページで説明されています。これらのフィールドに加え、以下のフィールドが表示されます。

- [カウンタ値]：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 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [アラームエントリ]：アラーム エントリ番号が表示されます。
- [インターフェイス]：RMON 統計情報の表示対象となるインターフェイスのタイプを選択します。
- [カウンタ名]：測定される発生タイプを示す MIB 変数を選択します。
- [サンプルタイプ]：アラームを生成するサンプリング方法を選択します。次のオプションがあります。
  - [絶対]：しきい値を超えると、アラームが生成されます。
  - [デルタ]：現在値から最後のサンプリング値を減算します。値間の差がしきい値と比較されます。しきい値を超えていると、アラームが生成されます。
- [上昇しきい値]：上昇しきい値アラームをトリガーする値を入力します。
- [上昇イベント]：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、[RMON イベント制御] ページで設定します。
- [下降しきい値]：下降しきい値アラームをトリガーする値を入力します。
- [下降イベント]：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。
- [始動アラーム]：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高い値のしきい値に向けてしきい値を超えることで定義されます。
  - [上昇アラーム]：上昇値が上昇しきい値アラームをトリガーします。
  - [下降アラーム]：下降値が下降しきい値アラームをトリガーします。
  - [上昇および下降]：上昇値と下降値の両方がアラームをトリガーします。

- [間隔]:アラーム間隔を秒単位で入力します。
- [オーナー]:アラームを受信するユーザまたはネットワーク管理システムの名前を入力します。

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

sFlow

sFlow 機能は、sFlow V5 に基づく sFlow サンプリング技術を使用した統計情報の収集を可能にします。

このサンプリング技術は、スイッチとルータに組み込まれています。この技術を使用すれば、一部または全部のインターフェイス上のトラフィック フローを同時に連続してモニタすることができます。

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に組み込まれている)と、sFlow コレクターと呼ばれる中央データ コレクターで構成されます。

sFlow エージェントは、サンプリング技術を使用してモニタしているデバイスからトラフィックと統計情報を収集します。サンプリングされたトラフィックと統計情報を分析のために sFlow コレクターに転送するときに sFlow データグラムが使用されます。

sFlow V5 で規定されている内容は次のとおりです。

- 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。
- sFlow エージェントから中央データ コレクターにデータを転送するときに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 サンプリングという 2 種類の sFlow サンプリングをサポートします。次のカウンタ サンプリングが sFlow V5(インターフェイスでサポートされている場合)に基づいて実行されます。
  - 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)

ワークフロー

デフォルトで、フロー サンプリングとカウンタ サンプリングは無効になっています。

sFlow サンプリングを有効にするには、次のようにします。

1. sFlow 統計情報のレシーバ(コレクタまたはサーバとも呼ばれる)の IP アドレスを設定します。これには [sFlow レシーバの設定] ページを使用します。
2. フロー サンプリングまたはカウンタ サンプリングを有効にして、サンプルを受信インデックスに転送し、平均サンプリング レートを設定します。これには [sFlow インターフェイス設定] ページを使用します。
3. sFlow 統計情報カウンタを表示してクリアします。これには [sFlow 統計情報] ページを使用します。

sFlow レシーバの設定

sFlow レシーバのパラメータを設定するには、次のようにします。

ステップ 1 [ステータスと統計情報] > [sFlow] > [sFlowレシーバ] の順にクリックします。

ステップ 2 次のフィールドを入力します。

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

  注 [自動] オプションが選択されている場合、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。

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

sFlow パラメータが sFlow レシーバ テーブルに表示されます。[レシーバ アドレス] フィールドは、[追加] ページの [サーバの IP アドレス/名前] フィールドと同じです。

ステップ 3 レシーバ(sFlow アナライザ)を追加するには、[追加] をクリックして、[レシーバ インデックス] 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 レシーバのアドレス フィールドに値を入力します。

- [サーバ指定方法]:sFlow サーバを 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。

[サーバ指定方法] が [IP アドレス別] の場合:

- [IPバージョン]:サーバが IPv4 または IPv6 のどちらのアドレスを使用するかを選択します。

- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 が使用される場合)。

ステップ 5 次のフィールドを入力します。

- [レシーバの IP アドレス/名前]:必要に応じて、レシーバの IP アドレスまたは名前を入力します。
- [ポート]:SYSLOG メッセージが送信されるポート。
- [最大データグラム サイズ]:単一のサンプル データグラム(フレーム)でレシーバに送信可能な最大バイト数。

ステップ 6 [適用] をクリックします。

sFlow インターフェイス設定

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

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、次のようにします。

ステップ 1 [ステータスと統計情報] > [sFlow] > [sFlowインターフェイス設定] 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 レシーバとポートを関連付けるには、ポートを選択して、[編集] をクリックし、次のフィールドに値を入力します。

- [インターフェイス]:情報を収集するユニット/ポートを選択します。

- [(フローサンプリング)状態]:フロー サンプリングを有効/無効にします。
- [サンプリングレート]: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。
- [最大ヘッダーサイズ]:サンプリングしたパケットからコピーする必要のある最大バイト数。
- [レシーバインデックス]:[sFlow レシーバの設定] ページで定義したインデックスのいずれかを選択します。
- [(カウンタサンプリング)状態]:カウンタ サンプリングを有効/無効にします。
- [サンプリング間隔]:x が入力された場合は、カウンタ サンプルが x 秒ごとに取得されるように指定されます。
- [レシーバインデックス]:これらの [sFlow レシーバの設定] 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 [適用] 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、次のようにします。

- [ステータスと統計情報] > [sFlow] > [sFlow統計情報] の順にクリックします。

  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。

  - [インターフェイス]:サンプルが収集されたポート。
  - [サンプリングパケット数]:サンプリングされたパケットの数。
  - [レシーバに送信されたデータグラム数]:送信された sFlow サンプリングパケットの数。

ログの表示

デバイスは、次のログに記録することができます。

- RAM へのログ(リブート時にクリア)
- フラッシュ メモリへのログ(ユーザ コマンドでのみクリア)

重大度により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 サーバ上のログを含む、複数のログに送信することができます。

RAM メモリ

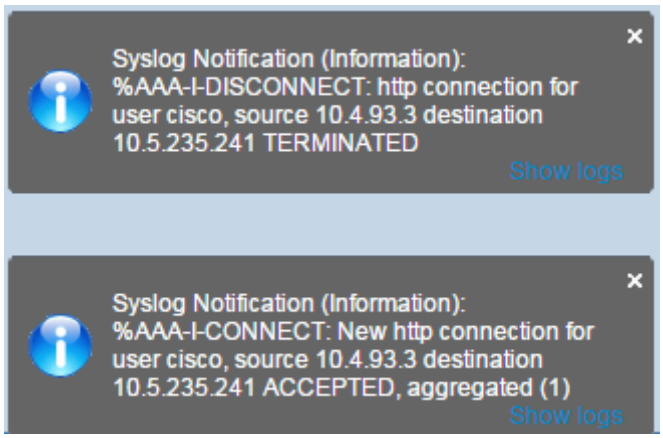
[RAM メモリ] ページには、RAM（キャッシュ）に保存されたすべてのメッセージが時間順に表示されます。エントリは、[ログ設定] ページ内のコンフィギュレーションに従って、RAM ログに保存されます。

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 に関する通知ポップアップが画面右下に表示されます。

通知ポップアップが表示されます以下を参照してください。



ログ エントリを表示するには、[ステータスと統計情報] > [ログの表示] > [RAMメモリ] の順にクリックします。

ページの上部に以下が表示されます。

- [アラートアイコン点滅]: 無効と有効を切り替えます。
- [ポップアップ Syslog 通知]: 前述したようにポップアップ SYSLOG の受信を有効にします。
- [現在のロギングしきい値]: 生成するロギングのレベルを指定します。フィールド名の横の [編集] をクリックすると、これを変更できます。

このページには、各ログ ファイルについての次のフィールドが含まれています。

- [ログ インデックス]: 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。
- [重大度]: イベントの重大度。
- [説明]: 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、[ログのクリア] をクリックします。メッセージがクリアされます。

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。ログの最小重大度は [ログ設定] ページで設定します。フラッシュ ログはデバイスの再起動時に保持されます。ログは手動でクリアできます。

フラッシュ ログを表示するには、[ステータスと統計情報] > [ログの表示] > [フラッシュ メモリ] の順にクリックします。

[現在のロギングしきい値] は、生成されるロギングのレベルを指定します。フィールド名の横の [編集] をクリックすると、これを変更できます。

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ています。

- [ログ インデックス]: 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。
- [重大度]: イベントの重大度。
- [説明]: 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、[ログのクリア] をクリックします。メッセージがクリアされます。

5

管理

この項では、システム情報の表示方法と、デバイスでのさまざまなオプションの設定方法について説明します。

具体的な内容は、次のとおりです。

- デバイス モデル
- システム設定
- コンソール設定（オートボー レート サポート）
- スタック管理
- ユーザ アカウント
- アイドルセッションタイムアウト
- 時間設定
- システム ログ
- ファイル管理
- プラグアンドプレイ（PNP）
- リブート
- ルーティング リソース
- ディスカバリ - Bonjour
- ディスカバリ - LLDP
- ディスカバリ - CDP
- デバイスの特定
- Ping
- トレースルート

デバイス モデル

全モデル、Web ベースのスイッチ設定ユーティリティ から完全に管理できます。

注 ポートの名前付け規則に関しては、インターフェイス命名規則をご覧ください。

次の表に、さまざまなモデル、それぞれのポートの個数とタイプ、およびそれらの PoE 情報を示します。

サポートされているデバイス モデルを次に示します。

SKU 名	説明	ファンの数	冗長ファンの数
SG350-10	SG350-10 10 ポート ギガビット マネージド スイッチ	0	0
SG350-10P	SG350-10P 10 ポート ギガビット POE マネージド スイッチ	0	0
SG355-10P	SG355-10P 10 ポート ギガビット POE マネージド スイッチ(内部電源)	0	0
SG350-10MP	SG350-10MP 10 ポート ギガビット Max-POE マネージド スイッチ	0	0
SG350-28	SG350-28 28 ポート ギガビット マネージド スイッチ	0	0
SG350-28P	SG350-28P 28 ポート ギガビット POE マネージド スイッチ	2	0
SG350-28MP	SG350-28MP 28 ポート ギガビット Max-POE マネージド スイッチ	3	0
SG350X-24	24 ポート ギガビット スタッカブル マネージド スイッチ	1	0
SG350X-24P	24 ポート ギガビット PoE スタッカブル マネージド スイッチ	2	0
SG350X-24MP	24 ポート ギガビット PoE スタッカブル マネージド スイッチ	3	0
SG350X-48	48 ポート ギガビット スタッカブル マネージド スイッチ	2	0

SKU 名	説明	ファンの数	冗長ファンの数
SG350X-48P	48 ポート ギガビット PoE スタッカブル マネージド スイッチ	4	0
SG350X-48MP	48 ポート ギガビット PoE スタッカブル マネージド スイッチ	4	0
SG350XG-24F	SG350XG-24F 24 ポート 10 G SFP+ スタッカブル マネージド スイッチ	4	0
SG350XG-24T	SG350XG-24T 24 ポート 10 G Base-T スタッカブル マネージド スイッチ	4	0
SG350XG-48T	SG350XG-48T 48 ポート 10GBase-T スタッカブル マネージド スイッチ	4	0
SG350XG-2F10	SG350XG-2F10 12 ポート 10G スタッカブル マネージド スイッチ	3	0
SG350-8PD	SG350-8PD 8 ポート 2.5 G POE マネージド スイッチ	0	0
SG350X-8PMD	SG350X-8PMD 8 ポート 2.5 G POE スタッカブル マネージド スイッチ	1	0
SG350X-24PD	SG350X-24PD 24 ポート 2.5 G POE スタッカブル マネージド スイッチ	2	0
SF550X-24	24 ポート 10/100 スタッカブル マネージド スイッチ	1	1
SF550X-24P	24 ポート 10/100 PoE スタッカブル マネージド スイッチ	2	1
SF550X-24MP	24 ポート 10/100 PoE スタッカブル マネージド スイッチ	3	1
SF550X-48	48 ポート 10/100 スタッカブル マネージド スイッチ	2	0
SF550X-48P	48 ポート 10/100 PoE スタッカブル マネージド スイッチ	3	1
SF550X-48MP	48 ポート 10/100 PoE スタッカブル マネージド スイッチ	5	1
SG550XG-8F8T	16 ポート 10 ギガビット スタッカブル スイッチ(RPS サポート付き)	3	1

SKU 名	説明	ファンの数	冗長ファンの数
SG550XG-24T	24 ポート 10 GBase-T スタッカブル スイッチ(2 コンボ、RPS サポート付き)	4	1
SG550XG-48T	48 ポート 10 GBase-T スタッカブル スイッチ(2 コンボ、RPS サポート付き)	5	1
SG550XG-24F	24 ポート SFP+ 10 ギガビット スタッカブル スイッチ(2 コンボ、RPS サポート付き)	4	1

システム設定

システム設定を入力するには、次のようにします。

ステップ 1 [各種管理] > [システム設定] の順にクリックします。

ステップ 2 システム設定を表示または変更します。

- [システムの説明]:デバイスの説明を表示します。
- [システム ロケーション]:デバイスの物理的な場所を入力します。
- [システム コンタクト先]:連絡先の担当者名を入力します。
- [ホスト名]:このデバイスのホスト名を選択します。これは CLI コマンドのプロンプトで使用されます。
  - [デフォルトを使用]:これらのスイッチのデフォルト ホスト名(システム名)は、switch123456 で、123456 は 16 進数のデバイス MAC アドレスの下位 3 バイトになります。
  - [ユーザ定義]:ホスト名を入力します。文字、数字、およびハイフンのみ使用できます。ホスト名の開始または終了はハイフンにできません。その他の記号、句読点、ブランクも使用できません(RFC1033、1034、1035 の規定により)。
- [カスタムバナー設定]:次のバナーを設定できます。
  - [ログイン バナー]:ここに入力するテキストはログイン前のログイン ページに表示されます。[プレビュー] をクリックすると、結果を表示できます。

- [ウェルカム バナー]:ここに入力するテキストはログイン後のログイン ページに表示されます。[プレビュー] をクリックすると、結果を表示できます。

注 Web ベースのコンフィギュレーション 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、および SSH)のバナーもアクティブになります。

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

コンソール設定(オートボー レート サポート)

コンソール ポートに設定できる速度は、次の値のいずれかです。4800、9600、19200、38400、57600、および 115200、または自動検出。

[自動検出] を選択すると、デバイスがコンソールの速度を自動的に検出します。

[自動検出] を有効にしていない場合、コンソール ポートの速度は手動で最後に設定した値に自動的に設定されます(デフォルトでは 115,200)。

[自動検出] が有効でもコンソール ボー レートが検出できない場合、システムはテキスト(ブートアップ情報など)の表示速度として 115,200 を使用します。

[コンソール設定] ページで自動検出を有効にした後で、コンソールをデバイスに接続し、Enter キーを 2 回押すと、自動検出が有効化されます。デバイスは、ボー レートを自動的に検出します。

自動検出を有効にする、またはコンソールのボー レートを手動で設定するには、次のようにします。

ステップ 1 [各種管理] > [コンソール設定] の順にクリックします。

ステップ 2 [コンソールポートのボーレート] フィールドにある次のいずれかのオプションを選択します。

- [自動検出]:コンソール ボー レートは自動的に検出されます。
- [スタティック]:使用可能ないずれかの速度を選択します。

ステップ 3 [適用] をクリックします。

スタック管理

「各種管理:スタック管理」を参照してください。

ユーザ アカウント

[ユーザアカウント] 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)を許可される追加のユーザを入力したり、既存のユーザのパスワードを変更したりできます。

レベル 15 ユーザを下記の説明に従って追加すると、既定のユーザはシステムから削除されます。

注 すべてのユーザを削除することはできません。すべてのユーザが選択されている場合は、[削除] ボタンは非アクティブになります。

新しいユーザを追加するには、次のようにします。

ステップ 1 [各種管理] > [ユーザアカウント] をクリックします。

このページには、システムで定義されたユーザと、各ユーザの特権レベルが表示されます。

ステップ 2 ユーザを新しく追加するために [追加] をクリックするか、既存のユーザを修正するために [編集] をクリックします。

ステップ 3 パラメータを入力します。

- [ユーザ名]:1 ～ 20 文字の新しいユーザ名を入力します。UTF-8 文字は使用できません。
- [パスワード]:パスワードを入力します(UTF-8 文字は使用できません)。パスワードの強度と複雑度が定義されている場合、ユーザ パスワードは、パスワード強度で設定されたポリシーに従う必要があります。
- [パスワードの確認]:パスワードを再び入力します。
- [パスワード強度メーター]:パスワードの強度が表示されます。パスワードの強度と複雑度に関するポリシーは、[パスワード強度] ページで設定します。

- [ユーザレベル]:追加/編集されるユーザの特権レベルを選択します。
  - [読み取り専用CLIアクセス (1)]:ユーザは GUI にアクセスできません。単に、デバイス構成を変更しない CLI コマンドにアクセスできるだけです。
  - [読み取り/制限付き書き込みCLIアクセス (7)]:ユーザは 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 コマンドにアクセスできるだけです。詳しくは、『CLI Reference Guide』を参照してください。
  - [読み取り/書き込み管理アクセス (15)]:ユーザは GUI にアクセスでき、デバイスの設定を行うことができます。

ステップ 4 [適用] をクリックします。ユーザ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。

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] では、タイムアウトが発生するまでに管理セッションがアイドル状態を継続できる時間を設定します。タイムアウトが発生した場合、次のセッションのいずれかを再構築するには、再度ログインする必要があります。

- [HTTPセッションタイムアウト]
- [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]

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、次のようにします。

ステップ 1 [各種管理] > [アイドルセッションタイムアウト] の順にクリックします。

ステップ 2 対応する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。デフォルトのタイムアウト値は 10 分です。

ステップ 3 [適用] をクリックして、デバイスのコンフィギュレーションを設定します。

時間設定

「各種管理:時刻設定」を参照してください。

システム ログ

ここでは、複数の個別のログをデバイスで生成できるようにするためのシステム ログ機能について説明します。各ログは、システム イベントを記述するメッセージの集まりです。

デバイスは、次のローカル ログを生成します。

- コンソール インターフェイスに送信されるログ。
- RAM 内のログ イベントの巡回リストに書き込まれるログ。デバイスの再起動時に消去されます。
- フラッシュ メモリに保存される巡回ログ ファイルに書き込まれるログ。再起動後も保持されます。

加えて、SNMP トラップおよび SYSLOG メッセージの形式で、リモート SYSLOG サーバにメッセージを送信することができます。

このセクションの内容は、次のとおりです。

- ログ設定
- リモート ログの設定

ログ設定

重大度別にロギングされるイベントを選択することができます。各ログ メッセージは、重大度の最初のアルファベットで示されます(ただし「緊急(Emergency)」のみアルファベット F を使用するので例外)。このアルファベットは両側がダッシュ(-)で連結されています。たとえば、ログ メッセージ「%INIT-I-InitCompleted: … 」の重大度は **I** で、これは「情報」を意味します。

イベントの重大度は、高いものから順に次のとおりです。

- [緊急]:システムが使用不能です。
- [アラート]:アクションが必要です。
- [重大]:システムに重大な状況が発生しています。

- [エラー]:システムがエラー状態にあります。
- [警告]:システム警告が発生しました。
- [通知]:システムは適切に動作していますが、システム通知が発生しています。
- [情報]:デバイス情報。
- [デバッグ]:イベントに関する詳細情報。

RAM ログおよびフラッシュ ログに対して重大度を選択できます。これらのログはそれぞれ、[RAM メモリ] ページと [フラッシュ メモリ] ページに表示されます。

ログに保存する重大度を選択することにより、それより重大度の高いイベントはすべて、自動的にログに保存されることになります。それより低い重大度のイベントはログに保存されません。

たとえば、[警告] が選択された場合、**警告**およびこれより高いすべての重大度(緊急、アラート、重要、エラー、および警告)がログに保存されます。**警告**より低い重大度(通知、情報、およびデバッグ)のイベントはログに保存されません。

グローバル ログ パラメータを設定するには、次のようにします。

ステップ 1 [各種管理] > [システムログ] > [ログ設定] の順にクリックします。

ステップ 2 パラメータを入力します。

- [ロギング]:これを選択するとメッセージ ロギングが有効になります。
- [Syslogアグリゲータ]:これを選択すると SYSLOG メッセージとトラップの集約が有効になります。これが有効になると、同一かつ連続する 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。集約メッセージは、到着順に送信されます。各メッセージには、集約された回数が示されます。
- [最大集約時間]:SYSLOG メッセージが集約される間隔を入力します。
- [発信元ID]:この設定により、SYSLOG メッセージに発信元 ID を追加できます。次のオプションがあります。
  - [なし]:SYSLOG メッセージに発信元 ID を含めません。
  - [ホスト名]:システム ホスト名を SYSLOG メッセージに含めます。
  - [IPv4アドレス]: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 アドレス]:送信元インターフェイスの IPv6 アドレスを SYSLOG メッセージに含めます。
  - [ユーザ定義]:SYSLOG メッセージに含める記述を入力します。

- [RAMメモリロギング]:RAM に記録するメッセージの重大度を選択します。
- [フラッシュメモリロギング]:フラッシュ メモリに記録するメッセージの重大度を選択します。
- [適用] 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 ログの設定

[リモートログサーバ] 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。各サーバについて、受け取るメッセージの重大度を設定できます。

SYSLOG サーバを定義するには、次のようにします。

ステップ 1 [各種管理] > [システムログ] > [リモートログサーバ] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [IPv4発信元インターフェイス]:SYSLOG サーバに送られる SYSLOG メッセージの発信元 IPv4 アドレスとして使われる IPv4 アドレスを持つ送信元インターフェイスを選択します。
- [IPv6 発信元インターフェイス]:SYSLOG サーバに送られる SYSLOG メッセージの送信元 IPv6 アドレスとして使われる IPv6 アドレスを持つ送信元インターフェイスを選択します。

  注 [自動] オプションが選択されている場合、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。

すでに設定されたログ サーバごとに情報が記述されます。[追加] ページ内のフィールドについては以下で説明します。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

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

- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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::/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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 アドレス タイプとしてリンク ローカルが選択されている場合)。
- [ログサーバのIPアドレス/名前]:ログ サーバの 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 サーバに送信されるシステム ログの出力元のファシリティの値を選択します。サーバに割り当てられるファシリティ値は 1 つだけです。ファシリティコードが 2 度割り当てられると、最初のファシリティ値は上書きされます。
- [説明]:サーバの説明を入力します。
- [最小重大度]:サーバに送信されるシステム ログ メッセージの最小重大度を選択します。

ステップ 5 [適用] をクリックします。[リモート ログ サーバの追加] ページが閉じ、SYSLOG サーバが追加されて、実行コンフィギュレーション ファイルが更新されます。

ファイル管理

「各種管理:ファイル管理」を参照してください。

プラグアンドプレイ(PNP)

新しいネットワーク デバイスの設置やデバイスの交換を手作業で行うと費用と時間がかかり、誤りが発生しやすくなります。通常、新しいデバイスは最初に中心的な準備施設に送られ、そこでデバイスを開梱し、ステージング ネットワークに接続し、適切なライセンス、設定、イメージを使って更新します。その後、デバイスを梱包して実際の設置場所に運びます。これらの手順が完了した後、専門的な担当者が設置場所まで出向いて設置作業を行う必要があります。デバイスが NOC/データ センター自体に設置される場合でも、デバイスの数が非常に多くて専門家が不足する可能性があります。このすべての問題のために、デプロイが遅れ、運用コストがさらに増えます。

Cisco Plug-n-Play ソリューションを使用するとネットワーク デバイスのデプロイ/設置に関連するコストを減らし、設置のスピードを上げ、セキュリティを損なわずにより簡単にデプロイできます。Cisco Plug-n-Play ソリューションを使用すると、さまざまなデプロイ シナリオやデプロイ場所でスイッチをゼロ タッチ インストールすることができます。

PNP 設定

PNP を設定するには、次のようにします。

注 この機能はデフォルトで有効になっています。

ステップ 1 [管理] > [PNP] > [PNP 設定] をクリックします。

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]:デフォルトで有効になっています。

[PNP トランスポート]:PNP エージェント セッション情報とパラメータを定義します。

- [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 アドレス、および使用する TCP ポートに関する設定情報を取得するためのオプションとして、次のいずれかを選択します。
  - [デフォルト設定]:このオプションを選択すると、DHCP オプション 43 から PNP 設定が取得されます。DHCP オプション 43 から一部または全部の情報が得られない場合、次のデフォルト値が使用されます:デフォルト トランスポート プロトコル HTTP、PNP サーバの DNS 名 "pnpserver"、ポートは HTTP に関連

    [デフォルト設定] オプションを選択すると、[PNP トランスポート] セクションのすべてのフィールドがグレーで表示されます。

- [手動設定]:PNP トランスポートに使用する TCP ポートとサーバを手動で設定します。

- [TCP ポート]:TCP ポートの番号。システムにより次のように自動入力されます:80(HTTP 用)
- [サーバ指定方法]:PNP サーバを **IP アドレスで**指定するか、それとも**名前で**指定するかを選択します。
- [IP バージョン]:サポートする IP 形式を選択します。
- [サーバ IPv6 アドレス タイプ]:IP バージョン タイプが IPv6 である場合は、次のいずれかのオプションを選択します。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンク ローカル インターフェイス]:送信元 IPv6 アドレス タイプが [リンク ローカル] 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。
- [サーバのIPアドレス/名前]:PNP サーバの IP アドレスまたはドメイン名を入力します。

PNP ユーザ

- [ユーザ定義]:サーバに送られる PNP パケットに含まれるユーザ情報。次のいずれかのオプションを選択します。
  - [デフォルト値]:このオプションを選択すると、PNP ユーザ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、ユーザ名とパスワードのフィールドがグレー表示になります。
  - [手動設定]:PNP ユーザ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。
- [ユーザ名]:PNP パケットに含めるユーザ名。
- [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]:次のパラメータを入力します。

- [再接続間隔]:接続が失われた後、セッションの再接続を試行するまでの間隔(秒数)。
- [ディスカバリ タイムアウト]:PNP サーバの検出に失敗した後、ディスカバリ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]:指数を使ってディスカバリ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)。
- [ディスカバリ タイムアウト最大値]:タイムアウトの最大値。[ディスカバリ タイムアウト] 値よりも大きくなければなりません。
- [ウォッチドッグ タイムアウト]:アクティブな PNP セッション中(たとえばファイル ダウンロード処理中)に PnP またはファイル サーバからの応答を待つ間隔。

ステップ 3 [適用] 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、[機密データを平文で表示] をクリックします。

PNP セッション

この画面には、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 パラメータについての情報を表示するには、次のようにします。

ステップ 1 [管理] > [PNP] > [PNP セッション] をクリックします。

次のフィールドが表示されます。

- [管理ステータス]:PNP が有効なにっているかどうか。
- [動作ステータス]:PNP が動作中。
- [PNP エージェント状態]:アクティブな PNP セッションが存在するかどうかを示します。可能な値は、[ディスカバリ待機]、[ディスカバリ]、[準備未完了]、[無効]、[セッション]、[セッション待機] です。
- [TCP ポート]:PNP セッションの TCP ポート。

- [サーバ アドレス]:PNP サーバの IP アドレス。
- [ユーザ名]:PNP パケットで送信されるユーザ名。
- [パスワード MD5]:PNP パケットで送信されるパスワード。
- [ディスカバリ タイムアウト]:設定済みのディスカバリ タイムアウト
- [セッション間隔タイムアウト]:設定済みのセッション間隔タイムアウト(PNP エージェント状態が「待機中」の場合にのみ表示されます)。
- [残りのタイムアウト]:残っているタイムアウトの値。

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

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

リブート

ジャンボ フレームのサポートを有効にするなど、コンフィギュレーションを変更した場合、その変更を有効にするためにシステムをリブートしなければならないことがあります。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に保存しておくことが重要です。[適用] 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。ファイルおよびファイル タイプの詳細については、「システム ファイル」の項をご覧ください。

[ファイル操作] ページを使用するか、ウィンドウの上にある [保存] をクリックして、デバイス設定をバックアップできます。同じページを使用して、リモート デバイスからコンフィギュレーションをアップロードすることもできます。

将来の時刻にリブートするようにリブート時刻を設定しておくとよい場合があります。次のようなケースが考えられます。

- ユーザがリモート デバイス上でアクションを実行しており、そのアクションのミスが原因でリモート デバイスへの接続が失われる可能性がある場合。リブートをあらかじめスケジュールしておけば、指定した時間の経過後に動作設定が復元され、リモート デバイスへの接続を復元することができます。これらのアクションが正常に終了した場合は、遅延リブートを手動でキャンセルできます。

- デバイスのリロードによってネットワーク接続が失われる場合。遅延リブートを使用することにより、ユーザにとって都合のよい時間（深夜など）にリブートをスケジュールできます。

デバイスをリブートするには、次のようにします。

ステップ 1 [各種管理] > [リブート] の順にクリックします。

ステップ 2 [リブート] ボタンをクリックし、デバイスをリブートします。

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

  次のオプションが選択できます。

  - [即時]：すぐにリブートします。
  - [日付]：スケジュールするリブートの日付（月/日）、および時間（時間と分）を入力します。ソフトウェアのリロードがスケジュールされ、指定した時刻（24 時間形式）に実行されます。月と日を指定すると、指定した日時にリロードを実行するようにスケジュールされます。月と日を指定しない場合は、その日（指定時刻が現在時より後の時刻である場合）か、翌日（指定時刻が現在時より前の時刻である場合）の指定時刻にリロードが実行されます。00 時 00 分を指定すると、午前 0 時にリロードがスケジュールされます。リロードは 24 日以内に行われる必要があります。

  注 このオプションを使用するには、システム時刻が手動もしくは SNTP で設定されている必要があります。

  注 リブートがスケジュールされている場合は、[リブートのキャンセル] をクリックしてスケジュールされたリブートをキャンセルします。

  - [以内]：指定した時間および分以内にリブートを実行します。指定できる最大時間は 24 日です。

- [工場出荷時設定に戻す]：工場出荷時のデフォルト設定を使用してデバイスをリブートします。このプロセスでアクティブ イメージ、非アクティブ イメージ、ミラー コンフィギュレーション、およびローカリゼーション ファイルを除くすべてが消去されます。

  スタック ユニット ID が [自動] に設定されます。

- [スタートアップコンフィギュレーションファイルのクリア]:次にデバイスを起動する際に、そのデバイスのスタートアップ コンフィギュレーションをクリアする場合、オンにします。

ルーティング リソース

TCAM エントリは次のグループに分かれています。

- [IPエントリ]:IP スタティック ルート、IP インターフェイス、および IP ホスト用に予約済みのルータ TCAM エントリ。
- [非IPエントリ]:ACL 規則、CoS ポリサー、VLAN レート制限など、他のアプリケーション用に予約済みの TCAM エントリ。

さまざまな機能で使用される TCAM エントリ数を、次の表に示します。

ローカル エンティティ	IPv4	IPv6(PCL TCAM)	IPv6(ルータ TCAM)
IP ネイバー	1 エントリ	1 エントリ	4 エントリ
インターフェイスの IP アドレス	2 エントリ	2 エントリ	8 エントリ
IP リモート ルート	1 エントリ	1 エントリ	4 エントリ
オン リンク プレフィックス		1 エントリ	4 エントリ

VLAN マッピングでは、すべてのケースにおいて 4 つの TCAM エントリが使用されます。

[ルーティングリソース] ページで、ルータ TCAM 割り当てを調整できます。

不適切なルータ TCAM 割り当てを行うと、エラーメッセージが表示されます。ルータ TCAM 割り当てが正しい場合は、新しい設定を使用して自動リブートが実行されることを示すメッセージが表示されます。次の場合、ルーティング リソースの変更が正しく行われない可能性があります。

- 割り当てたルータ TCAM エントリ数が、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 エントリ数が、そのカテゴリで使用可能な最大エントリ数より多い場合(最大エントリ数はそのページに表示されます)。

ルーティング リソースを表示および変更するには、次のようにします。

ステップ 1 [各種管理] > [ルーティング リソース] の順にクリックします。

次のフィールドが表示されます。

[IPv4 ルーティングリソース]

- [ネイバー(ネイバーあたり x 個の TCAM エントリ)]:[カウント] はデバイスに登録されているネイバーの数を表し、[TCAM エントリ] はネイバーに使用されているルータ TCAM エントリ数を表わします。SG550XG ファミリの場合はネイバーあたり 4 つの TCAM エントリが、SG350XG ファミリの場合はネイバーあたり 1 つの TCAM エントリが存在します。
- [インターフェイス(インターフェイスあたり x 個の TCAM エントリ)]:[カウント] はデバイス上のインターフェイスの IP アドレス数を表し、[TCAM エントリ] は IP アドレスに使用されているルータ TCAM エントリ数を表わします。
- [ルート(ルートあたり x 個の TCAM エントリ)]:[カウント] はデバイスに登録されているルートの数を表し、[TCAM エントリ] はルートに使用されているルータ TCAM エントリ数を表わします。
- [合計]:現在使用中のルータ TCAM エントリ数を表示します。
- [最大エントリ数]:次のいずれかを選択します。
  - [デフォルトを使用]:デフォルト値を使用します。
  - [ユーザ定義]:値を入力します。

[IPv4 マルチキャスト ルーティングリソース]

- [IPv4マルチキャストルート(ルートあたり2個のTCAMエントリ)]:[カウント] はデバイスに登録されているマルチキャスト ルート数を表し、[TCAMエントリ] はマルチキャスト ルートに使用されている TCAM エントリ数を表わします。
- [最大エントリ数]:次のいずれかを選択します。
  - [デフォルトを使用]:デフォルト値を使用します。
  - [ユーザ定義]:値を入力します。

[IPv4 ポリシーベースのルーティングリソース]

- [IPv4 ポリシー ベース ルート(ルートあたり x 個の TCAM エントリ)]:[カウント] はデバイスに登録されているマルチキャスト ルート数を表し、[TCAM エントリ] はマルチキャスト ルートに使用されている TCAM エントリ数を表わします。

- [最大エントリ数]:次のいずれかを選択します。
  - [デフォルトを使用]:デフォルト値を使用します。
  - [ユーザ定義]:値を入力します。

[IPv6 ルーティングリソース]

- [ネイバー(ネイバーあたりx個のTCAMエントリ)]:[カウント] はデバイスに登録されているネイバーの数を表し、[TCAMエントリ] はネイバーに使用されている TCAM エントリの数を表わします。
- [インターフェイス(インターフェイスあたりx個のTCAMエントリ)]:[カウント] はデバイスのインターフェイス数を表し、[TCAMエントリ] はインターフェイスに使用されている TCAM エントリ数を表わします。
- [オンリンクプレフィックス(プレフィックスあたりx個のTCAMエントリ)]:[カウント] はデバイスに登録されているオン リンク プレフィックス数を表し、[TCAMエントリ] はそれらのプレフィックスに使用されている TCAM エントリ数を表わします。
- [ルート(ルートあたりx個のTCAMエントリ)]:[カウント] はデバイスに登録されているオン リンク プレフィックス数を表し、[TCAMエントリ]TCAM はそれらのプレフィックスに使用されている TCAM エントリ数を表わします。
- [合計]:現在使用中の合計 TCAM エントリ数。
- [最大エントリ数]:次のいずれかを選択します。
  - [デフォルトを使用]:デフォルト値を使用します。
  - [ユーザ定義]:値を入力します。

[IPv6 マルチキャストルーティングリソース]

- [IPv6 マルチキャスト ルート(ルートあたり x 個の TCAM エントリ)]:[カウント] はデバイスに登録されているマルチキャスト ルート数を表し、[TCAM エントリ] はマルチキャスト ルートに使用されている TCAM エントリ数を表わします。
- [最大エントリ数]:次のいずれかを選択します。
  - [デフォルトを使用]:デフォルト値を使用します。
  - [ユーザ定義]:値を入力します。

[IPv6 ポリシーベースのルーティングリソース]

- [IPv6 ポリシー ベース ルート（ルートあたり 4 個の TCAM エントリ）]:[カウント] はデバイスに登録されているマルチキャスト ルート数を表し、[TCAM エントリ] はマルチキャスト ルートに使用されている TCAM エントリ数を表わします。
- [最大エントリ数]:次のいずれかを選択します。
  - [デフォルトを使用]:デフォルト値を使用します。
  - [ユーザ定義]:値を入力します。

[VLAN マッピング ルーティングリソース]

- [VLAN マッピング エントリ（4 個の TCAM エントリ マッピング）]:[カウント] はデバイス上で記録されている VLAN マッピング エントリ数を表し、[TCAM エントリ] はその VLAN マッピングに使用されている TCAM エントリ数を表します。
- [最大エントリ数]:次のいずれかを選択します。
  - [デフォルトを使用]:デフォルト値を使用します。
  - [ユーザ定義]:値を入力します。

ステップ 2 [適用] をクリックして、新しい設定を保存します。この操作により、ルーティング リソースの設定が適切かどうかのチェックが実行されます。正しくない場合、エラー メッセージが表示されます。正しい場合は、設定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。

[TCAMリソーステーブル]:実際に使用中および使用可能な TCAM の数を表示します。

- [ユニット番号]:スタック内のデバイスのユニットの番号。
- [ルーティングおよびマルチキャストルーティングの最大 TCAM エントリ数]:ルーティングおよびマルチキャスト ルーティングに使用可能な TCAM エントリ数。
- [IPv4 ルーティング]
  - [使用中]:IPv4 ルーティングに使用している TCAM エントリ数。
  - [最大]:IPv4 ルーティングに使用可能な最大 TCAM エントリ数。
- [IPv4 マルチキャスト ルーティング]
  - [使用中]:IPv4 マルチキャスト ルーティングに使用している TCAM エントリ数。
  - [最大]:IPv4 マルチキャスト ルーティングに使用可能な最大 TCAM エントリ数。

- [IPv4 ポリシーベースのルーティング]
  - [使用中]:IPv4 ポリシーベース 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 エントリの数。
- [IPv6 ルーティング]
  - [使用中]:IPv6 ルーティングに使用している TCAM エントリ数。
  - [最大]:IPv6 ルーティングに使用可能な最大 TCAM エントリ数。
- [IPv6 マルチキャスト ルーティング]
  - [使用中]:IPv6 マルチキャスト ルーティングに使用している TCAM エントリ数。
  - [最大]:IPv6 マルチキャスト ルーティングに使用可能な最大 TCAM エントリ数。
- [IPv6 ポリシーベースのルーティング]
  - [使用中]:IPv6 ポリシーベース 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 エントリの数。
- [非IPルールの最大TCAMエントリ数]:非 IP ルールに使用可能な TCAM エントリ数。
- [非IPルール]
  - [使用中]:非 IP ルールに使用している TCAM エントリ数。
  - [最大]:非 IP ルールに使用可能な最大 TCAM エントリ数。
- [VLAN マッピング]
  - [使用中]:非 IP ルールに使用されている VLAN マッピング エントリの数。
  - [最大]:非 IP ルールに使用可能な VLAN マッピング エントリの最大数。

ディスカバリ - Bonjour

「Bonjour」を参照してください。

ディスカバリ - LLDP

「ディスカバリ - LLDP」を参照してください。

ディスカバリ - CDP

「ディスカバリ - CDP」を参照してください。

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上のすべてのネットワーク ポート LED を点滅させることにより、そのデバイスを物理的に特定できるようにします。この機能は、複数のデバイスが相互接続された部屋の中でのデバイスの特定に役立ちます。この機能がアクティブになっている場合は、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（デフォルトは 1 分間）点滅します。スタック型デバイスでは、スタック内の特定のユニットまたはすべてのユニットを指定できます。

ステップ 1 [管理] > [デバイスの特定] 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。

- [時間]: ポートの LED を点滅させる時間（秒単位）を入力します。
- [残り時間]; このフィールドは、この機能がアクティブになっている場合にのみ表示されます。ここには、LED が点滅する残り時間が表示されます。
- [ユニット ID]: このフィールドは、デバイスがスタック内に存在する場合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 [すべて] を選択します。

ステップ 3 この機能をアクティブにするには、[開始] をクリックします。

この機能がアクティブになると、[開始] ボタンが [停止] ボタンに変わります。このボタンを使用すれば、定義されたタイマーが切れる前に 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、デバイスから宛先デバイスに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、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）エコー リクエスト パケットを対象ホストに送信し、pong とも呼ばれる ICMP 応答を待機することで動作します。往復にかかった時間が計測され、すべてのパケット ロスが記録されます。

ホストを ping するには、次のようにします。

ステップ 1 [各種管理] > [Ping] 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 Ping を設定します。

- [ホスト指定方法]：送信元インターフェイスを IP アドレスで指定するか、名前で指定するかを選択します。このフィールドは、次に説明する、[送信元IP] フィールドに表示されるインターフェイスに影響を及ぼします。
- [IP バージョン]：送信元インターフェイスを IP アドレスで指定する場合は、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。
- [ソース IP]：送信元インターフェイスを選択します。この IPv4 アドレスが、宛先との通信で送信元 IPv4 アドレスとして使用されます。[ホスト指定方法] フィールドに [名前] 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。[ホスト指定方法] フィールドに [IPアドレス] を指定した場合、[IPバージョン] 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 [自動] オプションを選択した場合、宛先アドレスを基に、システムが送信元アドレスを計算します。

- [送信先IPv6アドレスタイプ]：次のいずれかのオプションを選択します。
  - [リンク ローカル]：IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]：IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]:IPv6 アドレス タイプが [リンクローカル] である場合は、どこから IPv6 アドレスを受け取るかを選択します。
- [宛先 IP アドレス/名前]:ping 対象デバイスのアドレスまたはホスト名。IP アドレスかホスト名かは、[ホスト指定方法] によって決まります。
- [ping 間隔]: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、[ping 回数] 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、特定の値を指定します。
- [ping 回数]:ping 操作を実行する回数。デフォルト値を使用するか、特定の値を指定します。
- [ステータス]: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 ホストを ping するには、[ping の実行] をクリックします。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カウンタとステータス] セクションに Ping の結果が表示されます。

- [送信済みパケット数]:ping によって送信されたパケット数
- [受信済みパケット数]:ping によって受信されたパケット数
- [損失パケット数]:ping プロセス中に消失したパケットの割合
- [最低ラウンドトリップ時間]:パケットが戻るまでの最短時間
- [最大ラウンドトリップ時間]:パケットが戻るまでの最長時間
- [平均ラウンドトリップ時間]:パケットが戻るまでの平均時間
- [ステータス]:失敗か成功か

トレースルート

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、パケットが転送される IP ルートを検出します。[トレースルート] ページには、デバイスとターゲット ホスト間の各ホップ、および各ホップのラウンドトリップ時間が表示されます。

ステップ 1 [各種管理] > [トレースルート] の順にクリックします。

ステップ 2 次のフィールドに情報を入力して、トレースルートを設定します。

- [ホスト指定方法]:ホストを 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]:ホストを IP アドレスで指定する場合は、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。
- [ソース IP]:送信元インターフェイスを選択します。この 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。[ホスト指定方法] フィールドに [名前] 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。[ホスト指定方法] フィールドに [IPアドレス] を指定した場合、[IPバージョン] 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。
- [ホストの IP アドレス/名前]:ホスト アドレスまたは名前を入力します。
- [TTL]:トレースルートで許可する最大ホップ数を入力します。送信したフレームが無限ループに入るのを防ぐために使用します。トレースルート コマンドは、宛先に到達するか、設定した値に達すると終了します。デフォルト値(30)を使用する場合は [デフォルトを使用] を選択します。
- [タイムアウト]: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、[デフォルトを使用] を選択します。

ステップ 3 [トレースルートのアクティブ化] をクリックします。処理が実行されます。

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

- [インデックス]:ホップの数が表示されます。
- [ホスト]:宛先までのルートにある停止位置が表示されます。

[ラウンドトリップ時間(1-3)]:第 1 フレームから第 3 フレームまでのラウンドトリップ時間(ミリ秒単位)、および第 1 から第 3 までの操作のステータスが表示されます。

6

各種管理:ファイル管理

ここでは、システム ファイルの管理方法について説明します。

具体的な内容は、次のとおりです。

- システム ファイル
- ファームウェア操作
- ファイル操作
- ファイル ディレクトリ
- DHCP 自動コンフィギュレーション/イメージ更新

システム ファイル

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。

通常、**flash://system/** フォルダに含まれるファイルはシステム ファイルです。

これらのファイルを使用してさまざまなアクションが実行されます。たとえば、デバイス ブートの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 ファイルのコピー、外部サーバなどの外部デバイスとの間のファイルのコピーなどです。

デバイス上のコンフィギュレーション ファイルはそれぞれのタイプによって定義され、そのデバイスの設定やパラメータ値を格納します。

デバイス上の他のファイルには、ファームウェア ファイル、ログ ファイルがあり、これらは*動作ファイル*と呼ばれます。

コンフィギュレーション ファイルはテキスト ファイルであり、PC などの外部デバイスにコピーした後、メモ帳などのテキスト エディタで編集できます。

ファイルおよびファイル タイプ

デバイス上に存在するファイルのタイプの例を次に説明します。

- **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しているパラメータが含まれています。デバイスのパラメータ値を変更すると、このファイルが変更されます。

  デバイスがリブートされると、実行コンフィギュレーションは失われます。

  デバイスに対して加えた変更を保持するには、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か、他のファイル タイプに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**:別のコンフィギュレーション(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により保存されるパラメータ値。

  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存され、デバイスがリブートしても保持されます。デバイスがリブートすると、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認識されます。

- **ミラー コンフィギュレーション**:次の状況が生じている場合に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。

  - デバイスが 24 時間続けて稼動している。
  - 24 時間、実行コンフィギュレーションの内容が変更されていない。
  - スタートアップ コンフィギュレーションと実行コンフィギュレーションが同じである。

  スタートアップ コンフィギュレーションからミラー コンフィギュレーションへのコピーはシステムによってのみ行われます。ただし、ミラー コンフィギュレーションから別のファイル タイプや別のデバイスに手動でコピーすることはできます。

  実行コンフィギュレーションをミラーコンフィギュレーションに自動的にコピーするオプションは、[ファイル ディレクトリ] ページで無効にできます。

- **バックアップ ファイル**:システム シャットダウンからの保護や、特定の運用状態の維持のために、ファイルを手動でコピーしたもの。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、および実行コンフィギュレーションを、バックアップ ファイルにコピーできます。バックアップはフラッシュ内か、PC または USB ドライブ上に存在し、デバイスがリブートしても保持されます。

- **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。より一般的にはイメージ と呼ばれます。
- **言語ファイル**:Web ベースのコンフィギュレーション ユーティリティのウィンドウを、選択した言語で表示できるようにする辞書。
- **ロギング ファイル**:フラッシュ メモリ内に保存される SYSLOG メッセージ。

ファームウェア操作

[ファームウェア操作] ページは次の用途に使用できます。

- 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

次のファイル転送方法がサポートされています。

- ブラウザの機能を使用する HTTP/HTTPS
- USB
- TFTP サーバを必要とする TFTP
- SCP サーバを必要とする Secure Copy Protocol(SCP)

スタックが適切に動作するため、スタック内のユニットのソフトウェア イメージは同一のものである必要があります。スタック 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。

- デバイスをスタックに追加する前に、デバイスのファームウェアを手動でアップグレードできます(推奨)。
- 新しく追加されたユニットのファームウェアがマスターと同じではない場合、スタック マスターはそのユニットのファームウェアを自動的にアップグレードします。

デバイスには 2 つのファームウェア イメージが保存されています。一方のイメージはアクティブ イメージとなり、もう一方のイメージは非アクティブ イメージとなります。

デバイスのファームウェアを更新すると、新しいファームウェアが非アクティブ イメージを必ず上書きします。デバイスに新しいファームウェアをアップロードすると、次に起動する際には新しいバージョンが使用されます。リブート後、元のバージョンは非アクティブ バージョンになります。

HTTP/HTTPS または USB を使用してファームウェアを更新またはバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファームウェア操作] の順にクリックします。

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]:現在のアクティブなファームウェアファイルを表示します。
- [アクティブなファームウェアバージョン]:現在のアクティブなファームウェア ファイルのバージョンを表示します。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[ファームウェアの更新] または [ファームウェアのバックアップ] を選択します。
- [コピー方法]:[HTTP/HTTPS] または [USB] を選択します。
- [ファイル名]:更新するファイルの名前を入力します(HTTP/HTTPS によるバックアップは該当せず)。

ステップ 3 [適用] をクリックします。

ステップ 4 [リブート] をクリックします。

TFTP を使用してファームウェアを更新またはバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファームウェア操作] の順にクリックします。

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]:現在のアクティブなファームウェアファイルを表示します。
- [アクティブなファームウェアバージョン]:現在のアクティブなファームウェア ファイルのバージョンを表示します。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[ファームウェアの更新] または [ファームウェアのバックアップ] を選択します。
- [コピー方法]:[TFTP] を選択します。

- [サーバ指定方法]:TFTP サーバを 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。

[サーバ指定方法] がアドレス指定の場合:

- [IPバージョン]:([サーバ指定方法] がアドレス指定の場合)このサーバに IPv4 アドレスと IPv6 アドレスのどちらを使用するかを選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 が使用される場合)。
- [サーバのIPアドレス/名前]:TFTP サーバの 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。
- **(更新)**[ソース]:ソース ファイル名を入力します。
- **(バックアップ)**[宛先]:バックアップ ファイル名を入力します。

ステップ 3 操作を開始するには、[適用] をクリックします。

SCP を使用してファームウェアを更新またはバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファームウェア操作] の順にクリックします。

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]:現在のアクティブなファームウェア ファイルを表示します。
- [アクティブなファームウェアバージョン]:現在のアクティブなファームウェア ファイルのバージョンを表示します。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[ファームウェアの更新] または [ファームウェアのバックアップ] を選択します。
- [コピー方法]:[SCP] を選択します。

ステップ 3 **リモート SSH サーバ認証**による SSH サーバ認証(デフォルトでは無効)を有効にするには、[編集] をクリックします。そうすると、[SSH サーバ認証] ページに移動するので、ここで SSH サーバを設定します。

ステップ 4 このページに戻ります。

ステップ 5 [SSHクライアント認証] を実行するには、次のメソッドのいずれかを選択します。

- [SSHクライアントシステムクレデンシャルの使用]:固定 SSH ユーザ クレデンシャルを設定します。[SSHユーザ認証] ページに移動するには、[システムクレデンシャル] をクリックします。このページで、恒久的に使用するユーザとパスワードを設定できます。
- [SSHクライアントのワンタイムクレデンシャルを使用]:次の値を入力します。
  - [ユーザ名]:今回のコピー アクションに使用するユーザ名を入力します。
  - [パスワード]:今回のコピーに使用するパスワードを入力します。

  注 ワンタイム クレデンシャルに使用するユーザ名とパスワードは、コンフィギュレーション ファイルに保存されません。

ステップ 6 次のフィールドを入力します。

- [サーバ指定方法]:SCP サーバを IP アドレスで指定するか、ドメインの名前で指定するかを選択します。

[サーバ指定方法] がアドレス指定の場合:

- [IPバージョン]:IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。
- [IPv6アドレスタイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。

  [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

  [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPv6 タイプになります。

- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します。

- [サーバのIPアドレス/名前]:SCP サーバの IP アドレスまたはドメイン名を入力します。どちらでも構いません。
- (更新)[ソース]:ソース ファイル名を入力します。
- (バックアップ)[宛先]:バックアップ ファイル名を入力します。

ステップ 7 [適用] をクリックします。ファイル、パスワード、サーバ アドレスがすべて正しい場合は、次のいずれかの結果になります。

- SSH サーバ認証が([SSHサーバ認証] ページで)有効になっており、SCP サーバが信頼された場合、その操作は成功します。SCP サーバが信頼されない場合、操作は失敗し、エラーが表示されます。
- SSH サーバ認証が有効でない場合は、どの SCP サーバに対しても操作は成功します。

イメージ ファイルを切り替えるには:

ステップ 1 [各種管理] > [ファイル管理] > [ファームウェア操作] の順にクリックします。

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]:現在のアクティブなファームウェア ファイルを表示します。
- [アクティブなファームウェアバージョン]:現在のアクティブなファームウェア ファイルのバージョンを表示します。

ステップ 2 次のフィールドが表示されます。

- [操作タイプ]:[イメージの切り替え] を選択します。
- [リブート後のアクティブイメージ]:リブート後にアクティブにするファームウェア ファイルを選択します。
- [リブート後のアクティブイメージバージョン番号]:リブート後のファームウェア ファイルのバージョンが表示されます。

ステップ 3 [適用] をクリックします。新しいファームウェアを使用してすぐにリロードする場合は、成功メッセージが表示された後で [リブート] をクリックします。

ファイル操作

[ファイル操作] ページからは次の操作を行えます。

- デバイスのコンフィギュレーション ファイルやログを外部デバイスにバックアップする。
- 外部デバイスからデバイスにコンフィギュレーション ファイルを復元する。
- コンフィギュレーション ファイルを複製する。

注 デバイスがスタック内にある場合、コンフィギュレーション ファイルはマスター ユニットから取得されます。

コンフィギュレーション ファイルを実行コンフィギュレーションに復元すると、インポートされたファイルは、元のファイルにはなかったコンフィギュレーション コマンドを追加し、既存のコンフィギュレーション コマンド内のパラメータ値を上書きします。

コンフィギュレーション ファイルをスタートアップ コンフィギュレーションに復元すると、新しいファイルによって元のファイルが置換されます。

スタートアップ コンフィギュレーションに復元する場合は、その復元されたスタートアップ コンフィギュレーションを実行コンフィギュレーションとして使用するためにデバイスをリブートする必要があります。デバイスをリブートするには、「リブート」で説明されているプロセスを使用します。

いずれかのウィンドウで [適用] をクリックすると、デバイスのコンフィギュレーション設定に加えた変更内容が実行コンフィギュレーションにのみ保存されます。

注意 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か別のコンフィギュレーション ファイルにコピーしていない場合、デバイスをリブートすると、最後にファイルがコピーされた後に加えられた変更はすべて失われます。

次の組み合わせによる内部ファイル タイプのコピーが可能です。

- 実行コンフィギュレーションから、スタートアップ コンフィギュレーション、または他のバックアップ ファイルへのコピー。
- スタートアップ コンフィギュレーションから、実行コンフィギュレーション、または他のバックアップ ファイルへのコピー。
- バックアップ ファイルから、実行コンフィギュレーション、またはスタートアップ コンフィギュレーションへのコピー。

- ミラー コンフィギュレーションから、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、またはバックアップ ファイルへのコピー。

次の項でこれらの操作について説明します。

HTTP/HTTPS、USB、または内部フラッシュを使用してシステム コンフィギュレーション ファイルを更新するには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[更新ファイル] を選択します。
- [宛先ファイルタイプ]:更新するコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]:[HTTP/HTTPS]、[USB]、または [内部フラッシュ] を選択します。
- [ファイル名]:更新元になるファイル(ソース ファイル)の名前を入力します。

ステップ 3 操作を開始するには、[適用] をクリックします。

TFTP を使用してシステム コンフィギュレーション ファイルを更新するには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[更新ファイル] を選択します。
- [宛先ファイルタイプ]:更新するコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]:[TFTP] を選択します。
- [サーバ指定方法]:TFTP サーバを IP アドレスで指定するか、ドメイン名で指定するかを選択します。

  [サーバ指定方法] がアドレス指定の場合:

  - [IPバージョン]:IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。

    [サーバ指定方法] でサーバを名前で選択するように指定した場合、IP バージョン関連のオプションを選択する必要はありません。

- [IPv6アドレスタイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。

  [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

  [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します。

- [サーバのIPアドレス/名前]:TFTP サーバの IP アドレスまたは名前を入力します。
- [ソース]:更新ファイル名を入力します。

ステップ 3 操作を開始するには、[適用] をクリックします。

SCP を使用してシステム コンフィギュレーション ファイルを更新するには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[更新ファイル] を選択します。
- [宛先ファイルタイプ]:更新するコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]:[SCP] を選択します。

ステップ 3 **リモート SSH サーバ認証**による SSH サーバ認証(デフォルトでは無効)を有効にするには、[編集] をクリックします。そうすると、[SSH サーバ認証] ページに移動するので、ここで SSH サーバを設定します。

ステップ 4 このページに戻ります。

ステップ 5 [SSHクライアント認証] を実行するには、次のメソッドのいずれかを選択します。

- [SSHクライアントシステムクレデンシャルの使用]:固定 SSH ユーザ クレデンシャルを設定します。[SSHユーザ認証] ページに移動するには、[システムクレデンシャル] をクリックします。このページで、恒久的に使用するユーザとパスワードを設定できます。
- [SSHクライアントのワンタイムクレデンシャルを使用]:次の値を入力します。
  - [ユーザ名]:今回のコピー アクションに使用するユーザ名を入力します。
  - [パスワード]:今回のコピーに使用するパスワードを入力します。

  注 ワンタイム クレデンシャルに使用するユーザ名とパスワードは、コンフィギュレーション ファイルに保存されません。
- [サーバ指定方法]:SCP サーバを IP アドレスで指定するか、ドメインの名前で指定するかを選択します。

  [サーバ指定方法] がアドレス指定の場合:
  - [IPバージョン]:IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。
  - [IPv6アドレスタイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。

    [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

    [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
  - [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します。
- [サーバのIPアドレス/名前]:SCP サーバの IP アドレスまたは名前を入力します。
- [ソース]:ソース ファイル名を入力します。

ステップ 6 操作を開始するには、[適用] をクリックします。

HTTP/HTTPS を使用してシステム コンフィギュレーション ファイルをバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[バックアップファイル] を選択します。
- [ソースファイルタイプ]:バックアップするコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]:[HTTP/HTTPS] を選択します。
- [機密データの処理]:機密データをバックアップ ファイルに含める方法を選択します。次のオプションが選択できます。
  - [除外]:機密データをバックアップに含めません。
  - [暗号化]:機密データを暗号化してバックアップに含めます。
  - [プレーンテキスト]:機密データをプレーンテキスト形式でバックアップに含めます。

  注 使用可能な機密データ オプションは、現在のユーザの SSD ルールによって決まります。詳細については、「SSD ルール」のページを参照してください。

ステップ 3 操作を開始するには、[適用] をクリックします。

USB または内部フラッシュを使用してシステム コンフィギュレーション ファイルをバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[バックアップファイル] を選択します。
- [ソースファイルタイプ]:バックアップするコンフィギュレーション ファイル タイプを 1 つ選択します。
- [コピー方法]:[USB]、または [内部フラッシュ] を選択します。
- [ファイル名]:宛先バックアップ ファイルの名前を入力します。

- [機密データの処理]:機密データをバックアップ ファイルに含める方法を選択します。次のオプションが選択できます。
  - [除外]:機密データをバックアップに含めません。
  - [暗号化]:機密データを暗号化してバックアップに含めます。
  - [プレーンテキスト]:機密データをプレーンテキスト形式でバックアップに含めます。

  注 使用可能な機密データ オプションは、現在のユーザの SSD ルールによって決まります。詳細については、「SSD ルール」のページを参照してください。

ステップ 3 操作を開始するには、[適用] をクリックします。

TFTP を使用してシステム コンフィギュレーション ファイルをバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[バックアップファイル] を選択します。
- [ソースファイルタイプ]:バックアップするファイルのタイプを選択します。
- [コピー方法]:[TFTP] を選択します。
- [サーバ指定方法]:TFTP サーバを IP アドレスで指定するか、ドメイン名で指定するかを選択します。

  [サーバ指定方法] がアドレス指定の場合:
  - [IPバージョン]:IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。

    [サーバ指定方法] でサーバを名前で選択するように指定した場合、IP バージョン関連のオプションを選択する必要はありません。
  - [IPv6アドレスタイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。

    [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

[グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します。

- [サーバのIPアドレス/名前]:TFTP サーバの IP アドレスまたは名前を入力します。
- [宛先]:バックアップ ファイル名を入力します。
- [機密データの処理]:機密データをバックアップ ファイルに含める方法を選択します。次のオプションが選択できます。
  - [除外]:機密データをバックアップに含めません。
  - [暗号化]:機密データを暗号化してバックアップに含めます。
  - [プレーンテキスト]:機密データをプレーンテキスト形式でバックアップに含めます。

  注 使用可能な機密データ オプションは、現在のユーザの SSD ルールによって決まります。詳細については、[セキュア機密データ管理] > [SSDルール] ページをご覧ください。

ステップ 3 操作を開始するには、[適用] をクリックします。

SCP を使用してシステム コンフィギュレーション ファイルをバックアップするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[バックアップファイル] を選択します。
- [ソースファイルタイプ]:バックアップするファイルのタイプを選択します。
- [コピー方法]:[SCP] を選択します。

ステップ 3 詳細については、「SSH ユーザ認証」を参照してください。それから、次のフィールドを入力します。

- [リモートSSHサーバ認証]:SSH サーバ認証(デフォルトでは無効)を有効にするには、[編集] をクリックします。そうすると、この設定を行う [SSH サーバ認証] ページに移動します。設定後、このページに戻ります。[SSH サーバ認証] ページで、SSH ユーザ認証方式(パスワードまたはパブリック/秘密キー)の選択、デバイスのユーザ名とパスワードの設定(パスワード方式を選択した場合)、および必要に応じて RSA キーや DSA キーの生成を行うことができます。

[SSHクライアント認証]:クライアント認証は、次のいずれかの方法で実行できます。

- [SSHクライアントシステムクレデンシャルの使用]:固定 SSH ユーザ クレデンシャルを設定します。[SSHユーザ認証] ページに移動するには、[システムクレデンシャル] をクリックします。このページで、恒久的に使用するユーザとパスワードを設定できます。
- [SSHクライアントのワンタイムクレデンシャルを使用]:次の値を入力します。
  - [ユーザ名]:今回のコピー アクションに使用するユーザ名を入力します。
  - [パスワード]:今回のコピーに使用するパスワードを入力します。
- [サーバ指定方法]:SCP サーバを IP アドレスで指定するか、ドメインの名前で指定するかを選択します。
- [IPバージョン]:IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。
- [IPv6アドレスタイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します。
- [サーバのIPアドレス/名前]:SCP サーバの IP アドレスまたは名前を入力します。
- [宛先]:バックアップ ファイル名を入力します。
- [機密データの処理]:機密データをバックアップ ファイルに含める方法を選択します。次のオプションが選択できます。
  - [除外]:機密データをバックアップに含めません。
  - [暗号化]:機密データを暗号化してバックアップに含めます。
  - [プレーンテキスト]:機密データをプレーンテキスト形式でバックアップに含めます。

注 使用可能な機密データ オプションは、現在のユーザの SSD ルールによって決まります。詳細については、[セキュア機密データ管理] > [SSDルール] ページをご覧ください。

ステップ 4 操作を開始するには、[適用] をクリックします。

システム コンフィギュレーション ファイルをタイプの異なるコンフィギュレーション ファイルにコピーするには、次のようにします。

ステップ 1 [各種管理] > [ファイル管理] > [ファイル操作] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [操作タイプ]:[重複] を選択します。
- [ソースファイル名]:コピーするコンフィギュレーション ファイル タイプを1つ選択します。
- [宛先ファイル名]:宛先コンフィギュレーション ファイルの名前を入力します。

ステップ 3 操作を開始するには、[適用] をクリックします。

ファイル ディレクトリ

[ファイルディレクトリ] ページには、システム内に存在するシステム ファイルが表示されます。

注 スタック内にユニットが複数存在する場合、表示されるファイルはマスター ユニットから取得されます。

ステップ 1 [各種管理] > [ファイル管理] > [ファイルディレクトリ] の順にクリックします。

ステップ 2 必要に応じて、[自動ミラーコンフィギュレーション] 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 ファイルが自動的に作成されるようになります。ミラー コンフィギュレーション ファイルがある場合、この機能を無効にすると、そのファイルが削除されます。ミラー ファイルの説明、およびミラー コンフィギュレーション ファイルを自動作成しないほうがよいかもしれない状況については、システム ファイルをご覧ください。

ステップ 3 ファイルとディレクトリを表示するドライブを選択します。次のオプションが選択できます。

- [フラッシュ]:管理ステーションのルート ディレクトリに含まれ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 [実行] をクリックすると、以下のフィールドが表示されます。

- [ファイル名]:ファイルタイプに応じて、システム ファイルのタイプ、またはファイルの実際の名前。
- [パーミッション]:ユーザに付与されたファイルに対する読み取り/書き込みアクセス許可。
- [サイズ]:ファイル サイズ。
- [最終変更日]:ファイルが変更された日時。
- [フル パス]:ファイルのパス。

DHCP 自動コンフィギュレーション/イメージ更新

自動コンフィギュレーション/イメージ更新機能により、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。管理者はこのプロセスを使用して、ネットワーク内のこれらのデバイスのコンフィギュレーションとファームウェアをリモートから最新の状態に保つことができます。

この機能は次の部分で構成されています。

- [自動イメージ更新]:ファームウェア イメージをリモート TFTP/SCP サーバから自動的にダウンロードします。自動コンフィギュレーション/イメージ更新プロセスの終了時に、このファームウェア イメージに従ってデバイスがリブートします。
- [自動コンフィギュレーション]:コンフィギュレーション ファイルをリモート TFTP/SCP サーバから自動的にダウンロードします。自動コンフィギュレーション/イメージ更新プロセスの終了時に、このコンフィギュレーション ファイルに従ってデバイスがリブートします。

注 自動イメージ更新と自動コンフィギュレーションが両方ともリクエストされた場合は、自動イメージ更新が先に実行され、リブートしてから、自動コンフィギュレーションが実行されます。その後、最終的なリブートが実行されます。

この機能を使用するには、デバイスのコンフィギュレーション ファイルとファームウェア イメージの場所と名前を使用して、ネットワーク内の DHCP サーバを設定します。ネットワーク内のデバイスは、既定では DHCP クライアントとして設定されます。DHCP サーバによってデバイスに IP アドレスが割り当てられるとき、デバイスはコンフィギュレーション ファイルとファームウェア イメージに関する情報も受け取ります。コンフィギュレーション ファイルかファームウェア イメージが、現在デバイスで使用しているものと異なる場合、そのファイルまたはイメージをダウンロードしてから、デバイスはリブートします。ここでは、これらのプロセスについて説明します。

自動更新/コンフィギュレーションにより、最新のコンフィギュレーション ファイルとファームウェア イメージを使用してネットワーク内のデバイスを最新に保つことができるだけでなく、ネットワークへのデバイスのクイック インストールも可能となります。これは、開封直後のデバイスは、システム管理者が手動で介入しなくても、コンフィギュレーション ファイルとソフトウェア イメージをネットワークから取得するように設定されているためです。デバイスは、初めて IP アドレスを DHCP サーバに要求するとき、DHCP サーバが指定したコンフィギュレーション ファイルとイメージ(またはその一方)をダウンロードし、それに従ってリブートを実行します。

自動コンフィギュレーション プロセスは、RADIUS サーバ キーや SSH/SSL キーなどの機密情報を含むコンフィギュレーション ファイルのダウンロードをサポートしています。これには、Secure Copy Protocol(SCP)とセキュア機密データ(SSD)機能が使用されます(SSH クライアント認証、およびセキュリティ:セキュア機密データ管理をご覧ください)。

ダウンロード プロトコル(TFTP または SCP)

コンフィギュレーション ファイルとファームウェア イメージは、TFTP サーバか SCP サーバのどちらかからダウンロードできます。

使用するプロトコルを次のように設定します。

- [ファイル拡張子に基づく自動]:(デフォルト)このオプションを選択した場合、ユーザが設定するファイル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。たとえば、指定したファイル拡張子が .xyz の場合、拡張子が .xyz のファイルは SCP を使用してダウンロードされ、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。デフォルトの拡張子は .scp です。
- [TFTP のみ]:コンフィギュレーション ファイル名の拡張子が何であれ、TFTP 経由でダウンロードが行われます。
- [SCP のみ]:コンフィギュレーション ファイル名の拡張子が何であれ、SCP 経由(SSH を使用)でダウンロードが行われます。

SSH クライアント認証

SCP は SSH ベースです。デフォルトで、リモート SSH サーバ認証は無効になっているため、デバイスはリモート SSH サーバをすべてそのまま受け入れます。リモート SSH サーバ認証を有効にすると、信頼済みサーバ リストに含まれるサーバのみが使用されるようにできます。

[SSHクライアント認証] のパラメータは、クライアント(デバイス)が SSH サーバにアクセスするのに必要です。デフォルトの SSH クライアント認証パラメータは次のとおりです。

- [SSH認証方式]: ユーザ名/パスワード
- [SSHユーザ名]: anonymous
- [SSHパスワード]: anonymous

注 [SSHクライアント認証] のパラメータは、ファイルを手動でダウンロードする際(つまり、DHCP 自動設定/イメージ更新機能を使用しないダウンロード)にも使用できます。

自動コンフィギュレーション/イメージ更新プロセス

DHCP 自動コンフィギュレーションでは、受信した DHCP メッセージから取得したコンフィギュレーション サーバの名前とアドレス、およびコンフィギュレーション ファイルの名前とパスがあれば、それらが使用されます。加えて、DHCP イメージ更新では、メッセージ内にファームウェアの間接ファイル名が含まれていれば、そのファイル名が使用します。この情報は、DHCPv4 サーバから受信する**オファー** メッセージと、DHCPv6 サーバから受信する**情報応答**メッセージの中で [DHCPオプション] として指定されています。

この情報が DHCP サーバ メッセージ内に含まれていない場合は、[DHCP 自動コンフィギュレーション/イメージ更新] ページで設定されているバックアップ情報が使用されます。

[自動コンフィギュレーション/イメージ更新] プロセスがトリガーされると(自動コンフィギュレーション/イメージ更新のトリガーを参照)、次に示す一連のイベントが発生します。

自動イメージ更新の開始

- スイッチは、受信した DHCP メッセージに、オプション 125(DHCPv4)、およびオプション 60(DHCPv6)の間接ファイル名があれば、それを使用します。
- DHCP サーバがファームウェア イメージ ファイルの間接ファイル名を送信しなかった場合は、([DHCP 自動コンフィギュレーション/イメージ更新] ページの)バックアップ間接イメージファイル名が使用されます。

- スイッチは、間接イメージ ファイルをダウンロードし、その中から TFTP/SCP サーバのイメージ ファイル名を抽出します。
- スイッチは、TFTP サーバのイメージ ファイルのバージョンと、スイッチのアクティブ イメージのバージョンを比較します。
- 両者のバージョンが異なる場合、新しいバージョンが非アクティブ イメージにロードされ、リブートが実行されて、この非アクティブ イメージがアクティブ イメージになります。
- SCP プロトコルを使用している場合は、再起動が実行されることを通知する SYSLOG メッセージが生成されます。
- SCP プロトコルを使用している場合は、自動更新プロセスが完了したことを確認する SYSLOG メッセージが生成されます。
- TFTP プロトコルを使用している場合は、このコピー プロセスによって SYSLOG メッセージが生成されます。

自動コンフィギュレーションの開始

- このデバイスは、TFTP/SCP サーバの名前とアドレス、およびコンフィギュレーション ファイルの名前とパス(DHCPv4 オプション:66、150、および 67、DHCPv6 オプション:59 および 60)を使用します(受信した DHCP メッセージに含まれている場合)。
- DHCP サーバによってこれらの情報が送信されなかった場合は、([DHCP 自動コンフィギュレーション/イメージ更新] ページの)バックアップ サーバの IP アドレス/名前とバックアップ コンフィギュレーション ファイル名が使用されます。
- 新しいコンフィギュレーション ファイルの名前が、デバイス上で使用されていたコンフィギュレーション ファイルの名前と異なる場合、またはデバイスがまだ設定されていなかった場合は、新しいコンフィギュレーション ファイルが使用されます。
- 自動コンフィギュレーション/イメージ更新のプロセスの終了時に、新しいコンフィギュレーション ファイルを使用してデバイスがリブートされます。
- このコピー プロセスによって SYSLOG メッセージが生成されます。

オプションが未設定の場合

- DHCP サーバが DHCP オプションで TFTP/SCP サーバ アドレスを送信せず、バックアップ TFTP/SCP サーバ アドレス パラメータが設定されなかった場合、次の処理が実行されます。
  - **SCP**:自動コンフィギュレーション プロセスは中止されます。
  - **TFTP**:デバイスは、限定されたブロードキャスト アドレス(IPv4 の場合)、またはその IP インターフェイス上にあるすべてのノード アドレス(IPv6 の場合)に対して TFTP 要求メッセージを送信します。その後、最初に応答した TFTP サーバを使用して、自動コンフィギュレーション/イメージ更新のプロセスを続行します。

ダウンロード プロトコルの選択

- コピー プロトコル(SCP/TFTP)をダウンロード プロトコル(TFTP または SCP)の説明に従って選択します。

SCP

- SCP を使用してダウンロードする場合、次のどちらかが当てはまるなら、デバイスは指定した SCP/SSH サーバをすべて(認証なしで)許可します。
  - SSH サーバ認証プロセスが無効である。出荷時設定のままのデバイス(開封直後のデバイスなど)でコンフィギュレーション ファイルをダウンロードできるようにするため、SSH サーバ認証はデフォルトで無効になっています。
  - その SSH サーバが SSH 信頼済みサーバリストに設定されている。

  SSH サーバ認証プロセスが有効な場合、その SSH サーバが SSH 信頼済みサーバ リストにないと、自動コンフィギュレーション プロセスは中止されます。
- その情報が使用できる場合は、SCP サーバへのアクセスが実行され、そこからコンフィギュレーション ファイルやイメージがダウンロードされます。

自動コンフィギュレーション/イメージ更新のトリガー

DHCPv4 経由の自動コンフィギュレーション/イメージ更新は、次の条件が満たされた場合にトリガーされます。

- デバイスの IP アドレスがリブート時に動的に割り当てられるか更新された場合。または、管理アクションにより明示的に更新されるか、リース期間の終了により自動的に更新された場合。明示的な更新は、[IPv4インターフェイス] ページでアクティブ化できます。

- 自動イメージ更新が有効な場合は、DHCP サーバから間接イメージ ファイルを受信するか、バックアップ間接イメージ ファイル名が設定されたときに、自動イメージ更新プロセスがトリガーされます。「間接」という言葉は、それがイメージそのものではなく、イメージへのパス名を保持しているファイルであることを表しています。
- 自動コンフィギュレーションが有効な場合は、DHCP サーバからコンフィギュレーション ファイル名を受信したとき、または、バックアップ コンフィギュレーション ファイル名が設定されたときに、自動コンフィギュレーション プロセスがトリガーされます。

DHCPv6 経由の自動設定/イメージ更新は、次の条件が満たされた場合にトリガーされます。

- DHCPv6 サーバがデバイスに情報を送信する場合。次のケースが考えられます。
  - IPv6 が有効なインターフェイスが、DHCPv6 ステートレス コンフィギュレーション クライアントとして定義されたとき。
  - DHCPv6 メッセージをサーバから受信したとき(例:ユーザが [IPv6インターフェイス] ページで [再起動] ボタンをクリックしたとき)。
  - DHCPv6 情報がデバイスによって更新されたとき。
  - ステートレス DHCPv6 クライアントを有効にして、デバイスを再起動した後。
- DHCPv6 サーバ パケットにコンフィギュレーション ファイル名オプションが含まれている場合。
- DHCP サーバから間接イメージ ファイル名が提供されたとき、または、バックアップ間接イメージ ファイル名が設定されたときに、自動イメージ更新プロセスがトリガーされます。「間接」という言葉は、それがイメージそのものではなく、イメージへのパス名を保持しているファイルであることを表しています。

スタックでの自動コンフィギュレーション イメージ更新

スタックの現在のマスターが、スタック全体の自動コンフィギュレーション/イメージ更新を実行します。

自動コンフィギュレーションの場合、新しいコンフィギュレーション ファイルがマスター ユニットにダウンロードされ、リロードする前にバックアップに同期化されます。

自動イメージ更新の場合は、新しいイメージがコピーされ、マスター ユニットの非アクティブ イメージに保存されます。コピー プロセスの一部として、リロードする前に、マスター ユニットはこのイメージをスタック内のすべてのユニットに同期化します。

TFTP/SCP サーバ上のコンフィギュレーション ファイルは、サポートされているコンフィギュレーション ファイルの形式要件を満たしている必要があります。スタートアップ コンフィギュレーションにロードされる前に、ファイルの形式はチェックされますが、コンフィギュレーション パラメータの有効性はチェックされません。

DHCP 自動コンフィギュレーション/イメージ更新

デバイスを DHCP クライアントとして設定するには、[DHCP 自動コンフィギュレーション/イメージ更新] ページを使用します。

システムのデフォルトは次のとおりです。

- 自動コンフィギュレーション:有効。
- 自動イメージ更新:有効。
- デバイスは DHCP クライアントとして有効。
- リモート SSH サーバ認証:有効。

開始する前に

この機能を使用するには、デバイスが DHCPv4 クライアントか DHCPv6 クライアントとして設定されている必要があります。デバイスで定義される DHCP クライアントのタイプは、デバイスで定義されるインターフェイスのタイプと関連があります。

自動コンフィギュレーションの準備

DHCP サーバと TFTP/SCP サーバを準備するには、次のようにします。

TFTP/SCP サーバ

- コンフィギュレーション ファイルを作業ディレクトリに置きます。このファイルは、デバイスからコンフィギュレーション ファイルをコピーして作成できます。デバイスがブートされると、このファイルが実行コンフィギュレーション ファイルになります。

DHCP サーバ

次のオプションを使用して DHCP サーバを設定します。

- DHCPv4:
  - 66(単一のサーバ アドレス)、または 150(サーバ アドレスのリスト)
  - 67(コンフィギュレーション ファイル名)

- DHCPv6
  - オプション 59(サーバ アドレス)
  - オプション 60(コンフィギュレーション ファイル名と間接イメージ ファイル名を、カンマで区切って指定)

自動イメージ更新の準備

DHCP サーバと TFTP/SCP サーバを準備するには、次のようにします。

TFTP/SCP サーバ

1. メイン ディレクトリにサブ ディレクトリを作成します。ここにソフトウェア イメージ ファイルを置きます。
2. ファームウェア バージョンのパスと名前が含まれた間接ファイルを作成します(例:cisco\cisco-version.ros が含まれた indirect-cisco.txt ファイル)。
3. この間接ファイルを TFTP/SCP サーバのメイン ディレクトリにコピーします。

DHCP サーバ

次のオプションを使用して DHCP サーバを設定します。

- DHCPv4:オプション 125(間接ファイル名)
- DHCPv6:オプション 60(コンフィギュレーション ファイル名と間接イメージ ファイル名を、カンマで区切って指定)

DHCP クライアントのワーク フロー

ステップ 1 [DHCP 自動コンフィギュレーション/イメージ更新] ページで、自動コンフィギュレーションのパラメータと自動イメージ更新のパラメータ(またはどちらか一方)を設定します。

ステップ 2 [IPコンフィギュレーション] > [IPv4インターフェイス] ページで [IPアドレスタイプ] を [ダイナミック] に設定します。[IPv4 インターフェイス] ページで [IPアドレスタイプ] を [ダイナミック] に設定し、[Ipv6 インターフェイス] ページでデバイスをステートレス DHCPv6 クライアントとして定義します。

Web コンフィギュレーション

自動コンフィギュレーションや自動更新を設定するには、次のようにします。

ステップ 1 [各種管理] >[ファイル管理] >[DHCP自動設定/イメージ更新] の順にクリックします。

ステップ 2 値を入力します。

- [DHCP経由の自動コンフィギュレーション]: このフィールドを選択すると、DHCP 自動コンフィギュレーションが有効になります。この機能はデフォルトで有効になっていますが、このページで無効にすることもできます。
- [ダウンロードプロトコル]: 次のいずれかを選択します。
  - [ファイル拡張子に基づく自動]: これを選択すると、自動コンフィギュレーションで、コンフィギュレーション ファイルの拡張子に応じて TFTP プロトコルか SCP プロトコルが使用されます。このオプションを選択する場合、コンフィギュレーション ファイルの拡張子を必ず指定しなければならないわけではありません。指定されていない場合は、次に示すように、デフォルトの拡張子が使用されます。
  - [SCPのファイル拡張子]:[ファイル拡張子に基づく自動] を選択した場合、ファイル拡張子をここで指定できます。この拡張子を持つファイルはすべて、SCP を使用してダウンロードされます。拡張子を入力しなかった場合は、デフォルトの拡張子 **.scp** が使用されます。
  - [TFTPのみ]: これを選択すると、自動コンフィギュレーションには TFTP プロトコルのみが使用されます。
  - [SCPのみ]: これを選択すると、自動コンフィギュレーションには SCP プロトコルのみが使用されます。
- [DHCP を使用したイメージ自動更新]: このフィールドを選択すると、DHCP サーバからファームウェア イメージを更新できるようになります。この機能はデフォルトで有効になっていますが、このページで無効にすることもできます。
- [ダウンロードプロトコル]: 次のいずれかを選択します。
  - [ファイル拡張子に基づく自動]: これを選択すると、イメージ ファイルの拡張子に応じて TFTP プロトコルか SCP プロトコルが自動更新で使用されます。このオプションを選択する場合、イメージ ファイルの拡張子を必ず指定しなければならないわけではありません。指定されていない場合は、次に示すように、デフォルトの拡張子が使用されます。

- [SCPのファイル拡張子]:[ファイル拡張子に基づく自動] を選択した場合、ファイル拡張子をここで指定できます。この拡張子を持つファイルはすべて、SCP を使用してダウンロードされます。拡張子を入力しなかった場合は、デフォルトの拡張子 **.scp** が使用されます。
- [TFTPのみ]:これを選択すると、自動更新には TFTP プロトコルのみが使用されます。
- [SCPのみ]:これを選択すると、自動更新には SCP プロトコルのみが使用されます。

- [SCPのSSH設定]:SCP をコンフィギュレーション ファイルのダウンロードに使用する場合は、次のいずれかを選択します。
- [リモートSSHサーバ認証]:[有効/無効] リンクをクリックすると、[SSHサーバ認証] ページに移動します。このページで、ダウンロードに使用する SSH サーバの認証を有効にし、必要に応じて、信頼済み SSH サーバを入力できます。
- [SSHクライアント認証]:[システムクレデンシャル] リンクをクリックし、[SSHユーザ認証] ページでユーザ クレデンシャルを入力します。
- [バックアップサーバ定義]:バックアップ サーバを IP アドレス で設定するか、名前で設定するかを選択します。

ステップ 3 [サーバ指定方法] がアドレス指定の場合:

- [IPバージョン]:IPv4 と IPv6 のどちらのアドレスを使用するかを選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 が使用される場合)。

ステップ 4 次のオプション情報を入力します。この情報は、DHCP サーバから必要な情報が提供されなかった場合に使用されます。

- [バックアップサーバのIPアドレス/名前]:バックアップサーバの IP アドレスか名前を入力します。
- [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 コンフィギュレーション ファイル名を入力します。
- [バックアップ間接イメージ ファイル名]:使用する間接イメージ ファイル名を入力します。これは、イメージへのパスが含まれたファイルです。間接イメージ ファイル名の例: indirect-cisco.scp。このファイルには、ファームウェア イメージのパスと名前が含まれています。

  次のフィールドが表示されます。

- [最終自動コンフィギュレーション/イメージのサーバIPアドレス]:最後にバックアップを実行したサーバのアドレス。
- [最後に自動コンフィギュレーションで使用したファイル名]:最後のコンフィギュレーション ファイル名を入力します。

ステップ 5 [適用] 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。

7

各種管理:スタック管理

ここでは、スタックの管理方法について説明します。具体的な内容は、次のとおりです。

注 スタック構成は、デバイスの SG350 ファミリ(Sx350 を除く)と SG550 ファミリでのみサポートされます。

- 概要
- スタック内のユニットのタイプ
- スタック トポロジ
- ユニット ID 割り当て
- マスター選択プロセス
- スタック変更
- スタック内のユニット障害
- スタック内のソフトウェア自動同期
- スタック管理

概要

デバイスは、単体で機能するか、またはさまざまなスタック構成モード(スタック ユニット モードを参照)でデバイスのスタックに接続することができます。

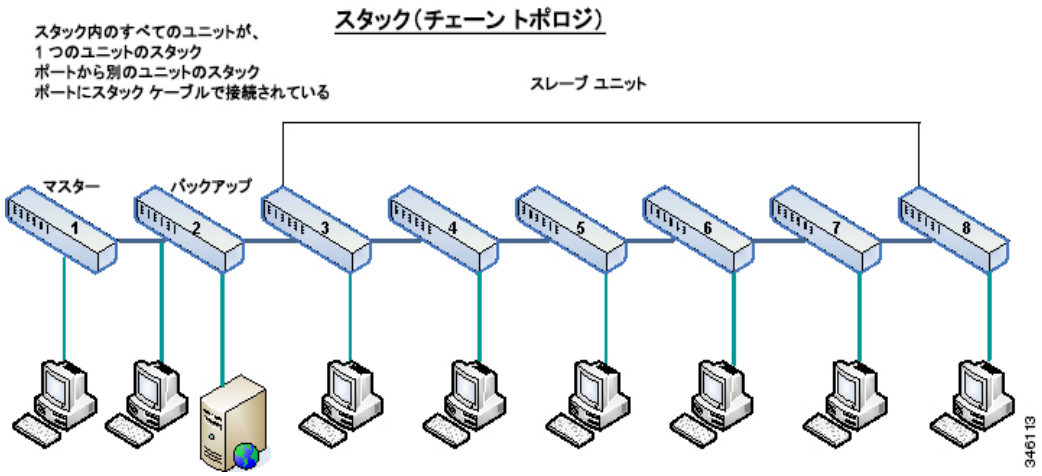
デフォルトで、デバイスは常にスタッカブルですが、スタック ポートとして設定されるポートを備えていません。デフォルトでは、デバイス上のすべてのポートがネットワーク ポートとして設定されています。スタック ポートを持たないデバイスは、それ自身のスタックのマスター デバイスか、またはスタンドアロン デバイスと考えることができます。複数のデバイスをスタックするには、デバイス上で必要なネットワーク ポートをスタック ポートとして再設定し、そのスタック ポートを備えたデバイスをリングまたはチェーン トポロジに接続します。

スタック内のデバイス(ユニット)はスタック ポートを介して接続されます。これにより、デバイスは単一の論理デバイスとして一括して管理されます。スタック ポートを Link Aggregation Group(LAG)のスタック内のメンバーにすることによって、スタック インターフェイスの帯域幅を増やすこともできます。「スタック ポート リンク アグリゲーション」を参照してください。

スタックは、1 つのマスター/バックアップと複数のスレーブからなるモデルを基本とします。

8 つのデバイスがスタックに接続されている(550 ファミリに対応)例を以下に示します。

スタック アーキテクチャ(チェーン トポロジ)



スタックは次のようなメリットを提供します。

- ネットワーク容量を動的に拡張または縮小することができます。ユニットを追加することによって、管理者は、単一管理点を維持しながら、スタック内のポート数を動的に増やすことができます。同様に、ユニットを削除することによってネットワーク容量を減らすことができます。
- スタック構成のシステムは、次の方法で冗長性をサポートします。
  - オリジナルのマスターで障害が発生すると、バックアップ ユニットがスタックのマスターになります。
  - スタック システムは、チェーンとリングという 2 種類のトポロジをサポートします。リング トポロジでは、スタック ポートの 1 つで障害が発生しても、スタックはチェーン トポロジ内で機能を継続します(「スタック トポロジ」を参照)。

- リング スタックのポートでは、ファスト スタック リンク フェールオーバーとして知られるプロセスがサポートされており、スタック ポート リンクの 1 つで障害が発生したときのデータ パケット損失期間を削減することができます。スタックが新しいチェーン トポロジに復旧するまで、スタック ユニットは障害が発生したスタッキング ポートを介して送信するはずだったパケットをループバックし、そのループバックしたパケットを残りのスタッキング ポートを介して宛先に送信します。ファスト スタック リンク フェールオーバー期間は、マスター/バックアップ ユニットがアクティブのまま正常に機能し続けます。

スタック内のユニットのタイプ

スタック内のユニットのタイプを以下に示します。

- **マスター**:マスター ユニットの ID は 1 か 2 にする必要があります。スタックは、それ自体を管理するマスター ユニット、バックアップ ユニット、およびスレーブ ユニットを介して管理されます。
- **バックアップ**:マスター ユニットで障害が発生した場合は、バックアップ ユニットがマスターの役割を引き継ぎます(スイッチオーバー)。バックアップ ユニットの ID は 1 か 2 にする必要があります。
- **スレーブ**:このユニットはマスター ユニットによって管理されます。

ユニットのグループをスタックとして機能させるためには、マスター対応ユニットを用意する必要があります。マスター対応ユニットで障害が発生した場合は、バックアップ ユニット(マスターの役割を引き継ぐアクティブ ユニット)が存在する限り、スタックが機能を継続します。

バックアップ ユニットで障害が発生し、マスターの他に機能しているユニットがスレーブ ユニットだけになった場合は、それらも 1 分後に機能を停止します。これは、1 分後に、マスターを使用せずに動作していたスレーブ ユニットのいずれかのポートにケーブルをつないでもリンクが確立されないことを意味します。

550 ファミリのユニット LED

デバイスには、1、2、3、および 4 とマークされた 4 つの LED が付いており、これらの数字はそれぞれのユニットのユニット ID を示しています(たとえば、ユニット ID 1 で LED 1 が点灯しており、他の LED は消灯している、というようになります)。4 を超えるユニット ID をサポートする場合は、以下の定義に従って LED 表示が変更されます。

- ユニット 1 ～ 4:LED 1 ～ 4 がそれぞれ点灯する。
- ユニット 5:LED 1 と 4 が点灯する。
- ユニット 6:LED 2 と 4 が点灯する。
- ユニット 7:LED 3 と 4 が点灯する。
- ユニット 8:LED 1、3、および 4 が点灯する。

SG350XG ファミリのユニット LED

デバイスには、1、2、3、および 4 とマークされた 4 つの LED が付いており、これらの数字はそれぞれのユニットのユニット ID を示しています(たとえば、ユニット ID 1 で LED 1 が点灯しており、他の LED は消灯している、というようになります)。

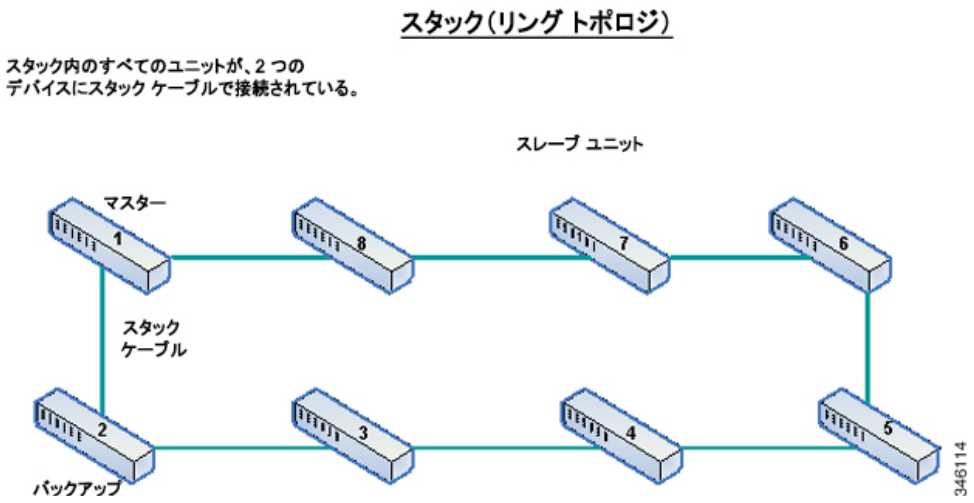
スタック トポロジ

スタック トポロジのタイプ

スタック内のユニットは、次のトポロジ タイプのいずれかで接続できます。

- [チェーン トポロジ]:それぞれのユニットが隣接するユニットに接続されますが、最初と最後のユニットはケーブルで接続されません。チェーン トポロジについては、「「スタック アーキテクチャ(チェーン トポロジ)」」を参照してください。
- [リングトポロジ]:それぞれのユニットが隣接するユニットに接続されます。最後のユニットが最初のユニットに接続されます。8 ユニット スタックのリング トポロジを以下に示します。

リング トポロジ内のスタック(550 ファミリ)



リング トポロジは、チェーン トポロジよりも高い信頼性を提供します。リング内のリンクの 1 つで障害が発生してもスタックの機能に影響はありませんが、チェーン接続内のリンクの 1 つで障害が発生した場合はスタックが分割される可能性があります。

トポロジ ディスカバリ

スタックは、トポロジ ディスカバリと呼ばれるプロセスによって構築されます。このプロセスは、スタック ポート内のアップ/ダウン ステータスの変化でトリガーされます。

このプロセスをトリガーするイベントの例を以下に示します。

- スタック トポロジのリングからチェーンへの変更
- 2 つのスタックの 1 つのスタックへのマージ
- スタックの分割
- 障害が発生してユニットがスタックから接続解除された場合などの他のスレーブ ユニットのスタックへの挿入。この現象は、チェーン トポロジ内でスタックの中心にあるユニットで障害が発生した場合に生じる可能性があります。

トポロジ ディスカバリ中は、スタック内のそれぞれのユニットがトポロジ情報を含むパケットを交換します。

トポロジ ディスカバリ プロセスが完了すると、それぞれのユニットにスタック内のすべてのユニットのスタック マッピング情報が保持されます。

ユニット ID 割り当て

トポロジ ディスカバリが完了したら、スタック内のそれぞれのユニットに一意のユニット ID が割り当てられます。

このユニット ID は、[スタック管理] ページで次のいずれかの方法で設定されます。

- [自動]:ユニット ID はトポロジ ディスカバリ プロセスによって割り当てられます。
- [手動]:ユニット ID は 1 からスタック内のユニットの最大数までの整数に手動で設定されます。

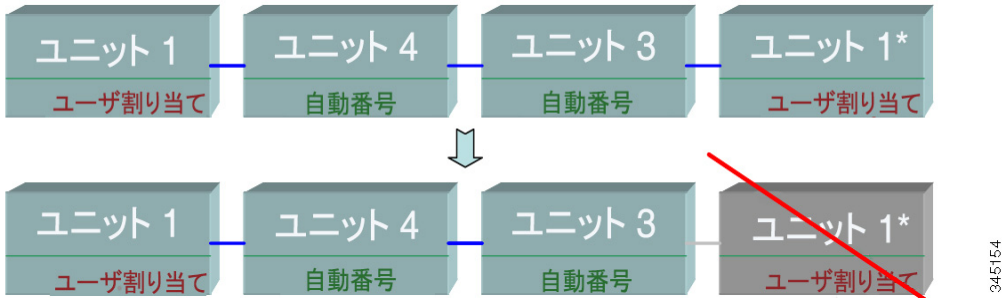
重複するユニット ID

2 つのユニットに同じユニット ID を割り当てると、それらのどちらかしかそのユニット ID を使用してスタックに参加することができません。

自動番号付与が選択されている場合は、重複ユニットに新しいユニット番号が割り当てられます。自動番号付与が選択されていない場合は、重複ユニットがシャットダウンされます。

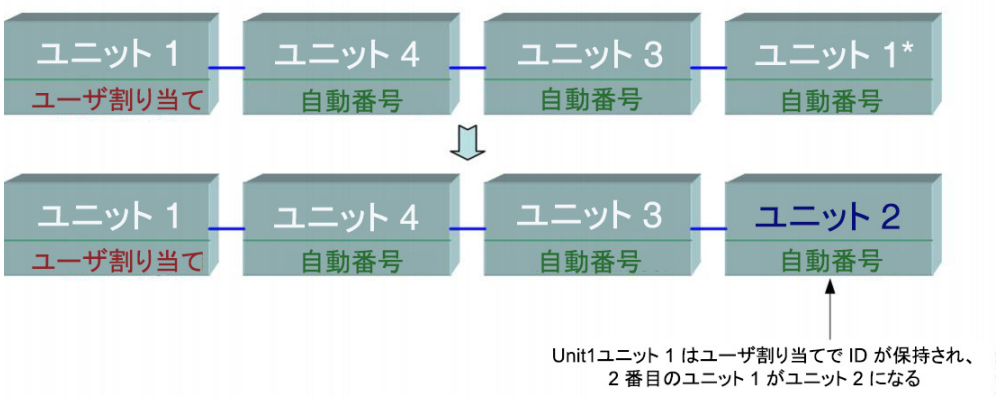
2 つのユニットに手動で同じユニット ID が割り当てられたケースを以下に示します。ユニット 1 はスタックに参加せず、シャットダウンされます。このユニットは、マスター対応ユニット(1 または 2)間のマスター選択プロセスで落選しました。

重複ユニットのシャットダウン



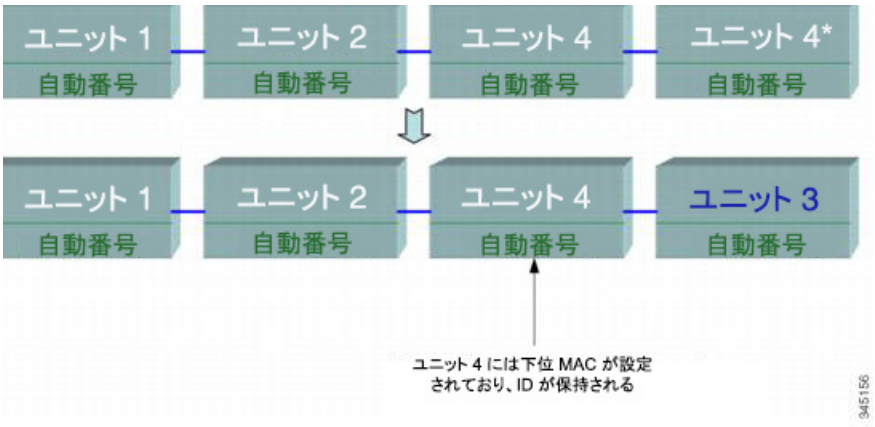
重複ユニットのどちらかの番号が再割り当てされる(自動番号付与)ケースを以下に示します。

重複ユニットの再番号割り当て



重複ユニットのどちらかの番号が再割り当てされるケースを以下に示します。MAC が小さい方のユニットがそのユニット ID を保持します(このプロセスの詳細については、「マスター選択プロセス」を参照)。

自動番号ユニット ID による 2 つのユニット間の重複



注 新しいスタックでユニットの最大数を超えている場合は、すべての余分なユニットがシャットダウンされます。

マスター選択プロセス

マスター ユニットは、マスター対応ユニット(1 または 2)から選択されます。マスター ユニットの選択の要因は、次の優先順位で考慮されます。

- [システム アップタイム]:マスター対応ユニットが 10 分間のセグメント単位で測定されたアップタイムを交換します。セグメント数の多いユニットが選択されます。両方のユニットの時間セグメントの数が同じで、どちらかのユニットのユニット ID が手動で設定され、他のユニットのユニット ID が自動で設定された場合は、ユニット ID が手動で定義されたユニットが選択されます。そうでない場合は、ユニット ID が最小のユニットが選択されます。両方のユニット ID が同じ場合は、MAC アドレスの小さい方が選択されます。

  注 スイッチ フェールオーバー プロセスでバックアップ ユニットがマスターとして選択された場合は、そのアップタイムが維持されます。

- [ユニットID]:両方のユニットの時間セグメントの数が同じ場合は、ユニット ID の小さい方が選択されます。

- [MAC　アドレス]:両方のユニット ID が同じ場合は、MAC アドレスの小さい方が選択されます。

注 スタックを動作させるためには、マスター ユニットが必要です。マスター ユニットは、マスターの役割を引き受けるアクティブ ユニットとして定義されます。スタックには、マスター選択プロセス後にユニット 1 またはユニット 2 を含める必要があります。そうしなかった場合は、スタックとそのすべてのユニットが、完全な電源オフとしてではなく、部分的にシャットダウンされますが、トラフィック通過機能は停止されます。

スタック変更

ここでは、スタックの変更を引き起こす可能性のあるさまざまなイベントについて説明します。スタック トポロジは、次のいずれかが発生したときに変更されます。

- 1 つ以上のユニットがスタックとの間で接続または接続解除された。
- スタック ポートのいずれかでリンクがアップまたはダウンした。
- スタックがリング構造とチェーン構造間で変化した。

ユニットをスタックに対して追加または削除すると、トポロジの変更、マスター選択プロセス、またはユニット ID 割り当てがトリガーされます。

新しいユニットの接続

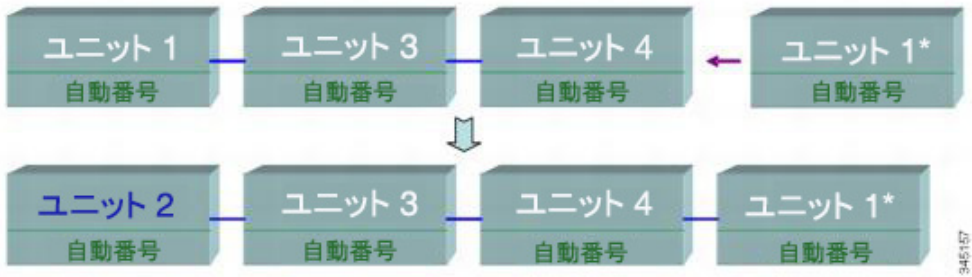
ユニットがスタックに挿入されたときに、スタック トポロジの変更がトリガーされます。ユニット ID が割り当てられ(自動番号付与の場合)、ユニットがマスターによって設定されます。

新しいユニットを既存のスタックに接続すると、次のいずれかになります。

- 重複するユニット ID が存在しない。
  - ユーザ定義の ID を持つユニットはそのユニット ID を保持します。
  - 自動割り当て ID を持つユニットはそのユニット ID を保持します。
  - 工場出荷時設定のユニットは、使用可能な最小の ID から始まるユニット ID を自動的に受け取ります。
- 重複するユニット ID が 1 つ以上存在する。自動番号付与が競合を解決してユニット ID を割り当てます。手動番号付与の場合は、1 つのユニットだけがそのユニット ID を保持し、他のユニットはシャットダウンされます。
- スタック内のユニット数が許容最大ユニット数を上回っている。スタックに参加した新しいユニットがシャットダウンされ、SYSLOG メッセージが生成されて、マスター ユニットに表示されます。

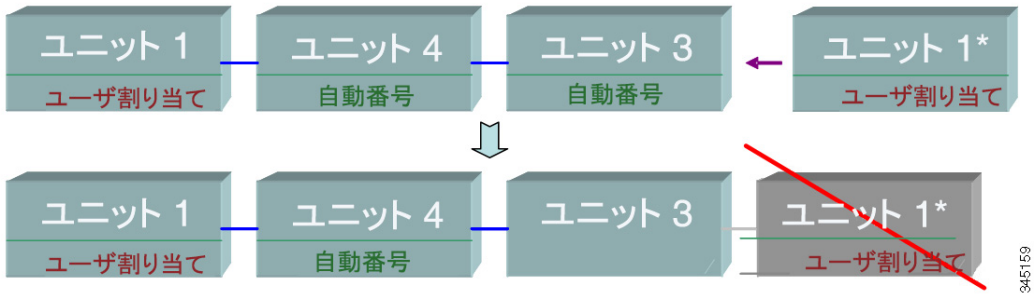
マスター対応ユニットがスタックに参加したときの自動番号付与の例を以下に示します。ユニット ID が 1 のユニットが 2 つ存在します。マスター選択プロセスを通して、マスター ユニットに最適なユニットが選択されます。最適なユニットとは、10 分間のセグメント単位でアップタイムがより高いユニットです。その他のユニットはバックアップにされます。

自動番号付与されたマスター対応ユニット



ユニット ID が 1 のユーザ割り当てマスター対応ユニットが、ユーザ割り当てユニット ID が 1 のマスター ユニットがすでに存在するスタックに参加するとどうなるかを以下に示します。新しいユニット 1 はスタックに参加せず、シャットダウンされます。

ユーザ割り当てマスター対応ユニット



スタック内のユニット障害

ここで説明する内容は次のとおりです。

- マスター ユニットの障害
- マスター/バックアップ スイッチオーバー
- スレーブ ユニット処理
- フェールオーバー後のオリジナルのマスター ユニットの再接続

マスター ユニットの障害

マスターで障害が発生すると、バックアップ ユニットがマスターの役割を引き継いで、スタックの正常な運用を継続します。

バックアップがマスターの代わりになるために、両方のユニットが常にウォーム スタンバイ状態を維持します。ウォーム スタンバイでは、マスター ユニットとそのバックアップ ユニットがスタティック 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 ファイルと実行コンフィギュレーション ファイルの両方に含まれている)を使用して同期されます。バックアップ コンフィギュレーション ファイルは同期されません。バックアップ コンフィギュレーション ファイルは以前のマスター上に残ります。

STP 状態テーブル、動的に学習された MAC アドレス、動的に学習された Smartport タイプ、MAC マルチキャスト テーブル、LACP、GVRP などの動的プロセス状態情報は同期されません。

マスターは設定中にすぐにバックアップを同期させます。同期は、コマンドの実行直後に実行されます。これは透過的に行われます。

ユニットが実行中のスタックに挿入され、バックアップ ユニットとして選択された場合は、それが最新のコンフィギュレーションになるようにマスターが同期を実行してから、SYNC COMPLETE SYSLOG メッセージを生成します。これは、バックアップがマスター ユニットとコンバージ中にのみ表示されるユニークな SYSLOG メッセージで、次のように表示されます。%DSYNCH-I-SYNCH_SUCCEEDED: ユニット 2 との同期が正常に終了しました。

マスター/バックアップ スイッチオーバー

スタック内のマスターで障害が発生すると、スイッチオーバーが発生します。

バックアップ ユニットがマスターになり、そのプロセスとプロトコル スタックのすべてがスタック全体を扱うように初期化されます。その結果、このユニット内のトラフィック転送が一時的に中断されますが、スレーブ ユニットはアクティブのままです。

注 STP が使用されており、ポートがリンクアップ状態の場合は、STP ポートの状態が一時的にブロッキングになり、トラフィックの転送や MAC アドレスの取得ができなくなります。これは、アクティブ ユニット間のスパニング ツリー ループを回避するためです。

スレーブ ユニット処理

バックアップがマスターになりますが、アクティブ スレーブ ユニットはアクティブのままで、オリジナルのマスターからのコンフィギュレーションに基づいてパケットの転送を継続します。これにより、ユニット内のデータ トラフィックの中断が最小限に抑えられます。

バックアップ ユニットがマスター状態への移行を完了したら、次の操作を実行することによって、スレーブ ユニットを一度に 1 つずつ初期化します。

- スレーブ ユニットのコンフィギュレーションをクリアしてデフォルトにリセットします(これは、新しいマスター ユニットからの不正なコンフィギュレーションを回避するためです)。その結果、スレーブ ユニット上のトラフィック転送が中断されます。
- 関連するユーザ コンフィギュレーションをスレーブ ユニットに適用します。

- ポートの STP 状態、動的 MAC アドレス、新しいマスターとスレーブ ユニット間のリンク アップ/ダウン ステータスなどの動的情報を交換します。マスターが STP に基づいてポートの状態を転送中に設定すると、スレーブ ユニット上でパケット転送が再開されます。

  注 MAC アドレスが学習または再学習されるまで、不明なユニキャスト MAC アドレスへのパケット フラッディングが発生します。

フェールオーバー後のオリジナルのマスター ユニットの再接続

フェールオーバー後に、オリジナルのマスターが再び接続された場合は、マスター選択プロセスが実行されます。オリジナルのマスター(ユニット 1)がマスターとして再選択された場合は、現在のマスター(ユニット 2、オリジナルのバックアップ ユニットだった)がリブートされ、再びバックアップになります。

注 マスター フェールオーバー中は、バックアップ ユニットのアップタイムが維持されます。

スタック ポート

デフォルトで、デバイス上のすべてのポートがネットワーク(アップリンク)ポートになっています。ユニットを接続するには、デバイスをスタック ポートとして接続するようにポートのタイプを変更する必要があります。このポートは、ユニット間のデータ パケットやプロトコル パケットの転送に使用されます。

スタック ポートとして使用するポートをシステムに指示(予約)する必要があります([スタック管理] ページで)。

次のポートをスタック ポートにすることができます。

- [XG デバイス]:すべてのポートをスタック ポートにすることができます。
- [X デバイス]:4 つの XG アップリンク ポートをスタック ポートにすることができます。

スタック ポート リンク アグリゲーション

隣接する 2 台のユニットがマルチ スタック リンクで接続されている場合は、それらを接続しているスタック ポートが自動的にスタック LAG に割り当てられます。この機能を使用すれば、スタック ポートのスタック帯域幅を単一ポートのスタック帯域幅より増やすことができます。

ユニットあたり最大 2 つのスタック LAG を割り当てることができます。

スタック LAG は、ユニット タイプに応じて、2 から最大数までのスタック ポートで構成できます。

Sx550X/SG350 デバイス上で、最大 2 個のインターフェイスが 2 つのユニット間のスタッキング LAG を構成できます。同じスタッキング LAG で許容されるインターフェイスの組み合わせは、インターフェイス XG1 と XG2 またはインターフェイス XG3 と XG4 のどちらかです。同じ LAG のその他のインターフェイスの組み合わせはサポートされていません。

スタック ポートの状態

スタック ポートの状態は次のいずれかになります。

- [ダウン]:ポートの動作ステータスがダウンになっているか、スタック ポートの動作ステータスはアップだが、トラフィックがポート上を通過できません。
- [アクティブ]:スタック ポートの動作ステータスがアップのスタック LAG にスタック ポートが追加され、トラフィックがポート上を通過 できるうえ、スタック LAG のメンバーになっています。
- [スタンバイ]:スタック ポートの動作ステータスはアップで、双方向のトラフィックがポート上を通過できますが、ポートをスタック LAG に追加できないため、そのポートからトラフィックが送信されません。ポートがスタンバイになる主な原因は次のとおりです。
  - 速度が異なるスタック ポートが単一のネイバーの接続に使用されている。
  - Sx550X/SG350 上で、3 個以上のインターフェイスまたはサポートされていないインターフェイスの組み合わせを使用して、単一のネイバーに接続します。

スタック LAG の物理的制限

スタック LAG の使用が制限される要因を以下に示します。

- スタック LAG 内のポートはすべて同じ速度にする必要があります。
- トポロジがリング/チェーンではないスタックにユニットを接続しようとした(たとえば、1 つのユニットを隣接する複数のユニットに接続しようとした(スター トポロジ))場合は、2 つの LAG しかアクティブにできず、残りのスタック ポートはスタンバイ モード(非アクティブ)に設定されます。

デフォルトのスタック ポートとネットワーク ポート

すべてのポートがデフォルトでネットワーク ポートとして設定されます。

ポート速度の自動選択

ケーブルをポートに接続すると、スタッキング ケーブル タイプが自動的に検出されます(自動検出がデフォルト設定です)。システムは、自動的に、スタック ケーブル タイプを識別して、ケーブルとポートでサポートされている最高速度を選択します。

ケーブル タイプが認識されなかった場合は、SYSLOG メッセージ(情報レベル)が表示されます。

ユニットの接続

スタック内の 2 台のユニットを接続できるのは、リンクの両端のスタック ポートが同じ速度の場合のみです。両方のポートが同じ速度をサポートしていることを確認する必要があります。

ケーブル タイプ

サポートされているケーブル タイプの説明を以下に示します。

スタック ポートまたはネットワーク ポート	
接続タイプ	すべてのポート
Cisco SFP-H10GB-CU1M – パッシブ銅ケーブル	1 G - 10 G
Cisco SFP-H10GB-CU3M – パッシブ銅ケーブル	1 G - 10 G
Cisco SFP-H10GB-CU5M – パッシブ銅ケーブル	1 G - 10 G
Cisco SFP-10G-SR	10 G
Cisco SFP-10G-LRM	未サポート
Cisco SFP-10G-LR	10 G
1 G SFP モジュール MGBSX1	1 G
1 G SFP モジュール MGBT1	1 G
1 G SFP モジュール MGBLX1	1 G
1 G SFP モジュール MGBBX1	1 G
100 Mbs SFP モジュール MFELX1	未サポート
100 Mbs SFP モジュール MFEFX1	未サポート
100 Mbs SFP モジュール MFEBX1	未サポート
その他の SFP	1 G

スタック内のソフトウェア自動同期

スタック内のすべてのユニットが同じソフトウェア バージョンを実行する必要があります。スタック内の各ユニットが実行しているファームウェアがマスターが実行しているものと異なっていた場合、各ユニットは自動的にマスター ユニットからファームウェアをダウンロードします。ユニットは、新しいバージョンを実行するために、それ自体を自動的にリブートします。

スタック ユニット モード

各ユニットには、次のように、スタック内のユニットのタイプを示す、スタック ユニット モードがあります。

ネイティブ スタック

スタックは、同じ製品ライン(350 または 550)で、同じサブファミリのデバイスのみで構成されます。たとえば、SG350X デバイスは同じタイプのデバイスとしかスタックできず、SG350XG デバイスとはスタックできません。その逆も同じです。同じルールが Sx550X デバイスと SG550XG デバイスにも適用されます。

ハイブリッド スタック

ハイブリッド スタック モードでは、SG350X デバイスを SG350XG デバイスと一緒にスタックしたり、Sx550X デバイスを SG550XG デバイスと一緒にスタックしたりできます。

ユニットをハイブリッド スタックに参加させるには、最初にハイブリッド モードで設定する必要があります。これは、後述するように、[スタック管理] ページで [スタック モード] を [ハイブリッド スタッキング] に設定することによって行います。

スタッキング モードの変更

スタッキング モードを変更するにはシステム リブートが必要であり、ネイティブ モードからハイブリッド モードに変更するとデバイス設定が消去されます。ネイティブ モードからハイブリッド モードに変更する前に、設定ファイルを(TFTP 経由や HTTP 経由などで)外部サーバに保存することをお勧めします。

ハイブリッド スタッキング モードをネイティブ スタッキング モードに変更しても設定は消去されません。

加えて、Sx350X/Sx550X ユニットの 2 ～ 4 XG ポートは、スタッキング ポートとして設定し、SG350XG/SG550XG デバイスのスタッキング ポートに接続する必要があります。

Sx350X と SG350XG の機能セットは同じです。同様に、Sx550X と SG550XG の機能セットも同じです。ただし、機能サポートとテーブル サイズに若干の違いがあります。機能に違いがある場合、ハイブリッド スタックはその最も低い基準をサポートします。ハイブリッド スタック タイプごとの違いのリストと、各ユニット タイプとハイブリッド スタックで使用される設定を以下に示します。

機能/テーブル	Sx550X	SG550XG	ハイブリッド スタック
OOB ポート	未サポート	サポート済み	未サポート
MAC テーブル サイズ	16K	64K	16K
ACL TCAM	3K - 予約済み	2K - 予約済み	2K - 予約済み
ARP テーブル サイズ	4K - 予約済み	8K - 予約済み	4K - 予約済み
最大 MAC テーブル エージング	400	630	400

機能/テーブル	SG350X	SG350XG	ハイブリッド スタック
OOB ポート	未サポート	サポート済み	未サポート
MAC テーブル サイズ	16K	64K	16K
ACL TCAM	1K - 予約済み	2K - 予約済み	1K - 予約済み
ルータTCAM	992(タイプごとのデフォルト設定と最大設定にも影響する)	7168(タイプごとのデフォルト設定と最大設定にも影響する)	992(タイプごとのデフォルト設定と最大設定にも影響する)
ARP テーブル サイズ	1K - 予約済み	8K - 予約済み	1K - 予約済み
マルチキャスト グループの数	2K	4K	2K
IPv6 インターフェイスの最大数	106	200	106
IPv6 ホストの最大数	210	1776	210
最大オンリンク IPv6 プレフィックス	200	256	200
最大 MAC テーブル エージング	400	630	400

機能/テーブル	SG350X	SG350XG	ハイブリッド スタック
IPv6 手動トンネル/ 6to4 トンネル/ ISATAP ルーティング トンネル	未サポート	サポート済み	未サポート

スタック内のスタック ユニット モードの一貫性

スタック内のすべてのユニットが同じスタック ユニットモードを備えている必要があります。

スタックは、初期化が完了すると、スタックのユニットに関する情報を収集するトポロジ ディスカバリ アルゴリズムを実行します。

マスターになるユニットが選択されたら、そのユニットは、一貫したスタック ユニット モードを備えていないネイバーのスタックへの参加要求を拒否することができます。スタック ユニット モードが原因でユニットが拒否された場合は、そのユニットが論理的にシャットダウンされ(ポートでトラフィックを送受信できなくなる)、そのすべての LED(システム、FAN、ユニット ID、ネットワーク ポート、およびスタック ポートの LED)が点灯します。スタック ユニット モードに関する情報が SYSLOG エラーとしてマスター ユニットに表示されます。

ユニットをこの状態から回復する唯一の方法は、電源からプラグを抜き、再び挿入することです。この操作は、影響を受けるユニットをスタックから切り離した状態で行う必要があります。そうすれば、影響を受けるユニット モードを現在のスタック モードに変更し、ユニットをスタックに再参加させることができます。

スタック ユニット タイプ

あるタイプ(GE/FE/XG)のユニットがスタックから削除され、別のタイプのユニットと交換された場合は、デバイスが以前のユニットの設定を新しいユニットに適用しようとします。通常、この処理は成功しますが、次のような例外もあります。

- ダウンリンク ポート設定:スタックにあるタイプのユニット(GE ユニットなど)が含まれており、このユニットが別のタイプのユニット(FE ユニットなど)に交換された場合は、ポートに基づく設定(VLAN、STP、ACL、802.1x など)のほとんどが自動的に新しいポート タイプに適用されます。一部の静的なポート タイプ関連の設定が失敗してエラーが報告される場合(ポート速度が 1 GB に設定されており、新しいユニット内のこのポート番号が最大 100 Mbps の速度をサポートする場合など)がありますが、これが原因で残りの設定が失敗することはありません。失敗したコマンドは、スタックの実行コンフィギュレーション ファイルとスタートアップ コンフィギュレーション ファイルの一部として残りますが、システムをリロードすると、新しい実行コンフィギュレーション ファイルから削除されます。

- アップリンク ポート設定:古いユニット タイプと新しいユニット タイプが FE と GE 間で変更された場合は、設定が新しいユニット タイプと古いユニット タイプの両方で一致します(アップリンク ポートが常に XG ポートのため)。したがって、アップリンク ポートの設定がエラーなしで新しいユニットに適用されます。

FE/GE デバイス(アップリンク ポート タイプをサポートする)を XG デバイス(アップリンク ポート タイプをサポートしない)に交換した場合、新しく加わった XG デバイス上のアップリンク ポート設定は、ID が 49 ～ 52 の特別なインターフェイス タイプに保存されます。このインターフェイス タイプは、インターフェイスが存在しないことを示すために予約されています。

ユニット/インターフェイス タイプを交換すると、実行コンフィギュレーション ファイルとスタートアップ コンフィギュレーション ファイルが正しいインターフェイス タイプを表示するように修正されます。たとえば、古いユニットがインターフェイス ID FE1/0/1 の FE ユニットで、それを GE ユニット タイプに交換すると、実行/スタートアップ コンフィギュレーション(および CLI show コマンド)でその設定が自動的に GE1/0/1 の下に表示されます。

スタック管理

スタックを設定するには、次のようにします。

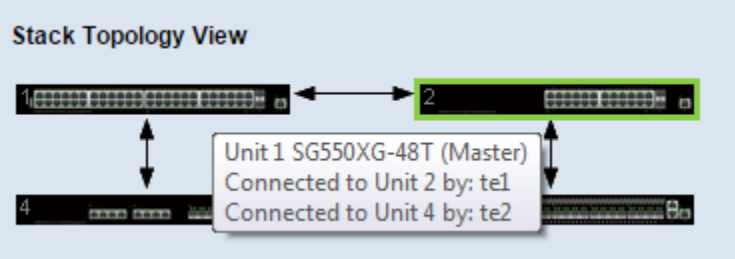
ステップ 1 [各種管理] > [スタック管理] の順にクリックします。

スタンドアロン デバイスまたはスタックの動作ステータスが [スタック動作ステータス] ブロックに表示されます。

- [スタック モード]:次のオプションのいずれかが表示されます。
  - [ネイティブ スタッキング]:デバイスは、すべてのユニットが同じタイプのスタックに属しています。
  - [ハイブリッド スタッキング]:デバイスは、350 デバイスの混合タイプと 550 デバイスの混合タイプのどちらか(350 デバイスと 550 デバイスの混合ではない)で構成可能なスタックの一部です。
- [スタックトポロジ]:スタックのトポロジがチェーンなのかリングなのかが表示されます。
- [スタックマスター]:スタックのマスター ユニットのユニット ID が表示されます。

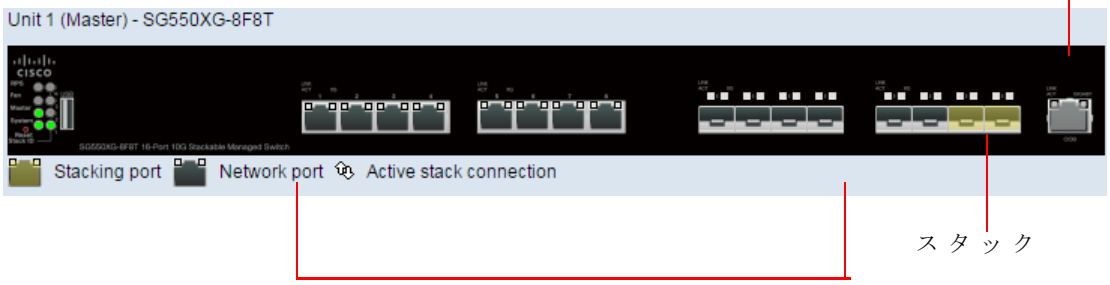
スタックトポロジビュー

このビューには、デバイスのグラフィック ビューが表示されます。この上にマウス カーソルを移動すると、ユニット番号、スタック内でのその機能(マスター、バック アップ、またはスレーブ)、およびスタック内でそれに接続されているデバイスと経由しているスタッキング ポートが表示されます。以下に例を示します。



ユニットビューおよびスタックポートコンフィギュレーション

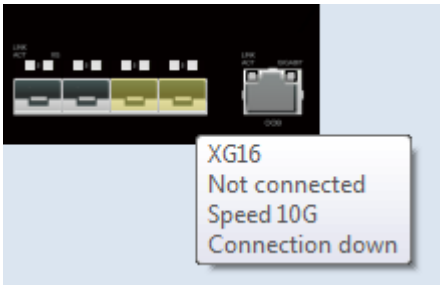
スタック トポロジ ビューで特定のデバイスをクリックすると、そのデバイスのグラフィック ビューが表示されます。以下に例を示します。



ステップ 2 デバイスのスタック ポートを選択するには、次のようにします。

a. [スタックトポロジビュー] でデバイスをクリックします。このデバイス上のポートが [ユニットビューおよびスタックポートコンフィギュレーション] に表示されます。

b. ポートの上にマウス カーソルを移動すると、ツール ヒントにスタッキング ポート番号、接続先のユニット(存在する場合)、ポート速度、および接続ステータスが表示されます。次の例を参照してください。スタッキング ポートとして選択するネットワーク ポート(黒色)をクリックします。そうすると、そのネットワーク ポートが黄色に変わり、スタッキング ポートになることを示します。(黄色のスタッキング ポートをクリックすると、それがネットワーク ポート(黒色)に変わります)。



ステップ　3　スタック内のデバイスのリセット後のユニット ID を設定するには、スタック トポロジ ビューでデバイスをクリックして、次のフィールドに値を入力します。

- [リセット後のユニットID]:ユニット ID を選択するか、ユニット ID をシステムに選択させる場合は [自動] を選択します。
- [ユニットxスタック接続速度]:スタック接続の速度が表示されます。

ステップ　4　[適用とリブート] 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、スタックがリブートされます。

8

各種管理:時刻設定

同期されたシステム クロックは、ネットワーク上のすべてのデバイス間で基準時刻になります。ネットワーク時刻の同期化は非常に重要です。ネットワークの管理、セキュリティ保護、計画、およびデバッグのすべての局面で、イベント発生の判断が必要になるためです。クロックが同期化されていなければ、セキュリティ違反やネットワーク使用率の追跡時に、デバイス間でログ ファイルを正しく関連付けられなくなります。

また、時刻が同期化されていれば、共有ファイル システムに混乱が生じるのを減らすこともできます。ファイル システムがどのマシン上にあるかに関係なく、変更時間が一貫していることが重要だからです。

以上の理由により、ネットワーク上のすべてのデバイスで設定される時刻が正確であることが必要です。

注 このデバイスは、Simple Network Time Protocol(SNTP; 簡易ネットワーク タイム プロトコル)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 サーバ時刻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、他のデバイスにタイム サービスを提供することはできません。

ここでは、システムの時刻、時間帯、および Daylight Savings Time(DST; 夏時間)を設定するときのオプションについて説明します。具体的な内容は、次のとおりです。

- システム時刻の設定
- SNTP モード
- システムの時刻
- SNTP ユニキャスト
- SNTP マルチキャスト/エニーキャスト
- SNTP 認証
- 時間範囲
- 繰り返し時間範囲

システム時刻の設定

システムの時刻を設定する方法としては、ユーザが手動で設定する方法、SNTP サーバを使用して動的に設定する方法、および GUI を実行している PC から同期化する方法があります。SNTP サーバを選択した場合、手動で設定した時刻は、サーバとの通信が確立したときに上書きされます。

デバイスでは、起動プロセスの実行中に、時刻、時間帯、および DST が必ず設定されます。これらのパラメータは、GUI を実行している PC、SNTP、または手動で設定した値から取得されます。ただし、取得に失敗した場合は、工場出荷時の初期状態になります。

時刻

次の方法により、デバイスのシステム時刻を設定することができます。

- [手動]:ユーザの操作で時刻を設定する必要があります。
- [PCから]:ブラウザの情報を使用して、PC から時刻を受信できます。

  コンピュータから取得した時刻の設定は、実行コンフィギュレーション ファイルに保存されます。リブート後にコンピュータから取得した時刻をデバイスで使用できるようにするため、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必要があります。リブート後、時刻は、デバイスへの初回 WEB ログイン時に設定されます。

  この機能を初めて構成したときに、時刻が未設定であった場合、デバイスでは、PC から取得した時刻が設定されます。

  この時刻設定方法は、HTTP 接続と HTTPS 接続のどちらでも有効です。
- [SNTP]:SNTP タイム サーバから時刻を受信できるようになります。SNTP を使用すると、クロック ソースとして SNTP サーバを使用して、ミリ秒まで、デバイスのネットワーク時刻の正確な同期化を行うことができます。SNTP サーバを指定する場合、ホスト名でサーバを識別することを選択すると、GUI で次の 3 つの選択候補が提示されます。
  - time-a.timefreq.bldrdoc.gov
  - time-b.timefreq.bldrdoc.gov
  - time-c.timefreq.bldrdoc.gov

上記の時刻ソースのいずれかに基づいて時刻が設定されると、以後、ブラウザによって時刻は再設定されません。

注 SNTP は、推奨されている時刻設定方法です。

時間帯と夏時間(DST)

時間帯と DST は、次の方法によりデバイスに設定できます。

- DHCP サーバを使用したデバイスのダイナミック設定。この場合、次のように設定されます。
  - ダイナミック DST が有効で使用可能な場合、常に、DST の手動設定より優先されます。
  - サーバからソース パラメータが提供されない場合、またはダイナミック設定がユーザによって無効になっている場合、手動設定が使用されます。
  - 時間帯と DST のダイナミック設定は、IP アドレスのリース時間が切れても続行します。
- 手動で設定した時間帯と DST が実際に使用されるのは、ダイナミック設定が無効になっているか失敗した場合のみです。

  注 ダイナミック時間帯の設定を適用するには、DHCP サーバは、DHCP オプション 100 を指定する必要があります。

SNTP モード

デバイスは、次のいずれかの方法で、SNTP サーバからシステム時刻を受け取ることができます。

- [クライアントブロードキャスト受信(パッシブモード)]:SNTP サーバは時刻をブロードキャストし、デバイスはこれらのブロードキャストをリッスンします。デバイスがこのモードである場合、ユニキャスト SNTP サーバを定義する必要はありません。
- [クライアントブロードキャスト送信(アクティブモード)]:デバイスは、SNTP クライアントとして、SNTP 時刻の更新を定期的に要求します。このモードは、次のいずれかの方法で機能します。
  - [SNTPエニーキャストクライアントモード]:デバイスのブロードキャスト時刻は、サブネットですべての SNTP サーバにパケットを要求し、応答を待機します。
  - [ユニキャストSNTPサーバモード]:デバイスはユニキャスト クエリーを、手動設定された SNTP サーバ リストに送信し、応答を待機します。

デバイスは、上記のすべてのモードを同時にアクティブにできます。最も近いストラタム(参照クロックからの距離)に基づくアルゴリズムに従って、SNTP サーバから受信された最適なシステム時刻が選択されます。

システムの時刻

[システムの時刻] ページを使用して、システム時刻のソースを選択します。ソースが手動である場合は、ここに時刻を入力できます。

注意　システムの時刻を手動で設定し、デバイスを再起動した場合は、手動時刻設定を再入力する必要があります。

システムの時刻を定義するには、次のようにします。

ステップ　1　[各種管理] > [時間設定] > [システムの時刻] の順にクリックします。

次のフィールドが表示されます。

- [実際の時刻(システム時刻源)]:デバイスのシステム時刻。ここには、DHCP 時間帯が表示されます。ユーザ定義の時間帯の頭字語が定義されている場合はそれが表示されます。
- [最後に同期されたサーバ]:システム時刻を最後に取得したときの SNTP サーバのアドレス、ストラタム、およびタイプ。

ステップ　2　次のパラメータを指定します。

- [クロックソース設定]:システム クロックの設定に使用するソースを選択します。
  - [メインクロックソース(SNTPサーバ)]:これが有効になっている場合、システムの時刻は SNTP サーバから取得されます。この機能を使用するには、[SNTP マルチキャスト/エニーキャスト] ページで SNTP サーバへの接続も設定する必要があります。(任意)[SNTP 認証] ページを使用して、SNTP セッションを強制認証します。
  - [代替クロックソース(アクティブHTTP/HTTPSセッションを介したPC)]:HTTP プロトコルを使用して設定コンピュータから日付と時刻を設定する場合に選択します。

  注　RIP MD5 認証を機能させるには、[クロックソース設定] を上記のいずれかに設定する必要があります。
- [手動設定]:日付と時刻を手動で設定します。SNTP サーバなどの代替時刻ソースがない場合は、現地時間が使用されます。
  - [日付]:システム日付を入力します。
  - [現地時間]:システム時刻を入力します。

- [時間帯設定]:現地時間は、DHCP サーバまたは時間帯のオフセットを介して使用されます。
  - [DHCPから時間帯を取得]:DHCP サーバからの時間帯と DST のダイナミック設定を有効にします。これらのパラメータを設定できるかどうかは、DHCP パケットから検出される情報によって異なります。このオプションを有効にした場合、*デバイスで DHCP クライアントを有効にする必要があります。*

    注 DHCP クライアントは、ダイナミック時間帯の設定を指定するオプション 100 をサポートします。
  - [DHCP からの時間帯]:DHCP サーバから設定された時間帯の頭字語を表示します。この頭字語は、[実際の時刻] フィールドに表示されます
  - [時間帯のオフセット]:*Greenwich Mean Time*(GMT; グリニッジ標準時)と現地時間との差を選択します。たとえば、パリの時間帯のオフセットは GMT +1、ニューヨークの時間帯のオフセットは GMT – 5 になります。
  - [時間帯の頭字語]:この時間帯を表す名前を入力します。この頭字語は、[実際の時刻] フィールドに表示されます。
- [サマータイム設定]:DST の定義方法を選択します。
  - [夏時間]:夏時間を有効にする場合に選択します。
  - [時間設定のオフセット]:GMT からのオフセットの分数を 1 ～ 1440 の範囲で入力します。デフォルトは 60 です。
  - [夏時間タイプ]:次のいずれかをクリックします。

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

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

    [日付指定]:通常、米国またはヨーロッパ諸国以外の国では、DST を手動で設定します。次のパラメータを指定します。

    [繰り返し]:DST を毎年同じ日付に発生させます。

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

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

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

- [開始]:毎年 DST が開始する日付。
  - [曜日]:毎年 DST が開始する曜日。
  - [週]:毎年 DST が開始する月の週。
  - [月]:毎年 DST が開始する月。
  - [時刻]:毎年 DST が開始する時刻。
- [終了]:毎年 DST が終了する日付。たとえば、DST を当地毎年 10 月の第 4 週目の金曜日 AM 5:00 に終了するとします。次のパラメータを指定します。
  - [曜日]:毎年 DST が終了する曜日。
  - [週]:毎年 DST が終了する月の週。
  - [月]:毎年 DST が終了する月。
  - [時刻]:毎年 DST が終了する時刻。

ステップ 4 [適用] をクリックします。システムの時刻値が、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

最大 16 台のユニキャスト SNTP サーバを設定できます。

注 ユニキャスト SNTP サーバを名前で指定するには、最初にデバイスで DNS サーバを設定する必要があります(「DNS 設定」を参照してください)。

ユニキャスト SNTP サーバを追加するには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [SNTPユニキャスト] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [SNTPクライアントユニキャスト]:これを選択すると、SNTP で事前定義されたユニキャスト クライアントをユニキャスト SNTP サーバと共にデバイスで使用できます。

- [IPv4送信元インターフェイス]:SNTP サーバとの通信に使用するメッセージのソース IPv4 アドレスとして使用する IPv4 アドレスの IPv4 インターフェイスを選択します。
- [IPv6送信元インターフェイス]:SNTP サーバとの通信に使用するメッセージのソース IPv6 アドレスとして使用する IPv6 アドレスの IPv6 インターフェイスを選択します。

  注 [自動] オプションが選択されている場合、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。

このページには、各ユニキャスト SNTP サーバについての次の情報が表示されます。

- [SNTPサーバ]:SNTP サーバの IP アドレス。ストラタム レベルによって、優先サーバまたはホスト名が選択されます。
- [ポール間隔]:ポーリングが有効か無効かを示します。
- [認証キーID]:SNTP サーバとデバイス間の通信に使用されるキー認証。
- [ストラタムレベル]: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場合、SNTP サーバはプライマリ サーバ(ストラタム レベル 1)に設定できません。
- [ステータス]:SNTP サーバのステータス。表示される値は次のとおりです。
  - [アップ]:SNTP サーバは現在正常に動作しています。
  - [ダウン]:SNTP サーバは現在使用できません。
  - [不明]:SNTP サーバの状態が不明です。
  - [処理中]:SNTP サーバへの接続は現在処理中です。
- [最後の応答]:前回この SNTP サーバからの応答が受信された日時。
- [オフセット]:ローカル クロックを基準としたサーバのクロック推定オフセット(ミリ秒)。ホストは、RFC 2030 で説明されているアルゴリズムを使ってこのオフセット値を決定します。
- [遅延]:ローカル クロックとサーバ クロック間のネットワーク パスにおける、ローカル クロックを基準としたサーバ クロックの推定ラウンド トリップ遅延(ミリ秒)。ホストは、RFC 2030 で説明されているアルゴリズムを使ってこの遅延値を決定します。
- [ソース]:SNTP サーバの定義方法(たとえば、手動、DHCPv6 サーバからなど)。
- [インターフェイス]: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 サーバを追加するには、[SNTPクライアントユニキャスト] を有効にします。

ステップ　4　[追加] をクリックします。

注 すべてのユーザ定義の SNTP サーバを削除するには、[デフォルトサーバの復元] をクリックします。

ステップ　5　次のパラメータを指定します。

- [サーバ指定方法]:SNTP サーバを IP アドレスで識別するか、リストから既知の SNTP サーバを名前で選択するかのいずれかを選択します。

  注 既知の SNTP サーバを指定するには、デバイスがインターネットに接続し、DNS サーバで設定されているか、DNS サーバが DHCP により識別されるように設定されている必要があります。(「DNS 設定」を参照してください)

- [IPバージョン]:IP アドレスのバージョンとして以下を選択します。[バージョン6] または [バージョン4]。

- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。

  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。

  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。

- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 アドレス タイプとしてリンク ローカルが選択されている場合)。

- [SNTPサーバのIPアドレス/名前]:SNTP サーバの IP アドレッサ名を入力します。この形式は、選択されているアドレス タイプによって異なります。

- [ポール間隔]: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 サーバがポーリングされ、クロックは、ストラタム レベル(参照クロックからの距離)が一番低い、アクセス可能なサーバから選択されます。ストラタムが一番低いサーバがプライマリ サーバと見なされます。次に低いストラタムのサーバがセカンダリ サーバと見なされ、それよりストラタムが低いサーバがその下に位置します。プライマリ サーバがダウンしている場合、デバイスはポーリング設定が有効になっているすべてのサーバをポーリングし、その中でストラタムが一番低いプライマリ サーバを新たに選択します。

- [認証]:認証を有効にする場合、このチェックボックスを選択します。
- [認証キーID]:認証が有効な場合、キー ID の値を選択します。(認証キーの作成は、[SNTP 認証] ページを使用して行います。)

ステップ 6 [適用] をクリックします。STNP サーバが追加され、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

デバイスは、アクティブ モード/パッシブ モードにすることができます(詳しくは、「SNTP モード」を参照してください)。

サブネット上ですべてのサーバからの SNTP パケットの受信を有効にしたり、SNTP サーバへの時刻要求の送信を有効にしたりするには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [SNTPマルチキャスト/エニーキャスト] の順にクリックします。

以下のオプションから選択します。

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

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

インターフェイスを選択します。

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

SNTP 認証

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 サーバはキーと関連付けられており、キーは応答自体とともに MD5 機能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認証] ページでは、認証が必要な SNTP サーバ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、使用している SNTP サーバのタイプに応じて、独立したプロセスで SNTP サーバに作成されます。詳細については、SNTP サーバのシステム管理者に確認してください。

ワークフロー

ステップ 1 後述する [SNTP認証] ページで認証を有効にします。

ステップ 2 後述する [SNTP認証] ページでキーを作成します。

ステップ 3 [SNTP ユニキャスト] ページで、このキーを SNTP サーバと関連付けます。

SNTP 認証を有効にして、キーを定義するには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [SNTP認証] の順にクリックします。

ステップ 2 デバイスと SNTP サーバ間の SNTP セッションの認証が必要な場合は、[SNTP認証] を選択します。

ステップ 3 [適用] をクリックしてデバイスを更新します。

ステップ 4 [追加] をクリックします。

ステップ 5 次のパラメータを指定します。

- [認証キーID]: この SNTP 認証キーを内部的に識別するための番号を入力します。
- [認証キー(暗号化)]:認証に使用するキーを暗号化形式で入力します(最大 8 文字)。SNTP サーバは、デバイスと同期化するために、このキーを送信する必要があります。
- [認証キー(プレーン テキスト)]: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、デバイスと同期化するために、このキーを送信する必要があります。

- [信頼済みキー]:デバイスが、この認証キーを使って、SNTP サーバからのみ同期化情報を受信できるようにする場合に選択します。

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

時間範囲

時間範囲を定義して、以下のタイプのコマンドと関連付けることにより、その時間範囲のみコマンドを適用することができます。

- ACL
- 8021X ポート認証
- ポート設定
- 時間ベースの PoE

時間範囲には以下の 2 つのタイプがあります。

- [絶対]:このタイプの時間範囲は、特定の日付または即時に開始し、特定の日付で終了するか、無制限に実行されます。これは、[時間範囲] ページで作成されます。繰り返し要素をそれに追加することができます。
- [繰り返し]:このタイプの時間範囲には、絶対範囲に追加される時間範囲要素が含まれており、繰り返しに基づいて開始および終了します。これは、[繰り返し時間範囲] ページで定義されます。

時間範囲に絶対範囲と繰り返し範囲の両方が含まれる場合、関連するコマンドの動作は、絶対開始時刻と繰り返し時間範囲の両方に達した場合にのみアクティブ化されます。関連するコマンドの動作は、いずれかの時間範囲に達した時点で非アクティブ化されます。

このデバイスでサポートされる絶対時間範囲は最大 10 個です。

すべての時間仕様はローカル時刻として解釈されます(夏時間はこれに影響しません)。その時間範囲エントリを目的の時刻に確実に実行するために、システム時刻を設定する必要があります。

時間範囲機能は、以下の目的で使用できます。

- 一例として、ネットワークへのコンピュータのアクセスをビジネス時間だけに制限し、その後にネットワーク ポートをロックし、残りのネットワークのアクセスをブロックします(「ポート設定」および「リンクアグリゲーション」を参照してください)。
- 指定した期間だけに PoE 操作を制限します。

絶対時間範囲

絶対時間範囲を定義するには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [時間範囲] の順にクリックします。

既存の時間範囲が表示されます。

ステップ 2 新規の時間範囲を追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [時間範囲名]:新規の時間範囲名を入力します。
- [絶対開始時間]:開始時間を定義するには、以下を入力します。
  - [即時]:時間範囲を即時に開始する場合に選択します。
  - [日付]、[時刻]:時間範囲の開始日時を入力します。
- [絶対終了時間]:開始時間を定義するには、以下を入力します。
  - [無期限]:時間範囲を終了させない場合に選択します。
  - [日付]、[時刻]:時間範囲の終了日時を入力します。

ステップ 4 [適用] をクリックします。

ステップ 5 繰り返しの時間範囲を追加するには、[繰り返し時間範囲] をクリックします。

繰り返し時間範囲

繰り返し時間要素は、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操作が制限されます。

繰り返しの時間範囲要素を絶対時間範囲に追加するには、次のようにします。

ステップ 1 [各種管理] > [時間設定] > [繰り返し時間範囲] の順にクリックします。

既存の繰り返し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されます。)

ステップ 2 繰り返し範囲を追加する絶対時間範囲を選択します。

ステップ 3 新規の繰り返し時間範囲を追加するには、[追加] 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。

- [繰り返し開始時刻]:時間範囲の繰り返しが開始する日時を入力します。
- [繰り返し終了時刻]:時間範囲の繰り返しが終了する日時を入力します。

ステップ　5　[適用] をクリックします。

ステップ　6　[時間範囲] をクリックして [絶対時間範囲] ページにアクセスします。

9

各種管理:ディスカバリ(検出)

ここでは、検出処理の設定について説明します。

具体的な内容は、次のとおりです。

- Bonjour
- LLDP および CDP
- ディスカバリ - LLDP
- ディスカバリ - CDP

Bonjour

Bonjour クライアントであるこのデバイスからは、直接接続している IP サブネットに Bonjour ディスカバリ プロトコル パケットが定期的にブロードキャストされます。これにより、このデバイスの存在およびこのデバイスが提供するサービス(HTTP、HTTPS、Telnet など)がアドバタイズされます。このデバイスが提供するサービスの有効/無効は、[TCP/UDP サービス] ページから切り替えることができます。この結果、このデバイスがネットワーク管理システムやサードパーティ製アプリケーションから検出できるようになります。デフォルトでは、管理 VLAN 上で Bonjour が有効になっています。

デバイス上で Bonjour が有効な場合、デバイスは Bonjour ディスカバリ インターフェイス コントロール テーブルで Bonjour に関連付けられている IP アドレスを持つインターフェイスに、Bonjour ディスカバリ パケットを送信します。インターフェイスに IP アドレスを設定するには、[IPv4 インターフェイス] を使用します。

VLAN などのインターフェイスが削除されると、デバイスは Bonjour Goodbye パケットをインターフェイスに送信し、デバイス自体とそのサービスの登録を解除します。Goodbye パケットを受信したネイバー デバイスは、ローカル サービス テーブルからそのサービスを削除します。Bonjour ディスカバリ インターフェイス コントロール テーブルには、Bonjour の機能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が表示されます。Bonjour アドバタイズメントは、このテーブルに表示されているインターフェイスに対してのみブロードキャストできます。サービスが有効または無

効にされると、それに応じてサービスを登録または登録解除するために、デバイスは Bonjour パケットを送信します。サービスが変更されると、デバイスは新しい情報を収めた Bonjour パケットを送信します。デバイスの IP アドレスが変更されると、デバイスもその新しい IP アドレスをアドバタイズします。

Bonjour を無効にすると、デバイスは Bonjour ディスカバリ アドバタイズメントを送信しなくなり、他のデバイスから送信される Bonjour ディスカバリ アドバタイズメントも待機しなくなります。

Bonjour を設定するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - Bonjour] の順にクリックします。

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

ステップ 3 特定のインターフェイスで Bonjour を有効にするには、[追加] 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。インターフェイスに IP アドレスが割り当てられている場合は、そのアドレスが表示されます。

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

注 インターフェイスで Bonjour を無効にするには、[削除] をクリックします(削除の場合、[適用] をクリックするなどの追加の操作はありません)。

LLDP および CDP

LLDP(Link Layer Discovery Protocol)、および CDP(Cisco Discovery Protocol)は、直接接続された LLDP および CDP 対応のネイバーが、自身とそれぞれの機能をアドバタイズするためのリンク層プロトコルです。デフォルトでは、デバイスはそのすべてのインターフェイスに定期的に LLDP/CDP アドバタイズメントを送信し、着信 LLDP および CDP パケットをプロトコルの要求に従って処理します。LLDP と CDP では、アドバタイズメントは TLV(Type, Length, Value)としてパケット内にエンコードされます。

CDP/LLDP の設定に関する注意点は次のとおりです。

- CDP/LLDP の有効または無効は、グローバルに設定することもポートごとに設定することもできます。ポートの CDP/LLDP 機能は、CDP/LLDP がグローバルに有効な場合のみ使用できます。
- CDP/LLDP がグローバルに有効な場合、デバイスは、CDP/LLDP が無効なポートの着信 CDP/LLDP パケットをフィルタリングします。

- CDP/LLDP がグローバルに無効な場合、デバイスの構成によって、すべての着信 CDP/LLDP パケットの廃棄、VLAN 対応フラッディング、または VLAN 非対応フラッディングを実行できます。VLAN 対応のフラッディングでは、着信 CDP/LLDP パケットは、入力ポートを除き、パケットを受信する VLAN にフラッディングされます。VLAN 非対応のフラッディングでは、着信 CDP/LLDP パケットは、入力ポートを除くすべてのポートにフラッディングされます。デフォルトでは、CDP/LLDP がグローバルに無効な場合は、CDP/LLDP パケットは廃棄されます。着信 CDP および LLDP パケットの廃棄またはフラッディングは、それぞれ [CDP のプロパティ] ページと [LLDP のプロパティ] ページで設定できます。
- Auto Smartport では、CDP または LLDP、もしくは両方を有効にする必要があります。Auto Smartport は、インターフェイスから受信した CDP/LLDP アドバタイズメントに基づいてインターフェイスを自動的に設定します。
- IP 電話などの CDP および LLDP エンド デバイスは、CDP および LLDP アドバタイズメントから音声 VLAN 設定を学習します。デフォルトでは、デバイスは、デバイスに設定された音声 VLAN に基づいて CDP および LLDP アドバタイズメントを送信できるようになっています。詳細については、「音声 VLAN」を参照してください。

注 CDP/LLDP は、ポートが LAG のメンバーであるかどうかを区別しません。複数のポートが 1 つの LAG のメンバーである場合、CDP/LLDP はそのポートが LAG のメンバーであるという事実を考慮せずに各ポートにパケットを送信します。

CDP/LLDP の動作は、インターフェイスの STP ステータスとは無関係です。

802.1x ポート アクセス コントロールがインターフェイスで有効な場合、デバイスは、インターフェイスが認証および承認されている場合にのみ、そのインターフェイスとの間で CDP/LLDP パケットを送受信します。

ポートがミラーリングの対象の場合、CDP/LLDP はそのポートをダウンしたものと見なします。

注 CDP および LLDP は、直接接続された CDP/LLDP 対応のデバイスが自身とそれぞれの機能をアドバタイズするためのリンク層プロトコルです。CDP/LLDP 対応のデバイスが直接接続されておらず、CDP/LLDP 非対応のデバイスと分離している展開では、CDP/LLDP 非対応のデバイスが受信した CDP/LLDP パケットをフラッディングする場合にのみ、CDP/LLDP 対応のデバイスは他のデバイスからアドバタイズメントを受信できます。CDP/LLDP 非対応のデバイスが VLAN 対応フラッディングを実行する場合、CDP/LLDP 対応のデバイスは、同じ VLAN 内に存在する場合のみ、互いにアドバタイズメントを受信できます。CDP/LLDP 非対応のデバイスが CDP/LLDP パケットをフラッディングする場合、CDP/LLDP 対応のデバイスは複数のデバイスからアドバタイズメントを受信することがあります。

ディスカバリ - LLDP

ここでは、LLDP の設定方法を説明します。具体的な内容は、次のとおりです。

- LLDP の概要
- LLDP 設定のワークフロー
- LLDP のプロパティ
- ポート設定
- LLDP MED ネットワーク ポリシー
- LLDP MED ポート設定
- LLDP ポート ステータス
- LLDP ローカル情報
- LLDP ネイバー情報
- LLDP 統計情報
- LLDP 過負荷

LLDP の概要

LLDP は、ネットワーク マネージャが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実行するためのプロトコルです。LLDP では、ネットワーク デバイスが、自身を他のデバイスにアドバタイズする方法、および検出された情報を格納する方法が標準化されています。

LLDP を使用した場合、各デバイスの ID、設定情報、および機能が近隣デバイスにアドバタイズされます。受信側デバイスでは、これらのデータが管理情報ベース(MIB)に格納されます。ネットワーク管理システムでは、これらの MIB データベースに照会することによって、ネットワークのトポロジがモデル化されます。

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、および処理を実行します。

LLDP プロトコルには、LLDP Media Endpoint Discovery(LLDP-MED; LLDP メディア エンドポイント検出)という拡張機能があります。LLDP-MED を利用すれば、VoIP 電話やテレビ電話などのメディア エンドポイント デバイスとの間で情報を送受信できます。LLDP-MED の詳細については、「LLDP MED ネットワーク ポリシー」をご覧ください。

LLDP 設定のワークフロー

LLDP 機能を使用して実行できる作業の例と推奨される手順を次に示します。LLDP を設定するためのより詳細なガイドラインは、LLDP/CDP に関するセクションを参照してください。LLDP の設定に関するページは、「LLDP および CDP」セクションからアクセスできます。

1. [LLDP のプロパティ] ページを使用して、LLDP 更新情報の送信間隔などの LLDP グローバル パラメータを入力します。
2. [ポート設定] ページを使用して、ポートごとに LLDP を設定します。このページでは、LLDP PDU の送受信、SNMP 通知の送信、アドバタイズする TLV の指定、デバイスの管理アドレスのアドバタイズについて、インターフェイスを設定できます。
3. [LLDP MED ネットワーク ポリシー] ページを使用して、LLDP MED ネットワーク ポリシーを作成します。
4. [LLDP MED ポート設定] ページを使用して、LLDP MED ネットワーク ポリシーとオプションの LLDP-MED TLV を必要なインターフェイスにバインドします。
5. Auto Smartport で LLDP デバイスの機能を検出する場合は、[プロパティ] ページで LLDP を有効にします。
6. [LLDP 過負荷] ページを使用して、過負荷情報を表示します。

LLDP のプロパティ

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

LLDP のプロパティ値を設定するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [プロパティ] 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。

- [LLDP ステータス]:選択するとデバイス上の LLDP が有効になります(デフォルトで有効)。
- [LLDP フレーム処理]:LLDP が有効でない場合は、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。
  - [フィルタリング]:パケットを削除します。
  - [フラッディング]:VLAN メンバーすべてにパケットを転送します。
- [TLV アドバタイズ間隔]:LLDP アドバタイズメント更新データの送信間隔(単位:秒)を入力するか、デフォルトを使用します。

- [トポロジ変更 SNMP 通知間隔]:SNMP 通知を実行する最短の時間間隔を入力します。
- [ホールド係数]:LLDP パケットを破棄せずに保持する時間を、[TLV アドバタイズ間隔] の値の倍数で入力します。たとえば、[TLV アドバタイズ間隔] の値が 30 秒であり、[ホールド係数] の値が 4 である場合、LLDP パケットは 120 秒後に破棄されます。
- [再初期化遅延]:LLDP 有効/無効サイクルの後、LLDP を無効にしてから再初期化するまでの間隔(単位:秒)を入力します。
- [送信遅延]:LLDP ローカル システム MIB の内容が変更されたときに LLDP フレームを送信する間隔(単位:秒)を入力します。
- [シャーシ ID アドバタイズメント]:LLDP メッセージのアドバタイズメントに関して、次のオプションのいずれかを選択します。
  - [MAC アドレス]:デバイスの MAC アドレスをアドバタイズします。
  - [ホスト名]:デバイスのホスト名をアドバタイズします。

ステップ 3 LED-MED の [プロパティ] の [Fast Startリピート回数] 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 Fast Start 機能は、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 [適用] 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

[LLDPポート設定] ページでは、ポートごとに LLDP や SNMP 通知を有効にしたり、LLDP PDU に送信される TLV を入力できます。

[LLDP MED ポート設定] ページで、アドバタイズされる LLDP-MED TLV を選択できます。また、デバイスの管理アドレス TLV も設定できます。

ポートの LLDP 情報を設定するには、次のようにします。

ステップ 1 [管理] > [ディスカバリ - LLDP] > [ポート設定] の順にクリックします。

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、[編集] 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。

- [インターフェイス]:編集するポート(OOB ポートを含む)を選択します。
- [管理ステータス]:このポートの LLDP 発行オプションを選択します。値は次のとおりです。
  - [Txのみ]:発行はしますが検出はしません。
  - [Rx のみ]:検出はしますが発行はしません。
  - [Tx および Rx]:発行も検出も行います。
  - [無効]:このポート上で LLDP を無効にします。
- [SNMP 通知]:トポロジの変更があったときに、SNMP 通知を受信者(たとえば、SNMP 管理システム)に送信する場合は、[有効] を選択します。

  通知送信間隔は、[LLDP のプロパティ] ページの [トポロジ変更SNMP通知間隔] フィールドで指定します。[SNMPv1,2 通知受信者] を使用して、SNMP 通知の受信者を定義します。
- [選択済みのオプションTLV]:デバイスが発行する情報を選択するには、[使用可能なオプションTLV] リストからその TLV をここへ移動します。選択可能な TLV は次のとおりです。
  - [ポートの説明]:ポートに関する情報(例:製造元、製品名、ハードウェア バージョン、ソフトウェア バージョン)。
  - [システム名]:システムに割り当てられている名前(英数字)。この値は sysName オブジェクトと同じです。
  - [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)。システムの名前、および、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、ネットワーキング ソフトウェアの各バージョンが含まれます。この値は sysDescr オブジェクトと同じです。

- [システム機能]: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。機能は 2 オクテットで表されます。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、ステーションを意味します。ビット 8 ～ 15 は予約されています。
- [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。また、現在の設定がオート ネゴシエーションと手動ネゴシエーションのどちらによって決定されたかも示します。
- [802.3 Power via MDI]:MDI 経由で伝送される最大電力。
- [802.3リンクアグリゲーション]:LLDP PDU 送信元ポートに関連付けられているリンクを集約できるかどうかを示します。また、現在リンクが集約されているかどうかも示し、集約されている場合はその集約ポート ID も表示します。
- [802.3最大フレームサイズ]:MAC/PHY の実装における許容最大フレームサイズ。
- [MDI 経由の 4 線式電源]:(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。
  - [自動アドバタイズ]: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も小さい IP アドレスを選択します。
  - [なし]:管理 IP アドレスをアドバタイズしません。
  - [手動アドバタイズ]:アドバタイズする管理 IP アドレスを選択します。デバイスに複数の IP アドレスが設定されている場合は、このオプションを選択することをお勧めします。
- [IPアドレス]:[手動アドバタイズ] 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。

802.1 VLANおよびプロトコル

- [PVID]:TLV で PVID をアドバタイズする場合に選択します。
- [ポートおよびプロトコル VLAN ID]:ポートで有効になっているプロトコルベースの VLAN を入力します。
- [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。
- [選択済みプロトコル ID]:[プロトコル ID] ボックスで使用するプロトコルを選択して、それらを [選択済みプロトコル ID] ボックスに移動します。

ステップ 3 関連情報を入力し、[適用] をクリックします。ポート設定が、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。

LLDP MED ネットワーク ポリシー

LLDP Media Endpoint Discovery(LLDP-MED; LLDP メディア エンドポイント検出)は LLDP の拡張機能で、メディア エンドポイント デバイスをサポートする次の付加機能を提供します。

- 音声やビデオなどのリアルタイム アプリケーションのネットワーク ポリシーをアドバタイズおよび検出することができます。
- デバイスの位置を検出して、位置データベースを作成することができます。たとえば Voice over Internet Protocol(VoIP)の場合、IP 電話位置情報を使用して、Emergency Call Service(E-911)にかかってきた電話の位置を特定することができます。
- トラブルシューティング情報。次の場合、LLDP MED はネットワーク管理者にアラートを送信します。
  - ポート速度や通信方式(全二重 / 半二重)が一致していない。
  - QoS ポリシーの設定が不適切である。

LLDP MED ネットワーク ポリシーの設定

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コンフィギュレーション設定のセットです。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 デバイス宛の発信 LLDP パケットにこ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 電話に対し、VoIP トラフィックについて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] ページを使用します。管理者は、複数のネットワーク ポリシーと、ポリシーの送信先インターフェイスを手動で設定できます。管理者には、手動で VLAN を作成し、ネットワーク ポリシーとバインドされた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責任があります。

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は、自動音声 VLAN に関する項を参照してください。

LLDP MED ネットワーク ポリシーを作成するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP MEDネットワークポリシー] の順にクリックします。

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 デバイスが、維持している音声 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およびアドバタイズするように設定する場合は、[音声アプリケーションの LLDP MED ネットワーク ポリシー] で [自動] 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 ポリシーを設定することはできません。

ステップ 3 [適用] 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 新たにポリシーを定義するには、[追加] をクリックします。

ステップ 5 値を入力します。

- [ネットワーク ポリシー番号]:作成するポリシーの番号を選択します。
- [アプリケーション]: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]:トラフィックの送信先 VLAN ID を入力します。
- [VLAN タイプ]:トラフィックをタグ付きにするかどうかを選択します。
- [ユーザ プライオリティ]:このネットワーク ポリシーで設定したトラフィックに適用するトラフィック プライオリティを選択します。これは、CoS 値です。
- [DSCP 値]:ネイバーから送信されるアプリケーション データに割り当てる DSCP 値を選択します。この値により、ネイバーからデバイスに送信するアプリケーション トラフィックにマークする方法をネイバーに通知できます。

ステップ 6 [適用] をクリックします。ネットワーク ポリシーが作成されます。

注 [LLDP MEDポート設定] ページを使用して、発信 LLDP パケットに関する手動で定義したネットワーク ポリシーを含めるには、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

[LLDP MED ポート設定] ページでは、インターフェイスに対して発信する LLDP アドバタイズメントに含める LLDP-MED TLV およびネットワーク ポリシーを選択できます。ネットワーク ポリシーは、[LLDP MED ネットワークポリシー] ページを使用して設定します。

注 [音声アプリケーションの LLDP-MED ネットワーク ポリシー]([LLDP MED ネットワーク ポリシー] ページ)が [自動] で、自動音声 VLAN が動作している場合、デバイスは、LLDP-MED が有効で音声 VLAN のメンバーあるすべてのポートについて、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。

各ポートで LLDP-MED を設定するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP MEDポート設定] の順にクリックします。

このページには、すべてのポートに関する以下の LLDP MED 設定が表示されます([編集] ページで説明されていないフィールドのみ一覧表示されます)。

- [ユーザ定義ネットワークポリシー]:トラフィックのタイプ(アプリケーションと呼ばれる)に関するポリシーが定義されます。これはLLDP MED ネットワーク ポリシーで定義されます。この場合は、ポート上のポリシーに関する次の情報が表示されます。
  - [アクティブ]:トラフィックのタイプがポート上でアクティブになっているかどうか。
  - [アプリケーション]:ポリシーを定義するトラフィックのタイプ。
- [ロケーション]:ロケーション TLV が送信されるかどうか。
- [PoE]:POE-PSE TLV が送信されるかどうか。
- [インベントリ]:インベントリ TLV が送信されるかどうか。

ステップ 2 ページ上部のメッセージは、音声アプリケーションの LLDP MED ネットワーク ポリシーが自動的に生成されるかどうかを示しています(LLDP の概要を参照)。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、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、必要なものを選択して、[編集] をクリックします。

ステップ 4 パラメータを入力します。

- [インターフェイス]:設定するインターフェイスを選択します。
- [LLDP MED ステータス]:このポート上で LLDP MED を有効にするか無効にするかを選択します。
- [SNMP 通知]:トポロジの変更があった場合、MED をサポートするエンド ステーション(たとえば、SNMP 管理システム)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。
- [選択したオプション TLV]:デバイスが発行できる TLV を選択するには、必要な TLV を [使用可能なオプション TLV] の一覧から [選択したオプション TLV] の一覧に移動させます。

- [選択したネットワークポリシー]:発行する LLDP MED ポリシーを選択するには、必要なポリシーを [使用可能なネットワークポリシー] の一覧から [選択したネットワークポリシー] の一覧に移動させます。これらは、[LLDP MED ネットワーク ポリシー] ページで作成されたものです。ユーザが定義したネットワーク ポリシーをアドバタイズメントに含めるには、[使用可能なオプション TLV] から [ネットワークポリシー] を選択する必要があります。

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

  - [デバイス場所の座標]:LLDP を使用して発行する座標を入力します。
  - [デバイス場所の住所]:LLDP を使用して発行する住所を入力します。
  - [デバイス場所の ECS ELIN]:LLDP を使用して発行する、Emergency Call Service(ECS)の ELIN の場所を入力します。

ステップ 5 [適用] をクリックします。LLDP MED ポート設定が、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。

LLDP ポート ステータス

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

ステップ 1 LLDP ポート ステータスを表示するには、[各種管理] > [ディスカバリ - LLDP] > [LLDPポートステータス] の順にクリックします。

OOB ポートを含む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 ローカル情報の詳細] 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 ネイバー情報の詳細] をクリックします。

- **LLDP ポート ステータス グローバル情報**
- [シャーシ ID サブタイプ]:シャーシ ID のタイプ(例:MAC アドレス)。
- [シャーシ ID]:シャーシの ID。シャーシ ID サブタイプが MAC アドレスである場合は、デバイスの MAC アドレスが表示されます。
- [システム名]:デバイスの名前。

- [システムの説明]:デバイスの説明(英数字)。
- [サポートされているシステム機能]:デバイスの主要機能(例:ブリッジ、WLAN AP、ルータ)。
- [有効なシステム機能]:デバイスで有効になっている主要機能。
- [ポート ID サブタイプ]:表示されるポート ID のタイプ。
- **LLDP ポート ステータス テーブル**
- [インターフェイス]:ポート ID。
- [LLDP ステータス]:LLDP 発行オプション。
- [LLDP MED ステータス]:有効または無効。
- [ローカル PoE(電力タイプ、電源、電力プライオリティ、電力値)]:アドバタイズされるローカル PoE 情報。
- [リモート PoE(電力タイプ、電源、電力プライオリティ、電力値)]:ネイバーによってアドバタイズされる PoE 情報。
- [ネイバー数]:検出されたネイバー数。
- [第 1 デバイスのネイバー機能]:ネイバーの主要機能(例:ブリッジ、ルータ)。

LLDP ローカル情報

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

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDPローカル情報] の順にクリックします。

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。

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

[グローバル]

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

- [システム名]:デバイスの名前。
- [システムの説明]:デバイスの説明(英数字)。
- [サポートされているシステム機能]:デバイスの主要機能(例:ブリッジ、WLAN AP、ルータ)。
- [有効なシステム機能]:デバイスで有効になっている主要機能。
- [ポート ID サブタイプ]:表示されるポート ID のタイプ。
- [ポート ID]:ポートの ID。
- [ポートの説明]:ポートに関する情報(例:製造元、製品名、ハードウェア バージョン、ソフトウェア バージョン)。

[管理アドレス]

ローカル LLDP エージェントのアドレス テーブルが表示されます。他のリモート マネージャはこのアドレスを使用して、ローカル デバイスに関する情報を取得できます。アドレスは次の要素で構成されています。

- [IPv4 アドレス]:管理用途に最も適した IPv4 戻りアドレス。
- [IPv6 グローバル アドレス]:管理用途に最も適した IPv6 戻りグローバル アドレス。
- [IPv6 リンク ローカル アドレス]: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 の詳細]

- [自動ネゴシエーション対応]:ポート速度の自動ネゴシエーションがサポートされているかどうか。
- [自動ネゴシエーション有効]:ポート速度の自動ネゴシエーションがアクティブかどうか。
- [自動ネゴシエーションアドバタイズ機能]:ポート速度の自動ネゴシエーション機能(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(例:100BASE-TX 全二重モード)へのビット挿入などの処理が実行されます。

[802.3の詳細]

- [802.3 最大フレーム サイズ]: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リンクアグリゲーション]

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

[802.3 Power via MDI]

- [MDI 電源対応ポート クラス]:アドバタイズされている電源対応ポート クラス。
- [PSE MDI 電源対応]:ポートで MDI 電源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 電源が有効になっているかどうか。
- [PSE 電源ペア制御機能]:ポートで電源ペア制御がサポートされているかどうか。
- [PSE 電源ペア]:ポートでサポートされている電源ペア制御タイプ。
- [PSE 電力クラス]:アドバタイズされている、ポートの電力クラス。
- [電力タイプ]:ポートに接続された POD デバイスのタイプ。
- [電源]:ポートの電源。
- [電力プライオリティ]:ポートの電力のプライオリティ。
- [PD要求電力値]:PSE から PD に割り当てられた電力量。
- [PSE 割り当て電力値]:給電側機器(PSE)に割り当てられた電力量。

[802.3 Energy Efficient Ethernet (EEE)](デバイスが EEE をサポートする場合)

- [ローカル Tx]: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)。
- [ローカル 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)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)。

- [リモート Tx エコー]: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。
- [リモート Rx エコー]: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。

[MDI 経由の 4 線式電源]

- [4ペアPoEサポート済み]: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)。
- [予備ペア検出/分類必要]:4 ペア線が必要なことを示します。
- [PD予備ペア所望状態]: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]:4 ペア能力が有効か無効かを示します。

[MEDの詳細]

- [サポートされている機能]:ポート上でサポートされている MED 機能。
- [現在の機能]:ポート上で有効になっている MED 機能。
- [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。
  - [エンドポイントクラス1]:汎用エンドポイント クラス。基本的な LLDP サービスを提供します。
  - [エンドポイントクラス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します。
  - [エンドポイントクラス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、位置、911、レイヤ 2 デバイス サポート、デバイス情報管理の各機能を提供します。
- [PoE デバイス タイプ]:ポートの PoE タイプ(例:PD)。
- [PoE 電源]:ポートの電源。
- [PoE 電力プライオリティ]:ポートの電力のプライオリティ。
- [PoE 電力値]:ポートの電力値。
- [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]:デバイスの製造業者名。
- [モデル名]:デバイスのモデル名。
- [アセット ID]:アセット ID。

[場所の情報]

- [住所]:住所。
- [座標]:マップ座標(緯度、経度、および標高)。
- [ECS ELIN]:Emergency Call Service(ECS)の Emergency Location Identification Number(ELIN)。

[ネットワークポリシーテーブル]

- [アプリケーション タイプ]:ネットワーク ポリシーのアプリケーション タイプ(例:音声)。
- [VLAN ID]:ネットワーク ポリシーが定義されている VLAN の ID。
- [VLAN タイプ]:ネットワーク ポリシーが定義されている VLAN のタイプ。表示されるフィールド値は次のとおりです。
  - [タグ付き]:ネットワーク ポリシーはタグ付き VLAN 用に定義されています。
  - [タグなし]:ネットワーク ポリシーはタグなし VLAN 用に定義されています。
- [ユーザ プライオリティ]:ネットワーク ポリシーのユーザ プライオリティ。
- [DSCP]:ネットワーク ポリシーの DSCP。

ステップ 3 ページの下部にある [LLDPポートステータステーブル] をクリックすると、[LLDP ポート ステータス テーブル] に詳細が表示されます(ポート設定を参照)。

LLDP ネイバー情報

[LLDPネイバー情報] 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。

タイムアウトになると、情報は削除されます。ネイバーの TTL TLV で表される時間内に、そのネイバーから LLDP PDU が 1 件も受信されなかった場合、タイムアウトになります。

LLDP ネイバー情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDPネイバー情報] の順にクリックします。

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

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

- [ローカル ポート]:ネイバーが接続されているローカル ポートの番号。
- [シャーシ ID サブタイプ]:シャーシ ID のタイプ(例:MAC アドレス)。
- [シャーシ ID]:802 LAN 近隣デバイスのシャーシの ID。
- [ポート ID サブタイプ]:表示されるポート ID のタイプ。
- [ポート ID]:ポートの ID。
- [システム名]:発行されたデバイスの名前。
- [存続可能時間]: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)。

ステップ 3 ローカル ポートを選択し、[詳細] をクリックします。

[LLDP ネイバー情報] ページには、次のフィールドが含まれています。

[ポートの詳細]

- [ローカル ポート]:ポート番号。
- [MSAP エントリ]:デバイスのメディア サービス アクセスポイント(MSAP)のエントリ番号。

[基本内容]

- [シャーシ ID サブタイプ]:シャーシ ID のタイプ(例:MAC アドレス)。
- [シャーシ ID]:802 LAN 近隣デバイスのシャーシの ID。
- [ポート ID サブタイプ]:表示されるポート ID のタイプ。
- [ポート ID]:ポートの ID。

- [ポートの説明]:ポートに関する情報(例:製造元、製品名、ハードウェア バージョン、ソフトウェア バージョン)。
- [システム名]:発行されるシステムの名前。
- [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)。システムの名前、および、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、ネットワーキング ソフトウェアの各バージョンが含まれます。この値は sysDescr オブジェクトと同じです。
- [サポートされているシステム機能]:このデバイスの主要機能。機能は 2 オクテットで表されます。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、ステーションを意味します。ビット 8 ～ 15 は予約されています。
- [有効なシステム機能]:デバイスで有効になっている主要機能。

[管理アドレステーブル]

- [アドレス サブタイプ]:管理アドレスのサブタイプ(例:MAC、IPv4)。
- [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 の詳細]

- [自動ネゴシエーション対応]:ポート速度の自動ネゴシエーションがサポートされているかどうか。表示されるフィールド値は [TRUE] または [FALSE] です。
- [自動ネゴシエーション有効]:ポート速度の自動ネゴシエーションがアクティブかどうか。表示されるフィールド値は [TRUE] または [FALSE] です。
- [自動ネゴシエーション アドバタイズ機能]:ポート速度の自動ネゴシエーション機能(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 インターフェイスから入ってきたデータに対して、デジタル データ変換、コリジョン検出、ビット挿入などの処理が実行され、ネットワーク(例:100BASE-TX 全二重モード)に送出されます。

[802.3 Power via MDI]

- [MDI 電源対応ポート クラス]:アドバタイズされている電源対応ポート クラス。
- [PSE MDI 電源対応]:ポートで MDI 電源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 電源が有効になっているかどうか。
- [PSE 電源ペア制御機能]:ポートで電源ペア制御がサポートされているかどうか。
- [PSE 電源ペア]:ポートでサポートされている電源ペア制御タイプ。
- [PSE 電力クラス]:アドバタイズされている、ポートの電力クラス。
- [電力タイプ]:ポートに接続された POD デバイスのタイプ。
- [電源]:ポートの電源。
- [電力プライオリティ]:ポートの電力のプライオリティ。
- [PD要求電力値]:受電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。

[MDI 経由の 4 線式電源]

- [4ペアPoEサポート済み]: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)。
- [予備ペア検出/分類必要]:4 ペア線が必要なことを示します。
- [PD予備ペア所望状態]: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予備ペア動作可能状態]:4 ペア能力が有効か無効かを示します。

[802.3の詳細]

- [802.3 最大フレーム サイズ]:ポートでサポートされている、アドバタイズされる最大フレーム サイズ。

[802.3リンクアグリゲーション]

- [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)]

- [リモート Tx]: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)。
- [リモート 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)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)。
- [ローカル Tx エコー]: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。
- [ローカル Rx エコー]: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。

[MEDの詳細]

- [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。
  - [エンドポイント クラス 1]:汎用エンドポイント クラス。基本的な LLDP サービスを提供します。
  - [エンドポイント クラス 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します。
  - [エンドポイント クラス 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、位置、911、レイヤ 2 スイッチ サポート、デバイス情報管理の各機能を提供します。
- [PoE デバイス タイプ]:ポートの PoE タイプ(例:PD/PSE)。
- [PoE 電源]:ポートの電源。
- [PoE 電力プライオリティ]:ポートの電力のプライオリティ。
- [PoE 電力値]:ポートの電力値。
- [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]:デバイスの製造業者名。
- [モデル名]:デバイスのモデル名。
- [アセット ID]:アセット ID。

[802.1 VLANおよびプロトコル]

- [PVID]:アドバタイズされているポートの VLAN ID。

[PPVID]

[PPVIDテーブル]

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

[VLAN ID]

[VLAN IDテーブル]

- [VID]:ポートおよびプロトコルの VLAN ID。
- [VLAN 名]:アドバタイズされている VLAN 名。

[プロトコルIDテーブル]

- [プロトコル ID]:アドバタイズされているプロトコル ID。

[場所の情報]

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 Emergency Call Service(ECS)の Emergency Location Identification Number(ELIN)。
- [不明]:不明なロケーション情報。

[ネットワークポリシーテーブル]

- [アプリケーション タイプ]:ネットワーク ポリシーのアプリケーション タイプ(例:音声)。
- [VLAN ID]:ネットワーク ポリシーが定義されている VLAN の ID。
- [VLAN タイプ]:ネットワーク ポリシーが定義されている VLAN のタイプ(タグ付きまたはタグなし)。
- [ユーザ プライオリティ]:ネットワーク ポリシーのユーザ 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 ポートを選択し、[LLDP ポート ステータス テーブル] をクリックすると、[LLDP ポート ステータス テーブル] に詳細が表示されます。

LLDP 統計情報

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

LLDP 統計情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP統計情報] の順にクリックします。

次のフィールドが各ポートに対して表示されます。

- [インターフェイス]:インターフェイス(OOB でもある可能性あり)の ID。
- [Txフレーム(合計)]:送信されたフレームの合計数。
- [Rxフレーム]
  - [合計]:受信したフレームの合計数。
  - [廃棄済み]:受信したフレームのうち、廃棄されたフレームの数。
  - [エラー]: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 TLV]
  - [廃棄済み]:受信した TLV のうち、廃棄された TLV の数。
  - [未認識]:受信した TLV のうち、認識されなかった TLV の数。
- [ネイバーの情報削除回数]:このインターフェイス上でネイバーがエージアウトされた回数。

ステップ 2 最新の統計情報を表示するには、[更新] をクリックします。

LLDP 過負荷

LLDP では、LLDP TLV および LLDP-MED TLV として情報を LLDP パケットに追加します。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過負荷] ページには、LLDP/LLDP-MED 情報のバイト数、追加の LLDP 情報に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、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - LLDP] > [LLDP過負荷] の順にクリックします。

このページには次の情報がポートごとに表示されます。

- [インターフェイス]:ポート ID。このインターフェイスは、OOB ポートでもある可能性があります。
- [使用中の合計バイト数]:各パケットの LLDP 情報の合計バイト数。
- [使用可能な残りのバイト数]:各パケットで追加の LLDP 情報用に残っている利用可能な合計バイト数。
- [ステータス]:TLV が送信されているか、それとも過負荷状態になっているか。

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

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

- [LLDP必須TLV]
  - [サイズ(バイト)]:必須 TLV の合計バイト数。
  - [ステータス]:必須 TLV グループが送信されているか、過負荷状態になっているか。
- [LLDP MED機能]
  - [サイズ(バイト)]:LLDP MED 機能パケットの合計バイト数。
  - [ステータス]:LLDP MED 機能パケットが送信されたか、過負荷状態であったか。

- [LLDP MEDの場所]
  - [サイズ(バイト)]:LLDP MED 位置パケットの合計バイト数。
  - [ステータス]:LLDP MED 位置パケットが送信されたか、過負荷状態であったか。
- [LLDP MEDネットワークポリシー]
  - [サイズ(バイト)]:LLDP MED ネットワーク ポリシー パケットの合計バイト数。
  - [ステータス]:LLDP MED ネットワーク ポリシー パケットが送信されたか、過負荷状態であったか。
- [LLDP MED拡張PoE]
  - [サイズ(バイト)]:MDI 経由 LLDP MED 拡張電力パケットの合計バイト数。
  - [ステータス]:MDI 経由 LLDP MED 拡張電力パケットが送信されたか、過負荷状態であったか。
- [802.3 TLV]
  - [サイズ(バイト)]:LLDP MED 802.3 TLV パケットの合計バイト数。
  - [ステータス]:LLDP MED 802.3 TLV パケットが送信されたか、過負荷状態であったか。
- [LLDPオプションTLV]
  - [サイズ(バイト)]:LLDP MED オプション TLV パケットの合計バイト数。
  - [ステータス]:LLDP MED オプション TLV パケットが送信されたか、過負荷状態であったか。
- [LLDP MEDコンポーネント]
  - [サイズ(バイト)]:LLDP MED インベントリ TLV パケットの合計バイト数。
  - [ステータス]:LLDP MED インベントリ パケットが送信されたか、過負荷状態であったか。
- [合計]
  - [合計(バイト)]:各パケットの LLDP 情報の合計バイト数。
  - [使用可能な残りのバイト数]:各パケットで追加の LLDP 情報用に未送信のまま残っている利用可能な合計バイト数。

ディスカバリ - CDP

ここでは、CDP の設定方法を説明します。

具体的な内容は、次のとおりです。

- CDP のプロパティ
- CDP インターフェイス設定
- CDP ローカル情報
- CDP ネイバー情報
- CDP 統計情報

CDP のプロパティ

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 を設定する手順

次に、デバイスに CDP を設定する手順の例を示します。CDP を設定するための詳細なガイドラインは、LLDP/CDP に関するセクションで参照できます。

ステップ 1 CDP の [プロパティ] ページを使用して、CDP グローバル パラメータを入力します。

ステップ 2 [CDP インターフェイス設定] ページを使用して、インターフェイスごとに CDP を設定します。

ステップ 3 Auto Smartport で CDP デバイスの機能を検出する場合は、[プロパティ] ページで CDP を有効にします。

CDP を使用して Smartport 機能に対応するデバイスを識別する方法については、Smartport タイプをご覧ください。

CDP の一般パラメータを入力するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [プロパティ] 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。

- [CDP ステータス]: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。
  - [ブリッジング]:VLAN に基づいてパケットを転送します。
  - [フィルタリング]:パケットを削除します。
  - [フラッディング]:入力ポートを除くすべてのポートに着信 CDP パケットを転送する VLAN 非対応のフラッディング。
- [CDP 音声 VLAN アドバタイズメント]:選択すると、CDP が有効で、音声 VLAN のメンバーであるすべてのポートで、デバイスが CDP を使用して音声 VLAN をアドバタイズできるようになります。音声 VLAN は、[音声 VLAN プロパティ] ページから設定します。
- [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、無効なエラー 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 アドバタイズ間隔] の値の倍数で入力します。たとえば、[TLV アドバタイズ間隔] の値が 30 秒であり、[ホールド係数] 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。次のオプションが選択できます。
  - [デフォルトを使用]:デフォルトの時間(180 秒)を使用します。
  - [ユーザ定義]:時間を秒単位で入力します。
- [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。次のオプションが選択できます。
  - [デフォルトを使用]:デフォルトのレート(60 秒)を使用します。
  - [ユーザ定義]:レートを秒単位で入力します。

- [デバイス ID 形式]:デバイス ID のフォーマットを選択します(MAC アドレスまたはシリアル番号)。次のオプションが選択できます。
  - [MAC アドレス]:デバイスの MAC アドレスをデバイス ID として使用します。
  - [シリアル番号]: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。
  - [ホスト名]: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。次のオプションが選択できます。
  - [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]フィールドに表示)の IP アドレスを使用します。
- [インターフェイス]:[送信元インターフェイス] で [ユーザ定義] が選択された場合は、インターフェイスを選択します。
- [Syslog 音声 VLAN 不一致]:オンにすると、音声 VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内の音声 VLAN 情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。
- [Syslogネイティブ VLAN不一致]:オンにすると、ネイティブ VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内のネイティブ VLAN 情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。
- [Syslogデュプレックス不一致]:オンにすると、デュプレックス情報が一致しないときに SYSLOG メッセージが送信されます。これは、着信フレーム内のデュプレックス情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。

ステップ 3 [適用] をクリックします。LLDP のプロパティ値が設定されます。

CDP インターフェイス設定

[インターフェイス設定] ページでは、ポートごとに CDP の有効/無効を設定できます。CDP ネイバーとの不一致が発生したときに、通知がトリガーされるようにすることもできます。不一致が生じる可能性があるのは、音声 VLAN データ、ネイティブ VLAN、またはデュプレックスです。

これらのプロパティ値を設定することにより、LLDP 対応デバイスに送信する情報のタイプを選択できます。

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

CDP インターフェイス設定を定義するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [インターフェイス設定] の順にクリックします。

このページには、OOB ポートを含む各インターフェイスに関する次の CDP 情報が表示されます。

- [CDPステータス]:ポートに対する CDP 発行オプション。
- [レポートが CDP ネイバーと競合しています]:[編集] ページで有効または無効になっているレポート オプションのステータスを表示します(音声 VLAN、ネイティブ VLAN、デュプレックス)。
- [ネイバー数]:検出されたネイバー数。

ページ下部に 4 つのボタンがあります。

- [設定のコピー]:選択すると、ポート間でコンフィギュレーションがコピーされます。
- [編集]:フィールドは後述のステップ 2 で説明されています。
- [CDP ローカル情報の詳細]:[CDP ローカル情報] ページに移動します。
- [CDP ネイバー情報の詳細]:[CDP ネイバー情報] ページに移動します。

ステップ 2 ポートを選択して、[編集] 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。

- [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 発行オプションを有効にするか無効にするかを選択します。

  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に使用可能となります。

- [Syslog 音声 VLAN 不一致]: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るようになります。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]: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るようになります。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]: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るようになります。これは、着信フレーム内のデュプレックス情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。

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

CDP ローカル情報

ローカル デバイスに関する CDP プロトコルによってアドバタイズされる情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [CDPローカル情報] **の順にクリックします。**

ステップ 2 ローカル ポートを選択すると、次のフィールドが表示されます。

- [インターフェイス]:ローカル ポート数。OOB ポートも選択できます。
- [CDP状態]:CDP が有効かどうかを表示します。
- [デバイス ID TLV]
  - [デバイス ID タイプ]:デバイス ID TLV でアドバタイズされるデバイス ID のタイプ。
  - [デバイスID]:デバイス ID TLV でアドバタイズされるデバイス ID。
- [システム名TLV]
  - [システム名]:デバイスのシステム名。
- [アドレスTLV]
  - [アドレス1-3]:デバイス アドレス TLV でアドバタイズされる IP アドレス。
- [ポート TLV]
  - [ポート ID]:ポート TLV でアドバタイズされるポートの ID。

- [機能の TLV]
  - [機能]:ポート TLV でアドバタイズされる機能。
- [バージョン TLV]
  - [バージョン]:デバイスが稼動しているソフトウェアのリリースに関する情報。
- [プラットフォーム TLV]
  - [プラットフォーム]:プラットフォーム TLV でアドバタイズされるプラットフォームの ID。
- [ネイティブ VLAN TLV]
  - [ネイティブVLAN]:ネイティブ VLAN TLV でアドバタイズされるネイティブ VLAN ID。
- [全/半二重 TLV]
  - [デュプレックス]: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。
- [アプライアンス TLV]
  - [アプライアンス ID]:アプライアンス TLV でアドバタイズされる、ポートに接続されたデバイスのタイプ。
  - [アプライアンス VLAN ID]:アプライアンスによって使用されるデバイス上の VLAN(例:アプライアンスが IP 電話の場合は、音声 VLAN)。
- [拡張信頼 TLV]
  - [拡張信頼]:有効な場合、そのポートは信頼できることを示しています。つまり、パケットの送信元となるホストまたはサーバが信頼でき、それ自体でパケットにマーキングできることを意味します。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、次のフィールドが関係します。
- [信頼できないポートの CoS TLV]
  - [信頼できないポートの CoS]:ポートの [拡張信頼] 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。

- [使用可能な電力 TLV]
  - [要求ID]:最新の電力要求 ID が、電力要求 TLV で最後に受信した [要求ID] フィールドに反映されます。インターフェイスが最後にアップした時点以降に電力要求 TLV を受信しなかった場合は、0 になります。
  - [電源管理ID]:次のイベントのいずれかが発生するたびに、値が 1 つ(または、0 を避けるため 2 つ)増加します。

    [有効電力] または [管理電力レベル] が変わった。

    最後に受信した設定値と異なる [要求ID] フィールド値を持つ電力要求 TLV を受信した(または、最初の値を受信したとき)。

    インターフェイスがダウンした。
  - [有効電力]:ポートが消費する電力量。
  - [管理電力レベル]: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を表示します。デバイスはこのフィールドに常に [設定なし] と表示します。
- [MDI(UPOE)TLV 経由の 4 線式電源]

  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ペアPoEサポート済み]:PoE がサポートされているかどうかが表示されます。
  - [予備ペア検出/分類必要]:この分類が必要かどうかが表示されます。
  - [PD予備ペア所望状態]:PD 予備ペアが必要な状態が表示されます。
  - [PD予備ペア動作状態]:PSE 予備ペアの状態が表示されます。

CDP ネイバー情報

[CDP ネイバー情報] 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。ネイバーの TTL TLV で表される時間内に、そのネイバーから CDP PDU が 1 件も受信されなかった場合、タイムアウトになります。

CDP ネイバー情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [CDPネイバー情報] の順にクリックします。

ステップ 2 フィルタを選択するには、[フィルタ] 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、[実行] をクリックします。

フィルタがトリガーされ、[フィルタのクリア] が有効になります。

ステップ 3 フィルタ処理を停止するには、[フィルタのクリア] をクリックします。

[CDPネイバー情報] 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。

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

ステップ 4 デバイスを選択し、[詳細] 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表示されます。

- [デバイス ID]:近隣デバイス ID の ID。
- [システム名]:近隣デバイス ID の名前。
- [ローカルインターフェイス]:フレームが到達する際に経由するポートのインターフェイス番号。
- [アドバタイズメントバージョン]:CDP のバージョン。
- [存続可能時間]: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)。

- [機能]:このデバイスの主要機能。機能は2オクテットで表されます。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、ステーションを意味します。ビット 8 ～ 15 は予約されています。
- [プラットフォーム]:ネイバーのプラットフォームの ID。
- [ネイバーインターフェイス]:フレームが到達する際に経由するネイバーのインターフェイス番号。
- [ネイティブVLAN]:ネイバーのネイティブ VLAN。
- [アプリケーション]:ネイバー上で実行中のアプリケーション名。
- [デュプレックス]:ネイバー インターフェイスが半二重か全二重か。
- [アドレス]:ネイバーのアドレス。
- [使用電力]:インターフェイスでネイバーによって消費される電力量。
- [バージョン]:ネイバーのソフトウェアのバージョン。
- [電力要求]: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。
- **[使用可能な電力]**
  - [要求ID]:最新の電力要求 ID が、電力要求 TLV で最後に受信した [要求ID] フィールドに反映されます。インターフェイスが最後にアップした時点以降に電力要求 TLV を受信しなかった場合は、0 になります。
  - [電源管理ID]:次のイベントのいずれかが発生するたびに、値が 1 つ(または、0 を避けるため 2 つ)増加します。

    [有効電力] フィールドまたは [管理電力レベル] フィールドの値が変わった。

    最後に受信した設定値と異なる [要求ID] フィールド値を持つ電力要求 TLV を受信した(または、最初の値を受信したとき)。

    インターフェイスがダウンした。
  - [有効電力]:ポートが消費する電力量。
  - [管理電力レベル]: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を表示します。デバイスはこのフィールドに常に [設定なし] と表示します。

- [MDI 経由の 4 線式電源]
  - [4ペアPoEサポート済み]: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)。
  - [予備ペア検出/分類必要]:4 ペア線が必要なことを示します。
  - [PD予備ペア所望状態]: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]:4 ペア能力が有効か無効かを示します。

注 [テーブルのクリア] 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統計情報] 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。詳細については、「ディスカバリ - CDP」を参照してください。

ポートの CDP 統計情報は、ポートで CDP がグローバルで有効になっている場合にのみ表示されます。これは、[CDP のプロパティ] ページ、および [CDP インターフェイス設定] ページで行います。

CDP 統計情報を表示するには、次のようにします。

ステップ 1 [各種管理] > [ディスカバリ - CDP] > [CDP 統計情報] の順にクリックします。

OOB ポートを含む各インターフェイスについて、次のフィールドが表示されます。

受信パケットおよび送信パケット

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

[CDPエラー統計情報] には、CDP エラー カウンタが表示されます。

- [無効なチェックサム]:無効なチェックサム値とともに受信したパケットの数。
- [その他のエラー]:無効なチェックサム以外のエラーとともに受信したパケットの数。
- [最大数を超えるネイバー]: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、[すべてのインターフェイスカウンタのクリア] をクリックします。1 つ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、そのインターフェイスを選択し、[インターフェイス カウンタのクリア] をクリックします。

10

ポート管理

ここでは、ポートの設定、リンク アグリゲーション、および Green Ethernet 機能について説明します。

具体的な内容は、次のとおりです。

- ワークフロー
- ポート設定
- エラー回復設定
- ループバック検出設定
- リンクアグリゲーション
- UDLD
- PoE
- Green Ethernet

ワークフロー

ポートを設定するには、次のようにします。

1. [ポート設定] ページでポートを設定します。
2. [LAG 管理] ページで、Link Aggregation Group（LAG; リンク アグリゲーション グループ）プロトコルを有効にするか無効にするかを設定し、また、各 LAG にメンバー ポートを追加します。デフォルトでは、すべての LAG は空になっています。
3. [LAG 設定] ページで、LAG のイーサネット パラメータ値（速度、自動ネゴシエーションなど）を設定します。
4. [LACP] ページで、ダイナミック LAG のメンバーまたはメンバー候補になっているポートの LACP パラメータ値を設定します。

5. [プロパティ] ページで、[Green Ethernet] および [802.3 Energy Efficient Ethernet] を設定します。
6. [ポート設定] ページで、ポートごとの Green Ethernet エネルギー モードおよび 802.3 Energy Efficient Ethernet を設定します。
7. デバイスで PoE がサポートされていて有効になっている場合、ポート管理:PoE の説明に従ってデバイスを設定します。

ポート設定

[ポート設定] ページには、ポートのグローバル設定情報およびポートごとの設定情報が表示されます。このページでポートを選択し、[ポート設定の編集] ページでそのポートを設定することができます。

ポート情報を設定するには、次のようにします。

ステップ 1 [ポート管理] > [ポート設定] をクリックします。

すべてのポートに対してポート設定が表示されます。

ステップ 2 次のフィールドを入力します。

- [リンクフラップ防止]:ネットワークの中断を最小化する場合に選択します。有効になっている場合は、このコマンドが、自動的に、リンク フラップ イベントが発生しているポートを無効にします。
- [ジャンボフレーム]:最大 9 KB のパケットをサポートする場合に選択します。[ジャンボ フレーム] を有効にしなかった場合(デフォルト)、サポートされる最大パケット サイズは 2,000 バイトになります。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。

  ジャンボ フレームを有効にするには、この機能を有効にした後でデバイスをリブートする必要があります。スタック システムでは、この設定を有効にするために、スタック ユニットが 2 回リブートする可能性があります。これは自動的に行われます。

ステップ 3 [適用] をクリックし、グローバル設定情報を更新します。

ジャンボ フレーム設定の変更内容が反映されるのは、[ファイル操作] 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、デバイスをリブートした後のみです。

ステップ 4 ポートの設定情報を更新するには、目的のポートを選択し、[編集] 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。

- [インターフェイス]:ポート番号を選択します。
- [ポートの説明]:ポートのユーザ定義名またはコメントを入力します。
- [ポートタイプ]:ポートのタイプおよび速度を表示します。次のオプションがあります。
  - [カッパー ポート]:コンボ ポートでない、標準のポート。10 M、100 M、1000 M(タイプ:カッパー)、および 10 G。
  - [コンボ ポート]:カッパー CAT6a ケーブルまたは *SFP ファイバ ギガビット インターフェイス*のどちらかで接続されたコンボ ポート。
  - 10 G 光ファイバ:伝送速度が 1 G または 10 G のポート。
  - OOB:アウトオブバンド ポート(SG550XG と SG350XG 上でのみサポート)。

  注 コンボ ポートの両方のポートが使用されている場合は、SFP Fiber が優先されます。
- [管理ステータス]:デバイスのリブート時にこのポートをアクティブ化する場合は [アップ]、アクティブ化しない場合は [ダウン] を選択します。
- [動作ステータス]:ポート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。ポートがエラーのためにアクティブ化されていない場合、エラーの説明が表示されます。
- [リンクステータスSNMPトラップ]:ポートのリンク ステータスへの変更を通知する SNMP トラップの生成を有効にするには、このフィールドを選択します。OOB ポートとは無関係です。
- [時間範囲]:ポートをアクティブ化する時間範囲を有効にするには、このフィールドを選択します。時間範囲がアクティブでない場合、ポートは停止されます。時間範囲が設定されている場合、ポートが管理者によりアクティブ化されている場合のみ有効です。
- [時間範囲名]:時間範囲を指定するプロファイルを選択します。OOB ポートとは無関係です。時間範囲がまだ定義されていない場合、[時間範囲] ページに移動するには [編集] をクリックします。OOB ポートとは無関係です。
- [動作時間範囲の状態]:時間範囲が現在アクティブ化されているかいないかを表示します。

- [自動ネゴシエーション]: このポート上で自動ネゴシエーションを有効にするには、このフィールドを選択します。自動ネゴシエーションを有効にした場合、送信速度、デュプレックス モード、フロー制御の各情報が、このポートからポート リンク パートナーにアドバタイズされます。
- [動作自動ネゴシエーション]: このポートの現在の自動ネゴシエーション ステータスが表示されます。
- [管理ポート速度]: ポートの速度を設定します。使用できる速度はポート タイプによって決まります。[管理速度] を選択できるのは、自動ネゴシエーションを無効にしている場合のみです。
- [動作ポート速度]: 自動ネゴシエーションによって決定された現在のポート速度が表示されます。
- [管理デュプレックスモード]: (非 XG ポートの場合にのみ表示) ポートのデュプレックス モードを選択します。このフィールド値を選択できるのは、自動ネゴシエーションが無効になっており、ポート速度が 10 M または 100 M に設定されている場合のみです。ポート速度が 1 G の場合、モードは常に全二重です。次のオプションがあります。
  - [半二重]: デバイスとクライアントの間で双方向通信を同時に行うことができません。
  - [全二重]: デバイスとクライアントの間で双方向通信を同時に行うことができます。
- [動作デュプレックスモード]: (非 XG ポート上でのみ表示) ポートの現在のデュプレックス モードが表示されます。
- [自動アドバタイズメント]: 自動ネゴシエーションが有効な場合に、このポートからアドバタイズする通信機能を選択します。

  注 すべてのデバイスに対してすべてのオプションが関連するわけではない点に注意してください。

  次のオプションがあります。
  - [最大機能]: すべてのポート速度と両方のデュプレックス モード。
  - [10 半二重]: 10 Mbps のスピードで半二重モード (XG デバイス上には表示されません)。
  - [10 全二重]: 10 Mbps のスピードで全二重モード (XG デバイス上には表示されません)。
  - [100 半二重]: 100 Mbps のスピードで半二重モード (XG デバイス上には表示されません)。

- [100全二重]:100 Mbps のスピードで全二重モード。
- [1000 全二重]:1000 Mbps のスピードで全二重モード。
- *[2500全二重]*:2500 Mbps のスピードのアドバタイズで全二重モード。これは、550 ファミリ上でのみサポートされます。
- [5000全二重]:5000 Mbps のスピードのアドバタイズで全二重モード。これは、550 ファミリ上でのみサポートされます。
- [10000全二重]:10000 Mbps のスピードのアドバタイズで全二重モード。これは、550 ファミリ上でのみサポートされます。

- [動作アドバタイズメント]:このポートのネイバーに現在送信されている機能が表示されます。表示されるオプションは、[管理アドバタイズメント] フィールドの選択項目と同じです。
- [プリファレンス モード]:自動ネゴシエーションが有効になっている場合にのみ使用できます。自動ネゴシエーション動作のための、インターフェイスのマスター スレーブ モードを選択します。次のいずれかのオプションを選択します。
  - [スレーブ]:デバイス ポートが自動ネゴシエーション プロセスにおいてスレーブであるプリファレンスを用いてネゴシエーションを開始します。
  - [マスター]:デバイス ポートが自動ネゴシエーション プロセスにおいてマスターであるプリファレンスを用いてネゴシエーションを開始します。
- [ネイバーアドバタイズメント]:このネイバー デバイス(リンク パートナー)からアドバタイズする機能を選択します。
- [バックプレッシャ]:(非 XG ポート上でのみサポート)このポートにおける バック プレッシャ モードを選択します。バック プレッシャとは、デバイスが輻輳状態のときにパケット受信速度を下げる方式のことであり、半二重通信モードでのみ使用できます。このオプションを選択すると、信号を混雑させ、リモート ポートからパケットが送信されないようにします。
- [フロー制御]:802.3x フロー制御を有効にするか無効にするかを選択します。または、ポートでフロー制御の自動ネゴシエーションを有効にするかを選択します(全二重モードの場合のみ)。コンボ ポートではフロー制御自動ネゴシエーションを有効にすることはできません。

- [MDI/MDIX]：このポートの *Media Dependent Interface*（MDI）/*Media Dependent Interface with Crossover*（MDIX）ステータスを選択します。

  次のオプションがあります。

  - [MDIX]：送信と受信のペアを入れ替える場合、このフィールドを選択します。
  - [MDI]：ストレート ケーブルを使用してこのデバイスをステーションに接続する場合、この項目を選択します。
  - [自動]：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、このフィールドを選択します。

- [動作MDI/MDIX]：現在の MDI/MDIX 設定情報が表示されます。
- [保護ポート]：このポートを保護ポートにするには、このフィールドを選択します。（保護ポートは、プライベート VLAN エッジ（PVE）とも呼ばれます）。保護ポートの特徴は次のとおりです。
  - 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したパケットは、非保護出力ポートにのみ転送することができます。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。
  - ポート保護は、VLAN メンバーシップには影響されません。保護ポートに接続されたデバイスは、それらが同じ VLAN のメンバーである場合でも、互いに通信することができません。
  - ポートと LAG は両方とも、保護または非保護として定義することができます。保護 LAG は「LAG 設定」セクションで説明されます。
- [LAG のメンバー]：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、このフィールドには何も表示されません。

ステップ 6 [適用] をクリックします。ポート設定が、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。

エラー回復設定

このページでは、エラー条件が原因でシャットダウンしたポートを、自動回復間隔が経過した後に自動で再アクティブ化する設定を有効にできます。

エラー回復を設定するには、次の手順を実行します。

ステップ 1 [ポート管理] > [エラー回復設定] をクリックします。

ステップ 2 次のフィールドを入力します。

- [自動回復間隔]: 有効にされている場合、ポートがシャットダウンしてから自動エラー回復までの遅延時間を指定します。
- [自動 ErrDisable 回復]
  - [ポートセキュリティ]: 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単一ホスト違反]: ポートが 802.1x によりシャットダウンされ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 拒否]: ACL 動作による自動エラー回復機能を有効にするには、これを選択します。
  - [STP BPDU ガード]: ポートが STP BPDU ガードによって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、これを選択します。
  - [STPループバックガード]: STP ループバック ガードにより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]: UDLD シャットダウン状態の自動エラー回復機能を有効にするには、このフィールドを選択します。
  - [ループバック検出]: ループバック検出によるポートのシャットダウンのエラー回復機能を有効にするには、このフィールドを選択します。
  - [ストーム制御]: ストーム制御によるポートのシャットダウンのエラー回復機能を有効にするには、このフィールドを選択します。
  - [リンクフラップ防止]: ネットワークの中断を最小化する場合に選択します。有効になっている場合は、このコマンドが、自動的に、リンク フラップ イベントが発生しているポートを無効にします。

ステップ 3 [適用] をクリックし、グローバル設定情報を更新します。

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 1 [ポート管理] > [エラー回復設定] 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 [保留理由] が表示されます。

ステップ 2 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 3 [再アクティブ化] 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(LBD)は、ループ保護が有効にされ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提供します。スイッチがループ プロトコル パケットを送信し、次いで同じパケットを受信する場合、スイッチは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 とは独立して動作します。ループが検出された後、ループを受信したポートはシャットダウン状態に置かれます。トラップが送信され、イベントが記録されます。ネットワーク マネージャは、LBD パケットの送信間隔を設定する検出間隔を定義することができます。

ループバック検出プロトコルは、次のようなループ状況を検出することができます。

- **ワイヤのショート**:すべての受信トラフィックをループバックするポート。
- **直接マルチポート ループ**:スイッチが、複数のポートにより他のスイッチに接続されており、STP が無効にされています。
- **LAN セグメント ループ**:スイッチが、ループがある LAN セグメントに、1 つまたは複数のポートにより接続されています。

LBD の動作

LBD プロトコルは、定期的にループバック検出パケットをブロードキャストします。スイッチは、自身の LBD パケットを受信すると、ループを検出します。

あるポートに対して LBD をアクティブにするには、次の条件が真でなければなりません。

- LBD がグローバルで有効になっている。
- LBD がそのポートに対して有効になっている。

- ポート動作ステータスがアクティブになっている。
- ポートが、STP フォワーディング ステートまたは無効状態にある（MSTP インスタンス フォワーディング ステート、インスタンス 0）。

LBD フレームは、LBD アクティブ ポートの最高プライオリティ キューに送信されます（LAG の場合、LBD は LAG の各アクティブポート メンバーに送信されます）。

ループが検出されると、スイッチは次の動作を実行します。

- 受信ポートまたは LAG をエラー無効状態に設定する。
- 適切な SNMP トラップを発行する。
- 適切な SYSLOG メッセージを生成する。

デフォルト設定とコンフィギュレーション

ループバック検出はデフォルトでは有効ではありません。

他の機能との連携

ループバック検出が有効にされているポートで STP が有効にされている場合、そのポートは STP フォワーディング ステートになければなりません。

LBD の設定

LBD を有効にして設定するには、次の手順を実行します。

ステップ 1 [ループバック検出設定] ページで、[ループバック検出] をシステム全体で有効にします（後述）。

ステップ 2 [ループバック検出設定] ページで、アクセス ポートに対して [ループバック検出] を有効にします（後述）。

ステップ 3 [エラー回復設定] ページで、ループバック検出の自動回復機能を有効にします。

ループバック検出を設定するには、次の手順を実行します。

ステップ 1 [ポート管理] > [ループバック検出設定] 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] グローバル フィールドで [有効] を選択します。

ステップ 3 [検出間隔] を入力します。これは LBD パケット送信の間隔です。

ステップ 4 [適用] をクリックし、実行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を保存します。

[ループバック検出状態] に関連して、各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。

- [管理]:ループバック検出が有効になっています。
- [動作]:ループバック検出が有効になっていますが、インターフェイスに対してアクティブ化されていません。

ステップ 5 フィルタ内の [インターフェイスタイプが次に等しい] フィールドで、ポートまたは LAG に対して 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、[編集] をクリックします。

ステップ 7 選択したポートまたは LAG の [ループバック検出状態] フィールドで [有効] を選択します。

ステップ 8 [適用] をクリックし、実行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を保存します。

リンクアグリゲーション

ここでは、LAG の設定方法について説明します。具体的な内容は、次のとおりです。

- リンク アグリゲーションの概要
- デフォルト設定とコンフィギュレーション
- スタティック LAG およびダイナミック LAG を設定する手順
- LAG 管理
- LAG 設定
- LACP

リンク アグリゲーションの概要

Link Aggregation Control Protocol（LACP; リンク アグリゲーション制御プロトコル）は IEEE 802.3az で規定されている規格です。複数の物理ポートを束ね、1 つの論理チャネル（LAG）として扱うことができます。LAG を作成した場合、2 つのデバイス間において、帯域幅が広がり、ポートの柔軟性が高まり、また、リンクを冗長構成にすることができます。

作成できる LAG のタイプは次の 2 つです。

- [スタティック]：LAG 内のポートを手動で設定します。LACP が無効になっている場合、LAG は静的に作成されます。スタティック LAG に割り当てられるポートのグループは、常にアクティブ メンバーになります。LAG を手動で作成した場合、LACP オプションを追加したり削除したりするには、その LAG を編集してメンバーを削除する必要があります（メンバーは適用前に再追加できます）。その後、[LACP] ボタンを使用して編集できるようになります。
- [ダイナミック]：LACP が有効になっている場合、LAG は動的に作成されます。ダイナミック LAG に割り当てられるポートのグループは、候補ポートになります。LACP によって、LAG のどの候補ポートをアクティブ メンバー ポートにするかが決定されます。非アクティブ候補ポートはスタンバイ ポートになります。つまり、アクティブ メンバー ポートに障害が発生した場合、*スタンバイ* ポートが代わりに使用されます。

ロード バランシング

LAG に転送されたトラフィックは、アクティブ メンバー ポート間で負荷分散されます。この結果、LAG のすべてのアクティブ メンバー ポートの合計帯域幅に近い帯域幅を効果的に利用できます。

LAG のアクティブ メンバー ポート間でトラフィックをロード バランシングする処理は、ハッシュに基づく分散機能によって管理されます。この機能により、レイヤ 2 またはレイヤ 3 のパケット ヘッダー情報に基づいてユニキャストおよびマルチキャスト トラフィックが分散されます。

このデバイスで使用できるロード バランシング モードは次の 2 種類です。

- **MAC アドレスを基準**：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されます。
- **IP アドレスと MAC アドレスを基準**：IP パケットの場合は、送信元 IP アドレスと宛先 IP アドレス、非 IP パケットの場合は、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されます。

LAG 管理

LAG は通常、1 つの論理ポートとして扱われます。たとえば、LAG のポート属性（状態、速度など）は通常のポートに似ています。

SG350XG デバイスは最大で 8 つの LAG をサポートします。SG550XG デバイスは最大で 32 個の LAG をサポートします。すべてのデバイスは、LAG グループ内で最大 8 つのポートをサポートします。

LAG の特徴は次のとおりです。

- LAG 内の各ポートのメディア タイプはすべて同じでなければなりません。
- LAG 内のポートは、別の LAG に追加しないようにしてください。
- 1 つのスタティック LAG には最大 8 個のポートを追加できます。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。
- ポートを LAG に追加すると、LAG の設定情報がポートに適用されます。そのポートを LAG から削除すると、そのポートの元々の設定情報が再度適用されます。
- Spanning Tree Protocol（STP）などのプロトコルでは、LAG 内のすべてのポートが 1 つのポートとして扱われます。

デフォルト設定とコンフィギュレーション

デフォルトで、ポートは LAG のメンバーではなく、LAG の一部になる候補でもありません。

スタティック LAG およびダイナミック LAG を設定する手順

LAG を手動で作成した場合、LACP オプションを追加したり削除したりするには、その LAG を編集してメンバーを削除する必要があります。これで、[LACP] ボタンを使用して編集できるようになります。

スタティック LAG を設定するには、次のようにします。

1. LAG で LACP を無効にしてスタティックにします。[ポート リスト] フィールドに表示されているポートを選択して [LAG メンバー] フィールドに移動し、最大 8 個のメンバー ポートをスタティック LAG に追加します。LAG のロード バランシング アルゴリズムを選択します。これらの処理を [LAG 管理] ページで実行します。
2. [LAG 設定] ページで、LAG のさまざまな設定（速度、フロー制御など）を行います。

ダイナミック LAG を設定するには、次のようにします。

1. LAG で LACP を有効にします。[LAG 管理] ページで、[ポート リスト] フィールドに表示されているポートを選択して [LAG メンバー] リストに移動し、最大 16 個の候補ポートをダイナミック LAG に追加します。
2. [LAG 設定] ページで、LAG のさまざまな設定（速度、フロー制御など）を行います。
3. [LACP] ページで、LAG 内のポートの LACP プライオリティおよびタイムアウトを設定します。

LAG 管理

[LAG 管理] ページには、LAG のグローバル管理情報と LAG ごとの管理情報が表示されます。このページでは、LAG のグローバル管理情報を設定できます。また、[LAG メンバーシップの編集] ページで LAG を選択し、LAG ごとの管理情報を設定することもできます。

LAG のロード バランシング アルゴリズムを選択するには、次のようにします。

ステップ 1 [ポート管理] > [リンクアグリゲーション] > [LAG管理] をクリックします。

ステップ 2 [ロードバランスアルゴリズム] で次のいずれかを選択します。

- [MACアドレス]：すべてのパケットの送信元 MAC アドレスと宛先 MAC アドレスに基づいて、ロード バランシングを実行します。
- [IP/MACアドレス]：IP パケットの場合は、送信元 IP アドレスと宛先 IP アドレス、非 IP パケットの場合は、送信元 MAC アドレスと宛先 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 [適用] をクリックします。ロード バランス アルゴリズ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。

LAG 内のメンバー ポートまたは候補ポートを定義するには、次のようにします。

ステップ 1 LAG を選択し、[編集] をクリックします。

各 LAG に対して、次のフィールドが表示されます（[編集] ページにないフィールドのみ説明します）。

- [リンクステート]：ポートがアクティブ化されているかどうか。
- [アクティブ メンバー]：LAG のアクティブ ポート。
- [スタンバイ メンバー]：この LAG の候補ポート。

ステップ 2 次のフィールドに値を入力します。

- [LAG]:LAG 番号を選択します。
- [LAG名]:LAG 名またはコメントを入力します。
- [LACP]:選択した LAG で LACP を有効にする場合に選択します。このフィールドを選択した場合、LAG はダイナミック LAG になります。このフィールドを有効にできるのは、次のフィールドでポートを LAG に移動した場合だけです。
- [ユニット/スロット]:LAG 情報が定義されているスタック メンバーを表示します。
- [ポート リスト]:LAG に追加するポートを [ポート リスト] フィールドで選択し、[LAG メンバー] フィールドに移動します。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。これらが候補ポートです。

ステップ 3 [適用] をクリックします。LAG メンバーシッ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。

LAG 設定

[LAG 設定] ページには、すべての LAG の現在の設定情報が表示されます。[LAG 設定の編集] ページでは、選択した LAG の情報の設定、また、一時停止されている LAG の再アクティブ化を行うことができます。

LAG 設定を構成したり一時停止されている LAG を再アクティブ化したりするには、次のようにします。

ステップ 1 [ポート管理] > [リンクアグリゲーション] > [LAG設定] 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、[編集] 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。

- [LAG]:LAG 番号を選択します。
- [LAGタイプ]: この LAG を構成しているポートのタイプが表示されます。
- [説明]:LAG 名またはコメントを入力します。
- [管理ステータス]:選択した LAG をアクティブ化する場合は [アップ]、アクティブ化しない場合は [ダウン] を選択します。

- [動作ステータス]:LAG が現在アクティブ化されているかどうかが表示されます。
- [リンクステータスSNMPトラップ]:ポートのリンク ステータスに変更を通知する SNMP トラップの生成を有効にするには、このフィールドを選択します。
- [時間範囲]:ポートをアクティブ化する時間範囲を有効にするには、このフィールドを選択します。時間範囲がアクティブでない場合、ポートは停止されます。時間範囲が設定されている場合、ポートが管理者によりアクティブ化されている場合のみ有効です。
- [時間範囲名]:時間範囲を指定するプロファイルを選択します。時間範囲がまだ定義されていない場合、[時間範囲] ページに移動するには [編集] をクリックします。
- [動作時間範囲の状態]:時間範囲が現在アクティブ化されているかいないかを表示します。
- [管理自動ネゴシエーション]:LAG で自動ネゴシエーションを有効にするか無効にするかを選択します。自動ネゴシエーションは、リンク相手との間で実行されます。自動ネゴシエーションを有効にした場合、自身の伝送速度とフロー制御が相手にアドバタイズされます。フロー制御のアドバタイズは、デフォルトでは [無効] になっています。アグリゲートされているリンクの両側で自動ネゴシエーションを有効にするか、または、両側で自動ネゴシエーションを無効にしてリンク速度を同じにすることを推奨します。
- [動作自動ネゴシエーション]:現在の自動ネゴシエーションのステータスが表示されます。
- [管理速度]:LAG 内のポートの速度を選択します。
- [動作LAG速度]:LAG の現在の速度が表示されます。
- [管理アドバタイズメント]:この LAG からアドバタイズする通信機能を選択します。次のオプションがあります。
  - [最大機能]:すべての LAG 速度と両方のデュプレックス モード。
  - [10全二重]:10 Mbps のスピードのアドバタイズで全二重モード。
  - [100全二重]:100 Mbps のスピードのアドバタイズで全二重モード。
  - [1000全二重]:1000 Mbps のスピードのアドバタイズで全二重モード。
  - *[2500全二重]*:2500 Mbps のスピードのアドバタイズで全二重モード。これは、550 ファミリ上でのみサポートされます。
  - [5000全二重]:5000 Mbps のスピードのアドバタイズで全二重モード。これは、550 ファミリ上でのみサポートされます。

- [10000全二重]:10000 Mbps のスピードのアドバタイズで全二重モード。これは、550 ファミリ上でのみサポートされます。

- [動作アドバタイズメント]:管理アドバタイズメントのステータスが表示されます。この LAG からその機能がネイバー LAG にアドバタイズされ、ネゴシエーション プロセスが開始します。表示される値は、[管理アドバタイズメント] フィールドの選択項目と同じです。
- [管理フロー制御]:[フロー制御] を [有効] または [無効] に設定するか、LAG で [フロー制御] の [自動ネゴシエーション] を有効にします。
- [動作フロー制御]:現在の [フロー制御] のステータスが表示されます。
- [保護LAG]:LAG をレイヤ 2 分離の保護ポートにするには、このフィールドを選択します。保護ポートおよび LAG の詳細については、「ポート設定」のポート設定の説明を参照してください。

ステップ 4 [適用] 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

ダイナミック LAG では LACP が有効になっており、LAG で定義されているすべての候補ポート上で動作します。

LACP におけるプライオリティとルール

候補ポートが 9 個以上追加されているダイナミック LAG では、LACP システム プライオリ ティと LACP ポート プライオリティの両方を使用して、どの候補ポートがアクティブ メンバ ポートになるかが決定されます。

選択された候補ポートは、すべて同じリモート デバイスに接続されます。ローカル スイッチとリモート スイッチのどちらにも LACP システム プライオリティが設定されます。

LACP ポート プライオリティがローカル デバイスとリモート デバイスのどちらから選ばれるかを決定するために、次のアルゴリズムが使用されます。ローカル LACP プライオリティは、リモート LACP システム プライオリティと比較されます。プライオリティが最も低いデバイスによって、LAG の候補ポートが選択されます。両者のプライオリティが同じである場合は、両者の MAC アドレスが比較されます。MAC アドレスが最も小さいデバイスのプライオリティによって、LAG の候補ポートが決定されます。

ダイナミック LAG には、同じタイプのイーサネット ポートを最大 16 個追加できます。アクティブにできるポートとスタンバイ モードにできるポートは、それぞれ最大 8 個です。ダイナミック LAG 内に 9 個以上のポートがある場合、このリンクの制御エンドであるデバイスでは、ポート プライオリティに基づいて、この LAG に割り当てるポート、および、ホットスタンバイ モードにするポートが決定されます。もう一方のデバイス（このリンクの非制御エンド）で設定されているポート プライオリティは無視されます。

次の追加ルールを使用して、ダイナミック LACP のアクティブ ポートまたはスタンバイ ポートが選択されます。

- 伝送速度が最速アクティブ メンバー ポートと異なるリンクや、半二重モードで動作しているリンクは、スタンバイ モードになります。ダイナミック LAG 内のアクティブ ポートは、すべて同じボー レートで動作します。
- リンクの LACP ポート プライオリティの値が現在のアクティブ メンバー ポートより小さく、アクティブ メンバー ポートの数がすでに上限数に達している場合、このリンクは非アクティブになり、スタンバイ モードに移行します。

リンク パートナーを持たない LACP

LACP が LAG を作成するには、両方のリンク エンドのポートが LACP に対して設定されなければなりません。つまり、ポートが LACP PDU を送信し、受信した PDU を処理しなければなりません。

しかしながら、1 つのリンク パートナーが LACP に対して一時的に設定されていないことがあります。そのような状況の一例は、リンク パートナーがデバイス上にあり、自動コンフィギュレーション プロトコルを使用して自身のコンフィギュレーションを受信するプロセスの最中である場合です。このデバイスのポートはまだ LACP に対して設定されていません。LAG リンクがアクティブ化できない場合、デバイスの設定を実行することはできません。同じような状況は、デュアル NIC ネットワークブート コンピュータ（例、PXE）でも起こり得ます。これは、起動後でなければ LAG コンフィギュレーションを受信することができません。

いくつかの LACP 設定ポートが設定され、リンクが 1 つ以上のポートでアクティブ化されたもののそれらのポートに対してリンク パートナーからの LACP 応答がない場合、アクティブ化されたリンクを持つ最初のポートは LACP LAG に追加され、アクティブ化されます（他のポートは非候補になります）。このようにして、ネイバー デバイスは、たとえば DHCP を使用して IP アドレスを取得し、自動コンフィギュレーションを使用して自身のコンフィギュレーションを取得します。

LACP 設定

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

LAG に対してアクティブ メンバー ポートの上限数(8)を超える候補ポートが追加されていて、かつ各候補ポートの特性が同じである場合、プライオリティが最も高いポートがデバイスのダイナミック LAG からアクティブ ポートとして選択されます。

注 LACP 設定情報は、ダイナミック LAG のメンバーでないポートでは関係ありません。

LACP 設定を定義するには、次のようにします。

ステップ 1 [ポート管理] > [リンクアグリゲーション] > [LACP] をクリックします。

ステップ 2 [LACPシステムプライオリティ] を入力します。

ステップ 3 ポートを選択して、[編集] 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。

- [ポート]: タイムアウト値とプライオリティを設定するポートの番号を選択します。
- [LACPポートプライオリティ]: このポートの LACP プライオリティを入力します。
- [LACPタイムアウト]: 連続する LACP PDU の送受信の時間間隔です。相手デバイスから定期的に送信される LACP PDU を待つ時間([ロング]/[ショート])を、表示される LACP タイムアウトの設定から選択します。

ステップ 5 [適用] 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

この項では、単方向リンク検出(UDLD)機能について説明します。

具体的な内容は、次のとおりです。

- UDLD の概要
- UDLD グローバル設定
- UDLD インターフェイス設定
- UDLD ネイバー

UDLD の概要

UDLD はレイヤ 2 プロトコルの 1 つで、この機能により、光ファイバ イーサネット ケーブルまたはツイストペア イーサネット ケーブルで接続されたデバイスが単方向リンクを検出できます。単方向リンクは、ネイバー デバイスからのトラフィックをローカル デバイスが受信しているのに、ローカル デバイスからのトラフィックをネイバーの方が受信していない場合に発生します。

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ていないポートを検出し、そのポートをシャットダウンすることです。

このプロトコルで単方向リンクを正常に検出するには、接続済みのデバイスがすべて UDLD をサポートしていることが必要です。ローカル デバイスのみが UDLD をサポートしている場合、このデバイスでリンクのステータスを検出することはできません。この場合、リンクのステータスは [未定] に設定されます。ユーザは、[未定] の状態のポートをシャットダウンするか、通知をトリガーするだけにしておくかを設定できます。

UDLD 状態およびモード

UDLD プロトコルでは、ポートが次の状態に割り当てられます。

- [検出]: リンクが双方向か単方向かをシステムが検出中です。これは一時的な状態です。
- [双方向]: ローカル デバイスから送信されたトラフィックはネイバーで受信され、ネイバーから送信されたトラフィックはローカル デバイスで受信されます。
- [シャットダウン]: このリンクは単方向です。ローカル デバイスから送信されたトラフィックはネイバーで受信されますが、ネイバーから送信されたトラフィックはローカル デバイスで受信されません。
- [未定]: 次のいずれかの原因により、システムがポートの状態を検出できません。
  - ネイバーが UDLD をサポートしていない。

    または

  - 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。

  この場合、デバイスの UDLD モードに基づき次の UDLD アクションが発生します。

UDLD では次の動作モードをサポートしています。

- [ノーマル]

  検出されたポートのリンク ステートが双方向で、ポートのリンクが依然としてアップ状態である間に UDLD 情報がタイムアウトした場合、UDLD はこのポートの状態を再確立しようとします。

- [アグレッシブ]

  検出されたポートのリンク ステートが双方向で、UDLD 情報がタイムアウトした場合、一定時間が経過してこのリンクが不良であると判断できれば、UDLD はポートをシャットダウンします。UDLD のポート状態は [未定] にマークされます。

次のいずれかに該当する場合、ポート上で UDLD が有効になります。

- ポートがファイバ ポートで、UDLD がグローバルに有効になっている場合。
- ポートが銅線ポートで、ユーザがこのポート上の UDLD を有効にした場合。

UDLD の動作方法

ポートで UDLD が有効な場合、次のアクションが実行されます。

- UDLD により、ポートの検出状態が開始されます。

  この状態で、UDLD はアクティブな各インターフェイス上でネイバーすべてに定期的にメッセージを送信します。これらのメッセージには既知のネイバーすべてのデバイス ID が含まれています。UDLD は、ユーザが定義したメッセージ時間に従ってこれらのメッセージを送信します。

- UDLD がネイバー デバイスから UDLD メッセージを受信します。期限切れ時間（メッセージ時間の 3 倍）の経過前に、UDLD がメッセージを受信します。期限切れ時間より前に新しいメッセージを受信すると、前のメッセージの情報は新しいメッセージの情報に置き換えられます。

- 期限切れ時間が経過すると、受信した情報に基づいてデバイスは次の処理を実行します。

  - **ネイバー メッセージにローカル デバイスの ID が含まれている場合**：ポートのリンク ステータスは [双方向] に設定されます。

  - **ネイバー メッセージにローカル デバイスの ID が含まれていない場合**：ポートのリンク ステータスは [単方向] に設定され、そのポートはシャットダウンされます。

- 期限切れ時間の経過前にネイバー デバイスから UDLD メッセージを受信しない場合、ポートのリンク ステータスは [未定] に設定され、次の処理が実行されます。
  - **デバイスがノーマル UDLD モードの場合:** 通知が送信されます。
  - **デバイスがアグレッシブ UDLD モードの場合:** ポートがシャットダウンされます。

インターフェイスが双方向か未定の状態である場合、デバイスはメッセージ時間ごとに定期的にメッセージを送信します。上記の手順が繰り返し実行されます。

シャットダウンされたポートは、[エラー回復設定] から手動で再アクティブ化できます。詳細については、「シャットダウンしたポートの再アクティブ化」を参照してください。

インターフェイスがダウンした場合、UDLD が有効であれば、デバイスはすべてのネイバー情報を削除し、ネイバーに少なくとも 1 つの UDLD メッセージを送信して、ポートがダウンしていることを通知します。ポートが復旧すると、UDLD 状態は [検出] に変更されます。

UDLD がネイバーで未サポートか無効な場合

UDLD がネイバー側でサポートされていないか無効になっている場合、ネイバーから UDLD メッセージを受信しません。この場合、デバイスはリンクが単方向か双方向かを検出できません。したがって、インターフェイスのステータスは [未定] に設定されます。

シャットダウンしたポートの再アクティブ化

UDLD によりシャットダウンしたポートは、次のどちらかの方法で再アクティブ化できます。

- [自動]:[エラー回復設定] から、UDLD によりシャットダウンしたポートが自動的に再アクティブ化されるようにシステムを設定できます。この場合、UDLD によってシャットダウンしたポートは、[自動回復間隔] の経過後に自動的に再アクティブ化されます。UDLD が再度ポートで実行されます。リンクが依然として単方向である場合は、UDLD 期限切れ時間の経過後に再度 UDLD によってリンクがシャットダウンされます。
- [手動]:[エラー回復設定] ページでポートを再アクティブにすることができます。

使用上のガイドライン

シスコは、UDLD がサポートされていないデバイスや、無効になっているデバイスと接続しているポートで UDLD を有効にすることを推奨していません。UDLD をサポートしていないデバイスに接続されたポートで UDLD パケットを送信しても、ポートのトラフィック増加の原因となり、利点がありません。

また、UDLD の設定に際しては、次の点も考慮してください。

- メッセージ時間は、単方向リンク状態のポートをどれほど緊急にシャットダウンする必要があるかに応じて設定します。メッセージ時間が短く設定されると、それだけ多くの UDLD パケットが送信されて分析されますが、リンクが単方向の場合にはポートがすぐにシャットダウンされることになります。
- 銅線ポートで UDLD を有効にするには、ポートごとに UDLD を有効にする必要があります。グローバルに UDLD を有効にした場合は、ファイバ ポートの UDLD のみが有効になります。
- リンクが単方向である場合以外、ポートがシャットダウンされないようにするには、UDLD モードを [ノーマル] に設定します。
- 単方向でも双方向でもリンク損失を必要とする場合は、UDLD モードを [アグレッシブ] に設定します。

他の機能への依存関係

- UDLD とレイヤ 1。

  UDLD がポートで有効な場合、ポートがアクティブであれば UDLD がアクティブに実行されます。ポートがダウンしていると、UDLD は UDLD シャットダウン状態になります。この状態では、UDLD は学習済みネイバーをすべて削除します。ポートがダウンからアクティブに変わると、UDLD が再びアクティブに実行されます。

- UDLD とレイヤ 2 プロトコル。

  UDLD は、同じポート上で実行中の他のレイヤ 2 プロトコル（STP や LACP など）とは独立して、ポート上で実行されます。たとえば、ポートの STP 状態や、ポートが LAG に所属しているかどうかには関係なく、UDLD はポートに状態を割り当てます。

デフォルト設定とコンフィギュレーション

この機能は、デフォルトで次のように設定されています。

- デフォルトでは、UDLD はデバイスのすべてのポートで無効です。
- デフォルトのメッセージ時間は 15 秒です。

- デフォルトの期限切れ時間は 45 秒です(メッセージ時間の 3 倍)。
- デフォルトのポート UDLD 状態は次のとおりです。
  - 光ファイバ インターフェイスは、グローバル UDLD 状態。
  - 光ファイバ インターフェイス以外は、無効状態。

開始する前に

事前に必要なタスクはありません。

UDLD の共通タスク

この項では、UDLD を設定する際の共通タスクについて説明します。

ワークフロー 1:ファイバ ポートで UDLD をグローバルに有効にするには、次の手順を実行します。

ステップ 1 [UDLD グローバル設定] ページを開きます。

a. [メッセージ時間] を入力します。

b. [ファイバポートUDLDデフォルト状態] フィールドで、[無効]、[ノーマル]、または [アグレッシブ] のいずれかのグローバル UDLD 状態を選択します。

ステップ 2 [適用] をクリックします。

ワークフロー 2:ファイバ ポートの UDLD 設定を変更したり、銅線ポートで UDLD を有効にしたりするには、次の手順を実行します。

ステップ 1 [UDLD グローバル設定] ページを開きます。

a. ポートを選択します。

b. ポートの UDLD 状態として、[デフォルト]、[無効]、[ノーマル]、または [アグレッシブ] のいずれかを選択します。[デフォルト] を選択した場合、ポートはグローバル設定になります。

ステップ 2 [適用] をクリックします。

ワークフロー 3: 自動再アクティブ化が設定されていない場合、UDLD によるシャットダウン後にポートを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 1 [エラー回復設定] ページを開きます。

a. ポートを選択します。

b. [再アクティブ化] をクリックします。

UDLD の設定

すべてのファイバ ポートの UDLD 機能を一度に設定することも ([UDLD グローバル設定] ページ)、ポートごとに UDLD 機能を設定することもできます ([UDLD インターフェイス設定] ページ)。

UDLD グローバル設定

ファイバ ポート UDLD デフォルト状態は、ファイバ ポートにのみ適用されます。

[メッセージ時間] フィールドは、銅線ポートとファイバ 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、次のようにします。

ステップ 1 [ポート管理] > [UDLD] > [UDLDグローバル設定] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [メッセージ時間]: UDLD メッセージの送信間隔を入力します。このフィールドは、ファイバ ポートと銅線ポートの両方に適用されます。
- [ファイバポートUDLDデフォルト状態]: このフィールドは、**ファイバ** ポートにのみ適用されます。銅線ポートの UDLD 状態は、[UDLD インターフェイス設定] ページで個別に設定する必要があります。選択可能な状態は次のとおりです。
  - [無効]: UDLDは、デバイスのすべてのポートで無効です。
  - [ノーマル]: リンクが単方向の場合、デバイスはインターフェイスをシャットダウンします。リンクが不明な場合は、通知が送信されます。
  - [アグレッシブ]: リンクが単方向の場合、デバイスはインターフェイスをシャットダウンします。リンクが双方向の場合、UDLD 情報がタイムアウトすると、デバイスはシャットダウンします。ポート状態は [未定] にマークされます。

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

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インターフェイス設定] ページを使用します。このページで、銅線ポートとファイバ ポートの状態を設定できます。

複数のポートに特定の値のセットをコピーするには、1 つのポートの値を設定してから、[コピー] ボタンを使用してそれを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、次のようにします。

ステップ 1 [ポート管理] > [UDLD] > [UDLDインターフェイス設定] 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の情報が表示されます。特定のグループのポートのみにフィルタ処理すると、そのグループのポートの情報が表示されます。

- [ポート]:ポート ID。
- [UDLD 状態]:選択可能な状態は次のとおりです。
  - [デフォルト]:ポートは、[UDLD グローバル設定] ページの [ファイバポート UDLDデフォルト状態] の値に設定されます。
  - [無効]:UDLD は、デバイスのすべてのファイバ ポート上で無効です。
  - [ノーマル]:リンクが単方向であることを検出すると、デバイスはインターフェイスをシャットダウンします。リンクが不明な場合は通知を送信します。
  - [アグレッシブ]:リンクが単方向の場合、デバイスはインターフェイスをシャットダウンします。リンクが双方向の場合、UDLD 情報がタイムアウトすると、デバイスはシャットダウンします。ポート状態は [未定] にマークされます。
- [双方向状態]:選択可能な状態は次のとおりです。
  - [検出]:ポートの最新の UDLD 状態を検出中です。最後の検出(もしあれば)から期限切れ時間がまだ経過していないか、UDLD がポートで実行し始めたところで、その状態が未検出である状態。
  - [双方向]:ローカル デバイスから送信されるトラフィックをネイバーが受信し、ネイバーからのトラフィックをローカル デバイスが受信している状態。
  - [未定]: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。
  - [無効(デフォルト)]:このポートの UDLD は無効になっています。

- [シャットダウン]:アグレッシブ モードで、接続済みデバイスとのリンクが未定なため、このポートはシャットダウンされています。
- [アイドル]:ポートがアイドル中です。

- [ネイバーの数]:検出された接続済みデバイスの数。

ステップ 2 特定のポートの UDLD 状態を変更するには、ポートを選択し、[編集] をクリックします。

ステップ 3 UDLD 状態の値を変更します。[デフォルト] を選択した場合、ポートは、[UDLD グローバル設定] ページの [ファイバポートUDLDデフォルト状態] の値に設定されます。

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

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、[ポート管理] > [UDLD] > [UDLDネイバー] の順にクリックします。

UDLD が有効なすべてのポートについて、次のフィールドが表示されます。

- [インターフェイス名]:UDLD が有効なローカル ポート名。
- [ネイバー情報]:
  - [デバイスID]:リモート デバイスの ID。
  - [デバイス MAC]:リモート デバイスの MAC アドレス。
  - [デバイス名]:リモート デバイスの名前。
  - [ポート ID]:リモート ポートの名前。
- [状態]:ローカル デバイスとローカル ポート上のネイバー デバイスとの間のリンクの状態。次の値のいずれかを示します。
  - [検出]:ポートの最新の UDLD 状態を検出中です。最後の検出(もしあれば)から期限切れ時間がまだ経過していないか、UDLD がポートで実行し始めたところで、その状態が未検出である状態。
  - [双方向]:ローカル デバイスから送信されるトラフィックをネイバーが受信し、ネイバーからのトラフィックをローカル デバイスが受信している状態。
  - [未定]: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。

- [無効]:このポートの UDLD は無効になっています。
- [シャットダウン]:アグレッシブ モードで、接続済みデバイスとのリンクが未定なため、このポートはシャットダウンされています。

- [ネイバー期限切れ時間(秒)]:どれほどの時間が経過してから、デバイスがポートの UDLD 状態を検出しようとするかを表示します。メッセージ時間の 3 倍です。
- [ネイバー メッセージ時間(秒)]:UDLD メッセージの間隔を表示します。

PoE

ここでは、PoE 機能を使用する方法について説明します。

注 PoE は、スタンドアロン デバイス上でのみサポートされます。スタンドアロン デバイスは、スタックの一部ではないデバイスを意味します。

具体的な内容は、次のとおりです。

- 概要
- PoE のプロパティ
- 設定
- 統計情報
- Green Ethernet の概要

概要

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、既存のカッパー ケーブルを介して、接続先の受電装置(PD)に電力を供給する給電側機器(PSE)です。

特徴

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 電源を確保する必要がなくなる。
- すべてのネットワーク デバイスを電源の近くに置く必要がなくなる。
- ケーブル システムを社内で二重に配置する必要がなくなるため、設置コストを大幅に削減できる。

Power over Ethernet は、イーサネット LAN に接続する比較的低出力の装置を配置する企業ネットワークで使用できます。たとえば、次のような装置があります。

- IP 電話
- 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 モニタリング デバイス

動作

PoE は次のステージで実装されます。

- **検出**:カッパー ケーブルに特殊パルスを送信します。PoE デバイスが相手側にある場合、そのデバイスがこのパルスに応答します。
- **分類**:検出ステージの後、給電側機器(PSE)と受電装置(PD)の間でネゴシエーションが開始します。ネゴシエーション中、PD は、自分が消費する最大電力を示すクラスを指定します。
- **電力消費**:分類ステージが完了した後、PSE は PD に電力を供給します。PoE 対応であっても分類が存在しない PD は、クラス 0(最大)と想定されます。PD が、規格で許可されている以上の電力を消費しようとすると、PSE はポートへの給電を停止します。

PoE は 2 つのモードをサポートしています。

- **ポート制限**:デバイスが供給に同意する最大電力は、分類ステージの結果にかかわらず、システム管理者が設定する値に制限されます。
- **クラス電力制限**:デバイスが供給に同意する最大電力は、分類ステージの結果によって決まります。つまり、クライアントの要求により設定されます。

PoE デバイス

アップリンク ポートは、1 または 2 つの PD ポートを備えた受電デバイス(PD)として機能します。8 ポート デバイスでは、最上位ポートが PD になります(PD ポートは給電側機器(PSE)機能を備えていません)。2 つの PD ポートが存在する場合は、それらを 1 つの PSE に接続することをお勧めします。両方の PD ポートに同じ電力標準(両方が AF、両方が AT、または両方が 60W PoE)から電力が供給されていれば、両方のポートが機能します。

60W PoE PSE デバイスの場合は、PSE ポート タイプが次のようになります。

	24 ポート デバイス	48 ポート デバイス
350	4 60W PoE ポート、20 ポート AT	8 ポート 60W PoE、40 ポート AT
550	8 60W PoE ポート、16 ポート AT	16 ポート 60W PoE、32 ポート AT

Power over Ethernet（PoE）機能は、次の PoE ベースのデバイス上でのみ使用できます。

SKU 名	PoE PD 60W PoE/AT/AF	PoE PSE AF/AT
SF350-08	AT	なし
SF352-08	AT	なし
SF352-08P	60W PoE/AF/AT	AF/AT
SF352-08MP	60W PoE/AF/AT	AF/AT
SF350-24P	なし	60W PoE/AF/AT
SF350-24MP	なし	60W PoE/AF/AT
SF350-48	なし	なし
SF350-48P	なし	60W PoE/AF/AT
SF350-48MP	なし	60W PoE/AF/AT
SG350-10P	60W PoE/AF/AT	AF/AT
SG355-10P	60W PoE/AF/AT	AF/AT
SG350-10MP	60W PoE/AF/AT	AF/AT
SG350-10SFP	AF/AT	なし
SG350-28P	なし	60W PoE/AF/AT
SG350-28MP	なし	60W PoE/AF/AT
SG350-52P	なし	60W PoE/AF/AT
SG350-52MP	なし	60W PoE/AF/AT
SG350X-24P	なし	60W PoE/AF/AT
SG350X-24MP	なし	60W PoE/AF/AT

SKU 名	PoE PD 60W PoE/AT/AF	PoE PSE AF/AT
SG350X-48P	なし	60W PoE/AF/AT
SG350X-48MP	なし	60W PoE/AF/AT
SG350-8PD	なし	AF/AT
SG350X-8PMD	なし	UPOE/AF/AT
SG350X-24PD	なし	UPOE/AF/AT
SF550X-24P	なし	60W PoE/AF/AT
SF550X-24MP	なし	60W PoE/AF/AT
SF550X-48P	なし	60W PoE/AF/AT
SF550X-48MP	なし	60W PoE/AF/AT
SG550X-24P	なし	60W PoE/AF/AT
SG550X-24MP	なし	60W PoE/AF/AT
SG550X-24MPP	なし	60W PoE/AF/AT
SG550X-48P	なし	60W PoE/AF/AT
SG550X-48MP	なし	60W PoEAF/AT

PoE 設定における考慮事項

PoE の設定をする際は、以下を考慮してください。

- PSE が供給できる電力量。
- PD が実際に消費しようとする電力量。

次の項目を設定できます。

- PSE から PD に給電できる最大電力。
- モード。デバイス稼動中に、クラス電力制限からポート制限へ、またはその反対へモードを変更できます。ポート制限モードで設定されたポート別電力値は保持されます。

  注 デバイスの動作中にモードをクラス制限からポート制限に（またはその逆に）変更すると、PD が強制的にリブートされます。

- ポート別数値制限(mW 単位)により許可される最大ポート制限(ポート制限モード)。
- PD が許容されている以上の電力を消費しようとした場合に生成されるトラップと、トラップが生成される最大電力割合。

PoE 対応ハードウェアが自動的に PD クラスを検出し、各ポートに接続されているデバイスのクラスに従い、電力制限を検出します(クラス制限モード)。

接続中に、(デバイスがクラス制限モードかポート制限モードかにかかわらず)設定済みの割り当てによって可能な量を超える電力を PD がデバイスに要求した場合、デバイスは次のことを行います。

- PoE ポート リンクのアップ/ダウン状態を維持します。
- PoE ポートへの給電を停止します。
- 電力停止の理由をログに記録します。
- SNMP トラップを生成します。

PoE のプロパティ

注 この項は PoE をサポートするデバイスのみに関連します。

PoE の [プロパティ] *ページでは*、PoE モードとしてポート制限またはクラス制限のいずれかを選択し、PoE トラップの生成を指定できます。

これらの設定は事前に入力されています。PD が実際に接続されて電力が消費されているとき、消費されている電力が許可されている最大電力よりずっと小さい場合があります。

リブート、初期化、およびシステム コンフィギュレーション中は、PD の損傷を避けるために出力電力はオフになります。

デバイスで PoE を設定し、現在の電力消費量を監視するには、次のようにします。

ステップ 1 [ポート管理] > [PoE] > [プロパティ] 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。

- [電力モード]:次のいずれかのオプションを選択します。
  - [クラス制限]:分類ステージの結果として、デバイスのクラスによりポート別最大電力量が決まります。
  - [ポート制限]:ユーザが、ポートごとの最大電力量を設定します。

注 ポート制限からクラス制限に(またはその逆に)変更する場合には、PoE ポートを無効にし、電力設定を変更した後でポートを有効にする必要があります。

- [トラップ]:トラップを有効または無効にします。トラップを有効にする場合は、SNMP もまた有効にして、少なくとも 1 つの通知受信者を設定する必要があります。
- [電力トラップしきい値]:消費量しきい値(電力制限のパーセンテージ)を入力します。電力がこの値を超えると、アラームが発生します。
- [ソフトウェア バージョン]:PoE チップのソフトウェア バージョンが表示されます。

それぞれのデバイスまたはスタックの全装置に関して、次のカウンタが表示されます。:

- [定格電力]:デバイスが、接続している全 PD に給電できる電力総量。
- [消費電力]:PoE ポートが現在消費している電力量。
- [有効電力]:定格電力から消費電力量を差し引いた値。
- [PSE チップセットとハードウェア リビジョン]:PoE チップセットとハードウェア リビジョン番号。

ステップ 3 [適用] をクリックして、PoE プロパティを保存します。

設定

[設定] ページには、システムの PoE 情報が表示され、PoE モードがポート制限の場合に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ポート別最大電力を監視したりすることができます。

注 デバイスで特定の期間にわたって PoE を設定することができます。この機能を使用して、PoE が有効になる曜日と時間帯をポートごとに定義できます。時間範囲がアクティブでないときには、PoE が無効になります。この機能を使用するには、まず [時間範囲] ページで時間範囲を定義しておく必要があります。

このページは、ポートあたりの電力を指定されたワット数に制限します。これらの設定をアクティブにするには、システムが PoE ポート制限モードになっている必要があります。このモードは、[PoE のプロパティ] ページで設定されます。

ポートで消費される電力がポート制限値を超えると、ポート電力はオフになります。

PoE プライオリティの例

想定:48 のポートを持つデバイスが合計 375 ワットを供給しているとします。

管理者は、すべてのポートに最大 30 ワットを割り当てるよう設定しています。48 のポートに 30 ワットを掛けると 1440 ワットになり、これは多すぎます。デバイスは各ポートに十分な電力を供給できないため、プライオリティに従って電力を供給します。

管理者は各ポートのプライオリティを設定して、受電可能な電力量を割り当てます。

これらのプライオリティは、PoE の [設定] ページで指定します。

PoE をサポートするデバイス モデルと、PoE ポートに割り当て可能な最大電力については、「デバイス モデル」の説明を参照してください。

PoE ポート制限を設定するには、次のようにします。

ステップ 1 [ポート管理] > [PoE] > [設定] をクリックします。

ポートと関連する PoE 情報が表示されます。これらのフィールドは [編集] ページで説明されます。ただし、次のフィールドを除きます。

- [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。
- [動作ステータス]:PoE がポートで現在アクティブかどうかが表示されます。
- [PoE標準]:サポートされている PoE のタイプが表示されます(60W PoE および 802.3 AT PoE など)。

ステップ 2 ポートを選択して、[編集] **をクリックします。**

ステップ 3 次のフィールドを入力します。

- [インターフェイス]:設定するポートを選択します。
- [管理ステータス]:ポートでの PoE を有効または無効にします。
- **[時間範囲]**:ポートでの PoE を有効にする場合に選択します。
- [時間範囲名]:[時間範囲] が有効になっている場合、使用する時間範囲を選択します。時間範囲は [時間範囲] ページで定義されます。新規の時間範囲を定義するには、[編集] をクリックします。
- [プライオリティレベル]:電力供給が低くなったときに使用するポートのプライオリティ(低、高、または重要)を選択します。たとえば、電力供給率が 99% であるとき、ポート 1 のプライオリティが高で、ポート 3 のプライオリティが低の場合、ポート 1 は電力を受け、ポート 3 は電力を受けられないことがあります。

- [管理電力割り当て]:PoE の [プロパティ] ページで電力モードとしてポート制限を設定した場合にのみ、このフィールドが表示されます。電力モードがポート制限モードである場合、ポートに割り当てる電力(ミリワット単位)を入力します。
- [4ペアの強制]:電源に予備ペアを強制する場合に選択します。これにより、CDP/LLDP PoE ネゴシエーションをサポートしない PD に 60 ワット PoE を使用できます。
- [最大電力割り当て]:PoE の [プロパティ] ページで設定した電力モードがポート制限モードである場合にのみ、このフィールドが表示されます。このポートで許可される電力の最大量が表示されます。
- [ネゴシエートされる電力]:デバイスに割り当てられる電力。
- [電力ネゴシエーションプロトコル]:ネゴシエートされる電力を決定するプロトコル。
- [電力消費]:設定(クラス制限)で割り当てられたミリワット単位の電力量が表示されます。
- [クラス]:発生する電力のクラスが表示されます。

[設定(クラス制限)] 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ポート別最大電力制限を監視したりすることができます。

注 デバイスで特定の期間にわたって PoE を設定することができます。この機能を使用して、PoE が有効になる曜日と時間帯をポートごとに定義できます。時間範囲がアクティブでないときには、PoE が無効になります。この機能を使用するには、まず [時間範囲] ページで時間範囲を定義しておく必要があります。

このページは、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 クラス制限モードになっている必要があります。このモードは、PoE の [プロパティ] ページで設定されます。

ポートで消費される電力がクラス制限値を超えると、ポート電力はオフになります。

PoE プライオリティの例

PoE をサポートするデバイス モデルと、PoE ポートに割り当て可能な最大電力については、「デバイス モデル」の説明を参照してください。

PoE クラス制限を設定するには、次のようにします。

ステップ 1 [ポート管理] > [PoE] > [設定(クラス制限)] の順にクリックします。

ポートと関連する PoE 情報が表示されます。これらのフィールドは [編集] ページで説明されます。ただし、次のフィールドを除きます。

- [PoE標準]:サポートされている PoE のタイプが表示されます(60W PoE および 802.3 AT PoE など)。
- [動作ステータス]:PoE がポートで現在アクティブかどうかが表示されます。

ステップ 2 ポートを選択して、[編集] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [インターフェイス]:設定するポートを選択します。
- [管理ステータス]:ポートでの PoE を有効または無効にします。
- [時間範囲]:ポートでの PoE を有効にする場合に選択します。
- [時間範囲名]:[時間範囲] が有効になっている場合、使用する時間範囲を選択します。時間範囲は [時間範囲] ページで定義されます。[編集] をクリックして、[時間範囲] ページに移動します。
- [プライオリティレベル]:電力供給が低くなったときに使用するポートのプライオリティ(低、高、または重要)を選択します。たとえば、電力供給率が 99% であるとき、ポート 1 のプライオリティが高で、ポート 3 のプライオリティが低の場合、ポート 1 は電力を受け、ポート 3 は電力を受けられないことがあります。
- [4ペアの強制]:拡張電源を提供する場合にこの機能を有効にします。
- [最大電力割り当て]:PoE の [プロパティ] ページで設定した電力モードがポート制限モードである場合にのみ、このフィールドが表示されます。このポートで許可される電力の最大量が表示されます。
- [電力消費]:割り当てられたミリワット単位の電力量が表示されます。設定(クラス制限)

- [クラス]:デバイスの最大電力レベルを示す、デバイスのクラスが表示されます。

クラス	デバイス ポートから送られる最大電力
0	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

- [最大電力割り当て]:PoE の [プロパティ] ページで設定した電力モードがポート制限モードである場合にのみ、このフィールドが表示されます。このポートで許可される電力の最大量が表示されます。
- [ネゴシエートされる電力]:デバイスに割り当てられる電力。
- [電力ネゴシエーションプロトコル]:ネゴシエートされる電力を決定するプロトコル。

ステップ 4 [適用] をクリックします。ポートの PoE 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。

統計情報

このページには、一定期間の平均電力消費を表す電力消費傾向が表示されます。これは、PoE 動作のモニタリングとデバッグに有効です。

デバイスは、一定期間の PoE ポート消費値(ワット単位)を保存しています。そのため、指定された日/週/月の期間の平均 PoE 消費の計算および表示が可能になるとともに、傾向の検出が可能になります。インターフェイスごとの情報とデバイス全体の情報が提供されます。

PoE 消費値は 1 分ごとに測定されます。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。

ポート/デバイスあたりの平均 PoE 消費のサンプルを以下に示します。

期間内の PoE 消費測定値の合計/サンプリング期間の時間(分)

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、以下のようにします。

ステップ 1 [ポート管理] > [PoE] > [統計情報] をクリックします。

ステップ 2 [ユニット] フィールドと [ポート] フィールドでユニットとポートを選択します。

ステップ 3 [インターフェイス] フィールド[リフレッシュ レート] 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が表示されます。

消費履歴

- [過去 1 時間の平均消費]:過去 1 時間のすべての PoE 消費測定値の平均。
- [過去 1 日の平均消費]:過去 1 日のすべての PoE 消費測定値の平均。
- [過去 1 週間の平均消費]:過去 1 週間のすべての PoE 消費測定値の平均。

PoE イベント カウンタ

- [過負荷カウンタ]:検出された過負荷状態の数。
- [ショート カウンタ]:検出されたショート状態の数。
- [拒否カウンタ]:検出された拒否状態の数。
- [未検出カウンタ]:検出された未検出状態の数。
- [無効な署名カウンタ]:検出された無効な署名状態の数。

次の操作をメインページで実行することができます。

- [イベント カウンタのクリア]:表示されたイベント カウンタをクリアします。
- [すべてのインターフェイス統計情報の表示]:すべてのインターフェイスに関する上記統計情報を表示します。
- [インターフェイス履歴グラフの表示]:カウントをグラフ形式で表示します。
- [リフレッシュ]:表示されたカウンタをリフレッシュします。

[すべてのインターフェイス統計情報の表示] をクリックすると、次の操作を実行できます。

- [イベント カウンタのクリア]:表示されたイベント カウンタをクリアします。
- [インターフェイス統計情報の表示]:選択されたインターフェイスに関する上記統計情報を表示します。

- [インターフェイス履歴グラフの表示]:選択されたインターフェイスに関するカウンタをグラフ形式で表示します。
- [リフレッシュ]:表示されたカウンタをリフレッシュします。

[インターフェイス履歴グラフの表示] をクリックすると、次の操作を実行できます。

- [インターフェイス統計情報の表示]:選択されたインターフェイスに関するグラフ統計情報を表形式で表示します。[期間] を時間、日、週、または年で入力します。
- [すべてのインターフェイス統計情報の表示]:すべてのインターフェイスに関する上記統計情報を表形式で表示します。[期間] を時間、日、週、または年で入力します。
- [イベント カウンタのクリア]:カウンタをクリアします。

Green Ethernet

ここでは、デバイスの電力を減らすために設計された Green Ethernet 機能について説明します。

内容は次のとおりです。

Green Ethernet の概要

Green Ethernet は、環境に配慮してデバイスの電力消費量を減らす機能の総称です。Green Ethernet は EEE と異なり、すべてのデバイスで Green Ethernet エネルギー検出が有効になります。EEE ではギガバイト ポートのみが有効になります。

Green Ethernet 機能では、次の方法で全体的な電力消費量を減らすことができます。

- [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「アップ」にしたまま電力を節約することができます。非アクティブ モードから完全動作モードに戻るのに要する時間は非常に短く、ユーザが意識することはありません。フレームが欠落することもありません。このモードは、GE ポートと FE ポートのどちらでも使用できます。このモードはデフォルトで無効になっています。

- [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。ケーブル長が解析されると、そのケーブル長に合わせて電力消費量が調整されます。ケーブルが Tengigabit ポートの場合は 30 m、その他のタイプのポートの場合は 50 m よりも短い場合、そのケーブル上でフレームを送信する際の電力消費量が減少します。これにより、電力を節約することができます。このモードは、RJ-45 GE ポートでのみ使用できます。コンボ ポートでは使用できません。このモードはデフォルトで無効になっています。

これらの Green Ethernet 機能の他に、GE ポートをサポートするデバイスには **802.3az Energy Efficient Ethernet（EEE）**もあります。EEE を使用すると、ポートにトラフィックが流れていない場合の電力消費を抑えることができます。詳細については、「802.3az Energy Efficient Ethernet 機能」を参照してください（GE モデルでのみ利用可能です）。

EEE はデフォルトでグローバルに有効になっています。あるポートで EEE が有効な場合、[ショートリーチモード] は無効になります。ユーザは、ショート リーチ モードを有効にする前に EEE を無効にする必要があります。

これらのモードは、ポートごとに設定され、ポートの LAG メンバーシップは考慮されません。

デバイスの LED は電力を消費します。ほとんどの時間、デバイスは誰もいない部屋にありますので、LED を点灯するのはエネルギーの無駄遣いです。Green Ethernet 機能により、必要のないときはポートの LED（リンク、速度および PoE）を無効にし、必要になったとき（デバッグ、追加のデバイスを接続するなど）に LED を有効にすることができます。

[システムの要約] ページでは、デバイス ボードの写真に表示される LED は LED 無効化の影響を受けません。

電力節約量、現在の電力消費量、および累積節電量を監視できます。合計電力節約量は、Green Ethernet 機能を利用していない場合のその物理インターフェイスの電力消費量に対するパーセント値で表示されます。

表示される節電量は、Green Ethernet に関連するものに限られます。EEE に節約されたエネルギーの量は表示されません。

ポート LED の無効化による電力節約

ポート LED の無効化機能により、デバイスの LED が消費する電力を節約することができます。デバイスはしばしば誰もいない部屋にありますので、LED を点灯するのはエネルギーの無駄遣いです。Green Ethernet 機能により、必要のないときはポートの LED（リンク、速度および PoE）を無効にし、必要になったとき（デバッグ、追加のデバイスを接続するなど）に LED を有効にすることができます。

[システムの要約] ページでは、デバイス ボードの写真に表示される LED は LED 無効化の影響を受けません。

ポート LED は、[プロパティ] ページで無効化することができます。

802.3az Energy Efficient Ethernet 機能

ここでは、802.3az Energy Efficient Ethernet（EEE）機能について説明します。

具体的な内容は、次のとおりです。

- 802.3az EEE の概要
- アドバタイズ機能のネゴシエーション
- 802.3Az EEE のリンク レベル検出
- 802.3az EEE の可用性
- デフォルト コンフィギュレーション
- 機能間の連携
- 802.3az EEE を設定する手順

802.3az EEE の概要

802.3az EEE は、リンクのトラフィックが流れていないときに電力を削減するように設計されています。Green Ethernet では、ポートが非アクティブ化されているときに電力が削減されます。802.3az EEE では、ポートがアクティブ化されていてもトラフィックがない場合に電力が削減されます。

802.3az EEE はアウトオブバンド ポートではサポートされません。

注 リモート リンク パートナー ステータスを表示できるのは、リンク速度が 1 G または 10 G の場合のみです。

802.3az EEE を使用すると、トラフィックが流れていないときに、リンクの両側のシステムではそれぞれの機能の一部を無効にして電力を削減することができます。

802.3az EEE では、100 Mbps および 1000 Mbps の IEEE 802.3 MAC 動作をサポートしています。

両方のデバイスで最適なパラメータの組み合わせを選択するために、LLDP が使用されます。リンク パートナーで LLDP がサポートされない場合、または LLDP が無効な場合、802.3az EEE はそのまま動作しますが、最適な動作モードにはならない可能性があります。

802.3az EEE 機能は、Low Power Idle（LPI）モードと呼ばれるポート モードで実装されます。トラフィックが流れていないときにこの機能が有効であれば、ポートは LPI モードに入り、電力消費が大幅に削減されます。

802.3az EEE が機能するには、接続の両側（デバイスのポートおよび接続しているデバイス）で 802.3az EEE がサポートされている必要があります。トラフィックが流れていないときは、両側から電力を削減しようとしていることを示す信号を送信されます。両側からの信号を受信すると、ポートが LPI ステータスであること（および非アクティブ化ステータスではないこと）がキープ アライブ信号で示され、電力が削減されます。

ポートを LPI モードのままにするには、キープ アライブ信号を両側から継続的に受信する必要があります。

アドバタイズ機能のネゴシエーション

802.3az EEE サポートは、自動ネゴシエーション段階でアドバタイズされます。自動ネゴシエーションにより、リンクされたデバイスは、リンクの他端側デバイスでサポートされる機能（動作モード）を検出したり、共通の機能を判断したり、結合操作用に自身を設定したりすることができます。自動ネゴシエーションは、リンクアップ時、管理のコマンド発行時、またはリンク エラーの検出時に実行されます。リンク確立プロセス時に、両方のリンク パートナーがそれぞれの 802.3az EEE 機能を交換します。自動ネゴシエーションがデバイスで有効になっている場合は、ユーザの操作なしで自動的に自動ネゴシエーションが行われます。

注 ポートで自動ネゴシエーションが有効でない場合、EEE は無効です。唯一の例外として、リンク速度が 1 GB または 10 G の場合は、自動ネゴシエーションが無効であっても、EEE が有効なままになります。

802.3Az EEE のリンク レベル検出

これらの機能の他に、802.3az EEE の機能および設定も、IEEE 規格 802.1AB プロトコル（LLDP）の Annex G で定義されている組織固有の TLV に基づいたフレームを使用してアドバタイズされます。LLDP は、自動ネゴシエーション完了後に、802.3az EEE の動作をさらに最適化するために使用されます。802.3az EEE TLV は、システムのウェイクアップ期間と更新期間を微調整するために使用されます。

802.3az EEE の可用性

EEE をサポートする製品の詳細な一覧については、リリース ノートを参照してください。

デフォルト コンフィギュレーション

デフォルトでは、802.3az EEE および EEE LLDP は、グローバルおよびポートごとに有効です。

機能間の連携

802.3az EEE と他の機能との連携について次に説明します。

- ポートで自動ネゴシエーションが有効でない場合、802.3az EEE 動作ステータスは無効です。このルールの例外として、リンク速度が 1 GB の場合は、自動ネゴシエーションが無効であっても、EEE が有効なままになります。
- 802.3az EEE が有効でポートがアクティブ化されている場合、ポートの最大ウェイク アップ時間値に従って、ただちに動作を開始します。
- GE ポートのポート速度が 10 Mbit に変更されると、802.3az EEE は無効になります。これは、GE モデルでのみサポートされています。

802.3az EEE を設定する手順

ここでは、802.3az EEE 機能を設定し、カウンタを表示する方法について説明します。

ステップ 1 [ポート管理] > [ポート設定] ページを開いて、ポートで自動ネゴシエーションが有効になっていることを確認します。

a. ポートを選択し、[ポート設定の編集] ページを開きます。

b. [自動ネゴシエーション] フィールドを選択して、有効にします。

ステップ 2 [プロパティ] ページで、[802.3 Energy Efficient Ethernet (EEE)] がグローバルに有効であることを確認します(デフォルトで有効です)。このページには、エネルギーの節約量も表示されます。

ステップ 3 [ポート設定] ページを開いて、ポートで 802.3az EEE が有効になっていることを確認します。

a. ポートを選択し、[ポート設定の編集] ページを開きます。

b. ポートの [802.3 Efficient Energy Ethernet(EEE)] モードを確認します(デフォルトで有効です)。

c. [802.3 Energy Efficient Ethernet (EEE) LLDP] で、LLDP を通じて 802.3az EEE 機能のアドバタイズメントを有効にするか無効にするかを選択します(デフォルトで有効です)。

ステップ 4 ローカル デバイスの 802.3 EEE 関連情報を表示するには、[LLDP ローカル情報] ページを開き、[802.3 Energy Efficient Ethernet (EEE)] ブロックで情報を表示します。

ステップ 5 リモート デバイスの 802.3az EEE 情報を表示するには、[LLDP ネイバー情報] ページを開き、[802.3 Energy Efficient Ethernet (EEE)] ブロックで情報を表示します。

プロパティ

[プロパティ] ページでは、デバイスの Green Ethernet モードを表示および設定できます。また、現在の電力節約量を表示できます。

Green Ethernet および EEE を有効にして電力節約量を表示するには、次のようにします。

ステップ 1 [ポート管理] > [Green Ethernet] > [プロパティ] 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。

- [エネルギー検出モード]: (非 XG デバイスの場合) これを有効にするにはチェックボックスをオンにします。
- [ショートリーチ]: (非 XG デバイスの場合) 有効にするにはチェックボックスをオンにします。
- [ポート LED]: ポート LED を有効にするには、このフィールドを選択します。無効になっている場合、リンク ステータス、アクティビティ等は表示されません。
- [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。

ステップ 3 [累積節電量] 情報をリセットするには、[節電カウンタのリセット] をクリックします。

ステップ 4 [適用] をクリックします。Green Ethernet 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

[ポート設定] ページには、ポートごとの現在の Green Ethernet モードおよび EEE モードが表示され、[ポート設定の編集] ページで Green Ethernet を設定できるようにします。ポートで Green Ethernet のいずれかのモードを使用するには、[プロパティ] ページでそのモードをグローバルで有効にしておく必要があります。

EEE 設定は、GE ポートを搭載するデバイスでのみ表示されます。EEE は、ポートが自動ネゴシエーションに設定されている場合のみ動作します。例外として、ポートが 1 GB 以上の速度の場合は、自動ネゴシエーションが無効であっても、EEE が動作し続けます。

ショート リーチおよびエネルギー検出の機能は XG デバイスで常に有効であり、無効にすることはできません。FE または GE ポートを持つデバイスで、これらの機能を有効または無効にすることができます。

ポートごとの Green Ethernet 情報を設定するには、次のようにします。

ステップ 1 [ポート管理] > [Green Ethernet] > [ポート設定] をクリックします。

[ポート設定] ページには、次のフィールドが表示されます。

- [グローバルパラメータステータス]: 以下が表示されます。
  - [エネルギー検出モード]: このモードが有効であるかどうか。
  - [ショートリーチモード]: このモードが有効であるかどうか。
  - [802.3 Energy Efficient Ethernet (EEE)モード]: このモードが有効であるかどうか。

次のフィールドが各ポートに対して表示されます。

注 一部の SKU ではいくつかのフィールドが表示されない場合があります。

- [ポート]: ポート番号。
- [エネルギー検出]: このポートのエネルギー検出機能の状態。
  - [管理]: エネルギー検出が有効になっているかどうかが表示されます。
  - [動作]: エネルギー検出がローカル ポート上で現在動作しているかどうかが表示されます。これは、有効であるかどうか(管理ステータス)、ローカル ポートで有効であるかどうか、およびローカル ポートで動作しているかどうかを示す機能です。
  - [理由]: エネルギー検出が有効になっているのに動作していない理由が表示されます。

- [ショートリーチ]:このポートのショート リーチ機能の状態。
  - [管理]:ショート リーチが有効になっているかどうかが表示されます。
  - [動作]:ショート リーチがローカル ポート上で現在動作しているかどうかが表示されます。これは、有効であるかどうか(管理ステータス)、ローカル ポートで有効であるかどうか、およびローカル ポートで動作しているかどうかを示す機能です。
  - [理由]:ショート リーチが有効になっているのに動作していない理由が表示されます。
  - [ケーブル長]: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。
  - [管理]:EEE が有効になっているかどうかが表示されます。
  - [動作]: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、有効であるかどうか(管理ステータス)、ローカル ポートで有効であるかどうか、およびローカル ポートで動作しているかどうかを示す機能です。
  - [LLDP管理]:LLDP 経由の EEE カウンタのアドバタイズが有効になっているかどうかが表示されます。
  - [LLDP動作]: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。
  - [リモートでのEEEサポート]:EEE がリンク パラメータ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の両方のリンク パラメータ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、[編集] をクリックします。

ステップ 3 (XG デバイス用のみ) このポートで [エネルギー検出] モードを有効にするか無効にするかを選択します。

ステップ 4 (XG デバイス用のみ)デバイスに GE ポートが搭載されている場合に、このポートで [ショートリーチ] モードを有効にするか無効にするかを選択します。

ステップ 5 このポートで [802.3 Energy Efficient Ethernet (EEE)] モードを有効にするか無効にするかを選択します。

ステップ 6 このポートで [802.3 Energy Efficient Ethernet(EEE)LLDP] モード(LLDP 経由の EEE 機能のアドバタイズメント)を有効にするか無効にするかを選択します。

ステップ 7 [適用] をクリックします。Green Ethernet 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。

11

Smartport

ここでは、Smartport 機能について説明します。

具体的な内容は、次のとおりです。

概要

Smartport 機能を使用すると、必要に応じて共通のコンフィギュレーションを保存して共有できるようになります。同じ Smartport マクロを複数のインターフェイスに適用することで、共通する一連のコンフィギュレーションをインターフェイス間で共有します。Smartport マクロは、CLI（コマンド ライン インターフェイス）コマンドのスクリプトです。

Smartport マクロをインターフェイスに適用する場合には、マクロ名を指定するか、マクロに関連付けられているSmartport タイプを指定します。マクロ名による Smartport マクロの適用は、CLI からのみ実行できます。詳細については、CLI ガイドを参照してください。

Smartport タイプ別に、Smartport マクロをインターフェイスに適用する方法として、次の 2 種類の方法があります。

- **Static Smartport**：ユーザが手動で Smartport タイプをインターフェイスに割り当てます。この操作により、対応する Smartport マクロがインターフェイスに適用されます。
- **Auto Smartport**：Auto Smartport では、インターフェイスにデバイスが接続された時点で、コンフィギュレーションが適用されます。インターフェイスからデバイスが検出されると、接続しているデバイスの Smartport タイプに対応する Smartport マクロ（割り当て済みの場合）が自動的に適用されます。

Smartport 機能はさまざまなコンポーネントで構成され、デバイスの他の機能と連携します。各コンポーネントと機能については、次の項で説明します。

- Smartport、Smartport タイプ、および Smartport マクロについては、この項で説明します。
- 音声 VLAN と Smartport については、「音声 VLAN」で説明します。
- Smartport の LLDP/CDP については、それぞれ「ディスカバリ - LLDP」セクションと「ディスカバリ - CDP」セクションで説明します。

さらに、一般的なワークフローについては、「Smartport の共通タスク」セクションで説明します。

Smartport とは

Smartport は、組み込み（またはユーザ定義）マクロを適用できるインターフェイスです。これらのマクロは、デバイスで通信要件をサポートするための設定作業を省力化するとともに、さまざまなタイプのネットワーク デバイスの機能を活用できるようにするための手段として設計されています。ネットワーク アクセスと QoS の要件は、IP 電話、プリンタ、ルータ、アクセス ポイント（AP）など、インターフェイスの接続先に応じて異なります。

Smartport タイプ

Smartport タイプは、Smartport に接続しているか、接続対象のデバイスのタイプを指します。このデバイスでは、次の Smartport タイプがサポートされています。

- プリンタ
- デスクトップ
- ゲスト

- サーバ
- ホスト
- IP カメラ
- IP 電話
- IP 電話 + デスクトップ
- スイッチ
- ルータ
- ワイヤレス アクセス ポイント

Smartport タイプには、インターフェイスに接続したデバイスのタイプを示す名前が設定されています。Smartport タイプごとに、2 種類の Smartport マクロが用意されています。1 つは、通常のマクロであり、対象のコンフィギュレーションを適用する機能があります。もう 1 つのマクロは、「アンチマクロ」と呼ばれるもので、インターフェイスが別の Smartport タイプに変化したときに、通常のマクロによって実行されたコンフィギュレーションをすべて取り消す機能があります。

次の方法により、Smartport マクロを適用することができます。

- 関連付けられている Smartport タイプを指定する。
- Smartport マクロの名前を静的に指定する。これは CLI からのみ可能です。

Smartport マクロは、CLI と GUI から Smartport タイプを静的に指定して適用することも、Auto Smartport によって自動的に適用することもできます。Auto Smartport では、CDP 機能、LLDP システム機能、および LLDP-MED 機能に基づいて、接続しているデバイスの Smartport タイプが導出されます。

次の表は、Smartport タイプと Auto Smartport の関係を示しています。

Smartport タイプ	Auto Smartport によるサポート	Auto Smartport によるサポート (デフォルト)
不明	いいえ	いいえ
デフォルト	いいえ	いいえ
プリンタ	いいえ	いいえ
デスクトップ	いいえ	いいえ
ゲスト	いいえ	いいえ
サーバ	いいえ	いいえ

Smartport タイプ	Auto Smartport によるサポート	Auto Smartport によるサポート（デフォルト）
ホスト	はい	いいえ
IP カメラ	いいえ	いいえ
IP 電話	はい	はい
IP 電話 + デスクトップ	はい	はい
スイッチ	はい	はい
ルータ	はい	いいえ
ワイヤレス アクセス ポイント	はい	はい

特殊な Smartport タイプ

特殊な Smartport タイプとして、[デフォルト] と [不明] の 2 つがあります。この 2 つのタイプはマクロとは関連付けられていませんが、Smartport に関するインターフェイスの状態を表すために用意されています。

この特殊な Smartport タイプについて、次に説明します。

- **デフォルト**

  Smartport タイプが（まだ）割り当てられていないインターフェイスには、Smartport ステータス [デフォルト] が設定されています。

  Auto Smartport によって Smartport タイプがインターフェイスに割り当てられて、インターフェイスが永続的に Auto Smartport として設定されていない場合は、次の条件に該当すると、Smartport タイプが [デフォルト] に再初期化されます。

  - リンクの停止/稼動を切り替える操作がインターフェイスで実行された。
  - デバイスが再起動された。
  - 指定した時間、デバイスからの CDP および LLDP アドバタイズメントが検出されず、インターフェイスに接続しているデバイスがすべて期限切れ状態になっている。

- **不明**

  Smartport マクロがインターフェイスに適用されて、エラーが発生した場合、インターフェイスにはステータス [不明] が割り当てられます。この場合、Smartport および Auto Smartport 機能は、エラーを修正して、Smartport ステータスをリセットするリセット操作([インターフェイス設定] ページで実行)を適用するまで、インターフェイスに対して機能しません。

  トラブルシューティング時のヒントについては、「Smartport の共通タスク」のワークフロー部分を参照してください。

注 このセクション全体を通して、TTL 経由の LLDP および CDP メッセージの説明で「期限切れ」という用語を使用しています。最新の CDP パケットと LLDP パケットの両方の TTL が 0 に低下する前に、「Auto Smartport が有効」、「永続性ステータスが無効」、「インターフェイスで CDP メッセージと LLDP メッセージがもはや受信されていない」という条件をすべて満たした場合、アンチマクロが実行され、Smartport タイプはデフォルトに戻ります。

Smartport マクロ

Smartport マクロは、特定のネットワーク デバイスに応じてインターフェイスを設定する CLI コマンドのスクリプトです。

Smartport マクロとグローバル マクロを混同しないでください。グローバル マクロはデバイス全体を設定するのに対して、Smartport マクロの適用範囲は対象のインターフェイスに限定されます。

マクロのソースは、CLI の特権 EXEC モードでパーサー マクロ名 [macro_name] 表示コマンドを実行するか、[タイプ設定] ページの [マクロソースの表示] ボタンをクリックすることにより、検索することができます。

マクロと対応するアンチマクロは、ペアで各 Smartport タイプに割り当てられています。マクロはコンフィギュレーションを適用するのに対して、アンチマクロはそのコンフィギュレーションを削除します。

次の 2 つのタイプの Smartport マクロがあります。

- [組み込み]:システムが提供するマクロです。1 つのマクロは設定プロファイルを適用するのに対して、もう一方のマクロはそれを削除します。組み込み Smartport マクロのマクロ名と、関連付けられた Smartport タイプは次のとおりです。
  - macro-name(例:printer)
  - no_macro-name(例:no_printer)

- [ユーザ定義]:ユーザが作成するマクロです。これらの詳細については、『*CLI Reference Guide*』を参照してください。ユーザ定義マクロを Smartport タイプに関連付けるには、アンチマクロも定義されている必要があります。
  - smartport-type-name（例：my_printer）
  - no_smartport-type-name（例：no_my_printer）

Smartport マクロは、[タイプ設定] ページで Smartport タイプにバインドされています。

各デバイス タイプの組み込み Smartport マクロのリストについては、「組み込み Smartport マクロ」を参照してください。

インターフェイスへの Smartport タイプの適用

Smartport タイプがインターフェイスに適用されたときに、関連付けられている Smartport マクロの Smartport タイプとコンフィギュレーションは、実行コンフィギュレーション ファイルに保存されます。管理者が実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルに保存した場合、リブート後、デバイスでは次の要領で、Smartport タイプと Smartport マクロがインターフェイスに適用されます。

- スタートアップ コンフィギュレーション ファイルでインターフェイスの Smartport タイプを指定していない場合、Smartport タイプは [デフォルト] に設定されます。
- スタートアップ コンフィギュレーション ファイルでスタティック Smartport タイプを指定している場合、インターフェイスの Smartport タイプは該当するスタティック タイプに設定されます。
- スタートアップ コンフィギュレーション ファイルで、Auto Smartport によって動的に割り当てられた Smartport タイプを指定している場合
  - Auto Smartport のグローバルな動作状態、インターフェイスの Auto Smartport 状態、永続性ステータスがすべて [有効] の場合、Smartport タイプは該当するダイナミック タイプに設定されます。
  - これ以外の場合、対応するアンチマクロが適用されて、インターフェイスのステータスは [デフォルト] に設定されます。

マクロ エラーとリセット操作

インターフェイスの既存のコンフィギュレーションと Smartport マクロの間に競合がある場合、Smartport マクロでエラーが発生する可能性があります。

Smartport マクロのエラーが発生すると、次のパラメータを含む SYSLOG メッセージが送信されます。

- ポート番号
- Smartport タイプ
- マクロでエラーが発生した CLI コマンドの行番号

Smartport マクロのエラーがインターフェイスで発生した場合、インターフェイスのステータスは [不明] に設定されます。エラーの理由は、[インターフェイス設定] ページの [診断の表示] ポップアップに表示されます。

問題の原因を確認して、既存のコンフィギュレーションまたは Smartport マクロを修正したら、リセット操作を実行し、インターフェイスをリセットしてから、Smartport タイプを再適用 ([インターフェイス設定] ページ) する必要があります。トラブルシューティング時のヒントについては、「Smartport の共通タスク」のワークフロー部分を参照してください。

Smartport 機能の動作

Smartport マクロをインターフェイスに適用する場合には、マクロ名を指定するか、またはマクロに関連付けられている Smartport タイプを指定します。マクロ名を指定することによる Smartport マクロの適用は、CLI からのみ実行できます。詳細については CLI ガイドを参照してください。

CDP と LLDP 経由で検出できないデバイスに対応する Smartport タイプに対してサポートが提供されているので、これらの Smartport タイプは対象のインターフェイスに静的に割り当てる必要があります。具体的には、[インターフェイス設定] ページに移動し、対象のインターフェイスのラジオ ボタンを選択して、[編集] をクリックします。次に、割り当てる Smartport タイプを選択して、必要に応じてパラメータを調整してから、[適用] をクリックします。

Smartport タイプ別に、Smartport マクロをインターフェイスに適用する方法として、次の 2 種類の方法があります。

- **Static Smartport**

  手動で Smartport タイプをインターフェイスに割り当てます。対応する Smartport マクロがインターフェイスに適用されます。[インターフェイス設定] ページから Smartport タイプをインターフェイスに手動で割り当てることができます。

- **Auto Smartport**

  インターフェイスからデバイスが検出されると、接続しているデバイスの Smartport タイプに対応する Smartport マクロ（存在する場合）が自動的に適用されます。Auto Smartport は、デフォルトでグローバルに有効になっています。また、インターフェイス レベルでも有効になっています。

どちらの場合でも、Smartport タイプがインターフェイスから削除されるときには、関連付けられているアンチマクロが実行されます。同様に、アンチマクロの実行により、すべてのインターフェイス コンフィギュレーションが削除されます。

Auto Smartport

Auto Smartport で Smartport タイプをインターフェイスに自動的に割り当てるには、Auto Smartport を設定できるように、Auto Smartport 機能をグローバルに有効にすると同時に、関連するインターフェイスで有効にする必要があります。デフォルトでは、Auto Smartport は有効になっており、すべてのインターフェイスを設定できる状態です。各インターフェイスに割り当てられている Smartport タイプは、それぞれのインターフェイスで受信された CDP および LLDP パケットによって判別されます。

- 複数のデバイスがインターフェイスに接続されている場合、可能であれば、すべてのデバイスに適したコンフィギュレーション プロファイルがインターフェイスに適用されます。
- デバイスが期限切れ（他のデバイスからアドバタイズを受信していない状態）である場合、インターフェイス コンフィギュレーションはその永続性ステータスに従って変更されます。永続性ステータスが有効である場合、インターフェイス コンフィギュレーションは保持されます。有効でない場合、Smartport タイプは [デフォルト] に戻ります。

Auto Smartport の有効化

Auto Smartport は、次の方法により [プロパティ] ページでグローバルに有効にできます。

- [有効]: Auto Smartport を手動で有効にして、すぐに動作状態に移行します。
- [自動音声VLANで有効化]: 自動音声 VLAN が有効で動作している場合に、Auto Smartport を動作可能にします。[自動音声 VLAN ごとに有効にする] がデフォルト設定です。

注 Auto Smartport をグローバルに有効にすることに加えて、Auto Smartport を対象のインターフェイスでも有効にする必要があります。デフォルトでは、Auto Smartport はすべてのインターフェイスで有効になっています。

自動音声 VLAN を有効にする場合の詳細については、「音声 VLAN」を参照してください。

Smartport タイプの識別

Auto Smartport が [プロパティ] ページでグローバルに有効になっていると同時に、インターフェイス ([インターフェイス設定] ページ) で有効になっている場合、デバイスでは、接続しているデバイスの Smartport タイプに基づいて、Smartport マクロがインターフェイスに適用されます。Auto Smartport では、接続しているデバイスからアドバタイズされる CDP および LLDP に基づいて、そのデバイスの Smartport タイプが導出されます。

たとえば、IP 電話をポートに接続した場合、その機能をアドバタイズする CDP または LLDP パケットが送信されます。この CDP および LLDP パケットの受信後、デバイスでは、電話に適した Smartport タイプが導出され、IP 電話が接続されるインターフェイスに、対応する Smartport マクロが適用されます。

永続的な Auto Smartport がインターフェイスで有効になっている場合を除き、接続しているデバイスの期限切れ、リンク ダウン、リブート、または接続されたデバイスが競合機能を受信した場合、その Smartport タイプと、Auto Smartport によって適用されるコンフィギュレーションは削除されます。指定した時間、デバイスから CDP および LLDP のアドバタイズメントが検出されなかった場 合、期限切れとして扱われます。

CDP/LLDP 情報による Smartport タイプの識別

デバイスでは、CDP/LLDP 機能に基づいて、ポートに接続しているデバイスのタイプが検出されます。

次の表はこのマッピングを示しています。

CDP 機能と Smartport タイプのマッピング

機能名	CDP ビット	Smartport タイプ
ルータ	0x01	ルータ
TB ブリッジ	0x02	ワイヤレス アクセス ポイント
SR ブリッジ	0x04	無視
スイッチ	0x08	スイッチ
ホスト	0x10	ホスト
IGMP 条件付きフィルタリング	0x20	無視
リピータ	0x40	無視
VoIP 電話	0x80	ip_phone
リモート管理デバイス	0x100	無視
CAST 電話ポート	0x200	無視
2 ポート MAC リレー	0x400	無視

LLDP 機能と Smartport タイプのマッピング

機能名	LLDP ビット	Smartport タイプ
その他	1	無視
リピータ IETF RFC 2108	2	無視
MAC ブリッジ IEEE 規格802.1D	3	スイッチ
WLAN アクセス ポイント IEEE 規格 802.11 MIB	4	ワイヤレス アクセス ポイント
ルータ IETF RFC 1812	5	ルータ
電話 IETF RFC 4293	6	ip_phone

LLDP 機能と Smartport タイプのマッピング（続き）

機能名	LLDP ビット	Smartport タイプ
DOCSIS ケーブル デバイス IETF RFC 4639 および IETF RFC 4546	7	無視
ステーション専用 IETF RFC 4293	8	ホスト
C-VLAN コンポーネント。VLAN ブリッジ IEEE 規格802.1Q	9	スイッチ
S-VLAN コンポーネント。VLAN ブリッジ IEEE 規格802.1Q	10	スイッチ
2 ポート MAC リレー（TPMR）IEEE 規格 802.1Q	11	無視
予約済み	12-16	無視

注 IP 電話とホストのビットのみが設定されている場合、Smartport タイプは ip_phone_desktop になります。

複数のデバイスをポートに接続している場合

デバイスでは、接続しているデバイスから CDP および LLDP パケットでアドバタイズされている機能に基づいて、そのデバイスの Smartport タイプが導出されます。

複数のデバイスが単一のインターフェイスを介してデバイスに接続されている場合、Auto Smartport では、正しい Smartport タイプを割り当てるため、各機能のアドバタイズメントはそのインターフェイスから受信されたものとして扱われます。この割り当ては、次のアルゴリズムに基づいています。

- インターフェイス上のすべてのデバイスが同じ機能をアドバタイズしている場合（競合が存在しない状況）、一致する Smartport タイプがインターフェイスに適用されます。
- いずれかのデバイスがスイッチである場合、Smartport タイプとして [スイッチ] が使用されます。
- いずれかのデバイスが AP である場合、Smartport タイプとして [ワイヤレスアクセスポイント] が使用されます。
- いずれかのデバイスが IP 電話であり、別のデバイスがホストである場合、Smartport タイプとして ip_phone_desktop が使用されます。

- いずれかのデバイスが IP 電話 + デスクトップであり、別のデバイスが IP 電話またはホストである場合、Smartport タイプとして ip_phone_desktop が使用されます。
- 上記以外のケースでは、Smartport タイプとして [デフォルト] が使用されます。

LLDP/CDP の詳細については、それぞれ「ディスカバリ - LLDP」セクションと「ディスカバリ - CDP」セクションを参照してください。

永続的な Auto Smartport インターフェイス

インターフェイスの永続性ステータスが有効である場合、接続しているデバイスの期限切れ、インターフェイスの停止、およびデバイスのリブートが発生しても、そのインターフェイスの Smartport タイプと、Auto Smartport によって動的に適用済みのコンフィギュレーションは、インターフェイスでそのまま使用されます(コンフィギュレーションは保存されているという前提)。接続しているデバイスに別の Smartport タイプが Auto Smartport で検出される場合を除き、インターフェイスの Smartport タイプとコンフィギュレーションは変更されません。インターフェイスの永続性ステータスが無効である場合、そこに接続しているデバイスの期限切れ、インターフェイスの停止、またはデバイスのリブートが発生すると、インターフェイスの Smartport タイプはデフォルトに戻ります。インターフェイスの永続性ステータスを有効にすると、無効のときに発生していたデバイス検出の遅延は発生しなくなります。

注 インターフェイスに適用されている Smartport タイプの永続性は、インターフェイスに適用された Smartport タイプによる実行コンフィギュレーションがスタートアップコンフィギュレーション ファイルに保存されている場合にのみ、複数回リブートを実行した後でも有効です。

エラー処理

Smartport マクロをインターフェイスに適用する処理でエラーが発生した場合、問題点を [インターフェイス設定] ページで確認し、[インターフェイス設定] ページからエラーを修正した後で、ポートをリセットしてマクロを再適用できます。

デフォルト コンフィギュレーション

Smartport は常に使用可能な状態です。デフォルトでは、Auto Smartport は自動音声 VLAN によって有効になっています。CDP と LLDP の両方に基づいて、接続しているデバイスの Smartport タイプが検出され、Smartport タイプ（IP 電話、IP 電話 + デスクトップ、スイッチ、ワイヤレス アクセス ポイント）が判別されます。

音声の工場出荷時の初期状態の説明については、「音声 VLAN」を参照してください。

他の機能との関係

Auto Smartport はデフォルトで有効になっており、無効にすることができます。テレフォニー OUI は、Auto Smartport および自動音声 VLAN とは同時に使用できません。テレフォニー OUI を有効にする前に、Auto Smarport を無効にしてください。

Smartport の共通タスク

この項では、Smartport および Auto Smartport を設定する際の共通タスクについて説明します。

ワークフロー 1：Auto Smartport をデバイスでグローバルに有効にして、ポートに Auto Smartport を設定するには、次の手順を実行します。

ステップ 1 デバイスで Auto Smartport 機能を有効にするため、[プロパティ] ページを開きます。[管理Auto Smartport] を [有効] または [自動音声VLANで有効化] に設定します。

ステップ 2 デバイスで処理する対象（接続しているデバイスからの CDP および LLDP アドバタイズメント）を選択します。

ステップ 3 [Auto Smartportデバイス検出] フィールドで、検出するデバイスのタイプを選択します。

ステップ 4 [適用] をクリックします。

ステップ 5 Auto Smartport 機能を 1 つまたは複数のインターフェイスで有効にするため、[インターフェイス設定] ページを開きます。

ステップ 6 インターフェイスを選択し、[編集] をクリックします。

ステップ 7 [Smartport適用] フィールドで [Auto Smartport] を選択します。

ステップ 8 必要に応じて、[永続性ステータス] チェックボックスをオンまたはオフにします。

ステップ 9 [適用] をクリックします。

ワークフロー 2：インターフェイスを Static Smartport として設定するには、次の手順を実行します。

ステップ 1 インターフェイス上の Smartport 機能を有効にするため、[インターフェイス設定] ページを開きます。

ステップ 2 インターフェイスを選択し、[編集] をクリックします。

ステップ 3 [Smartport適用] フィールドで、インターフェイスに適用する Smartport タイプを選択します。

ステップ 4 必要に応じて、マクロ パラメータを設定します。

ステップ 5 [適用] をクリックします。

ワークフロー 3：Smartport マクロのパラメータのデフォルト値を調整し、ユーザ定義マクロ ペアを Smartport タイプにバインドするには、次の手順を実行します。

この手順により、次の操作を実行できます。

- マクロ ソースを表示する。
- パラメータのデフォルト値を変更する。
- パラメータのデフォルト値を工場出荷時設定に復元する。
- ユーザ定義マクロ ペア（マクロと、それに対応するアンチマクロ）を、Smartport タイプにバインドします。

ステップ 1 [タイプ設定] ページを開きます。

ステップ 2 [Smartport タイプ] を選択します。

ステップ 3 選択した Smartport タイプに関連付けられている現在の Smartport マクロを表示するため、[マクロ ソースの表示] をクリックします。

ステップ 4 [編集] をクリックし、新しいウィンドウを開きます。このウィンドウで、選択した Smartport タイプにユーザ定義マクロをバインドしたり、その Smartport タイプにバインドされているマクロのパラメータのデフォルト値を変更したりすることができます。各パラメータのデフォルト値は、選択した Smartport タイプ（該当する場合）が Auto Smartport でインターフェイスに適用される場合に使用されます。

ステップ 5 [編集] ページで、フィールドの値を変更します。

ステップ 6 パラメータを変更した場合は、[適用] をクリックしてマクロを返します。

ワークフロー 4:エラーが発生した Smartport マクロを再実行するには、次の手順を実行します。

ステップ 1 [インターフェイス設定] ページで、Smartport タイプが [不明] であるインターフェイスを選択します。

ステップ 2 [診断の表示] をクリックし、問題を確認します。

ステップ 3 トラブルシューティングを実行して、問題を解決します。以下のトラブルシューティングのヒントを検討してください。

ステップ 4 [編集] をクリックします。開いた新しいウィンドウで、[リセット] をクリックし、インターフェイスをリセットします。

ステップ 5 Smartport マクロをインターフェイス上で実行するには、メインページに戻り、[再適用] (スイッチ、ルータ、AP 以外のデバイスの場合) または、[Smartportマクロの再適用] (スイッチ、ルータ、または AP の場合) を使用してマクロを再適用します。

次の方法でも、単一または複数の [不明] インターフェイスをリセットできます。

ステップ 1 [インターフェイス設定] ページで、[ポートタイプが次に等しい] チェックボックスをオンにします。

ステップ 2 [不明] を選択し、[実行] をクリックします。

ステップ 3 [すべての不明な Smartport のリセット] をクリックします。次に、上で説明したようにマクロを再適用します。

ヒント マクロが失敗する原因は、マクロを適用する前のインターフェイスのコンフィギュレーションとの衝突 (ほとんどの場合、セキュリティおよびストーム制御の設定で発生) である場合があります。また、ユーザ定義マクロ内の不適切なポート タイプ、入力ミス、または不適切なコマンド、あるいは、無効なパラメータ設定などが原因である場合もあります。マクロの適用前にパラメータのタイプや範囲はチェックされないので、パラメータに不正な値や無効な値が含まれていると、マクロの適用時に、ほぼ確実にエラーが発生します。

Web ベースのインターフェイスを使用した Smartport の設定

Smartport 機能は、[Smartport] > [プロパティ] の [Smartportタイプ設定] および [インターフェイス設定] ページで設定します。

音声 VLAN の設定については、「音声 VLAN」を参照してください。

LLDP/CDP の設定については、それぞれ「ディスカバリ - LLDP」セクションと「ディスカバリ - CDP」セクションで説明します。

プロパティ

Smartport 機能をグローバルに設定するには、次のようにします。

ステップ 1 [Smartport] > [プロパティ] 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。

- [管理Auto Smartport]: Auto Smartport をグローバルに有効にするか無効にするかを選択します。次のオプションが選択できます。
  - [無効]: デバイスで Auto Smartport を無効にする場合に選択します。
  - [有効]: デバイスで Auto Smartport を有効にする場合に選択します。
  - [自動音声VLANで有効化]: Auto Smartport を有効にしますが、自動音声 VLAN も有効で動作している場合にのみ、Auto Smartport を動作状態に移行します。[自動音声 VLAN ごとに有効にする] がデフォルト設定です。
- [動作Auto Smartport],: Auto Smartport ステータスが表示されます。
- [Auto Smartportデバイス検出方式]: 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、またはこの両方) を選択します。Auto Smartport でデバイスの識別を可能にするため、少なくとも 1 つのタイプを選択する必要があります。
- [動作CDPステータス]: CDP の動作ステータスが表示されます。Auto Smartport で 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、CDP を有効にします。
- [動作LLDPステータス]: LLDP の動作ステータスが表示されます。Auto Smartport で 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、LLDP を有効にします。

- [Auto Smartportデバイス検出]: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 タイプをどのインターフェイスにも割り当てません。

ステップ 3 [適用] をクリックします。この操作により、デバイスでグローバル Smartport パラメータが設定されます。

タイプ設定

[Smartport タイプ設定] ページでは、Smartport タイプ設定の編集や、マクロ ソースの表示を実行できます。

デフォルトでは、各 Smartport タイプは組み込み Smartport マクロのペアと関連付けられています。マクロとアンチマクロの詳細については、「Smartport タイプ」を参照してください。または、自分で作成したユーザ定義マクロ ペアを、Smartport タイプのカスタマイズしたコンフィギュレーションに関連付けることができます。ユーザ定義マクロは、CLI からのみ準備できます。詳細については、『CLI Reference Guide』を参照してください。

組み込みマクロおよびユーザ定義マクロには、パラメータを設定できます。組み込みマクロには、最大 3 つのパラメータを設定できます。

Auto Smartport によって適用された Smartport タイプの各パラメータを [Smartportタイプ設定] ページで編集することで、各パラメータのデフォルト値を設定します。このデフォルト値は、Auto Smartport によって使用されます。

注 Auto Smartport タイプを変更すると、Auto Smartport によってそのタイプが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について、ステータスが [不明] になります。

ステップ 1 [Smartport] > [Smartportタイプ設定] 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 マクロを表示するため、Smartport タイプを選択して、[マクロ ソースの表示] 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 か、ユーザ定義マクロを割り当てるには、Smartport タイプを選択して、[編集] 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。

- [ポートタイプ]:Smartport タイプを選択します。
- [マクロ名]:現在 Smartport タイプに関連付けられている Smartport マクロ名が表示されます。
- [マクロ タイプ]:この Smartport タイプに関連付けられているマクロとアンチマクロのペアが、[組み込みマクロ](組み込み Smartport マクロを参照)か [ユーザ定義マクロ] かを選択します。
- [ユーザ定義マクロ]:必要であれば、選択された Smartport タイプと関連付けられるユーザ定義マクロを選択します。マクロはすでにアンチマクロとペアになっていなければなりません。

  2 つのマクロのペアリングは名前によって実行され、「Smartport マクロ」セクションで説明されています。
- [マクロ パラメータ]:マクロ内の 3 つのパラメータに対して、次のフィールドを表示します。
  - [パラメータ名]:マクロ内のパラメータ名です。
  - [パラメータ値]:マクロ内の現在のパラメータ値です。この値はここで変更することができます。
  - [パラメータの説明]:パラメータの説明です。

ステップ 5 [適用] をクリックし、実行コンフィギュレーションに変更を保存します。Smartport タイプに関連付けられている Smartport マクロおよびそのパラメータ値が変更された場合、Auto Smartport では、Auto Smartport によって現在 Smartport タイプで割り当てられているインターフェイスに、マクロが自動的に適用されます。Auto Smartport では、Smartport タイプが静的に割り当てられたインターフェイスに、変更内容は適用されません。

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、エントリはすべて有効になります。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、パラメータ値が無効な場合、エラーの原因になる可能性があります。

インターフェイス設定

次のタスクを実行するには、[インターフェイス設定] ページを使用します。

- マクロ パラメータのインターフェイス固有の値で、特定の Smartport タイプをインターフェイスに静的に適用する。
- インターフェイスで Auto Smartport を有効にする。
- 適用時にエラーが発生し、Smartport タイプを [不明] に変化させた Smartport マクロを診断する。
- Smartport マクロが失敗した後、すべてのインターフェイスまたは次のタイプのインターフェイスに再適用する。スイッチ、ルータ、および AP。[適用] をクリックする前に、必要な修正を実施しておく必要があります。トラブルシューティング時のヒントについては、「Smartport の共通タスク」のワークフロー部分を参照してください。
- Smartport マクロをインターフェイスに再適用する。環境によっては、Smartport マクロを再適用して、インターフェイスのコンフィギュレーションを最新の状態にできると便利です。たとえば、スイッチの Smartport マクロをデバイスのインターフェイスで再適用すると、そのインターフェイスは、最後のマクロ適用後に作成された VLAN のメンバーになります。再適用によってインターフェイスに影響が現れるかどうか判別するには、デバイスの現在の構成とマクロの定義内容を十分に把握している必要があります。
- [不明] インターフェイスをリセットする。これにより [不明] のインターフェイスのモードをデフォルトに設定します。

Smartport マクロを適用するには、次のようにします。

ステップ 1 [Smartport] > [インターフェイス設定] 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最後の 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クリックします。

- [すべてのスイッチ、ルータ、およびワイヤレスアクセスポート]:すべてのインターフェイスにマクロを再適用します。
- [すべてのスイッチ]:スイッチとして定義されたすべてのインターフェイスにマクロを再適用します。
- [すべてのルータ]:ルータとして定義されたすべてのインターフェイスにマクロを再適用します。

- [すべてのワイヤレスアクセスポート]:アクセス ポイント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。

  特定の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(アップしている必要がある)を選択して [再適用] をクリックし、そのインターフェイスに適用されていた最後のマクロを再適用します。

  [再適用] アクションにより、新しく作成したすべての VLAN にインターフェイスも追加されます。

ステップ 2 Smartport 診断

Smartport マクロのエラーが発生した場合、インターフェイスの Smartport タイプは [不明] になります。タイプが [不明] のインターフェイスを選択して、[診断の表示] をクリックします。この操作により、マクロ適用時のエラーの原因になったコマンドが表示されます。トラブルシューティング時のヒントについては、「Smartport の共通タスク」のワークフロー部分を参照してください。問題を訂正した後、マクロの再適用に進みます。

ステップ 3 すべての [不明] のインターフェイスをデフォルト タイプにリセットします。

- [Smartportタイプが次に等しい] チェックボックスを選択します。
- [不明] を選択します。
- [実行] をクリックします。
- [すべての不明な Smartport のリセット] をクリックします。次に、上で説明したようにマクロを再適用します。これにより、タイプが [不明] のすべてのインターフェイスがリセットされます。つまり、すべてのインターフェイスがデフォルト タイプに戻ります。マクロか現在のインターフェイス コンフィギュレーション、またはこの両方のエラーの修正が終わったら、新しいマクロを適用できます。

注 タイプが [不明] のインターフェイスをリセットしても、エラーが発生したマクロによって実行されたコンフィギュレーションはリセットされません。この場合、手動で消去する必要があります。

Smartport タイプをインターフェイスに割り当てるか、インターフェイスで Auto Smartport をアクティブ化するには、次のようにします。

ステップ 1 インターフェイスを選択し、[編集] をクリックします。

ステップ 2 次のフィールドを入力します。

- [インターフェイス]:ポートまたは LAG を選択します。
- [Smartportタイプ]:ポート/LAG に現在割り当てられている Smartport タイプが表示されます。
- [Smartport適用]:[Smartport適用] プルダウンから Smartport タイプを選択します。
- [Smartport適用方式]:Auto Smartport を選択した場合、Auto Smartport で、接続しているデバイスから受信された 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ると同時に、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て、対応する Smartport マクロをインターフェイスに適用するには、対象の Smartport タイプを選択します。
- [永続性ステータス]:永続性ステータスを有効にする場合、これを選択します。有効にした場合、インターフェイスの停止やデバイスのリブートが発生しても、インターフェイスへの Smartport タイプの関連付けはそのまま使用されます。永続性が適用されるのは、インターフェイスの [Smartport適用] が Auto Smartport である場合に限定されます。インターフェイスで永続性を有効にすると、無効のときに発生していたデバイス検出の遅延は発生しなくなります。
- [マクロ パラメータ]:マクロ内の最大 3 つのパラメータに対して、次のフィールドが表示されます。
  - [パラメータ名]:マクロ内のパラメータ名です。
  - [パラメータ値]:マクロ内の現在のパラメータ値です。この値はここで変更することができます。
  - [パラメータの説明]:パラメータの説明です。

ステップ 3 インターフェイスのステータスが(マクロの適用が成功しなかった結果として)[不明]の場合、そのインターフェイスをデフォルトに設定するには、[リセット] をクリックします。マクロはメインページで再適用することができます。

ステップ 4 変更内容を更新して Smartport タイプをインターフェイスに割り当てるには、[適用] をクリックします。

組み込み Smartport マクロ

各 Smartport タイプの組み込みマクロのペアについて、次に説明します。Smartport タイプごとに、インターフェイスを設定するマクロと、コンフィギュレーションを削除するアンチ マクロが用意されています。

次の Smartport タイプのマクロ コードが提供されています。

- desktop
- printer
- guest
- server
- host
- ip_camera
- ip_phone
- ip_phone_desktop
- switch
- router
- ap

desktop

```
[desktop]
#interface configuration, for increased network security and reliability when
connecting a desktop device, such as a PC, to a switch port.
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
```

```
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

printer

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
#macro key description: $native_vlan: The untag VLAN which will be configured
on the port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
```

```
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

guest

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
```

```
#
spanning-tree portfast
#
@
```

no_guest]]

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

server

```
[server]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                         $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
```

```
spanning-tree portfast
#
@
```

no_server

```
[no_server]
#macro description No server
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
spanning-tree portfast auto
#
@
```

host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                         $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
```

```
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_camera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#Default Values are
#$native_vlan = Default VLAN
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description No ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                          $voice_vlan: The voice VLAN ID
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: The voice VLAN ID
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone_desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: The untag VLAN which will be
configured on the port
#                          $voice_vlan: The voice VLAN ID
#                        $max_hosts: The maximum number of allowed devices on
the port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
```

```
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: The voice VLAN ID
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

switch

```
[switch]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#                        $voice_vlan: The voice VLAN ID
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: The voice VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

router

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
#                        $voice_vlan: The voice VLAN ID
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree link-type point-to-point
#
@
```

no_router

```
[no_router]
#macro description No router
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: The voice VLAN ID
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
```

```
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
no spanning-tree link-type
#
@
```

ap

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: The untag VLAN which will be
configured on the port
```

12

VLAN 管理

ここで説明する内容は次のとおりです。

- 標準 VLAN
- プライベート VLAN 設定
- GVRP 設定
- VLAN グループ
- 音声 VLAN
- アクセス ポート マルチキャスト TV VLAN
- カスタマー ポート マルチキャスト TV VLAN

VLAN は、接続しているブリッジ型ネットワークの物理 LAN セグメントには関係なく、VLAN に関連付けられたデバイスがイーサネット MAC レイヤ上で互いに通信できる、ポートの論理グループです。

VLAN について

各 VLAN には、1 から 4094 の値で一意の VLAN ID（VID）が設定されます。ブリッジ型ネットワーク内のデバイスのポートが、VLAN にデータを送信したり VLAN からデータを受信できる場合、VLAN のメンバーになります。あるポートから VLAN に向かうすべてのパケットに VLAN タグが付いていない場合、そのポートは VLAN のタグなしメンバーになります。あるポートから VLAN に向かうすべてのパケットに VLAN タグが付いている場合、そのポートは VLAN のタグ付きメンバーになります。タグなし VLAN については、1 つのポートは 1 つのタグなし VLAN にしかメンバーとして所属できませんが、タグ付き VLAN については、複数のタグ付き VLAN のメンバーになることができます。

VLAN アクセス モードのポートは 1 つの VLAN のみのメンバーになれます。一般モードまたはトランク モードのポートは、1 つ以上の VLAN のメンバーになれます。

VLAN はセキュリティとスケーラビリティの問題を解決します。VLAN からのトラフィックは VLAN 内で通信され、VLAN 内のデバイスが終端になります。また、これらのデバイスの位置を物理的に変更することなく、デバイスを論理的に接続することにより、ネットワーク構成が簡単になります。

フレームが VLAN タグ付きである場合、4 バイトの VLAN タグが各イーサネット フレームに追加されます。タグには、1 から 4094 までの VLAN ID と、0 から 7 までの VLAN Priority Tag（VPT）が含まれます。VPT の詳細については、「サービス品質」を参照してください。

フレームが VLAN 対応デバイスに到着すると、フレーム内の 4 バイトの VLAN タグに応じて、VLAN に分類されます。

フレームに VLAN タグが含まれていない場合またはフレームが優先タグのみの場合、そのフレームは、受信した入力ポートに設定されている PVID（ポート VLAN 識別子）に基づいて VLAN に分類されます。

入力フィルタリングが有効になっており、入力ポートが、パケットが所属する VLAN のメンバーでない場合、そのフレームは入力ポートで破棄されます。VLAN タグ内の VID が 0 の場合のみ、そのフレームは優先タグ付きと見なされます。

VLAN に所属するフレームはその VLAN 内で通信されます。これは、ターゲット VLAN のメンバーの出力ポートだけにフレームを送信または転送することにより可能になります。出力ポートは、VLAN のタグ付きメンバーにでもタグなしのメンバーにでもなれます。

出力ポートで次のことが行われます。

- 出力ポートがターゲット VLAN のタグ付きメンバーであり、元のフレームに VLAN タグが付いていない場合、フレームに VALN タグを追加します。
- 出力ポートがターゲット VLAN のタグなしメンバーであり、元のフレームに VLAN タグが付いている場合、フレームから VALN タグを削除します。

VLAN の役割

VLAN はレイヤ 2 で動作します。VLAN トラフィック（ユニキャスト、ブロードキャスト、マルチキャスト）はすべてその VLAN 内で通信されます。別の VLAN に接続しているデバイスは、イーサネット MAC レイヤでは直接通信できません。異なる VLAN のデバイスは、レイヤ 3 ルータを介してのみ、相互に通信できます。たとえば、それぞれの VLAN が IP サブネットを表している場合、VLAN 間での IP トラフィックの転送には IP ルータが必要です。

IP ルータが従来型のルータである場合、ルータの各インターフェイスはそれぞれ 1 つの VLAN にのみ接続します。従来型 IP ルータで送受信されるトラフィックは、タグなし VLAN トラフィックでなければなりません。IP ルータが VLAN 対応型のルータである場合、ルータの各インターフェイスはそれぞれ 1 つ以上の VLAN に接続できます。VLAN 対応型 IP ルータで送受信されるトラフィックは、タグ付き VLAN トラフィックでもタグなし VLAN トラフィックでも構いません。

隣接する VLAN 対応デバイスは、Generic VLAN Registration Protocol（GVRP）を使用して、相互の VLAN 情報を交換します。これにより、ブリッジ型ネットワークに VLAN 情報が伝達されます。

デバイス上の VLAN は、デバイスで交換される GVRP 情報に基づいて、静的にも動的にも作成できます。VLAN は、（GVRP に応じて）静的 VLAN か動的 VLAN にできますが、その両方にはできません。GVRP に関する詳細は、「GVRP 設定」を参照してください。

VLAN によっては、別の役割を持つものもあります。

- 音声 VLAN：詳細については、「音声 VLAN」を参照してください。
- ゲスト VLAN：[プロパティ] ページで設定します。
- デフォルト VLAN：VLAN1。

QinQ

Q-in-Q を使用すると、サービス プロバイダー ネットワークとカスタマー ネットワークとを分離できます。デバイスは、ポートベースの C タグ付きサービス インターフェイスをサポートするプロバイダー ブリッジです。

QinQ では、デバイスがサービス タグ（S タグ）と呼ばれる ID タグを追加して、プロバイダー ネットワークにパケットを転送します。S タグは、カスタマー VLAN タグを維持しながら、さまざまなカスタマーの間のトラフィックを分離するために使用されます。

カスタマー トラフィックは、元々 C タグ付きだったかタグなしであったかには関係なく、TPID 0x8100 の S タグを使用してカプセル化されます。S タグがあることで、ブリッジングが S タグ VID（S-VID）のみに基づくプロバイダー ブリッジ ネットワーク内の集約としてこのトラフィックを扱うことができます。

S タグは、トラフィックがネットワーク サービス プロバイダーのインフラストラクチャを経由して転送される間は維持され、その後、出力デバイスによって削除されます。

Q-in-Q には、カスタマーのエッジ デバイスを設定する必要がないという別の利点もあります。

QinQ は [インターフェイス設定] ページで有効にします。

プライベート VLAN

プライベート VLAN 機能は、ポート間でのレイヤ 2 隔離を実現します。これは、IP ルーティングとは対照的に、トラフィックのブリッジングのレベルでは、同一のブロードキャスト ドメインを共有するポートが互いと通信できないことを意味します。プライベート VLAN 内のポートは、レイヤ 2 ネットワーク内の任意の場所に配置できます。つまり、同一のスイッチ上に配置す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ように設計されています。

プライベート VLAN のメンバーになれるのは、次のタイプのポートです。

- **プロミスキャス**:プロミスキャス ポートは、同じプライベート VLAN のすべてのポートと通信できます。これらのポートはサーバおよびルータと接続します。
- **コミュニティ(ホスト)**:コミュニティ ポートは、同じレイヤ 2 ドメイン内のメンバーになっているポートのグループを定義できます。これらは、他のコミュニティや隔離ポートから、レイヤ 2 で隔離されています。これらのポートはホスト ポートに接続します。
- **隔離(ホスト)**:隔離ポートは、同一のプライベート VLAN 内にある他の隔離ポートやコミュニティ ポートとは、レイヤ 2 で完全に隔離されています。これらのポートはホスト ポートに接続します。

次のタイプのプライベート VLAN が存在します。

- **プライマリ VLAN**:プライマリ VLAN は、プロミスキャス ポートから隔離ポートやコミュニティ ポートへのレイヤ 2 接続を可能にするために使用されます。プライマリ VLAN は、プライベート VLAN ごとに 1 つのみ存在できます。
- **隔離 VLAN(セカンダリ VLAN とも呼ばれる)**:隔離 VLAN は、隔離ポートからプライマリ VLAN にトラフィックを送信するために使用されます。隔離 VLAN は、プライベート VLAN ごとに 1 つのみ存在できます。
- **コミュニティ VLAN(セカンダリ VLAN とも呼ばれる)**:VLAN 内にポートのサブグループ(コミュニティ)を作成するには、それらのポートをコミュニティ VLAN に追加する必要があります。コミュニティ VLAN は、コミュニティ ポートからプロミスキャス 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 接続のために使用されます。コミュニティ VLAN はコミュニティごとに 1 つのみ存在でき、同じプライベート VLAN の複数のコミュニティ VLAN がシステムに共存できます。

これらの VLAN の使用例は、図 1 と図 2 でご確認ください。

ホスト トラフィックは隔離 VLAN とコミュニティ VLAN で送信され、サーバ トラフィックやルータ トラフィックはプライマリ VLAN で送信されます。

スイッチでは独立した VLAN 学習がサポートされていますが、同一のプライベート VLAN 内のメンバーであるすべての VLAN の間には、共有 MAC アドレス学習が存在します。ホストの MAC アドレスは隔離 VLAN やコミュニティ VLAN で学習され、ルータとサーバの MAC アドレスはプライマリ VLAN で学習されるにもかかわらず、これが存在することにより、ユニキャスト トラフィックが有効になります。

1 つのプライベート VLAN ポートは、1 つのプライベート VLAN にのみ追加できます。アクセス ポートやトランク ポートなどの他のポート タイプは、プライベート VLAN を構成するそれぞれの VLAN に追加できます（これらは通常の 802.1Q VLAN であるため）。

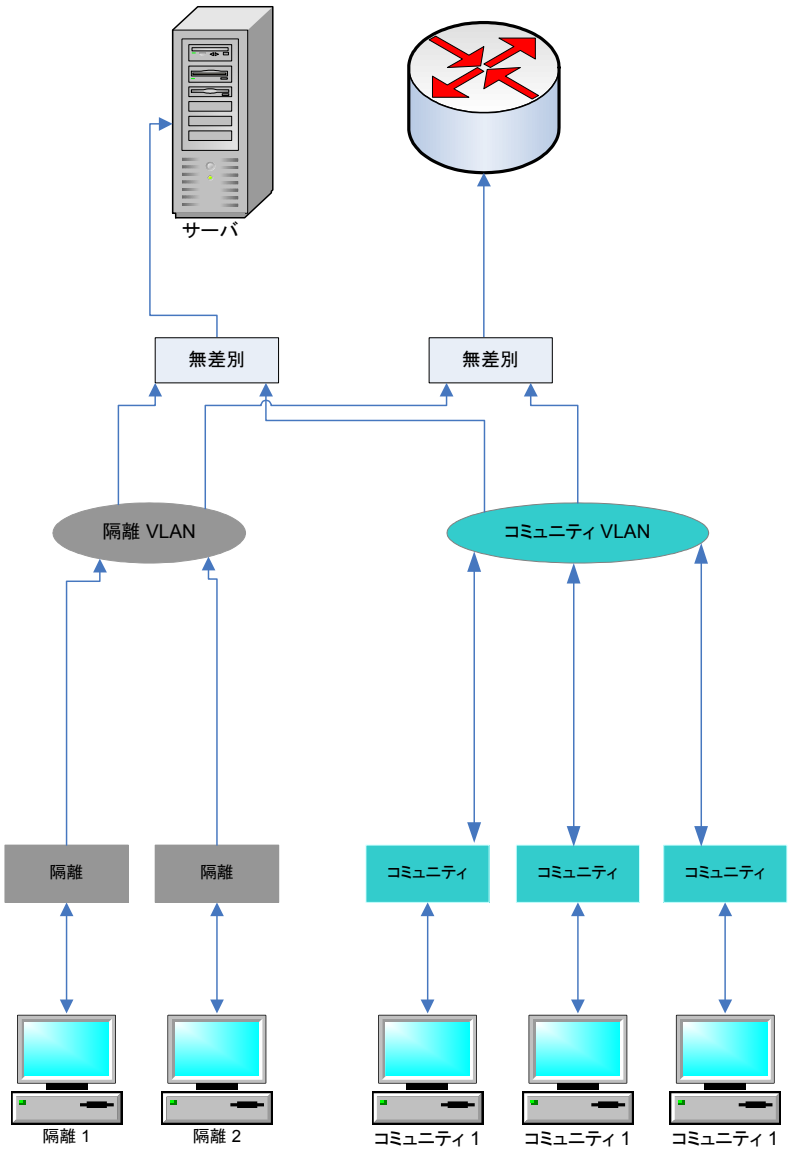
スイッチ間ポートをトランク ポートとして設定し、それらをプライベート VLAN 内のすべての VLAN に追加することにより、プライベート VLAN が複数のスイッチにまたがるように設定できます。スイッチ間トランク ポートは、プライベート VLAN のさまざまな VLAN（プライマリ、隔離、およびコミュニティ）のタグ付きトラフィックを送受信します。

スイッチは、16 個のプライマリ VLAN と 256 個のセカンダリ VLAN をサポートします。

トラフィック フロー

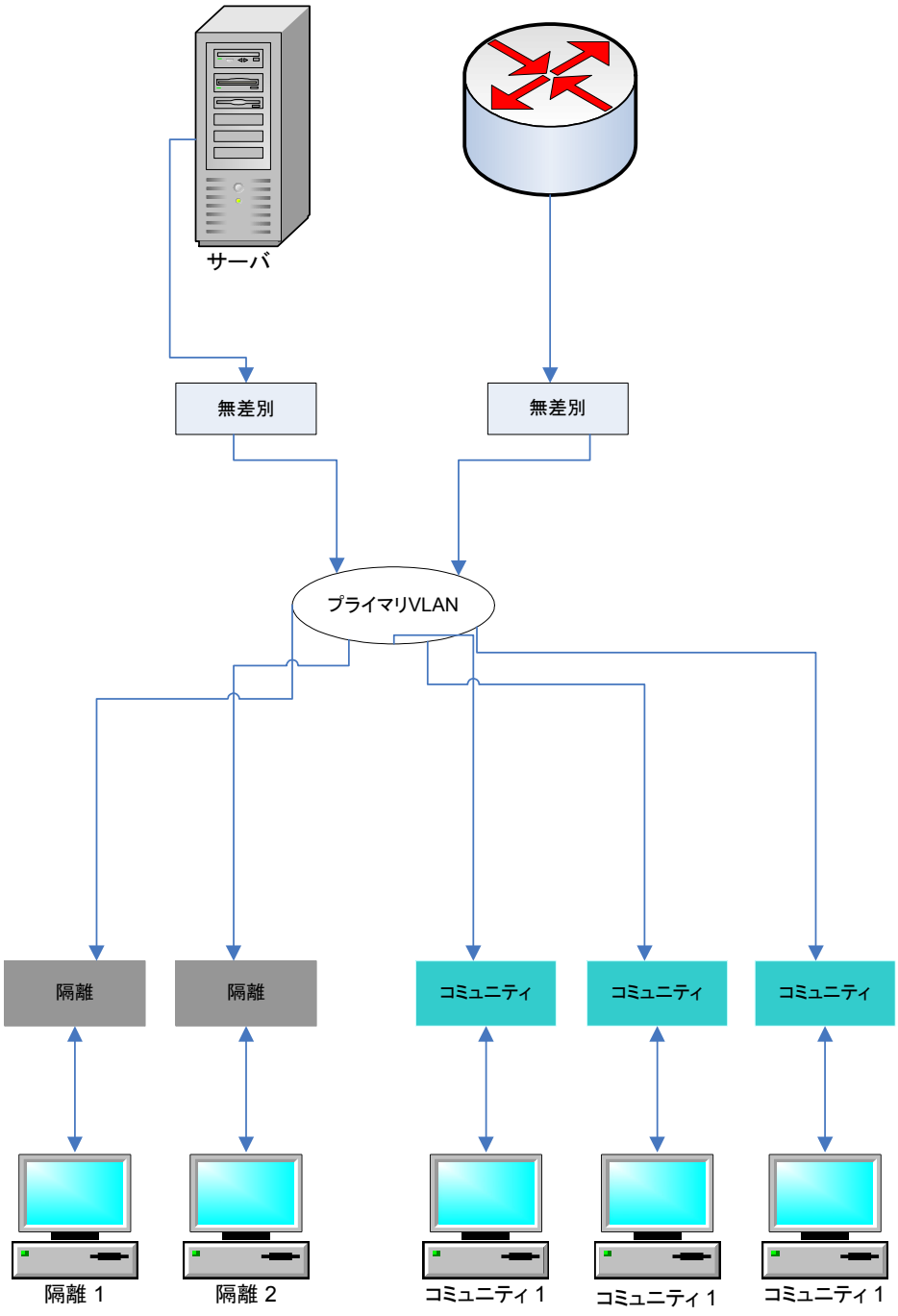
以下は、ホストからサーバやルータ、または他のホストへのトラフィック フローを表しています。

図 1　ホストからサーバやルータへのトラフィック



以下は、サーバやルータのトラフィック（ホストへの応答）を表しています。

図 2　サーバやルータからホストへのトラフィック



他の機能との連携

ここでは、プライベート VLAN と他のシステム機能との間の連携について説明します。

プライベート VLAN でサポートされている機能

次の機能は、プライマリ VLAN でのみ有効にできます（隔離 VLAN やコミュニティ VLAN では有効にできません）。ただし、これらの機能はプライベート VLAN 内のすべての VLAN に影響します。

- IGMP スヌーピングおよび MLD スヌーピング。IGMP レポートとクエリーはプライベート VLAN 内のすべての VLAN で検出されますが、その結果のマルチキャスト エントリはプライマリ VLAN の FDB にのみ追加されます。これは、マルチキャスト トラフィックが転送され、プライマリ VLAN でフラッディングされないようにするためです。隔離 VLAN とコミュニティ VLAN は引き続きマルチキャスト トラフィックをフラッディングします。
- DHCP スヌーピング。
- ARP インスペクション。
- IP ソース ガード。

上述の機能が有効になっているときは、プライベート VLAN に対して、隔離 VLAN やコミュニティ VLAN を追加したり削除したりすることができなくなります。

プライベート VLAN でサポートされていない機能

次の機能は、プライベート VLAN とプライベート VLAN を構成する VLAN のいずれでもサポートされていません。

- 自動音声 VLAN
- デフォルト VLAN
- DHCP リレー
- 802.1x 非認証 VLAN
- ゲスト VLAN
- IPv4 および IPv6。両方ともプライマリ VLAN 上で定義できます。隔離ポートとコミュニティ ポートでは IP 接続が許可されていません。IP 接続の場合、トラフィックをプライマリ VLAN で送信する必要があります。

プライベート VLAN ポート モードでサポートされていない機能

次の機能は、プライベート VLAN ポート モードでサポートされていません。

- GVRP
- 音声 VLAN OUI 自動検出
- 802.1x ポート ゲスト VLAN
- 802.1x ポート ダイナミック VLAN 割り当て
- マルチキャスト TV VLAN。

注 次の分類にご注意ください。

- ポート セキュリティ：VLAN FDB テーブル内の MAC エントリは、ポートのロックの解除時にフラッシュされます。
- 機能連携上の制約に関しては、プライベート VLAN 内のポート メンバーシップは、802.1Q VLAN のポート メンバーシップと同等です。次のような制約があります。
  - ポートを LAG/LACP には追加できません。
  - ポートをポート監視の対象には設定できません。

必要なリソース

プライベート VLAN は複数の 802.1Q VLAN で構成されているため、プライベート VLAN 内のセカンダリ VLAN ごとに、追加のシステム リソースが必要になります。次の機能のリソースは、プライベート VLAN 内の VLAN ごとに割り当てられます。

- **ダイナミック MAC アドレス**：プライマリ VLAN で学習された MAC アドレスは、すべてのコミュニティ VLAN と隔離 VLAN にコピーされます。隔離 VLAN とコミュニティ VLAN で学習された MAC アドレスは、プライマリ VLAN にコピーされます。
- **DHCP スヌーピング**：DHCP トラフィックをトラップするために、TCAM ルールが必要です。
- **ARP インスペクション**：ARP トラフィックをトラップするために、TCAM ルールが必要です。
- **IP ソースガード**：IP トラフィックを転送またはドロップするために、TCAM ルールが必要です。
- **ファースト ホップ セキュリティ**：IPv6 トラフィックをトラップするために、TCAM ルールが必要です（IPv6 ソース ガードが有効な場合）。

設定ガイドライン

次の機能設定ガイドラインを考慮してください。

- **MSTP**:プライベート VLAN 内のすべての VLAN を、同じ MSTP インスタンスに割り当てる必要があります。
- **IP ソース ガード**:IP ソース ガード ポート上の ACL をプライベート VLAN とバインドすることは、TCAM リソースが大量に必要となるため、推奨されていません。

標準 VLAN

ここでは、さまざまなタイプの VLAN を設定する際に使用する GUI ページについて説明します。ここでは、以下について説明します。

- 標準 VLAN の概要
- VLAN 設定
- インターフェイス設定
- VLAN へのポート
- ポート VLAN メンバーシップ
- VLAN 変換
- GVRP 設定
- MAC ベース VLAN グループの概要
- サブネット ベース VLAN グループの概要
- プロトコル ベース VLAN グループの概要

標準 VLAN の概要

VLAN を設定する手順

VLAN を設定するには、次のようにします。

ステップ 1 VLAN 設定の説明に従って、必要な VLAN を作成します。

ステップ 2 「インターフェイス設定」*の説明に従って、ポートの VLAN 関連コンフィギュレーションを設定し、インターフェイスで QinQ を有効にします。*

ステップ 3 「VLAN へのポート」または「ポート VLAN メンバーシップ」の説明に従って、VLAN にインターフェイスを割り当てます。

ステップ 4 「ポート VLAN メンバーシップ」の説明に従って、すべてのインターフェイスの現在の VLAN ポート メンバーシップを確認します。

1. 必要に応じ、「MAC ベース VLAN グループの概要」および「サブネット ベース VLAN グループの概要」の説明に従って、VLAN グループを設定します。
2. 必要に応じ、アクセス ポート マルチキャスト TV VLANおよびカスタマー ポート マルチキャスト TV VLANの説明に従って、TV VLAN を設定します。

デフォルト VLAN 設定

デバイスは自動的に VLAN 1 をデフォルト VLAN として作成し、すべてのポートのデフォルト インターフェイス ステータスが「アクセス」になり、すべてのポートがデフォルト VLAN のタグなしメンバーとして設定されます。

デフォルト VLAN には次の特徴があります。

- デフォルト VLAN は、独立した、スタティックでもダイナミックでもない VLAN で、すべてのポートがタグなしメンバーになります。
- 削除はできません。
- ラベルは指定できません。
- 自動的に、OUI 対応音声 VLAN 用の音声 VLAN として使用されます。
- ポートがどの VLAN のメンバーでもなくなると、デバイスは自動的にそのポートをデフォルト VLAN のタグなしメンバーに設定します。VLAN が削除されたり、ポートが VLAN から削除されると、ポートはその VLAN のメンバーでなくなります。
- RADIUS サーバでは、ダイナミック VLAN 割り当てを使用してデフォルト VLAN を 802.1x サプリカントに割り当てることはできません。

VLAN 設定

VLAN は作成できますが、その VLAN が手動または動的に少なくとも 1 つのポートに接続されるまで有効にはなりません。ポートは必ず 1 つ以上の VLAN に所属している必要があります。

デバイスでは、デフォルト VLAN を含めて、最大 4000 の VLAN をサポートします。

各 VLAN には、1 から 4094 の値で一意の VID を設定する必要があります。VID 4095 はデバイスで廃棄 VLAN として予約されています。廃棄 VLAN に分類されるパケットはすべて入力時に廃棄され、ポートに転送されません。

VLAN を作成するには、次のようにします。

ステップ 1 [VLAN管理] > [VLAN設定] の順にクリックします。

定義済みのすべての VLAN の情報が表示されます。これらのフィールドは、[追加] ページで定義されるものです。次のフィールドは、[追加] ページに表示されません。

- [発信元]: この VLAN の作成方法。
  - [GVRP]: Generic VLAN Registration Protocol（GVRP）によって動的に作成された VLAN。
  - [スタティック]: ユーザ定義の VLAN。
  - [デフォルト]: デフォルト VLAN。

ステップ 2 新しい VLAN を追加するには、[追加] をクリックします。

このページから、1 つの VLAN または複数の VLAN を作成できます。

ステップ 3 VLAN を 1 つだけ作成する場合は、[VLAN] ラジオ ボタンを選択し、[VLAN ID] と、任意で、[VLAN名] を入力します。

複数の VLAN を作成する場合は、[範囲] ラジオ ボタンを選択し、[開始VID] と [終了VID] を入力して、作成する VLAN の範囲を指定します。[範囲] 機能を使用する場合、1 回に作成できる VLAN の最大数は 100 個です。

注 一部の VLAN は、システムが内部的に使用するために必要であり、ユーザが作成または設定することはできません。システムは内部で以下の VLAN を使用する必要があります。

- イーサネット ポートまたはポート チャネル（LAG）上で直接定義された IP インターフェイスごとに 1 つの VLAN。
- IPv6 トンネルごとに 1 つの VLAN。
- 802.1x 用の 1 つの VLAN。

IPv6 トンネル用と 802.1x 用の VLAN は事前に割り当てられるのに対して、イーサネット ポート/ポート チャネルの IP 設定用の VLAN は IP 設定が適用されたときに割り当てられます。内部 VLAN は、最大の空き VLAN（デフォルトは VLAN 4094）から順に割り当てられます。

ステップ 4 新しい VLAN に次のフィールドを追加します。

- [VLANインターフェイス状態]：VLAN をシャットダウンするかどうかを選択します。シャットダウンされた状態の VLAN は、上位レベルとの間でメッセージの送受信を行いません。たとえば、IP インターフェイスが設定されている VLAN をシャットダウンすると、VLAN へのブリッジングは継続されますが、スイッチは VLAN 上で IP トラフィックを送受信できなくなります。
- [リンクステータスSNMPトラップ]：SNMP トラップのリンクステータス生成を有効にするかどうかを選択します。

ステップ 5 VLAN を作成するには、[適用] をクリックします。

インターフェイス設定

[インターフェイス設定] ページでは、すべてのインターフェイスの VLAN 関連パラメータのコンフィギュレーションが表示され、それらの設定を行うことができます。

VLAN 設定を行うには、次のようにします。

ステップ 1 [VLAN管理] > [インターフェイス設定] の順にクリックします。

ステップ 2 S-VLAN タグ用の [グローバル イーサタイプ タギング] 方式を選択します。

- Dot1q-8100
- Dot1ad-88a8
- 9100
- 9200

ステップ 3 インターフェイス タイプ（ポートまたは LAG）を選択し、[実行] をクリックします。ポートまたは LAG とその VLAN パラメータが表示されます。

ステップ 4 ポートまたは LAG を設定するには、ポートまたは LAG を選択して、[編集] 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。

- [インターフェイス]:ポートか LAG を選択します。
- [スイッチポート モード]:レイヤ 2 とレイヤ 3 のどちらかを選択します。
- [インターフェイスVLANモード]:VLAN のインターフェイス モードを選択します。次のオプションがあります。
  - [全般]: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 つ以上の VLAN のタグ付きまたはタグなしメンバーになれます。
  - [アクセス]:インターフェイスは、1 つの VLAN のタグなしメンバーになります。このモードのポートはアクセス ポートと呼ばれます。
  - [トランク]:インターフェイスは、最大 1 つの VLAN のタグなしメンバーと、0 個以上の VLAN のタグ付きメンバーになります。このモードのポートはトランク ポートと呼ばれます。
  - [カスタマー]:このオプションを選択すると、インターフェイスが QinQ モードになります。それにより、ユーザがプロバイダー ネットワーク上で独自の VLAN 配置(PVID)を使用できるようになります。デバイスに 1 つ以上のカスタマー ポートがある場合、デバイスは QinQ モードになります。「QinQ」を参照してください。
  - [プライベートVLAN - ホスト]: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は、これを選択します。その後、[セカンダリVLAN-ホスト] フィールドで [隔離VLAN] と [コミュニティVLAN] のどちらかを選択します。
  - [プライベートVLAN-プロミスキャス]:インターフェイスをプロミスキャスとして設定する場合は、これを選択します。
  - [VLAN マッピング - トンネル]: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 マッピング - ワンツーワン]:インターフェイスを VLAN マッピング ワンツーワン エッジ ポートとして使用するように設定する場合に選択します。
- [イーサタイプ タギング]:S-VLAN タグ用のイーサタイプ タギング方式を選択します(前述の [グローバル イーサタイプ タギング] フィールドを参照)。

- [フレーム タイプ]:(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。設定したフレーム タイプでないフレームは入力時に破棄されます。選択項目は次のとおりです。
  - [すべて通過]:インターフェイスはすべてのフレーム タイプ(タグなしフレーム、タグ付きフレーム、プライオリティ タグ付きフレーム)を受け入れます。
  - [タグ付きのみ通過]:インターフェイスはタグ付きフレームのみを受け入れます。
  - [タグなしのみ通過]:インターフェイスはタグなしフレームとプライオリティ フレームのみ受け入れます。
- [入力フィルタリング]:(一般モードのみ)入力フィルタリングを有効にするには、これを選択します。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。入力フィルタリングは、一般ポートで有効または無効にできます。アクセス ポートとトランク ポートでは常に有効になります。
- [プライマリ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、プロミスキャス ポートから隔離ポートやコミュニティ ポートへのレイヤ 2 接続のために使用されます。[なし] が選択された場合は、インターフェイスがプライベート VLAN モードになりません。
- [セカンダリVLAN-ホスト]:セカンダリ VLAN が 1 つだけ必要なホストの隔離 VLAN またはコミュニティ VLAN を選択します。
- [使用可能なセカンダリ VLAN から、選択されたセカンダリ VLAN へ]:プロミスキャス ポートの場合は、通常のパケット転送に必要なすべてのセカンダリ VLAN を [使用可能なセカンダリ VLAN] から移動します。プロミスキャス ポートとトランク ポートは、複数の VLAN のメンバーにできます。

ステップ 6 [適用] 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。

VLAN 変換

VLAN 変換には、VLAN トンネリング機能と VLAN マッピング ワンツーワン機能が含まれます。

VLAN トンネリングは、QinQ/Nested VLAN/カスタマー モード VLAN 機能の拡張です。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 を所有している顧客をサポートできるようにします。カスタマー VLAN ID を管理しながら、分離された複数のカスタマー VLAN でトラフィックを維持します。通常の 802.1Q タグ（カスタマー VLAN/C-VLAN）に加えて、スイッチがトラフィックをネットワーク経由で転送するためのサービス タグ（S-VLAN）と呼ばれる第 2 の ID タグが追加されることから、「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 にマップされ、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ドロップされます。

フレームが非エッジ タグ付きインターフェイス上で送信される場合は、オリジナルの C-VLAN-ID がマップされた S-VLAN タグの別のレイヤを使用してカプセル化されます。そのため、非エッジ インターフェイス フレーム上で伝送されるパケットは、外側の S-VLAN タグと内側の C-VLAN タグからなる二重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 タグが保持されます。出力デバイスで、フレームがエッジ インターフェイスから送出されるときに S-VLAN タグが除去されます。タグなしフレームはドロップされます。

VLAN トンネリング機能は、オリジナルの QinQ/Nested VLAN 実装とは別のコマンドセットを使用し、オリジナルの実装にはない以下の機能も提供します。

- エッジ インターフェイスごとに異なる C-VLAN と S-VLAN の複数のマッピングを可能にします。
- エッジ インターフェイス上で受信された特定の C-VLAN に対するドロップ アクションを設定できます。
- S-VLAN に明示的にマップされていない C-VLAN に対するアクション（ドロップまたは特定の S-VLAN へのマップ）を設定できます。
- S-VLAN タグのイーサタイプをグローバルにまたは NNI インターフェイス（ネットワーク ノード インターフェイスとバックボーン ポート間）単位で設定できます。以前の QinQ 実装では、S-VLAN タグに対して 0x8100 のイーサタイプのみがサポートされていました。

ユーザによって指定された S-VLAN は、デバイス上で作成してから、インターフェイス上で S-VLAN として設定する必要があります。この VLAN が存在しない場合は、コマンドが失敗します。

IPv4/IPv6 フォワーディングと VLAN トンネリングは相互排他的です。つまり、IPv4 または IPv6 フォワーディングが有効になっている場合は、インターフェイスを VLAN トンネリング モードに設定できません。また、インターフェイスが VLAN トンネリング モードに設定されているデバイス上では、IPv4 または IPv6 フォワーディングを有効にすることができません。

以下の機能も VLAN トンネリング機能と相互排他的です。

- 自動音声 VLAN
- Auto Smartport
- 音声VLAN

IPv4 インターフェイスと IPv6 インターフェイスは、エッジ インターフェイスを含む VLAN 上で定義できません。

以下のレイヤ 2 機能は、エッジ インターフェイスを含む VLAN 上で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

以下のプロトコルは、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）上で有効にすることができません。

- STP
- GVRP

以下の機能は、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）上で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 キーワードを含む宛先ポートとして、またはネットワーク キーワードかリフレクタ ポートを含むリフレクタ ポート宛先ポートとして。

インターフェイス上で VLAN トンネリングを適用するには、ルータ TCAM ルールを使用する必要があります。十分な数のルータ TCAM リソースが存在しない場合は、コマンドが失敗します。ユーザは、[各種管理] > [ルーティング リソース] 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/削除できます（これには、システム リブートが必要です）。

新しい VLAN トンネリングの実装と一緒に、オリジナルの QinQ 実装（カスタマー モード関連コマンド）もそのまま使用できます。カスタマー ポート モードは、VLAN マッピング トンネル ポート モードの特殊なケースであり、TCAM リソースを割り当てる必要がありません。

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 にマップされ、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ドロップされます。

フレームが非エッジ タグ付きインターフェイス上で送信されるときに、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転送されている間は、サービス VLAN タグが保持されます。出力デバイスで、フレームがエッジ インターフェイスに送信されるときに S-VLAN タグが C-VLAN タグに置き換えられます。

VLAN マッピング ワンツーワン 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 PVID は 4095 に設定されます。

VLAN マッピング

VLAN マッピングを設定するには、次のようにします。

ステップ 1 [VLAN 管理] > [VLAN 変換] > [VLAN マッピング] の順にクリックします。

事前に定義された 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 次のマッピング タイプのいずれかを選択します。

- [ワンツーワン]: このオプションは、ワンツーワン 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して編集する場合に選択します。
- [トンネル マッピング]: このオプションは、トンネル VLAN マッピング モードに設定されたインターフェイスの設定を表示して編集する場合に選択します。

ステップ 3 [追加] をクリックして、以下のフィールドに入力します。

- [インターフェイス]: ポートを選択します。
- [インターフェイス VLAN モード]: 現在のインターフェイス モードが表示されます。
- [マッピング タイプ]: 次のいずれかを選択します。
  - [ワンツーワン]: このオプションは、ワンツーワン VLAN マッピング設定を定義する場合に選択します。

- [トンネル マッピング]: このオプションは、トンネル VLAN マッピング設定を定義する場合に選択します。

- [ワンツーワン変換]: このオプションは、[マッピング タイプ] の選択時に [ワンツーワン] オプションが選択された場合に表示されます。次のいずれかを選択します。
  - [ソース VLAN]: S-VLAN（変換済み VLAN）に変換されるカスタマー VLAN（C-VLAN）の ID を設定します。
  - [変換済み VLAN]: 指定された C-VLAN を置き換える S-VLAN を設定します。
- [トンネル マッピング]: このオプションは、[マッピング タイプ] の選択時に [トンネル マッピング] オプションが選択された場合に表示されます。次のいずれかを選択します。
  - [カスタマー VLAN]: 明示的に指定されていない C-VLAN に必要なアクションを定義する場合は [デフォルト] 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 リスト] を選択します。
  - [トンネリング]: [ドロップ] または [外側の VLAN ID] を選択します。[外側の VLAN ID] を選択した場合は、VLAN を入力します。

ステップ 4 [適用] 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。

VLAN へのポート

[VLAN へのポート] ページと [ポート VLAN メンバーシップ] ページには、ポートの VLAN メンバーシップがさまざまな表現で表示されます。VLAN にメンバーシップを追加したり、VLAN からメンバーシップを削除するには、これらのページを使用します。

ポートが、禁止されているデフォルト VLAN メンバーシップを持っている場合、そのポートにその他の VLAN のメンバーシップを設定することはできません。そのポートには内部 VID の 4095 が割り当てられます。

パケットを適切に転送するには、エンド ノード間のパスで VLAN トラフィックを運ぶ VLAN 対応の中間デバイスを手動で設定するか、このデバイスが VLAN とそのポート メンバーシップを Generic VLAN Registration Protocol（GVRP）から学習する必要があります。

2 つの VLAN 対応デバイス間のタグなしポート メンバーシップは、仲介する VLAN 対応デバイスがない場合、同じ VLAN になっている必要があります。つまり、2 つのデバイス間にあるポートの PVID は、そのポートと VLAN 間でタグなしパケットの送受信を行う場合、同じである必要があります。同じになっていない場合、VLAN 間を行き来するトラフィックがリークする可能性があります。

VLAN タグ付きフレームは、VLAN 対応や VLAN 非対応の他のネットワーク デバイスを通過できます。宛先エンド ノードが VLAN 未対応であり、VLAN からのトラフィックを受信する場合、最後の VLAN 対応デバイスが（ある場合）、宛先 VLAN のフレームをタグなしのエンド ノードに送信する必要があります。

特定の VLAN 内のポートを表示して設定するには、[VLANへのポート] ページを使用します。

ポートまたは LAG を VLAN にマップするには、次のようにします。

ステップ 1 [VLAN管理] > [VLANへのポート] の順にクリックします。

ステップ 2 VLAN とインターフェイス タイプ（ポートまたは LAG）を選択し、[実行] をクリックして、ポートの VLAN 関連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 モードに、[インターフェイス設定] ページから設定した現在のポート モード（アクセス、トランク、全般、プライベート - ホスト、プライベート - プロミスキャス、またはカスタマー）が表示されます。

各ポートまたは LAG に、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モード]: VLAN 内のポートのタイプが表示されます。
- [メンバーシップ タイプ]: 次のいずれかのオプションを選択します。
  - [禁止]: 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。ポートがその他の VLAN のメンバーでない場合、ポートに対してこのオプションを有効にすると、このポートは、内部 VLAN 4095（予約 VID）のポートになります。
  - [除外済み]: 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 を新しく作成するとき、これがすべてのポートと LAG のデフォルトになります。
  - [タグ付き]: このインターフェイスは、VLAN のタグ付きメンバーです。
  - [タグなし]: このインターフェイスは、VLAN のタグなしメンバーです。VLAN のフレームはインターフェイス VLAN にタグなしで送信されます。

- [マルチキャスト MTV VLAN]:マルチキャスト IP を使用するデジタル テレビ用のインターフェイス。このポートは、マルチキャスト TV VLAN の VALN タグを使用してこの VLAN に参加します。詳細については、「アクセス ポート マルチキャスト TV VLAN」を参照してください。

- [PVID]:インターフェイスの PVID を VLAN の VID に設定する場合は、これを選択します。PVID はポート単位の設定です。

ステップ 3 [適用] をクリックします。インターフェイスが VLAN に割り当てられ、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。

別の VLAN ID を選択することによって、引き続き、別の VLAN のポート メンバーシップを表示または設定できます。

ポート VLAN メンバーシップ

[ポート VLAN メンバーシップ] ページには、デバイス上のすべてのポートとともに、各ポートが所属する VLAN のリストが表示されます。

インターフェイスのポートベース認証方式が 802.1x であり、[管理ポート制御] が [自動] の場合は、次のようになります。

- ポートは、認証されるまで、ゲスト VLAN および未認証 VLAN を除くすべての VLAN から除外されます。[ポートへのVLAN] ページで、このポートには大文字の P がマークされます。

- ポートは、認証されると、設定された VLAN でメンバーシップを受け取ります。

注 VLAN IS モードがサポートされます。これは、さまざまな VLAN モードのポート VLAN メンバーシップを事前に設定できることを意味します。ポートが特定の VLAN モードになると、コンフィギュレーションがアクティブになります。別のモードに変更すると、変更前のモードの設定が保存され、インターフェイス上でそのモードが再アクティブ化されたときにその設定が再適用されます。

ポートを 1 つ以上の VLAN に割り当てるには、次のようにします。

ステップ 1 [VLAN管理] > [ポートVLANメンバーシップ] の順にクリックします。

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、[実行] をクリックします。選択したタイプのすべての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。

- [LAG]:ポート ID または LAG ID。

- [モード]:[インターフェイス設定] ページで選択されたインターフェイス VLAN モード。

- [管理 VLAN]:インターフェイスがメンバーになる可能性のあるすべての VLAN を表示するドロップダウン リスト。
- [動作 VLAN]:インターフェイスが現在メンバーになっているすべての VLAN を表示するドロップダウン リスト。
- [LAG]:選択したインターフェイスが [ポート] 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、[VLANへの参加] 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。

- [インターフェイス]:ポートか LAG を選択します。
- [現在の VLAN モード]:[インターフェイス設定] ページで選択したポート VLAN モードが表示されます。
- [アクセス モード メンバーシップ(アクティブ)]
  - [アクセス VLAN ID]:ポートがアクセス 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。
  - [マルチキャストTV VLAN]:ポートがアクセス 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。
- [トランク モード メンバーシップ]
  - [ネイティブ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。
  - [タグ付き VLAN]: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。次のオプションが選択できます。

    [すべての VLAN]: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。

    [ユーザ定義]: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。
- [一般モード メンバーシップ]
  - [タグなし VLAN]: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。
  - [タグ付き VLAN]: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。

- [禁止VLAN]: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。ポートがその他の VLAN のメンバーでない場合、ポートに対してこのオプションを有効にすると、このポートは、内部 VLAN 4095(予約 VID)のポートになります。
- [一般 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。

• [カスタマー モード メンバーシップ]

- [カスタマー 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。
- [カスタマーマルチキャストVLAN]:ポートがカスタマー モードになっている場合は、このマルチキャスト TV VLAN のメンバーになります。

ステップ 5 ポートを選択して、[詳細] をクリックし、次のフィールドを表示します。

• [管理 VLAN]:ポートはこれらの VLAN 用に設定されます。
• [動作 VLAN]:ポートは現在これらの VLAN のメンバーです。

ステップ 6 [適用] をクリックします([VLANへの参加] の場合)。設定が修正され、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。

プライベート VLAN 設定

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

新しいプライベート VLAN を作成するには、次のようにします。

ステップ 1 [VLAN管理] > [プライベートVLAN設定] の順にクリックします。

ステップ 2 [追加] ボタンをクリックします。

ステップ 3 次のフィールドに値を入力します。

• [プライマリVLAN ID]:プライベート VLAN 内のプライマリ VLAN として定義する VLAN を選択します。プライマリ VLAN は、プロミスキャス ポートから隔離ポートやコミュニティ ポートへのレイヤ 2 接続のために使用されます。
• [隔離VLAN]:隔離 VLAN は、隔離ポートからプライマリ VLAN にトラフィックを送信するために使用されます。

- [使用可能なコミュニティ VLAN]:コミュニティ VLAN にする VLAN を [選択されたコミュニティ VLAN] リストに移動します。コミュニティ VLAN は、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 接続のために使用されます。メイン ページでは、[コミュニティVLAN範囲] と表示されます。

ステップ 4 [適用] をクリックします。設定が修正され、実行コンフィギュレーション ファイルに書き込まれます。

GVRP 設定

隣接する VLAN 対応デバイスは、Generic VLAN Registration Protocol(GVRP)を使用して、相互に VLAN 情報を交換できます。GVRP は Generic Attribute Registration Protocol(GARP)に基づいており、ブリッジ型ネットワークに VLAN 情報を伝達します。

インターフェイスで GVRP を有効にするには、全般モードで設定する必要があります。

GVRP を使用してポートが VLAN に参加すると、[ポート VLAN メンバーシップ] ページで明示的に禁止されていない限り、このポートはタグ付きダイナミック メンバーとしてその VLAN に追加されます。VLAN が存在しない場合、([GVRP 設定] ページで)このポートに対して [ダイナミック VLAN 作成] が有効にされていれば、VLAN が動的に作成されます。

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。有効化されると、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非アクティブな VLAN の情報は伝達されません。VLAN 情報を伝達するには、その VLAN が少なくとも 1 つのポート上でアクティブである必要があります。

デフォルトで、GVRP はグローバルにもポートでも無効です。

GVRP 設定

インターフェイスの GVRP 設定を定義するには、次のようにします。

ステップ 1 [VLAN管理] > [GVRP設定] の順にクリックします。

ステップ 2 GVRP をグローバルに有効にするために、[GVRPグローバルステータス] を選択します。

ステップ 3 [適用] をクリックし、グローバルな GVRP のステータスを設定します。

ステップ 4 インターフェイス タイプ(ポートまたは LAG)を選択し、[実行] をクリックして、そのタイプのインターフェイスをすべて表示します。

ステップ 5 ポートの GVRP 設定を定義するために、ポートを選択し、[編集] をクリックします。

ステップ 6 次のフィールドに値を入力します。

- [インターフェイス]:編集するインターフェイス(ポートまたは LAG)を選択します。
- [GVRP状態]:このインターフェイス上で GVRP を有効にすることを選択して指定します。
- [ダイナミックVLAN作成]:このインターフェイス上でのダイナミック VLAN 作成を有効にすることを選択して指定します。
- [GVRP登録]:このインターフェイス上で GVRP を使用した VLAN 登録を有効にすることを選択して指定します。

ステップ 7 [適用] 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

ここでは、VLAN グループの設定方法を説明します。また、次の機能についても説明します。

- MAC ベース VLAN グループの概要
- プロトコル ベース VLAN グループの概要
- サブネット ベース VLAN グループの概要

VLAN グループは、レイヤ 2 ネットワーク上のトラフィックのロード バランシングのために使用されます。

パケットは、さまざまな分類に基づいて VLAN に割り当てられます。

いくつかの分類スキームが定義されている場合、パケットは次の順序に従って VLAN に割り当てられます。

- [タグ]:パケットにタグが付いている場合、VLAN はタグに基づいて決定されます。
- [MACベースVLAN]:MAC ベース VLAN が定義されている場合、VLAN は入力インターフェイスの送信元 MAC から VLAN へのマッピングに基づいて決定されます。

- [サブネットベースVLAN]:サブネットベース 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 へのマッピングに基づいて決定されます。
- [プロトコルベース VLAN]:プロトコルベース VLAN が定義されている場合、VLAN は入力インターフェイスの(イーサネットタイプの)プロトコルから VLAN へのマッピングに基づいて決定されます。
- [PVID]:VLAN はポートのデフォルト VLAN ID に基づいて決定されます。

MAC ベース VLAN グループの概要

MAC ベースの VLAN 分類を使用すると、パケットを送信元 MAC アドレスに基づいて分類できます。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。

各々に異なる MAC アドレスが含まれた複数の MAC ベース VLAN グループを定義することができます。

これらの MAC ベース グループを、特定のポートや LAG に割り当てることができます。MAC ベース VLAN グループには、同じポート上の重複する範囲の MAC アドレスを含めることはできません。

ワークフロー

MAC ベース VLAN グループを定義するには、次のようにします。

1. [MAC ベース グループ] ページを使用して、MAC アドレスを VLAN グループ ID に割り当てます。
2. 必要な各インターフェイスについて、次のことを行います。
   a. [VLAN に対する MAC ベース グループ] ページを使用して、VLAN グループを VLAN に割り当てます。インターフェイスは全般モードである必要があります。
   b. インターフェイスが VLAN に所属していない場合は、[VLAN へのポート] ページを使用して手動で VLAN に割り当てます。

MAC ベース グループ

この機能が使用できるかどうかについては、「表 1」を参照してください。

MAC アドレスを VLAN グループに割り当てるには、次のようにします。

ステップ 1 [VLAN管理] > [VLANグループ] > [MACベースグループ] の順にクリックします。

ステップ 2 [追加] 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アドレス]:VLAN グループに割り当てる MAC アドレスを入力します。

  注 この 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。

- [プレフィックス マスク]:次のいずれかを入力します。
  - [ホスト(48)]:MAC アドレスのすべてのビットをプレフィックス マスク(48 ビット)に含める場合
  - [長さ]:MAC アドレスのプレフィックス
- [グループID]:ユーザが作成した VLAN グループ ID 番号を入力します。

ステップ 4 [適用] 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

この機能が使用できるかどうかについては、「表 1」を参照してください。

ポートと LAG は全般モードである必要があります。

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、次のようにします。

ステップ 1 [VLAN管理] > [VLANグループ] > [VLANに対するMACベースグループ] の順にクリックします。

ステップ 2 [追加] 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。

- [グループタイプ]:グループが MAC ベースであることが表示されます。
- [インターフェイス]:トラフィックの受信経路となる一般インターフェイス(ポートまたは LAG)を入力します。

- [グループID]:[MAC ベース VLAN グループの概要] ページで定義した VLAN グループを選択します。
- [VLAN ID]:VLAN グループから受信したトラフィックの転送先 VLAN を選択します。

ステップ 4 [適用] をクリックして、VLAN に対する VLAN グループのマッピングを設定します。このマッピングでは、インターフェイスは VLAN に動的にバインドされません。インターフェイスは手動で VLAN に追加する必要があります。

サブネット ベース VLAN グループの概要

サブネット ベース グループ VLAN 分類を使用すれば、パケットをそのサブネットに基づいて分類することができます。その場合は、インターフェイスごとにサブネットと VLAN のマッピングを定義できます。

グループごとにサブネットが異なる複数のサブネット ベース VLAN グループを定義することができます。

これらのグループを特定のポート/LAG に割り当てることができます。サブネットベース VLAN グループには、同じポート上の範囲が重複しているサブネットを含めることができません。

ワークフロー

サブネット ベース VLAN グループを定義するには、次のようにします。

1. [サブネット ベース グループ] ページを使用して、サブネット ベース グループを定義します。
2. [VLAN に対するサブネット ベース グループ] ページを使用して、必要なインターフェイスごとに、サブネット ベース グループを VLAN に割り当てます。インターフェイスにダイナミック VLAN(DVA)を割り当てることはできません。IS モードでは、デバイスが全般モードでなくても、設定を保存して、後でアクティブにすることができます。

   注 インターフェイスが VLAN に所属していない場合は、[VLANへのポート] ページを使用して手動で VLAN に割り当てます。そうでない場合は、サブネット ベース グループと VLAN 間の設定が有効になりません。

3. DVA とサブネット ベース グループ間の制限はありません。

サブネット ベース グループ

サブネット ベース グループを追加するには、次のようにします。

ステップ 1 [VLAN管理] > [VLANグループ] > [サブネットベースグループ] の順にクリックします。

ステップ 2 [追加] ボタンをクリックします。

ステップ 3 次のフィールドを入力します。

- [IPアドレス]: サブグループが基づく IP アドレスを入力します。
- [プレフィックス マスク]: サブネットを定義するプレフィックス マスクを入力します。
- [グループID]: グループ ID を入力します。

ステップ 4 [適用] 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(インターフェイス設定を参照)。

いくつかのグループを単一のポートにバインドし、各ポートはそれぞれ独自の VLAN に関連付けることができます。

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。

サブネット ポートを VLAN にマップするには、次のようにします。

ステップ 1 [VLAN管理] > [VLANグループ]VLAN > [VLANに対するサブネットベースグループ] の順にクリックします。

定義済みのマッピングが表示されます。

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、[追加] をクリックします。

[グループタイプ] フィールドに、マッピングされているグループのタイプが表示されます。

ステップ 3 次のフィールドを入力します。

- [インターフェイス]:プロトコルベース グループに従って VLAN に割り当てられているポートまたは LAG の番号。
- [グループ ID]:プロトコル グループ ID。
- [VLAN ID]:このインターフェイスに対して指定されたグループをユーザ定義の VLAN ID に対応付けます。

ステップ 4 [適用] をクリックします。サブネット ベース グループ 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 VLAN グループの概要

プロトコルのグループを定義し、ポートにバインドすることができます。プロトコル グループがポートにバインドされると、そのグループ内のプロトコルが発信元となっている各パケットは、[プロトコルベースグループ] ページで設定されている VLAN に割り当てられます。

ワークフロー

プロトコル ベース VLAN グループを定義するには、次のようにします。

1. [プロトコルベースグループ] ページを使用して、プロトコル グループを定義します。
2. [VLAN に対するプロトコル ベース グループ] ページを使用して、必要なインターフェイスごとに、プロトコル グループを VLAN に割り当てます。インターフェイスは全般モードである必要があります。また、そのインターフェイスにダイナミック VLAN(DVA)を割り当てることはできません。

プロトコルベースグループ

プロトコルのセットを定義するには、次のようにします。

ステップ 1 [VLAN管理] > [VLANグループ] > [プロトコルベースグループ] の順にクリックします。

[プロトコルベースグループ] ページには次のフィールドが含まれています。

- [カプセル化]:VLAN グループの基になっているプロトコルが表示されます。
- [プロトコル値(16 進)]:プロトコル値が 16 進形式で表示されます。
- [グループ ID]:インターフェイスの追加先となるプロトコル グループ ID が表示されます。

ステップ 2 [追加] ボタンをクリックします。

ステップ 3 次のフィールドを入力します。

- [カプセル化]:プロトコル パケット タイプ。次のオプションが選択できます。
  - [Ethernet V2]:これを選択した場合は [イーサネットタイプ] を選択します。
  - [LLC-SNAP(rfc1042)]:これを選択した場合は [プロトコル値] を入力します。
  - [LLC]:これを選択した場合は [DSAP-SSAP 値] を選択します。
- [イーサネット タイプ]:Ethernet V2 カプセル化のイーサネット タイプを選択します。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。
- [プロトコル値]:LLC-SNAP(rfc 1042)カプセル化のプロトコルを入力します。
- [グループ ID]:プロトコル グループ ID を入力します。

ステップ 4 [適用] 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 グループをポートにマッピングするには、ポートが全般モードであることが必要です。また、そのポート上に DVA を設定することはできません(「インターフェイス設定」を参照)。

いくつかのグループを単一のポートにバインドし、各ポートはそれぞれ独自の VLAN に関連付けることができます。

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 にマップするには、次のようにします。

ステップ 1 [VLAN管理] > [VLANグループ] > [VLANに対するプロトコルベースグループ] の順にクリックします。

定義済みのマッピングが表示されます。

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、[追加] をクリックします。

[グループタイプ] フィールドに、マッピングされているグループのタイプが表示されます。

ステップ　3　次のフィールドを入力します。

- [インターフェイス]:プロトコルベース グループに従って VLAN に割り当てられているポートまたは LAG の番号。
- [グループ ID]:プロトコル グループ ID。
- [VLAN ID]:インターフェイスがユーザ定義 VLAN ID に関連付けられます。

ステップ　4　[適用] 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。

音声 VLAN

LAN では、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は、同じ VLAN 内に配置されます。この VLAN は、音声 VLAN と呼ばれます。音声デバイスが別々の音声 VLAN 内にある場合、通信を行うには IP(レイヤ 3)ルータが必要です。

ここで説明する内容は次のとおりです。

- 音声 VLAN の概要
- 音声 VLAN 設定
- テレフォニー OUI

音声 VLAN の概要

ここで説明する内容は次のとおりです。

- ダイナミック音声 VLAN モード
- 自動音声 VLAN、Auto Smartport、CDP、および LLDP
- 音声 VLAN の QoS
- 音声 VLAN の制限事項
- 音声 VLAN のワークフロー

適切な設定を使用した典型的な音声展開シナリオは、次のとおりです。

- **UC3xx/UC5xx がホストされている場合:**すべてのシスコ製電話および VoIP エンドポイントがこの展開モデルに対応しています。このモデルの場合、UC3xx/UC5xx、シスコ製電話機、および VoIP エンドポイントは、同じ音声 VLAN 内にあります。UC3xx/UC5xx のデフォルト音声 VLAN は VLAN 100 です。
- **サードパーティ製 IP PBX がホストされている場合:**Cisco SBTG CP-79xx、SPA5xx 電話機、および SPA8800 エンドポイントがこの展開モデルに対応しています。このモデルの場合、電話機で使用される VLAN は、ネットワーク構成によって決まります。音声とデータの VLAN は別々の場合も同じ場合もあります。電話機と VoIP エンドポイントは、構内 IP PBX に登録されます。
- **IP Centrex/ITSP がホストされている場合:**Cisco CP-79xx、SPA5xx 電話機、および SPA8800 エンドポイントがこの展開モデルに対応しています。このモデルの場合、電話機で使用される VLAN は、ネットワーク構成によって決まります。音声とデータの VLAN は別々の場合も同じ場合もあります。電話機と VoIP エンドポイントは、「クラウド」内の構外 SIP プロキシに登録されます。

VLAN の観点からすると、上記のモデルは VLAN 対応環境および VLAN 非対応環境の両方で動作します。VLAN 対応環境で、音声 VLAN は設置時に設定された多くの VLAN のうちのいずれかです。VLAN 非対応環境でのシナリオは、VLAN が 1 つだけの VLAN 対応環境と同等です。

デバイスは VLAN 対応スイッチとして常に動作します。

デバイスは、単一の音声 VLAN をサポートします。デフォルトで、音声 VLAN は VLAN 1 です。音声 VLAN のデフォルトは、VLAN 1 です。手動で別の音声 VLAN に設定できます。また、自動音声 VLAN が有効な場合は、動的に学習することもできます。

ポートを音声 VLAN に手動で追加するには、「VLAN インターフェイスの設定」の説明に従って基本 VLAN コンフィギュレーションを使用するか、音声関連の Smartport マクロをポートに手動で適用します。デバイスがテレフォニー OUI モードの場合、または Auto Smartport が有効な場合は、動的にポートを追加することもできます。

ダイナミック音声 VLAN モード

デバイスは 2 種類のダイナミック音声 VLAN モードをサポートしています。それは、テレフォニー OUI（組織固有識別子）モード、および自動音声 VLAN モードです。これら 2 つのモードは、音声 VLAN や音声 VLAN ポート メンバーシップの構成に影響を与えます。2 つのモードは相互に排他的です。

- **テレフォニー OUI**

  テレフォニー OUI モードでは、音声 VLAN は手動設定の VLAN である必要があり、デフォルト VLAN に設定することはできません。

  デバイスがテレフォニー OUI モードで、ポートが音声 VLAN への参加候補として手動で設定される場合、送信元 MAC アドレスが設定済みテレフォニー OUI のいずれかと一致するパケットをデバイスが受信すると、デバイスはこのポートを音声 VLAN に動的に追加します。OUI は、イーサネット MAC アドレスの先頭 3 バイトです。テレフォニー OUI の詳細については、「テレフォニー OUI」を参照してください。

- **自動音声 VLAN**

  自動音声 VLAN モードでは、音声 VLAN はデフォルト音声 VLAN、手動構成、外部デバイス（UC3xx/5xx など）からの学習結果、または CDP や VSDP で音声 VLAN をアドバタイズするスイッチからの学習結果のいずれかを使用できます。VSDP は、音声サービスのディスカバリ用に Cisco で定義されたプロトコルです。

  テレフォニー OUI モードではテレフォニー OUI に基づいて音声デバイスを検出しますが、自動音声 VLAN モードはそれとは異なり、Auto Smartport に基づいてポートを音声 VLAN に動的に追加します。Auto Smartport が有効な場合、CDP や LLDP-MED を介して電話またはメディア エンドポイントとしてアドバタイズするポートに接続されたデバイスを検出すると、そのポートを音声 VLAN に追加します。

音声エンドポイント

音声 VLAN が適切に機能するには、シスコ製電話や VoIP エンドポイントなどの音声デバイスが音声トラフィックを送受信する音声 VLAN に割り当てられている必要があります。たとえば次のシナリオが考えられます。

- 電話やエンドポイントは、音声 VLAN で静的に構成されています。
- 電話やエンドポイントは、TFTP サーバからダウンロードするブート ファイルで音声 VLAN を取得できます。DHCP サーバでは、IP アドレスを電話に割り当てるときにブート ファイルと TFTP サーバを指定できます。
- 電話機やエンドポイントは、ネイバーの音声システムおよびスイッチから受け取る CDP および LLDP-MED のアドバタイズメントから音声 VLAN の情報を取得できます。

デバイスは、接続する音声デバイスが音声 VLAN のタグ付きパケットを送信することを前提とします。音声 VLAN がネイティブ VLAN でもあるポートでは、音声 VLAN のタグなしパケットも使用可能です。

自動音声 VLAN、Auto Smartport、CDP、および LLDP

デフォルト

工場出荷時のデフォルトにより、CDP、LLDP、LLDP-MED、Auto Smartport モード、および信頼できる DSCP による基本 QoS が有効になります。すべてのポートは、デフォルトの音声 VLAN であるデフォルトの VLAN 1 のメンバーです。

音声 VLAN のトリガー

[ダイナミック音声VLAN] のモードが [自動音声VLANの有効化] に設定されている場合、1 つ以上のトリガーが発生した場合に限り、自動音声 VLAN が動作状態になります。トリガーになりうるものとしては、スタティック音声 VLAN コンフィギュレーション、ネイバー CDP アドバタイズメントで受信した音声 VLAN 情報、Voice VLAN Discovery Protocol (VSDP) で受信した音声 VLAN 情報などがあります。必要に応じて、トリガーを待機せず、直ちに自動音声 VLAN モードを動作させることもできます。

Auto Smartport が有効である場合、自動音声 VLAN モードに従い、自動音声 VLAN が動作状態になると Auto Smartport が有効になります。必要に応じて、自動音声 VLAN とは無関係に動作するよう Auto Smartport を設定できます。

注 ここに示すデフォルト コンフィギュレーション リストは、出荷時に自動音声 VLAN をサポートしているファームウェア バージョンを使用するスイッチに適用されます。また、自動音声 VLAN をサポートするファームウェア バージョンにアップグレードした、未構成のスイッチにも適用されます。

注 デフォルトおよび音声 VLAN トリガーは、音声 VLAN を含まないインストールや、設定済みのスイッチには影響しないように設計されています。自動音声 VLAN や Auto Smartport は、必要に応じて展開に合わせて手動で無効や有効にすることができます。

自動音声 VLAN

自動音声 VLAN は音声 VLAN の維持を行いますが、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。

- 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 の情報を検出します。
- 複数のネイバー スイッチやルータ（シスコ ユニファイド コミュニケーション（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。

  注 デバイスを Cisco UC デバイスに接続するには、UC デバイスがポートの CDP で音声 VLAN をアドバタイズするように、*`switchport voice vlan`* コマンドを使用して UC デバイスのポートを設定することが必要になる場合があります。

- 音声 VLAN 関連パラメータは、Voice VLAN Discovery Protocol（VSDP; 音声 VLAN 検出プロトコル）を使用して他の自動音声 VLAN 対応スイッチと同期されます。デバイス自体は、常に、認識されているプライオリティの最も高いソースからの音声 VLAN を使用して構成されます。プライオリティは、音声 VLAN 情報を提供するソースのソース タイプおよび MAC アドレスに基づきます。ソース タイプのプライオリティは、高いほうから順に、静的 VLAN コンフィギュレーション、CDP アドバタイズメント、変更されたデフォルト VLAN に基づくデフォルト コンフィギュレーション、デフォルト音声 VLAN です。数値の小さい MAC アドレスのほうが数値の大きい MAC アドレスよりもプライオリティが高くなります。
- 音声 VLAN は、プライオリティがさらに高いソースからの新しい音声 VLAN が検出されるか、自動音声 VLAN がユーザによって再起動されるまで維持されます。再起動されると、デバイスは音声 VLAN をデフォルト音声 VLAN にリセットし、自動音声 VLAN 検出を再起動します。
- 新しい音声 VLAN が設定されるか検出されると、デバイスはその音声 VLAN を自動作成し、既存の音声 VLAN のポート メンバーシップすべてを新しい音声 VLAN に置き換えます。これにより、既存の音声セッションが中断または終了することがあります。ネットワーク トポロジが変更されたと見なされるためです。

  注 デバイスは、同じ管理 VLAN 内とデバイスで設定された直接接続 IP サブネット内の VSDP 対応スイッチと同期できます。

Auto Smartport は CDP/LLDP を使用して、ポートから音声エンドポイントが検出されたときにも音声 VLAN のポート メンバーシップを維持します。

- CDP および LLDP が有効な場合、デバイスは CDP パケットと LLDP パケットを定期的に送信して、使用する音声 VLAN を音声エンドポイントにアドバタイズします。
- ポートに接続しているデバイスが CDP や LLDP を使用して自身を音声エンドポイントとしてアドバタイズすると、Auto Smartport により対応する Smartport マクロがポートに適用され、ポートが音声 VLAN に自動的に追加されます（競合する機能や優れた機能をアドバタイズするポートからのデバイスが他にない場合）。デバイスが自身を電話としてアドバタイズする場合、デフォルト Smartport マクロは phone です。デバイスが自身を電話およびホスト、または電話およびブリッジとしてアドバタイズする場合、デフォルト Smartport マクロは phone+desktop です。

音声 VLAN の QoS

音声 VLAN は、LLDP-MED ネットワーク ポリシーを使用して CoS/802.1p 設定や DSCP 設定を伝達できます。LLDP-MED のデフォルトでは、アプライアンスが LLDP-MED パケットを送信する場合に、音声 QoS 設定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は、LLDP-MED 応答で受け取った CoS/802.1p 値および DSCP 値と同じ値を使用して音声トラフィックを送信します。

ユーザは、音声 VLAN と LLDP-MED の間の自動更新を無効にしたり、独自のネットワーク ポリシーを使用したりできます。

OUI モードでは、デバイスで OUI に基づく音声トラフィックのマッピングおよびリマーキング（CoS/802.1p）を追加設定できます。

デフォルトでは、すべてのインターフェイスが CoS/802.1p 信頼モードです。デバイスは、音声ストリームで見つかった CoS/802.1p 値に基づいてサービス品質を適用します。自動音声 VLAN では、拡張 QoS を使用して、音声ストリームの値をオーバーライドできます。テレフォニー OUI 音声ストリームでは、サービス品質をオーバーライドできるのに加え、必要に応じて音声ストリームの 802.1p をリマークできます。これは [テレフォニー OUI] で希望の CoS/802.1p 値を指定したり、リマーキング オプションを使用したりすることにより、これを実行できます。

音声 VLAN の制限事項

次のような制限事項があります。

- 音声 VLAN は 1 つしかサポートされません。
- 音声 VLAN として定義された VLAN は削除できません。

テレフォニー OUI の場合は、さらに次の制限事項が適用されます。

- 音声 VLAN は Smartport を有効にできません。
- 音声 VLAN は DVA（ダイナミック VLAN 割り当て）をサポートできません。
- 音声 VLAN のモードが [OUI] の場合、音声 VLAN をゲスト VLAN には指定できません。音声 VLAN のモードが [自動] の場合は、音声 VLAN をゲスト VLAN に指定できます。
- 音声 VLAN の QoS 決定は、ポリシー/ACL QoS 決定以外のその他の QoS 決定より優先されます。
- 現在の音声 VLAN に候補ポートがない場合のみ、新しい VLAN ID を音声 VLAN に設定できます。
- 候補ポートのインターフェイス VLAN は、一般モードまたはトランク モードである必要があります。

- 音声 VLAN の QoS は、音声 VLAN に参加している候補ポートとスタティックポートに適用されます。
- 音声フローは、転送データベース（FDB）がその MAC アドレスを学習できる場合に受け入れられます。（FDB に空きスペースがない場合、アクションは発生しません）。

音声 VLAN のワークフロー

自動音声 VLAN、Auto Smartport、CDP、および LLDP のデバイス デフォルト設定は、大半の音声展開シナリオに対応します。ここでは、デフォルト コンフィギュレーションが適用されないときに音声 VLAN を展開する方法について説明します。

ワークフロー 1: 自動音声 VLAN を設定するには、次のようにします。

ステップ 1 [音声 VLAN プロパティ] ページを開きます。

ステップ 2 音声 VLAN ID を選択します。VLAN ID 1 には設定できません（ダイナミック音声 VLAN の場合、この手順は必要ありません）。

ステップ 3 [ダイナミック音声VLAN] を [自動音声VLANの有効化] に設定します。

ステップ 4 [自動音声VLANアクティブ化] の方式を選択します。

注 現在、デバイスがテレフォニー OUI モードの場合は、無効にしてから自動音声 VLAN を設定する必要があります。

ステップ 5 [適用] をクリックします。

ステップ 6 「Smartport の共通タスク」の項の説明に従って、Smartport を設定します。

ステップ 7 「ディスカバリ - LLDP」および「ディスカバリ - CDP」の説明に従って、LLDP/CDP を設定します。

ステップ 8 [インターフェイス設定] ページで、適切なポートの Smartport 機能を有効にします。

注 手順 7 および手順 8 は、デフォルトで有効な設定です。必要に応じて設定してください。

ワークフロー 2:テレフォニー OUI 方式を設定するには、次のようにします。

ステップ 1 [VLAN管理] > [音声VLAN] > [プロパティ] ページを開きます。[ダイナミック音声 VLAN] を [テレフォニーOUIの有効化] に設定します。

注 現在、デバイスが自動音声 VLAN モードの場合は、無効にしてからテレフォニー OUI を有効にする必要があります。

ステップ 2 [テレフォニー OUI テーブル] ページでテレフォニー OUI を設定します。

ステップ 3 [テレフォニー OUI インターフェイス] ページで、ポートの [テレフォニー OUI VLAN メンバーシップ] を設定します。

音声 VLAN 設定

ここでは、音声 VLAN の設定方法について説明します。具体的な内容は、次のとおりです。

- 音声 VLAN プロパティ
- 自動音声 VLAN 設定
- テレフォニー OUI

音声 VLAN プロパティ

音声 VLAN の [プロパティ] ページで次の操作を行います。

- 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 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 がトリガーされる方法を設定します。

音声 VLAN プロパティを表示して設定するには、次のようにします。

ステップ 1 [VLAN管理] > [音声VLAN] > [プロパティ]の順にクリックします。

- デバイスで設定された音声 VLAN 設定は、[音声VLAN設定] の [管理ステータス] ブロックに表示されます。
- 音声 VLAN 展開に実際に適用されている音声 VLAN 設定は、[音声VLAN設定] の [動作ステータス] ブロックに表示されます。

ステップ 2 次の [管理ステータス] フィールドに値を入力します。

- [音声VLAN ID]: 音声 VLAN にする VLAN を入力します。

  注 音声 VLAN ID、CoS/802.1p、DSCP のすべてまたはいずれかを変更すると、デバイスは、管理音声 VLAN をスタティック音声 VLAN としてアドバタイズします。外部音声 VLAN によってトリガーされる [自動音声VLANアクティブ化] オプションを選択した場合は、デフォルト値のままにしておく必要があります。

- [CoS/802.1p]: 音声ネットワーク ポリシーとして LLDP-MED で使用される CoS/802.1p 値を選択します。詳細については、[各種管理] > [ディスカバリ] > [LLDP] > [LLDP MEDネットワークポリシー] をご覧ください。
- [DSCP]: 音声ネットワーク ポリシーとして LLDP-MED で使用される DSCP 値を選択します。詳細については、[各種管理] > [ディスカバリ] > [LLDP] > [LLDP MEDネットワークポリシー] をご覧ください。

次の [動作ステータス] フィールドが表示されます。

- [音声VLAN ID]: 音声 VLAN。
- [CoS/802.1p]: 音声ネットワーク ポリシーとして LLDP-MED で使用される値。詳細については、[各種管理] > [ディスカバリ] > [LLDP] > [LLDP MEDネットワークポリシー] をご覧ください。
- [DSCP]: 音声ネットワーク ポリシーとして LLDP-MED で使用される値。

次の [ダイナミック音声VLAN設定] フィールドが表示されます。

- [ダイナミック音声 VLAN]: 次のいずれかの方法で音声 VLAN 機能を無効または有効にするにはこのフィールドを選択します。
  - [自動音声VLANの有効化]: ダイナミック音声 VLAN を自動音声 VLAN モードで有効にします。
  - [テレフォニーOUIの有効化]: ダイナミック音声 VLAN をテレフォニー OUI モードで有効にします。
  - [無効]: 自動音声 VLAN またはテレフォニー OUI を無効にします。

- [自動音声 VLAN のアクティブ化]: 自動音声 VLAN が有効な場合は、自動音声 VLAN をアクティブ化するためのオプションを次の中から選択します。
  - [即時]: 有効にすると、デバイスでただちに自動音声 VLAN がアクティブになり、動作状態になります。
  - [外部音声VLANトリガーを使用]: 音声 VLAN をアドバタイズするデバイスをデバイスが検出した場合にのみ、デバイス上の自動音声 VLAN がアクティブになり、動作状態になります。

  注 音声 VLAN ID、CoS/802.1p、DSCP のすべてまたはいずれかを手動でデフォルト値から再設定すると、外部ソースから学習した自動音声 VLAN よりもプライオリティが高いスタティック音声 VLAN になります。

ステップ 3 [適用] をクリックします。VLAN のプロパティは、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。

自動音声 VLAN 設定

自動音声 VLAN モードが有効な場合は、[自動音声 VLAN] ページを使用して、関連のグローバル パラメータおよびインターフェイス パラメータを表示します。

このページの [自動音声VLANの再起動] をクリックして、自動音声 VLAN を手動で再起動することもできます。少し待った後、音声 VLAN はデフォルト音声 VLAN にリセットされ、LAN 内の自動音声 VLAN 対応スイッチすべてで自動音声 VLAN 検出および同期化プロセスが再起動します。

注 [ソースタイプ] が [非アクティブ] の状態の場合、音声 VLAN をデフォルトの音声 VLAN にリセットする処理のみが実行されます。

自動音声 VLAN パラメータを表示するには、次のようにします。

ステップ 1 [VLAN管理] > [音声VLAN] > [自動音声VLAN] の順にクリックします。

このページの [動作状態] 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 が有効かどうかが表示されます。
- [音声VLAN ID]: 現在の音声 VLAN の ID。
- [ソース タイプ]: 音声 VLAN がルート デバイスによって検出されたソースのタイプを表示します。
- [CoS/802.1p]: 音声ネットワーク ポリシーとして LLDP-MED で使用される CoS/802.1p 値が表示されます。

- [DSCP]:音声ネットワーク ポリシーとして LLDP-MED で使用される DSCP 値が表示されます。
- [ルートスイッチMACアドレス]:自動音声 VLAN のルート デバイスの MAC アドレス。自動音声 VLAN ルート デバイスは、この音声 VLAN を検出している、またはこの音声 VLAN が設定されているデバイスであり、この音声 VLAN の学習元のデバイスです。
- [スイッチ MAC アドレス]: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] である場合、そのデバイスは自動音声 VLAN ルート デバイスです。
- [音声 VLAN ID 変更時間]:音声 VLAN の最終更新時刻。

ステップ 2 [自動音声VLANの再起動] をクリックして、音声 VLAN をデフォルト音声 VLAN にリセットし、LAN 内の自動音声 VLAN 対応スイッチすべてで自動音声 VLAN 検出を再起動します。

[音声VLANローカルソーステーブル] 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。次のフィールドが含まれています。

- [インターフェイス]:音声 VLAN 設定が受信または設定されたインターフェイスを表示します。[N/A] が表示される場合、その設定はデバイスそれ自体で行われています。インターフェイスが表示される場合、音声設定がネイバーから受信されています。
- [送信元 MAC アドレス]:音声設定の受信元 UC の MAC アドレス。
- [ソース タイプ]:音声設定の受信元 UC のタイプ。次のオプションが選択できます。
  - [デフォルト]:デバイスのデフォルト音声 VLAN 設定。
  - [スタティック]:デバイス上に定義されている、ユーザ定義の音声 VLAN 設定。
  - [CDP]:音声 VLAN 設定をアドバタイズした UC は、CDP を実行しています。
  - [LLDP]:音声 VLAN 設定をアドバタイズした UC は、LLDP を実行しています。
  - [音声 VLAN ID]:アドバタイズまたは設定された音声 VLAN の ID。
- [音声 VLAN ID]:現在の音声 VLAN の ID。
- [CoS/802.1p]:音声ネットワーク ポリシーとして LLDP-MED で使用される、アドバタイズまたは設定された CoS/802.1p 値。

- [DSCP]: 音声ネットワーク ポリシーとして LLDP-MED で使用される、アドバタイズまたは設定された DSCP 値。
- [最適なローカルソース]: この音声 VLAN がデバイスによって使用されたかどうかが表示されます。次のオプションが選択できます。
  - [はい]: デバイスはこの音声 VLAN を使用して他の自動音声 VLAN 対応スイッチと同期化します。この音声 VLAN は、よりプライオリティの高いソースが検出されない限り、ネットワークの音声 VLAN として機能します。ベスト ローカル ソースになるローカル ソースは 1 つだけです。
  - [いいえ]: 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 [更新] をクリックして、ページの情報を更新します。

テレフォニー OUI

OUI は、Institute of Electrical and Electronics Engineers, Incorporated（IEEE; 電気電子学会）登録機関により割り当てられます。IP 電話製造元数には制限があり、既知のものなので、既知の OUI 値を使用すると、関連フレームおよびそのフレームを受信するポートは自動的に音声 VLAN に割り当てられます。

OUI グローバル テーブルには最大 128 OUI まで格納できます。

ここで説明する内容は次のとおりです。

- テレフォニー OUI テーブル
- テレフォニー OUI インターフェイス

テレフォニー OUI テーブル

[テレフォニーOUI] ページで、テレフォニー OUI の QoS プロパティを設定します。また、自動メンバーシップ エージング タイムを設定することもできます。テレフォニー アクティビティがないまま指定した時間が経過すると、ポートは音声 VLAN から削除されます。

[テレフォニー OUI] ページを使用して、既存の OUI を表示し、新しい OUI を追加します。

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、次のようにします。

ステップ 1 [VLAN管理] > [音声VLAN] > [テレフォニーOUI]の順にクリックします。

[テレフォニーOUI] ページには、次のフィールドが含まれています。

- [テレフォニーOUIの動作ステータス]:OUI が音声トラフィックの識別に使用されているかどうかを表示します。
- [CoS/802.1p]:音声トラフィックに割り当てる CoS キューを選択します。
- [CoS/802.1p の再マーキング]:出力トラフィックを再マーキングするかどうかを選択します。
- [自動メンバーシップ エージング タイム]:ポートで検出された電話の MAC アドレスすべてが期限切れになった後、音声 VLAN からそのポートを削除するまでの遅延時間を入力します。

ステップ 2 [適用] をクリックし、これらの値でデバイスの実行コンフィギュレーションを更新します。

[テレフォニーOUIテーブル] が表示されます。

- [テレフォニー OUI]:OUI 用に予約されている MAC アドレスの先頭 6 桁。
- [説明]:ユーザが割り当てた OUI の説明。

ステップ 3 [デフォルトOUIの復元] をクリックすると、ユーザが作成した 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。復元が完了するまでは、OUI 情報が正確でない場合があります。復元には数秒かかる場合があります。数秒後に、このページを閉じてから開き直して、ページを更新します。

OUI をすべて削除するには、一番上のチェックボックスを選択します。すべての OUI が選択されるので、[削除] をクリックすると、すべて削除できます。その後で、[デフォルトOUIの復元] をクリックすると、システムが既知の OUI を復元します。

ステップ 4 OUI を新規に追加するには、[追加] をクリックします。

ステップ 5 次のフィールドに値を入力します。

- [テレフォニー OUI]:新しい OUI を入力します。
- [説明]:OUI の名前を入力します。

ステップ 6 [適用] 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

QoS アトリビュートは、次のいずれかのモードで、音声パケットにポートごとに割り当てられます。

- [すべて]: そのインターフェイスで受信され、音声 VLAN に分類されるすべての着信フレームに、その音声 VLAN に設定されているサービス品質（QoS）値が適用されます。
- [テレフォニー送信元MACアドレス]: 音声 VLAN に分類され、設定済みテレフォニー OUI と一致する送信元 MAC アドレスに OUI が含まれている着信フレームに、その音声 VLAN 用に設定されている QoS 値が適用されます。

[テレフォニーOUIインターフェイス] ページを使用して、OUI ID 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、次のようにします。

ステップ 1 [VLAN管理] > [音声VLAN] > [テレフォニーOUIインターフェイス]の順にクリックします。

[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 パラメータが含まれています。

ステップ 2 テレフォニー OUI ベースの音声 VLAN の候補ポートとしてインターフェイスを設定するには、[編集] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [インターフェイス]: インターフェイスを選択します。
- [テレフォニー OUI VLAN メンバーシップ]: 有効にすると、そのインターフェイスがテレフォニー OUI ベースの音声 VLAN の候補ポートになります。設定済みテレフォニー OUI のいずれかと一致するパケットが受信されると、ポートは音声 VLAN に追加されます。
- [音声VLAN QoSモード]（メイン ページの [テレフォニーOUI QoSモード]）: 次のオプションのいずれかを選択します。
  - [すべて]: この音声 VLAN に分類されるすべてのパケットに QoS 属性が適用されます。
  - [テレフォニー送信元 MAC アドレス]: IP 電話からのパケットのみに QoS 属性が適用されます。

ステップ 4 [適用] をクリックします。OUI が追加されます。

アクセス ポート マルチキャスト TV VLAN

マルチキャスト TV VLAN では、同じデータ VLAN 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、各サブスクライバ VLAN に対して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。

同じデータ VLAN 上に存在せず（レイヤ 2 隔離）、別の VLAN ID メンバーシップを使用してデバイスに接続しているサブスクライバが、同じマルチキャスト ストリームを共有できます。これは、ポートを同じマルチキャスト VLAN ID に参加させることにより、実現できます。

マルチキャスト サーバに接続するネットワーク ポートは、マルチキャスト VLAN ID のメンバーとして静的に設定されます。

IGMP メッセージを送信することにより、サブスクライバを介してマルチキャスト サーバと通信するネットワーク ポートは、マルチキャスト サーバからマルチキャスト ストリームを受信します。このとき、マルチキャスト パケットのヘッダーにマルチキャスト TV VLAN を含めます。このため、ネットワーク ポートは次のように静的に設定する必要があります。

- トランクまたは一般ポート タイプ（「インターフェイス設定」を参照）
- マルチキャスト TV VLAN のメンバー

サブスクライバ受信ポートは、アクセス ポートとして定義されている場合のみ、マルチキャスト TV VLAN に関連付けることができます。

1 つ以上の IP マルチキャスト アドレス グループを同一のマルチキャスト TV VLAN に関連付けることができます。

任意の VLAN をマルチキャスト 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、次の特徴を持ちます。

- 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、タグなしパケットです。
- ポートのフレーム タイプ パラメータは [すべて通過] に設定され、タグなしパケットが許可されます（「インターフェイス設定」を参照）。

マルチキャスト TV VLAN 設定はポートごとに定義されます。カスタマー ポートは、[ポート マルチキャスト VLAN メンバーシップ] 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。

IGMP スヌーピング

マルチキャスト TV VLAN は、ポート上で設定された IGMP スヌーピングに依存します。

- サブスクライバは IGMP メッセージを使用して、マルチキャスト グループに参加したりグループから脱退したりします。
- デバイスは IGMP スヌーピングを実行し、マルチキャスト TV VLAN 上のマルチキャスト メンバーシップに従ってアクセス ポートを設定します。

デバイスは、アクセス ポートで受信する各 IGMP パケットに関して、そのパケットをアクセス VLAN に関連付けるかマルチキャスト TV VLAN に関連付けるかを、次のルールで決定します。

- IGMP メッセージをアクセス ポートで受信し、そのメッセージの宛先マルチキャスト IP アドレスがポートのマルチキャスト TV VLAN に関連している場合、その IGMP パケットは、ソフトウェアによりマルチキャスト TV VLAN に関連付けられます。
- それ以外の場合は、IGMP メッセージはアクセス VLAN に関連付けられ、その IGMP メッセージは VLAN 内でのみ転送されます。
- 次の場合、IGMP メッセージは廃棄されます。
  - アクセス ポートの STP/RSTP 状態が [廃棄] に設定されている。
  - アクセス VLAN の MSTP 状態が [廃棄] に設定されている。
  - マルチキャスト TV VLAN の MSTP 状態が [廃棄] に設定されており、IGMP メッセージがこのマルチキャスト TV VLAN に関連付けられている。

標準 VLAN とマルチキャスト TV VLAN の相違点

表 1　標準 VLAN とマルチキャスト TV VLAN の特徴

	標準 VLAN	マルチキャスト TV VLAN
VLAN メンバーシップ	送信元ポートとすべての受信ポートは、同一のデータ VLAN 内の静的メンバーである必要があります。	送信元ポートと受信ポートを同一のデータ VLAN 内のメンバーにすることはできません。

	標準 VLAN	マルチキャスト TV VLAN
グループ登録	マルチキャスト グループの登録はすべて動的に行われます。	グループはマルチキャスト VLAN に静的に関連付ける必要がありますが、ステーションの実際の登録は動的に行われます。
受信ポート	VLAN は、トラフィックの送信と受信のどちらにも使用できます(マルチキャストとユニキャスト両方)。	マルチキャスト VLAN は、ポートのステーションでトラフィックを受信するためにのみ使用できます(マルチキャストのみ)。
セキュリティと隔離	同じマルチキャスト ストリームの受信者は、同一のデータ VLAN 上に存在しており、相互に通信できます	同じマルチキャスト ストリームの受信者は、異なるアクセス VLAN に存在しており、相互に隔離されています

コンフィギュレーション

次の手順で TV VLAN を設定します。

1. 1 つ以上のマルチキャスト グループまたはグループ範囲を VLAN に関連付けることにより、TV VLAN を定義します([VLAN に対するマルチキャスト グループ] ページを使用)。
2. [ポート マルチキャスト VLAN メンバーシップ] ページで、各マルチキャスト VLAN にアクセス ポートを指定します。

VLAN に対するマルチキャスト グループ

最大 256 の IPv4 アドレス範囲を 1 つのマルチキャスト TV VLAN にマップすることができます。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。

マルチキャスト TV VLAN 設定を定義するには、次のようにします。

ステップ 1 [VLAN管理] > [アクセスポートマルチキャストTV VLAN] > [VLANに対するマルチキャストグループ] の順にクリックします。

次のフィールドが表示されます。

- [マルチキャスト TV VLAN]: マルチキャストパケットの割り当て先 VLAN。
- [マルチキャスト グループの先頭]: マルチキャスト グループの最初の IP アドレス。
- [グループの最後]: マルチキャスト グループ範囲の最後の IPv4 アドレス。
- [グループ サイズ]: 最初のマルチキャスト グループ範囲に含まれるアドレスの数。

ステップ 2 [追加] 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 を選択できます。

次のフィールドを入力します。

- [マルチキャスト TV VLAN]: マルチキャストパケットの割り当て先 VLAN。ここで選択された VLAN がマルチキャスト TV VLAN になります。
- [マルチキャスト グループの先頭]: マルチキャスト グループ範囲の最初の IPv4 アドレス。
- [グループ定義]: 次の範囲オプションのいずれかを選択します。
  - [グループ サイズ指定]: グループ範囲に含まれるマルチキャスト アドレスの数を指定します。

- [範囲指定]:[マルチキャスト グループの先頭] フィールド内のアドレスより大きい IPv4 マルチキャスト アドレスを指定します。これが範囲内の最後のアドレスになります。

ステップ 3 [適用] 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 VLAN メンバーシップ

マルチキャスト TV VLAN 設定を定義するには、次のようにします。

ステップ 1 [VLAN管理] > [アクセスポートマルチキャストTV VLAN] > [ポートマルチキャストVLANメンバーシップ] の順にクリックします。

ステップ 2 [マルチキャストTV VLAN] から VLAN を選択します。

ステップ 3 [インターフェイス タイプ] からインターフェイスを選択します。

ステップ 4 [候補アクセスポート] リストに、そのデバイス上に設定されているすべてのアクセスポートが表示されます。必要なポートを [メンバー アクセス ポート] フィールドに移動します。

ステップ 5 [適用] 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 サービスは、単一のブロードバンド接続で 3 種類のブロードバンド サービスをプロビジョニングします。

- 高速インターネット アクセス
- ビデオ
- 音声

トリプル プレイ サービスは、サービス プロバイダーのサブスクライバ向けにプロビジョニングされており、サブスクライバ間にはレイヤ 2 隔離が維持されます。

各サブスクライバに CPE MUX ボックスが用意されています。MUX には、サブスクライバのデバイス（PC や電話など）に接続された複数のアクセス ポートと、アクセス デバイスに接続されたネットワークポートが 1 つあります。

このボックスは、ネットワーク ポートで受信したパケットを、パケットの VLAN タグに基づいてサブスクライバのデバイスに転送します。各 VLAN は、MUX アクセス ポートのいずれかにマッピングされます。

サブスクライバからサービス プロバイダー ネットワークへのパケットは、サービス タイプを区別するために VLAN タグ付きフレームとして転送されます。つまり、それぞれのサービス タイプごとに一意の VLAN ID が CPE ボックスに用意されています。

サブスクライバからサービス プロバイダー ネットワークへのパケットはすべて、アクセス デバイスによってカプセル化され、サブスクライバの VLAN がカスタマー VLAN（外部タグまたは S-VID）として設定されます。ただし、TV 受信者からの IGMP スヌーピング メッセージは例外です。このメッセージは、マルチキャスト TV VLAN に関連付けられます。TV 受信者から送信される VoD 情報は、他のトラフィック タイプと同様に送信されます。

ネットワーク ポートで受信される、サービス プロバイダー ネットワークからサブスクライバへのパケットは、ダブル タグ パケットとしてサービス プロバイダー ネットワークで送信されます。このとき、外部タグ（サービス タグまたは S-タグ）は次の 2 つの VLAN タイプのどちらかを表しています。

- サブスクライバの VLAN（インターネットや IP 電話など）
- マルチキャスト TV VLAN

内部 VLAN（C-タグ）は、サブスクライバのネットワーク内の宛先を CPE MUX によって決定するタグです。

ワークフロー

1. [インターフェイス設定] ページで、アクセス ポートをカスタマー ポートとして設定します。詳細については、「QinQ」を参照してください。
2. ネットワーク ポートを、トランク ポートまたは一般ポートとして設定し、サブスクライバとマルチキャスト TV VLAN をそのタグ付き VLAN として設定します。([インターフェイス設定] ページを使用して)。
3. 最大 4094 個の異なる VLAN を持つマルチキャスト TV VLAN を作成します。(この VLAN 作成には、標準の VLAN 管理設定を使用します)
4. [ポート マルチキャスト VLAN メンバーシップ] ページで、カスタマー ポートをマルチキャスト TV VLAN に関連付けます。
5. [VLAN への CPE VLAN] ページで、CPE VLAN(C-タグ)をマルチキャスト TV VLAN(S-タグ)にマッピングします。

VLAN への CPE VLAN

サブスクライバの VLAN で CPE MUX をサポートするには、サブスクライバに、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(内部)マルチキャスト VLAN は、マルチキャスト プロバイダー(外部)VLAN にマッピングする必要があります。

CPE VLAN が IGMP スヌーピングに参加するには、まずマルチキャスト VLAN にマッピングされる必要があります。

CPE VLAN をマップするには、次のようにします。

ステップ 1 [VLAN管理] > [カスタマーポートマルチキャストTV VLAN] > [VLANへのCPE VLAN] の順にクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [CPE VLAN]:CPE ボックスで定義した VLAN を入力します。
- [マルチキャスト 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 [適用] 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 メンバーシップ

マルチキャスト VLAN に関連付けるポートは、カスタマー ポートとして設定する必要があります(「インターフェイス設定」を参照)。

ポートをマルチキャスト TV VLAN にマップするには、次のようにします。

ステップ 1 [VLAN管理] > [カスタマーポートマルチキャストTV VLAN] > [ポートマルチキャストVLANメンバーシップ] の順にクリックします。

ステップ 2 [マルチキャストTV VLAN] から VLAN を選択します。

ステップ 3 [インターフェイス タイプ] からインターフェイスを選択します。

ステップ 4 [候補カスタマーポート] リストに、そのデバイス上に設定されているすべてのアクセス ポートが表示されます。必要なポートを [メンバー カスタマー ポート] フィールドに移動します。

ステップ 5 [適用] 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。

13

スパニング ツリー

このセクションでは、スパニング ツリー プロトコル（STP）（IEEE802.1D および IEEE802.1Q）について説明します。具体的な内容は、次のとおりです。

- STP の種類
- STP のステータスとグローバル設定
- STP インターフェイス設定
- RSTP インターフェイス設定
- マルチ スパニング ツリーの概要
- MSTP プロパティ
- MSTP インスタンスへの VLAN
- MSTP インスタンス設定
- MSTP インターフェイス設定

STP の種類

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 モードになっているリンク上では、ユーザ データの転送が一時的に停止します。トポロジが変更されてデータ転送が可能になると、リンクは自動的に有効化されます。

ホスト間に代替パスが存在する場合、ループが発生します。ループは、スイッチが同じパケットを永久に中継することになり、宛先にパケットが届かなかったり、ブロードキャスト/マルチキャスト ストームを引き起こしたり、ネットワーク効率が低下したりします。

STP を使用すると、ネットワーク上のエンド ステーション間に 1 本の固有のパスが生成され、ループが解消されるので、スイッチと相互接続リンクがツリー トポロジになります。

このデバイスでサポートされているスパニング ツリー プロトコルのバージョンは次のとおりです。

- 従来の STP では、任意の 2 台のエンド ステーション間に生成されるパスが 1 本のみになるため、ループが解消されます。
- Rapid STP（RSTP; 高速 STP）では、ネットワーク トポロジが検出され、スパニング ツリーが構成されるまでの収束時間が短くなります。ネットワーク トポロジが元々ツリー構造になっている場合、RSTP は非常に効果的であり、収束に要する時間が短くなる可能性があります。RSTP はデフォルトで有効になっています。
- 多重 STP（MSTP）：MSTP は RSTP に基づきます。レイヤ 2 のループを検知し、関係するポートからトラフィックが送信されないようにすることでループを軽減します。レイヤ 2 ドメイン単位にループが存在するため、STP ループを排除するためにポートがブロックされたときに、この状況になる可能性があります。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。この場合は、ブロックされているポートが常に使用されないため、帯域幅が効率的に消費されません。
- MSTP では、この問題を解決するため、インスタンスごとにループを個別に検知して軽減できるように、複数の STP インスタンスが有効になります。これにより、ポートは 1 つ以上の STP インスタンスに対してブロックされますが、他の STP インスタンスに対してはブロックされなくなります。複数の VLAN が複数の STP インスタンスに関連付けられている場合は、それらのトラフィックが関連する MST インスタンスの STP ポート状態に基づいて中継されます。帯域幅利用率が改善されます。

STP のステータスとグローバル設定

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

各モードを設定するには、[STPインターフェイス設定] ページ、[RSTPインターフェイス設定] ページ、および [MSTPプロパティ] ページをそれぞれ使用します。

STP のステータスとグローバル設定を設定するには、次のようにします。

ステップ 1 [スパニングツリー] > [STPステータス&グローバル設定] 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。

[グローバル設定]:

- [スパニングツリー状態]:選択すると、デバイスで有効になります。
- [STPループバックガード]:選択すると、デバイスでループバック ガードが有効になります。
- [STP動作モード]:STP モードを選択します。
- [BPDU処理]:ポートまたはデバイス上で STP が無効になっている場合のブリッジ プロトコル データ ユニット(BPDU)パケットの管理方法を選択します。BPDU は、スパニング ツリー情報を送信する目的で使用されます。
  - [フィルタリング]:インターフェイス上でスパニング ツリーが無効になっている場合に BPDU パケットをフィルタリングします。
  - [フラッディング]:インターフェイス上でスパニング ツリーが無効になっている場合に BPDU パケットをフラッディングします。
- [パスコストデフォルト値]:STP ポートにデフォルト パス コストを割り当てる際に使用する方法を選択します。インターフェイスに割り当てられるデフォルトのパス コストは、このフィールドで選択した方法によって変わります。
  - [ショート]: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。
  - [ロング]: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]:

- [プライオリティ]:ブリッジ プライオリティ値を入力します。スイッチ間で BPDU が交換された後、プライオリティ値が最も小さいデバイスがルート ブリッジになります。すべてのスイッチのプライオリティ値が同じである場合は、MAC アドレスに基づいてルート ブリッジが決まります。このプライオリティ値は、4096 の倍数にしてください。たとえば、4096、8192、12288 などの値を入力します。
- [ハロータイム]:ルート ブリッジが設定メッセージを待機する時間間隔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」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。(これはブリッジがルートでない場合に重要です。)
- [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。日/時間/分/秒の形式で表示されます。

ステップ 3 [適用] をクリックします。STP 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。

STP インターフェイス設定

[STPインターフェイス設定] ページでは、ポート単位の STP 情報を設定するや、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することができます。

入力された定義設定は、すべての種類の STP プロトコルで有効です。

インターフェイス単位の STP 情報を設定するには、次のようにします。

ステップ 1 [スパニングツリー] > [STPインターフェイス設定] の順にクリックします。

インターフェイスが表示されます。フィールドは [編集] ページで説明されますが、次のフィールドは例外で、ここにのみ表示されます。

- [ポートロール]:STP パスを構成するために MSTP アルゴリズムによって割り当てられた、ポート単位のポートまたは LAG ロール、あるいはインスタンス単位の LAG を表示します。

- [ルート]: このインターフェイスを経由してパケットを転送すると、ルート デバイスにパケットを転送するコスト パスが最小になります。
- [指定]: このブリッジを LAN に接続するためのインターフェイス。MST 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。
- [代替]: この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に使用されます。
- [バックアップ]: このインターフェイスは、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。バックアップ ロールは、2 つのポートがポイントツーポイント リンクによってループに接続されている場合に割り当てられます。また、バックアップ ポートは、共有セグメントへの接続が LAN 上に複数確立されている場合にも発生します。
- [無効]: この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。
- [境界]: このインスタンスのポートは境界ポートになっています。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] ページで確認できます。

ステップ 2 インターフェイスを選択し、[編集] 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。ポートに対してファスト リンク モードを有効にした場合、そのポートはリンクアップすると自動的にフォワーディング ステートに設定されます。ファスト リンクを有効にすると、STP プロトコルにおける収束処理が最適化されます。次のオプションがあります。
  - [有効]: ファスト リンクをすぐに有効にします。
  - [自動]: 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。
  - [無効]: ファスト リンクを無効にします。

  注 値を [自動] 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。これはループの回避に役立ちます。

エッジ ポートは MSTP モードでは動作しません。

- **ルート ガード**:デバイスのルート ガードを有効または無効にします。ルート ガード オプションにより、ネットワークのルート ブリッジの配置を適用できるようになります。

  ルート ガードにより、この機能が有効になっているポートが指定ポートになります。通常、ルート ブリッジの 2 つ以上のポートが接続されている場合を除き、すべてのルート ブリッジのポートが指定ポートになります。ルート ガードが有効になっているポートでブリッジが上位の BPDU を受信すると、ルート ガードがこのポートをルートの矛盾した STP 状態に移行します。このルートの矛盾した状態は、リスニング ステートと実質上同じです。このポート間でトラフィックは転送されません。このように、ルート ガードはルート ブリッジの配置を適用します。

- [BPDUガード]:ポートのブリッジ プロトコル データ ユニット(BPDU)ガード機能を有効または無効にします。

  BPDU ガードにより、STP のドメインの障壁が適用され、アクティブ トポロジの予測可能な状態を保持することができます。BPDU ガードが有効になっているポートの背後にあるデバイスは、STP トポロジに影響を与えることはありません。BPDU の受信後、BPDU ガードの動作によって、BPDU が設定されたポートが無効になります。この場合、BPDU メッセージが受信され、適切な SNMP トラップが生成されます。

- [BPDU処理]:ポート上またはデバイス上で STP が無効になっている場合の BPDU パケットの処理方法を選択します。BPDU は、スパニング ツリー情報を送信する目的で使用されます。

  - [グローバル設定を使用]:[STP のステータスとグローバル設定] ページで定義した設定を使用する場合に選択します。
  - [フィルタリング]:インターフェイス上でスパニング ツリーが無効になっている場合に BPDU パケットをフィルタリングします。
  - [フラッディング]:インターフェイス上でスパニング ツリーが無効になっている場合に BPDU パケットをフラッディングします。

- [パスコスト]:ルート パス コストにおけるこのポートのコストを入力するか、または、このシステムによって生成されたデフォルトのコストを使用します。

- [プライオリティ]:このポートのプライオリティ値を入力します。このスイッチの 2 つのポートがループに接続されている場合、このプライオリティ値がポートの選択に影響を及ぼします。プライオリティは 0 ～ 240 の範囲の値で、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。
  - [無効]: このポートに対して STP は現在無効になっています。トラフィックが転送され、MAC アドレスが学習されます。
  - [ブロッキング]: このポートは現在ブロックされており、BPDU データ以外のトラフィックを転送したり、MAC アドレスを学習したりすることはできません。
  - [リスニング]: このポートはリスニング モードになっています。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。
  - [ラーニング]: このポートは学習モードになっています。トラフィックを転送することはできませんが、新しい MAC アドレスを学習することはできます。
  - [フォワーディング]: このポートはフォワーディング モードになっています。トラフィックを転送したり、新しい MAC アドレスを学習したりすることができます。
- [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。
- [指定コスト]: 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]: 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、ポートの設定情報よりも LAG の設定情報が優先されます。

ステップ 4 [適用] をクリックします。インターフェイ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。

RSTP インターフェイス設定

高速スパニング ツリー プロトコル(RSTP)を使用した場合、転送ループが解消されるため、通常の STP 収束処理がより高速になります。

[RSTPインターフェイス設定] ページでは、ポート単位で 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 または MSTP 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、次のようにします。

ステップ 1 [スパニングツリー] > [STPステータス&グローバル設定] の順にクリックします。

ステップ 2 [RSTP] を有効にします。

ステップ 3 [スパニングツリー] > [RSTPインターフェイス設定] の順にクリックします。[RSTP インターフェイス設定] ページが表示されます。

ステップ 4 ポートを選択します。

注 [プロトコル移行のアクティブ化] は、テスト対象のブリッジ パートナーに接続しているポートを選択した場合にのみ使用可能になります。

ステップ 5 STP によってリンク パートナーが検出された場合、[プロトコル移行のアクティブ化] をクリックし、プロトコル移行テストを実行します。このテストにより、まだ STP を使用しているリンク相手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。リンク相手が STP リンクにまだ存在している場合、引き続き STP を使用してそのリンク相手と通信します。そうではなく、すでに RSTP または MSTP に移行されている場合は、デバイスが RSTP または MSTP を使用して通信します。

ステップ 6 インターフェイスを選択し、[編集] をクリックします。

ステップ 7 パラメータを入力します。

- [インターフェイス]: インターフェイスを設定し、RSTP を設定するポートまたは LAG を指定します。
- [ポイントツーポイント管理ステータス]:ポイントツーポイント リンクのステータスを指定します。全二重と定義されているポートは、ポイントツーポイント ポート リンクであると見なされます。
  - [有効]: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。
  - [無効]: 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。

- [自動]:RSTP BPDU を使用して、デバイスのステータスを自動的に決定します。

- [ポイントツーポイント動作ステータス]:[ポイントツーポイント管理ステータス] を [自動] に設定した場合、ポイントツーポイントの動作ステータスが表示されます。
- [ロール]:STP パスを構成するために、STP によってこのポートに割り当てられているロールが表示されます。表示されるロールは次のとおりです。
  - [ルート]: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。
  - [指定]:このスイッチを 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。
  - [代替]: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。
  - [バックアップ]: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、2 つのポートがポイントツーポイント リンクによってループに接続されている場合に割り当てられます。また、バックアップ ポートは、共有セグメントへの接続が LAN 上に複数確立されている場合にも割り当てられます。
  - [無効]:このポートはスパニング ツリーに属していません。
- [モード]:現在のスパニング ツリーのモードを表示します。従来の STP または RSTP です。
- [ファストリンク動作ステータス]:このインターフェイスに対するファスト リンク(エッジ ポート)のステータス(有効、無効、または自動)が表示されます。値は次のとおりです。
  - [有効]:ファスト リンクが有効になっています。
  - [無効]:ファスト リンクが無効になっています。
  - [自動]: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。
- [ポートステータス]:特定のポートの RSTP ステータスが表示されます。
  - [無効]:このポートに対して STP は現在無効になっています。
  - [ブロッキング]:このポートは現在ブロックされており、トラフィックを転送したり、MAC アドレスを学習したりすることはできません。
  - [リスニング]:このポートはリスニング モードになっています。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。

- [ラーニング]:このポートは学習モードになっています。トラフィックを転送することはできませんが、新しい MAC アドレスを学習することはできます。
- [フォワーディング]:このポートはフォワーディング モードになっています。トラフィックを転送したり、新しい MAC アドレスを学習したりすることができます。

ステップ 8 [適用] 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。

マルチ スパニング ツリーの概要

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 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、VLAN A のループにより、ポート A がある STP インスタンスでブロックされている場合に、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プロパティ] ページでは、グローバル MSTP 設定を定義できます。

MSTP を設定するには、次のようにします。

ステップ 1 「*STP のステータスとグローバル設定*」ページで説明するように、[STP 動作モード] を [MSTP] に設定します。

ステップ 2 MSTP インスタンスを定義します。各 MSTP インスタンスは、ループフリー トポロジを計算して作成し、インスタンスにマップする VLAN からのパケットをブリッジします。「MSTP インスタンスへの VLAN」セクションを参照してください。

ステップ 3 どの VLAN のどの MSTP インスタンスをアクティブにするか決定し、それらの MSTP インスタンスをそれぞれ VLAN に関連付けます。

ステップ 4 MSTP の属性を次のように設定します。

- *MSTP プロパティ*
- MSTP インスタンス設定
- *MSTP インスタンスへの VLAN*

MSTP プロパティ

グローバル MSTP は、VLAN グループごとに別個のスパニング ツリーを設定し、各スパニング ツリー インスタンス内の可能な代替パスの 1 つを除くすべてをブロックします。MSTP は複数 MST インスタンス（MSTI）を実行できる MST リージョンの構成を有効にします。複数リージョンとその他の STP ブリッジは、単一の共通スパニングツリー（CST）を使用して相互接続されます。

MSTP BPDU が RSTP ブリッジによって RSTP BPDU として解釈できるという点で、MSTP は RSTP ブリッジと完全に互換性があります。これを使用すると、設定を変更しないで RSTP ブリッジとの互換性が有効になるだけでなく、MSTP リージョン自体の内部にある MSTP ブリッジの数に関係なく、MSTP リージョンの外部にある RSTP ブリッジで、リージョンが単一の RSTP ブリッジとして認識されるようになります。

複数のスイッチを同じ MST リージョンに配置するには、VLAN から MST インスタンスへの同じマッピング、同じ設定リビジョン番号、同じリージョン名を持っている必要があります。

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。分離されると、リージョンは 2 つの分離したリージョンになります。

このマッピングは、[MSTP インスタンスへの VLAN] ページで実行できます。

システムが MSTP モードで動作している場合にこのページを使用します。

MSTP を定義するには、次のようにします。

ステップ 1 [スパニングツリー] > [STPステータス&グローバル設定] の順にクリックします。

ステップ 2 MSTP を有効にします。

ステップ 3 [スパニングツリー] > [MSTPプロパティ] の順にクリックします。

ステップ 4 パラメータを入力します。

- [リージョン名]: MSTP リージョン名を定義します。
- [リビジョン]: 現在の MST 設定のリビジョンを識別する符号なしの 16 ビットの数値を定義します。フィールドの範囲は 0 ～ 65535 です。
- [最大ホップ]: BPDU を廃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 を廃棄すると、ポート情報が期限切れになります。フィールドの範囲は 1 ～ 40 です。
- [ISTマスター]: リージョン マスターを表示します。

ステップ　5　[適用] 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 インスタンスへの VLAN

[MSTPインスタンスへのVLAN] ページでは、各 VLAN をマルチ スパニング ツリー インスタンス（MSTI）にマップできます。デバイスを同じリージョンに配置するには、VLAN から MSTI への同じマッピングを持っている必要があります。

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、システムの STP モードが MSTP である場合に適用されます。

インスタンス ゼロに加えて、最大で 16 個の MST インスタンスを定義できます。

MST インスタンスの 1 つに明示的にマップされていない 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プします。CIST インスタンスは、MST インスタンス 0 です。

VLAN を MST インスタンスにマップするには、次のようにします。

ステップ　1　[スパニングツリー] > [MSTPインスタンスへのVLAN] の順にクリックします。

[MSTPインスタンスへのVLAN] ページには、次のフィールドがあります。

- [MSTPインスタンス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　VLAN を MSTP インスタンスに追加するには、MST インスタンスを選択して、[編集] 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インスタンスID]：MST インスタンスを選択します。
- [VLAN]：この MST インスタンスにマップされる VLAN を定義します。
- [アクション]：VLAN を MST インスタンスに**追加**（マップ）するか**削除**するかを定義します。

ステップ 4 [適用] をクリックします。MSTP VLAN の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。

MSTP インスタンス設定

[MSTPインスタンス設定] ページでは、MST インスタンスごとにパラメータを設定して表示できます。これは、*STP ステータスとグローバル設定を設定する作業*をインスタンス単位で行う機能と同等です。

MSTP インスタンス設定を入力するには、次のようにします。

ステップ 1 [スパニングツリー] > [MSTPインスタンス設定] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インスタンスID]:表示して定義する MST インスタンスを選択します。
- [含まれるVLAN]:選択したインスタンスにマップされる VLAN を表示します。デフォルトのマッピングでは、すべての VLAN が Common and Internal Spanning Tree(CIST) インスタンス 0 にマップされています。
- [ブリッジプライオリティ]:選択された MST インスタンスに対するこのブリッジのプライオリティを設定します。
- [代表ルートブリッジID]:MST インスタンスに対するルート ブリッジのプライオリティと MAC アドレスが表示されます。
- [ルートポート]:選択されたインスタンスのルート ポートを表示します。
- [ルートパスコスト]:選択されたインスタンスのルート パス コストを表示します。
- [ブリッジ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 プライオリティと MAC アドレスが表示されます。
- [残存ホップ]:次の宛先まで残っているホップの数を表示します。

ステップ 3 [適用] をクリックします。MST インスタンス構成が定義され、実行コンフィギュレーション ファイルが更新されます。

MSTP インターフェイス設定

[MSTPインターフェイス設定] ページでは、すべての MST インスタンスに対してポートの MSTP 設定を行い、MST インスタンス単位の代表ブリッジなど、プロトコルによって現在学習されている情報を表示できます。

MST インスタンスでポートを設定するには、次のようにします。

ステップ 1 [スパニングツリー] > [MSTPインターフェイス設定] の順にクリックします。

ステップ 2 パラメータを入力します。

- [インスタンスが次に等しい]:設定する MSTP インスタンスを選択します。
- [インターフェイスタイプが次に等しい]:ポートまたは LAG のリストを表示するかどうかを選択します。

ステップ 3 [実行] をクリックします。インスタンスのインターフェイスに対する 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、[編集] をクリックします。

ステップ 5 パラメータを入力します。

- [インスタンスID]:設定する MST インスタンスを選択します。
- [インターフェイス]:MSTI 設定の定義対象となるインターフェイスを選択します。
- [インターフェイスプライオリティ]: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 プライオリティを設定します。
- [パスコスト]:[ユーザ定義] テキストボックスのルート パス コストにポートのコストを指定するか、[デフォルトを使用] を選択してデフォルト値を使用します。
- [ポート状態]:特定の MST インスタンスの特定のポートの MSTP ステータスを表示します。パラメータは次のように定義されます。
  - [無効]:STP は現在無効です。
  - [ブロッキング]:このインスタンスのポートは現在ブロックされており、BPDU データ以外のトラフィックを転送したり、MAC アドレスを学習したりすることはできません。
  - [リスニング]:このインスタンスのポートはリスニング モードになっています。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。

- [ラーニング]:このインスタンスのポートは学習モードになっています。トラフィックを転送することはできませんが、新しい MAC アドレスを学習することはできます。
- [フォワーディング]:このインスタンスのポートはフォワーディング モードになっています。トラフィックを転送したり、新しい MAC アドレスを学習したりすることができます。
- [境界]:このインスタンスのポートは境界ポートになっています。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] ページで確認できます。

• [ポート ロール]:STP パスを構成するために MSTP アルゴリズムによって割り当てられた、ポート単位のポートまたは LAG ロール、あるいはインスタンス単位の LAG を表示します。

- [ルート]:このインターフェイスを経由してパケットを転送すると、ルート デバイスにパケットを転送するコスト パスが最小になります。
- [指定ポート]:このブリッジを LAN に接続するためのインターフェイス。MST 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。
- [代替]:このインターフェイスは、ルート ポートからルート デバイスへの代替パスに使用されます。
- [バックアップ]:このインターフェイスは、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。バックアップ ロールは、2 つのポートがポイントツーポイント リンクによってループに接続されている場合に割り当てられます。また、バックアップ ポートは、共有セグメントへの接続が LAN 上に複数確立されている場合にも発生します。
- [無効]:この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。
- [境界]:このインスタンスのポートは境界ポートになっています。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] ページで確認できます。

• [モード]:現在のインターフェイス スパニング ツリーのモードを表示します。

- 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 になります。
- 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 になります。

- [タイプ]: このポートの MST タイプが表示されます。
  - [境界]: 境界ポートは、MST ブリッジをリモート リージョンの LAN にアタッチします。ポートが境界ポートの場合、リンクの反対側のデバイスが RSTP モードと STP モードのどちらで動作しているかどうかも示します。
  - [内部]: ポートが内部ポートです。
- [代表ブリッジ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 番号を表示します。
- [指定ポートID]: リンクまたは共有 LAN をルートに接続する代表ブリッジのポート ID 番号を表示します。
- [指定コスト]: 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。
- [残存ホップ]: 次の宛先まで残っているホップを表示します。
- [フォワーディングへの移行]: このポートがフォワーディング ステートからブロッキング ステートに移行した回数が表示されます。

ステップ 6 [適用] 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。

14

MAC アドレス テーブルの管理

このセクションでは、MAC アドレスをシステムに追加する方法について説明します。具体的な内容は、次のとおりです。

- スタティック アドレス
- ダイナミック アドレス
- 予約済み MAC アドレス

MAC アドレスにはスタティック（静的）とダイナミック（動的）の 2 種類があります。MAC アドレスは、その種類に応じて、*スタティック アドレス* テーブルまたは *ダイナミック アドレス* テーブルに、VLAN 情報およびポート情報と共に格納されます。

スタティック アドレスはユーザによって構成されるため、期限切れになりません。

デバイスに到着するフレーム内に表示される新しい送信元 MAC アドレスは、ダイナミック アドレス テーブルに追加されます。構成可能な一定期間にわたって、この MAC アドレスが保持されます。この有効期間に達する前に、同じ送信元 MAC アドレスを持つ別のフレームがデバイスに到着しない場合、この MAC エントリは期限切れになり、テーブルから削除されます。

デバイスにフレームが到着するとき、デバイスはスタティックまたはダイナミック テーブル内に一致する宛先 MAC アドレス エントリがないか検索します。一致が見つかった場合、そのフレームは、テーブルで指定されたポートで出力されるようマークが付けられます。テーブル内に見つからない MAC アドレスに送信されるフレームは、該当する VLAN 上の全ポートに伝送/ブロードキャストされます。このようなフレームを、不明なユニキャスト フレームといいます。

デバイスでは、最大 8,000 個のスタティックおよびダイナミック MAC アドレスがサポートされます。

スタティック アドレス

スタティック MAC アドレスは、デバイス上の特定の物理インターフェイスおよび VLAN に割り当てられます。そのアドレスが別のインターフェイスで見つかった場合、それは無視され、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、次のようにします。

ステップ 1 [MACアドレステーブル] > [スタティックアドレス] の順にクリックします。

[スタティックアドレス] ページには、現在定義されているスタティック アドレスが含まれます。

ステップ 2 [追加] 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]: ポートの VLAN ID を選択します。
- [MAC アドレス]: インターフェイス MAC アドレスを入力します。
- [インターフェイス]: エントリのインターフェイス(ユニット/スロット、ポート、または LAG)を選択します。
- [ステータス]: エントリの処理方法を選択します。次のオプションがあります。
  - [固定]: システムはこの MAC アドレスを決して削除しません。スタートアップ コンフィギュレーションでスタティック MAC アドレスを保存すると、それは再起動後も保持されます。
  - [リセット時に削除]: デバイスがリセットされると、スタティック MAC アドレスは削除されます。
  - [タイムアウト時に削除]: 期限が切れると、MAC アドレスは削除されます。
  - [セキュア]: インターフェイスが従来のロック モードである場合、MAC アドレスが保護されます(「ポート セキュリティ」を参照)。

ステップ 4 [適用] 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。

ダイナミック アドレス

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、デバイスに入ってくるフレームの発信元アドレスを監視することにより得られる MAC アドレスが含まれます。

このテーブルのオーバーフローを防いで新しい MAC アドレスを追加する余地を残すために、対応するトラフィックが一定期間(エージング タイム)にわたって受信されないアドレスは削除されます。

ダイナミック アドレスの設定

ダイナミック アドレスのエージング タイム(有効期限)を設定するには、次のようにします。

ステップ 1 [MACアドレステーブル] > [ダイナミックアドレス設定] の順にクリックします。

ステップ 2 [エージング タイム] を入力します。エージング タイムは、ユーザ設定値から、その値の 2 倍から 1 を引いた値までになります。たとえば、300 秒と入力した場合、エージング タイムは 300 ～ 599 秒になります。

ステップ 3 [適用] 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、次のようにします。

ステップ 1 [MACアドレステーブル] > [ダイナミックアドレス] の順にクリックします。

ステップ 2 [フィルタ] ブロックで、次の照会条件を入力できます。

- [VLAN ID]:テーブルで照会する VLAN ID を入力します。
- [MAC アドレス]:テーブルで照会する MAC アドレスを入力します。
- [インターフェイス]:テーブルで照会するインターフェイスを選択します。照会で特定のユニット/スロット、ポート、または LAG を検索することができます。

ステップ 3 [実行] をクリックします。ダイナミック MAC アドレス テーブルが照会され、照会結果が表示されます。

ステップ 4 すべてのダイナミック MAC アドレスを削除するには、[テーブルのクリア] をクリックします。

予約済み MAC アドレス

(IEEE 標準に基づく)予約済み範囲に属する MAC アドレスが宛先として指定されたフレームがデバイスで受信された場合、そのフレームを破棄またはブリッジすることができます。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、または予約済み MAC アドレスとフレーム タイプを次のように指定できます。

予約済み MAC アドレスのエントリを追加するには、次のようにします。

ステップ 1 [MACアドレステーブル] > [予約済みMACアドレス] の順にクリックします。

MAC アドレスが表示されます。フィールドは [追加] ページで説明されます。ただし、次のフィールドを除きます。

[プロトコル]:デバイス(ピアと呼ばれる)上でサポートされているプロトコルが表示されます。

ステップ 2 [追加] 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 アドレス]:予約する MAC アドレスを選択します。
- [フレーム タイプ]:次の基準に基づいてフレーム タイプを選択します。
  - [Ethernet V2]:特定の MAC アドレスが指定された Ethernet V2 パケットに適用されます。
  - [LLC]:特定の MAC アドレスが指定された論理リンク制御(LLC)パケットに適用されます。
  - [LLC-SNAP]:特定の MAC アドレスが指定された論理リンク制御/サブネットワーク アクセス プロトコル(LLC-SNAP)パケットに適用されます。
  - [すべて]:特定の MAC アドレスが指定されたすべてのパケットに適用されます。

- [アクション]: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いずれか 1 つのアクションを以下から選択します。
  - [ブリッジ]:すべての VLAN メンバーにパケットを転送します。
  - [破棄]:パケットを削除します。

ステップ 4 [適用] をクリックします。新しい MAC アドレスが予約されます。

15

マルチキャスト

ここでは、マルチキャスト転送機能について説明します。具体的な内容は次のとおりです。

- マルチキャスト転送の概要
- プロパティ
- MAC グループ アドレス
- IP マルチキャスト グループ アドレス
- IPv4 マルチキャスト コンフィギュレーション
- IPv6 マルチキャスト コンフィギュレーション
- IGMP/MLD スヌーピング IP マルチキャスト グループ
- マルチキャスト ルータ ポート
- すべて転送
- 未登録マルチキャスト

マルチキャスト転送の概要

マルチキャスト転送機能を利用すれば、「1 対多」型の情報配信を行うことができます。マルチキャスト転送が役に立つのは、情報を多数のクライアントに配信する場合です。各クライアントは、コンテンツ全体を受信する必要はありません。典型的な用途の 1 つにケーブル テレビがあります。ケーブル テレビの場合、クライアントは配信の途中でチャネルの視聴を開始し、配信が終わる前に視聴をやめることができます。

データは受信対象ポートにのみ送信されます。そのため、リンク上の帯域幅とホスト リソースを節約できます。

デフォルトでは、すべてのマルチキャスト フレームが VLAN のすべてのポートにフラッディングされます。プロパティ ページでブリッジ マルチキャスト フィルタリング ステータスを有効にすると、対象ポートにのみマルチキャスト フレームを転送し、それ以外のポートへのマルチキャストはフィルタリング(ドロップ)して、それらのポートにマルチキャスト フレームを転送しないようにすることができます。

フィルタリングを有効にした場合、マルチキャスト フレームは、マルチキャスト転送データベース(MFDB)で定義されている対象 VLAN 上のポートのサブセットに転送されます。マルチキャスト フィルタリングは、すべてのトラフィックに適用されます。

マルチキャスト メンバーを表す一般的な方法は(S,G)表記です。「S」はマルチキャスト ストリーム データの(単一の)送信元、「G」は IPv4 または IPv6 のグループ アドレスを意味します。あるマルチキャスト クライアントが、特定のマルチキャスト グループの任意の送信元からマルチキャスト トラフィックを受信できる場合、これは(*,G)として保存されます。

マルチキャスト フレームの転送方法として、以下のいずれか 1 つを設定できます。

- [MACグループアドレス]: イーサネット フレーム内の宛先 MAC アドレスに基づいて転送されます。

  注 1 つまたは複数の IP マルチキャスト グループ アドレスが 1 つの MAP アドレスにマッピングされる可能性があります。つまり、MAC グループ アドレスに基づく転送の場合、IP マルチキャスト ストリームが、そのストリームの受信対象でないポートに転送される可能性があります。

- [IPグループアドレス]: IP パケットの宛先 IP アドレスに基づいて転送されます(*,G)。

- [送信元固有IPグループアドレス]: IP パケットの宛先 IP アドレスと送信元 IP アドレスの両方に基づいて転送されます(S,G)。

IGMPv3 と MLDv2 では、(S,G)がサポートされていますが、IGMPv1/2 と MLDv1 では、(*.G)のみがサポートされています。

このデバイスでは、スタティック マルチキャスト グループ アドレスとダイナミック マルチ キャスト グループ アドレスを合わせて最大 256 個登録できます。

各 VLAN に対して、いずれか 1 つのフィルタリング オプションだけを設定できます。

マルチキャスト転送を行うための一般的な構成

マルチキャスト ルータが IP サブネット間でマルチキャスト パケットをルーティングするのに対し、マルチキャスト対応レイヤ 2 スイッチは、LAN 内または VLAN 内の登録済みノードにマルチキャスト パケットを転送します。

マルチキャスト転送を行うための一般的な構成要素は、プライベート/パブリック IP ネットワーク間でマルチキャスト ストリームを転送するルータ、IGMP/MLD スヌーピング機能を備えたデバイス、およびマルチキャスト ストリームを受信するマルチキャスト クライアントです。この構成では、ルータが IGMP/MLD クエリーを定期的に送信します。

マルチキャストの動作

レイヤ 2 マルチキャスト サービスでは、レイヤ 2 スイッチが、特定のマルチキャスト アドレス宛の 1 つのフレームを受信します。スイッチ上で、各受信対象ポートに送信するため、フレームが複製されます。

IGMP/MLD スヌーピングが有効になっているデバイスは、マルチキャスト ストリームのフレームを受信すると、IGMP/MLD 参加メッセージを使用してマルチキャスト ストリームを受信するよう登録されたすべてのポートにそのマルチキャスト フレームを転送します。

システム上では、各 VLAN に対するマルチキャスト グループのリストが保持されており、各ポートが受信すべきマルチキャスト情報が管理されています。マルチキャスト グループおよびその受信ポートは、静的（スタティック）に設定することも、IGMP または MLD プロトコル スヌーピングを使って動的（ダイナミック）に学習させることもできます。

マルチキャスト登録（IGMP/MLD スヌーピング）

マルチキャスト登録とは、マルチキャスト登録プロトコルを待機して、それに応答するプロセスのことです。使用可能なプロトコルは、IPv4 の場合は IGMP、IPv6 の場合は MLD です。

デバイス上で、ある VLAN に対して IGMP/MLD スヌーピングが有効になっている場合、デバイスに接続されている VLAN およびネットワーク上のマルチキャスト ルータから受信される IGMP/MLD パケットが解析されます。

ホストが IGMP/MLD メッセージを使用してマルチキャスト ストリーム（あるいは特定ソースからのマルチキャスト ストリーム）を受信するよう登録しているということをデバイスが学習すると、その登録情報がデバイスの MFDB に追加されます。

サポートされているバージョンは次のとおりです。

- IGMP v1、v2、v3
- MLD v1、v2

注 このデバイスは、スタティック VLAN に対する IGMP/MLD スヌーピングのみをサポートしています。ダイナミック VLAN に対する IGMP/MLD スヌーピングはサポートしていません。

IGMP/MLD スヌーピングがグローバルに、または特定の VLAN に対して有効になっている場合、すべての IGMP/MLD パケットが CPU に転送されます。CPU では着信パケットが解析され、次の情報が特定されます。

- VLAN 上のマルチキャスト グループへの参加を要求しているポート、および、参加先の VLAN とマルチキャスト グループ。
- IGMP/MLD クエリーを生成しているマルチキャスト ルータ（Mrouter）に接続しているポート。
- PIM、DVMRP、または IGMP/MLD クエリー プロトコルを受信しているポート。

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

特定のマルチキャスト グループへの参加を要求するポートから、IGMP/MLD 報告メッセージが送信されます。この報告メッセージの中で、ホストがどのグループへの参加を要求しているかが指定されます。この結果、マルチキャスト転送データベースに転送エントリが作成されます。

IGMP スヌーピング クエリア

マルチキャスト ルータが存在しない場合にスヌーピング スイッチのレイヤ 2 マルチキャスト ドメインをサポートするために、IGMP/MLD スヌーピング クエリアが使用されます。たとえば、ローカル サーバによってマルチキャスト コンテンツが提供されても、そのネットワーク上のルータ（存在する場合）がマルチキャストをサポートしないことがあります。

デバイスを、バックアップの IGMP クエリアとして設定したり、正規の IGMP クエリアが存在しない場合に IGMP クエリアとなるよう設定したりすることができます。デバイスは全機能を備えた IGMP クエリアではありません。

IGMP クエリアとして有効になっているデバイスは、マルチキャスト ルータから IGMP トラフィック（クエリー）が検出されない状態が 60 秒経過した後、機能を開始します。他の IGMP クエリアが存在する場合、デバイスは、標準的なクエリア選択プロセスの結果に基づいて、クエリーの送信を停止することも、停止しないこともあります。

IGMP/MLD クエリア アクティビティの速度は、IGMP/MLD スヌーピングが有効になったスイッチと整合する必要があります。スヌーピング テーブル エージング タイムに整合する速度で、クエリーが送信される必要があります。エージング タイムより低い速度でクエリーが送信される場合、サブスクライバはマルチキャスト パケットを受信できません。この操作は [IGMP/MLD スヌーピング IP マルチキャスト グループ] ページで行います。

IGMP/MLD クエリア選出メカニズムが無効になっている場合、IGMP/MLD スヌーピング クエリアは有効化後に一般クエリー メッセージを送る操作を 60 秒間遅らせます。他のクエリアが存在しない場合は、一般クエリー メッセージを送信し始めます。他のクエリアが検出されると、一般クエリー メッセージの送信を停止します。

IGMP/MLD スヌーピング クエリアは、次の間隔で別のクエリアの機能を検出した場合に一般クエリー メッセージの送信を再開します。

クエリー パッシブ間隔 = ロバストネス X クエリー間隔 + 0.5 X クエリー応答間隔

注 VLAN に IPM マルチキャスト ルータが存在する場合は、IGMP/MLD クエリア選出メカニズムを無効にすることを推奨します。

マルチキャスト アドレスの特徴

マルチキャスト アドレスには次の特徴があります。

- IPv4 のマルチキャスト アドレス範囲は、224.0.0.0 ～ 239.255.255.255 です。
- IPv6 のマルチキャスト アドレス範囲は、FF00:/8 です。
- IP マルチキャスト グループ アドレスをレイヤ 2 マルチキャスト アドレスにマッピングするには、次のようにします。
  - IPv4 の場合、IPv4 アドレスの下位 23 ビットを 01:00:5e というプレフィックスの後ろに追加します。標準では、IP アドレスの上位 9 ビットは無視されます。また、マッピングに使用される下位 23 ビットは互いに同じであるため、上位 9 ビットの値だけが異なる IP アドレスは、同じレイヤ 2 アドレスにマッピングされます。たとえば、234.129.2.3 は 01:00:5e:01:02:03 というレイヤ 2 マルチ キャスト グループ アドレス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 アドレスを、同じレイヤ 2 アドレスにマッピングできます。
  - IPv6 の場合、IPv6 マルチキャスト アドレスの下位 32 ビットを 33:33 というプレフィックスの後ろに追加します。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。

IGMP/MLD プロキシ

IGMP/MLD プロキシは単純な IP マルチキャスト プロトコルです。

IGMP/MLD プロキシを使用して、エッジ ボックスなどのデバイス上のマルチキャスト トラフィックを複製することで、これらのデバイスの設計と実装が大幅に簡略化される可能性があります。Protocol Independent Multicast（PIM）、ディスタンス ベクター マルチキャスト ルーティング プロトコル（DVMRP）などの複雑なマルチキャスト ルーティング プロトコルをサポートしないことにより、デバイスのコストだけでなく運用上のオーバーヘッドも削減されます。別の利点は、コア ネットワーク ルータで使用されるマルチキャスト ルーティング プロトコルにプロキシ デバイスが依存しないことです。そのため、任意のマルチキャスト ネットワークにプロキシ デバイスを簡単に展開できます。

IGMP/MLD プロキシ ツリー

IGMP/MLD プロキシは、（PIM などの）堅牢なマルチキャスト ルーティング プロトコルの実行を必要としない単純なツリー トポロジで機能します。グループ メンバーシップ情報とプロキシ グループ メンバーシップ情報の学習に基づく単純な IPM ルーティング プロトコルを使用し、その情報に基づいてマルチキャスト パケットを転送するだけで十分です。

各プロキシ デバイスでのアップストリーム インターフェイスとダウンストリーム インターフェイスを指定することにより、手動でツリーを設定する必要があります。さらに、プロキシ ツリー トポロジに適用する IP アドレス指定スキームを設定する際は、プロキシ デバイスが IGMP/MLD クエリア選出で確実に選出されてマルチキャスト トラフィックを転送できるように設定する必要があります。ツリー内にプロキシ デバイス以外の他のマルチキャスト ルータが存在してはならず、ツリーのルートはより広範なマルチキャスト インフラストラクチャに接続されるべきです。

IGMP/MLD に基づく転送を行うプロキシ デバイスには、1 つのアップストリーム インターフェイスと 1 つ以上のダウンストリーム インターフェイスがあります。これらの指定は明示的に行われます。各インターフェイスのタイプを決定するプロトコルは存在しません。プロキシ デバイスはダウンストリーム インターフェイスで IGMP/MLD のルータ部分を実行し、アップストリーム インターフェイスで IGMP/MLD のホスト部分を実行します。

ただ 1 つのツリーを使用できます。

転送ルールとクエリア

次のように転送ルールが適用されます。

- アップストリーム インターフェイスで受信されたマルチキャスト パケットが以下に転送されます。
  - アップストリーム インターフェイス上
  - パケットを要求しているすべてのダウンストリーム インターフェイス上（ただし、プロキシ デバイスがそのインターフェイス上のクエリアである場合のみ）
- ダウンストリーム インターフェイスで受信されたマルチキャスト パケットは、プロキシ デバイスがそのインターフェイスのクエリアでない場合、ドロップされます。
- プロキシ デバイスがクエリアであるダウンストリーム インターフェイスで受信されたマルチキャスト パケットは、アップストリーム インターフェイスに転送され、パケットを要求するすべてのダウンストリーム インターフェイスにも転送されます（ただしプロキシ デバイスがそれらのインターフェイス上のクエリアである場合のみ）。

ダウンストリーム インターフェイスの保護

デフォルトでは、IGMP/MLD ツリーのインターフェイスに到達する IP マルチキャスト トラフィックが転送されます。ダウンストリーム インターフェイスに到達する IP マルチキャスト トラフィックの転送を無効にすることができます。これはグローバルに行うことも、特定のダウンストリーム インターフェイスに対して行うこともできます。

プロパティ

マルチキャスト フィルタリングを有効にしてフォワーディング方式を選択するには、次のようにします。

ステップ 1 [マルチキャスト] > [プロパティ] をクリックします。

ステップ 2 パラメータを入力します。

- [ブリッジマルチキャストフィルタリングステータス]: これを選択するとフィルタリングが有効になります。
- [VLAN ID]: フォワーディング（転送）方式の設定対象となる VLAN ID を選択します。

- [IPv6 用フォワーディング方式]:IPv6 アドレス用に、次のいずれかの転送方式を設定します。
  - [MACグループアドレス]:MAC マルチキャスト グループ アドレスに従ってパケットを転送します。
  - [IPグループアドレス]: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。
  - [送信元固有IPグループアドレス]: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 アドレスと送信元固有 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。宛先マルチキャスト アドレスの場合、グループ ID の最後の 4 バイトが照合されます。送信元アドレスの場合、最後の 3 バイトと最後のバイトから 5 番目が照合されます。

- [IPv4用フォワーディング方式]:IPv4 アドレス用に、次のいずれかの転送方式を設定します。
  - [MACグループアドレス]:MAC マルチキャスト グループ アドレスに従ってパケットを転送します。
  - [IPグループアドレス]:IPv4 マルチキャスト グループ アドレスに従ってパケットを転送します。
  - [送信元固有IPグループアドレス]:送信元 IPv4 アドレスおよび 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 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

MAC グループ アドレス

[MAC グループ アドレス] ページでは、次の操作が可能です。

- 特定の VLAN ID または特定の MAC アドレス グループに関する情報を、マルチキャスト転送データベース(MFDB)から照会して表示できます。この情報は、IGMP/MLD スヌーピング機能によって動的に取得されたもの、または手動で設定したものです。
- 宛先 MAC アドレスに基づく静的な転送情報を設定するスタティック エントリを MFDB に追加したり、エントリを削除したりすることができます。
- 各 VLAN ID および MAC アドレス グループのメンバーであるポート/LAG のリストを表示したり、トラフィックをその VLAN ID および MAC アドレス グループに転送するかどうかを設定できます。

MAC マルチキャスト グループを定義および表示するには、次のようにします。

ステップ 1 [マルチキャスト] > [MACグループアドレス] をクリックします。

ステップ 2 フィルタ パラメータを入力します。

- [VLAN ID が次に等しい]: 表示するグループの VLAN ID を設定します。
- [MACグループアドレスが次に等しい]: 表示するマルチキャスト グループの MAC アドレスを設定します。MAC グループ アドレスを指定しない場合、選択した VLAN のすべての MAC グループ アドレスがこのページに含まれます。

ステップ 3 [実行] をクリックすると、MAC マルチキャスト グループが下部に表示されます。

このページと、[IP マルチキャスト グループ アドレス] ページの両方で作成されたエントリが表示されます。IP マルチキャスト グループ アドレス ページで作成されたエントリは、IP アドレスが MAC アドレスに変換されます。

ステップ 4 [追加] をクリックして、スタティック 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]: 新しいマルチキャスト グループの VLAN ID を定義します。
- [MACグループアドレス]: 新しいマルチキャスト グループの MAC アドレスを定義します。

ステップ 6 [適用] 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に関する登録情報を設定および表示するには、アドレスを選択して [詳細] をクリックします。

このページにあるフィールドは次のとおりです。

- [VLAN ID]: マルチキャスト グループの VLAN ID。
- [MAC グループ アドレス]: グループの MAC アドレス。

ステップ 7 ポートまたは LAG を、[フィルタ]: [インターフェイスタイプ] メニューから選択します。

ステップ 8 [実行] をクリックすると、VLAN のポートまたは LAG のメンバーシップが表示されます。

ステップ 9 各インターフェイスをマルチキャスト グループに関連付ける方法を選択します。

- [スタティック]: インターフェイスがスタティック メンバーとしてマルチキャスト グループに関連付けられます。
- [ダイナミック]: IGMP/MLD スヌーピングの結果としてインターフェイスがマルチキャスト グループに追加されたことを示します。
- [禁止]: このポートがこの VLAN 上のこのマルチキャスト グループに参加できないことを指定します。
- [なし]: このポートが現在、この VLAN 上のこのマルチキャスト 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 [適用] 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 [IP マルチキャスト グループ アドレス] ページで作成されたエントリを選択しても、このページでは削除できません。

IP マルチキャスト グループ アドレス

[IPマルチキャストグループアドレス] ページは [MACグループアドレス] ページに似ていますが、マルチキャスト グループは IP アドレスで識別される点が異なります。

[IPマルチキャストグループアドレス] ページでは、IP マルチキャスト グループを照会したり追加したりできます。

IP マルチキャスト グループを定義および表示するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPマルチキャストグループアドレス] をクリックします。

スヌーピング機能によって学習されたすべての IP マルチキャスト グループ アドレスがこのページに含まれます。

ステップ 2 フィルタリングに必要なパラメータを入力します。

- [VLAN IDが次に等しい]:表示するグループの VLAN ID を定義します。
- [IPバージョンが次に等しい]:IPv6 または IPv4 を選択します。
- [IPマルチキャストグループアドレスが次に等しい]:表示するマルチキャスト グループの IP アドレスを定義します。この値は、転送モードが(S,G)の場合にのみ意味を持ちます。
- [送信元IPアドレスが次に等しい]:送信元デバイスの IP アドレスを定義します。モードが (S,G) である場合は、送信側 S を入力します。この値と IP グループ アドレスの組み合わせが、表示されるマルチキャスト グループ ID (S,G) になります。モードが (*.G) である場合は「*」と入力します。これは、マルチキャスト グループが宛先でのみ定義されることを意味します。

ステップ 3 [実行] をクリックします。結果が下部に表示されます。

ステップ 4 [追加] をクリックして、スタティック 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 を定義します。
- [IPバージョン]:IP アドレス タイプを選択します。
- [IPマルチキャストグループアドレス]:新しいマルチキャスト グループの IP アドレスを定義します。
- [送信元固有]:特定の送信元がエントリに含まれることを示し、[送信元 IP アドレス] フィールドのアドレスを追加します。このフィールドを選択しなかった場合、このエントリは(*,G)として定義されます。つまり、送信元 IP アドレスが任意であることを意味します。
- [送信元IPアドレス]:含める送信元アドレスを定義します。

ステップ 6 [適用] をクリックします。IP マルチキャスト グループが新規に作成され、デバイスが更新されます。

ステップ 7 IP グループ アドレスの登録情報を設定および表示するには、アドレスを選択して [詳細] をクリックします。

ウィンドウの上部に、選択された VLAN ID、IP バージョン、IP マルチキャスト グループ アドレス、および送信元 IP アドレスが読み取り専用で表示されます。フィルタ タイプを選択できます。

- [インターフェイスタイプが次に等しい]: ポートまたは LAG のどちらを表示するかを選択します。

ステップ 8 インターフェイスごとに、関連付けタイプを選択します。選択項目は次のとおりです。

- [スタティック]: インターフェイスがスタティック メンバーとしてマルチキャスト グループに関連付けられます。
- [ダイナミック]: インターフェイスがダイナミック メンバーとしてマルチキャスト グループに関連付けられます。
- [禁止]: このポートがこの VLAN 上のこのグループに参加できないことを指定します。
- [なし]: このポートが現在、この VLAN 上のこのマルチキャスト グループのメンバーでないことを示します。[スタティック] または [禁止] が選択されるまでは、デフォルトで [なし] が選択されています。

ステップ 9 [適用] 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

次のページで、IPv4 マルチキャスト コンフィギュレーションを設定します。

- IGMP スヌーピング
- IGMP インターフェイス設定
- IGMP VLAN 設定
- IGMP プロキシ

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、([プロパティ] ページで) ブリッジ マルチキャスト フィルタリング機能を有効にするとともに、([IGMP スヌーピング] ページで) グローバルに、および該当する VLAN ごとに IGMP スヌーピングを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、次のようにします。

ステップ 1 [マルチキャスト] > [IPv4マルチキャストコンフィギュレーション] > [IGMPスヌーピング] をクリックします。

IGMP スヌーピングをグローバルで有効にした場合、デバイスでネットワーク トラフィックが監視され、マルチキャスト トラフィックの受信を要求したホストが特定されます。デバイスで IGMP スヌーピングが実行されるのは、IGMP スヌーピングとブリッジ マルチキャスト フィルタリングの両方が有効になっている場合だけです。

IGMP スヌーピング テーブルが表示されます。表示されたフィールドの説明が下の [編集] ページに表示されます。加えて、次のフィールドが表示されます。

- [IGMPスヌーピングステータス]: IGMP スヌーピングが有効になっているかどうか ([管理]) とそれが実際に VLAN 上で動作しているかどうか ([動作]) を表示します。
- [IGMP クエリア ステータス]: IGMP クエリアが有効になっているかどうか ([管理]) と、それが実際に VLAN 上で動作しているかどうか ([動作]) を表示します。

次の機能を有効または無効にします。

- [IGMPスヌーピングステータス]: これを選択すると、すべてのインターフェイスで IGMP スヌーピングがグローバルに有効になります。
- [IGMP クエリア ステータス]: これを選択すると、すべてのインターフェイスで IGMP クエリアがグローバルに有効になります。

ステップ 2 インターフェイス上で IGMP を設定するには、スタティック VLAN を選択して [編集] をクリックします。次のフィールドを入力します。

- [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。デバイスでネットワーク トラフィックが監視され、マルチキャスト トラフィックの受信を要求したホストが特定されます。デバイスで IGMP スヌーピングが実行されるのは、IGMP スヌーピングとブリッジ マルチキャスト フィルタリングの両方の機能が有効になっている場合だけです。
- [マルチキャストルータポート自動学習]: これを選択すると、マルチキャスト ルータの自動学習が有効になります。

- [即時脱退]: これを選択すると、スイッチは、脱退メッセージを送信してきたインターフェイスを転送テーブルから削除する際、まず最初に MAC に基づく一般クエリーをそのインターフェイスに送らなくても削除できるようになります。ホストから IGMP グループ脱退メッセージを受け取った場合、システムはテーブル エントリからそのホストのポートを削除します。マルチキャスト ルータからの IGMP クエリーを中継した後、マルチキャスト クライアントから IGMP メンバーシップ報告を受け取らなければ、エントリを定期的に削除します。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 IGMP 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。
- [最終メンバー クエリー カウンタ]: このデバイスがクエリアとして選出されている場合に、グループ メンバーがこれ以上存在しないとデバイスが判断する基準となる、MLD グループ固有のクエリーの送信回数。この値に達すると、デバイスはグループ メンバーがこれ以上存在しないと見なします。
  - [クエリーロバストネスの使用(x)]: この値は、[MLD インターフェイス設定] ページで設定されます。括弧内の数字は現在のクエリー ロバストネス値です。
  - [ユーザ定義]: ユーザ定義値を入力します。
- [IGMP クエリア ステータス]: 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]: IGMP クエリアの選出を有効にするか、無効にするか。IGMP クエリア選出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 で指定された標準的な IGMP クエリア選出メカニズムをサポートします。

  IGMP クエリア選出メカニズムが無効になっている場合、IGMP スヌーピング クエリアは、有効化された後に一般クエリー メッセージの送信を 60 秒間遅らせ、他のクエリアがなければ一般クエリー メッセージを送信し始めます。他のクエリアを検出すると、一般クエリー 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、次に示すクエリー パッシブ間隔で別のクエリアの機能を検出した場合、一般クエリー メッセージの送信を再開します。ロバストネス * (クエリー間隔) + 0.5 * クエリー応答間隔
- [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。それ以外の場合は 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、デバイスの送信元インターフェイスを選択します。MLD では、システムによってこのアドレスが自動選択されます。

注 [自動] オプションが選択されている場合、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。

ステップ 3 [適用] 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 IGMP スヌーピング タイマー設定(クエリー ロバストネス(堅牢性)、クエリー間隔など)を変更しても、すでに作成済みのタイマーに対しては影響を及ぼしません。

IGMP インターフェイス設定

マルチキャスト ルータ ポートとして定義されたインターフェイスは、すべての IGMP パケット(報告とクエリー)およびすべてのマルチキャスト データを受信します。

インターフェイス上で IGMP を定義するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPv4マルチキャストコンフィギュレーション] > [IGMPインターフェイス設定] をクリックします。

IGMP が有効になっているそれぞれの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。

- [インターフェイス名]:IGMP スヌーピングが定義されるインターフェイス。
- [ルータIGMPバージョン]:IGMP バージョン。
- [クエリー ロバストネス]:リンクで想定されるパケット損失数を入力します。
- [クエリー間隔](秒):このデバイスがクエリアとして選出された場合に使用される、一般クエリーの送信間隔。
- [クエリー最大応答間隔](秒):定期的な一般クエリーに挿入される最大応答コードを計算するために使われる遅延時間。
- [最終メンバー クエリー間隔(ミリ秒)]:選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延。
- [マルチキャストTTLしきい値]: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)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。

値 256 は、どのマルチキャスト パケットもインターフェイスで転送されないことを意味します。

境界ルータでのみ TTL しきい値を設定してください。逆に言うと、TTL しきい値が設定されたルータは自動的に境界ルータになります。

ステップ 2 インターフェイスを選択し、[編集] をクリックします。上記で説明されたフィールドの値を入力します。

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

IGMP VLAN 設定

特定の VLAN における IGMP を設定するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPv4マルチキャストコンフィギュレーション] > [IGMP VLAN設定] をクリックします。

IGMP が有効になっているそれぞれの VLAN について、次のフィールドが表示されます。

- [インターフェイス名]: IGMP スヌーピングが定義される VLAN。
- [ルータIGMPバージョン]: IGMP スヌーピングのバージョン。
- [クエリー ロバストネス]: リンクで想定されるパケット損失数を入力します。
- [クエリー間隔](秒): このデバイスがクエリアとして選出された場合に使用される、一般クエリーの送信間隔。
- [クエリー最大応答間隔](秒): 定期的な一般クエリーに挿入される最大応答コードを計算するために使われる遅延時間。
- [最終メンバー クエリー間隔(ミリ秒)]: 選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延を入力します。
- [マルチキャストTTLしきい値]: インターフェイス上で転送されるパケットの存続可能時間(TTL)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。

値 256 は、どのマルチキャスト パケットもインターフェイスで転送されないことを意味します。

境界ルータでのみ TTL しきい値を設定してください。逆に言うと、TTL しきい値が設定されたルータは自動的に境界ルータになります。

ステップ 2 インターフェイスを選択し、[編集] をクリックします。上記で説明されたフィールドの値を入力します。

ステップ 3 [適用] 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

IGMP プロキシを設定するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPv4マルチキャストコンフィギュレーション] > [IGMPプロキシ] をクリックします。

ステップ 2 次のグローバル フィールドを入力します。

- [IGMP マルチキャストルーティング]: これを選択すると、IPv4 マルチキャスト ルーティングが有効になります。
- [ダウンストリーム保護]: これを選択すると、デバイスに必要でないダウンストリーム パケットが破棄されます。
- [ソース固有マルチキャスト]: これを選択すると、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 パケットを送信できるようになります。
- [SSM Ipv4アクセスリスト]: マルチキャスト パケット送信の送信元アドレスを含むリストを定義します。
  - [デフォルトリスト]: SSM 範囲アクセス リストを 232.0.0.0/8 に定義します。
  - [ユーザ定義アクセスリスト]: SSM 範囲を定義する標準的な IPv4 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、[アクセス リスト] で定義されます。

ステップ 3 [適用] 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、[追加] 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はこのフィールドがグレーで表示されます。

- [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。ダウンストリーム インターフェイスは複数存在できます。
- [ダウンストリーム保護]:次のいずれかのオプションを選択します。
  - [グローバルの使用]:グローバル ブロックで設定されたステータスを使用します。
  - [無効]:ダウンストリーム インターフェイスからの IPv4 マルチキャスト トラフィックの転送が可能になります。
  - [有効]:ダウンストリーム インターフェイスからの転送が不可になります。

ステップ 5 [適用] 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 ルートごとに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。
- [グループアドレス]:マルチキャスト宛先 IPv4 アドレス。
- [入力インターフェイス]:送信元からのマルチキャスト パケットに期待されるインターフェイス。このインターフェイスで受信されないパケットは、破棄されます。
- [出力インターフェイス]:パケットの転送に使われるインターフェイス。
- [アップタイム]:アイテムが IP マルチキャスト ルーティング テーブルに存在している経過時間の長さ(時間、分、秒)。
- [期限切れ時間]:アイテムが 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

次のページで、IPv6 マルチキャスト コンフィギュレーションを設定します。

- MLD スヌーピング
- MLD インターフェイス設定
- MLD VLAN 設定
- MLD プロキシ

MLD スヌーピング

選択的な IPv6 マルチキャスト転送を可能にするには、(プロパティ ページで)ブリッジ マルチキャスト フィルタリング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、次のようにします。

ステップ 1 [マルチキャスト] > [IPv6マルチキャストコンフィギュレーション] > [MLDスヌーピング] をクリックします。

MLD スヌーピング ステータスをグローバルで有効にした場合、デバイス上でネットワーク トラフィックが監視され、マルチキャスト トラフィックの受信を要求したホストが特定されます。デバイスで MLD スヌーピングが実行されるのは、MLD スヌーピングとブリッジ マルチキャスト フィルタリングの両方が有効になっている場合だけです。

MLD スヌーピング テーブルが表示されます。表示されたフィールドの説明が下の [編集] ページに表示されます。加えて、次のフィールドが表示されます。

- [MLDスヌーピングステータス]:MLD スヌーピングが有効になっているかどうか([管理]) とそれが実際に VLAN 上で動作しているかどうか([動作]) を表示します。
- [MLD クエリア ステータス]:MLD クエリアが有効になっているかどうか([管理]) と、それが実際に VLAN 上で動作しているかどうか([動作]) を表示します。

ステップ 2 次の機能を有効または無効にします。

- [MLDスヌーピングステータス]: これを選択すると、すべてのインターフェイスで MLD スヌーピングがグローバルに有効になります。
- [MLD クエリア ステータス]: これを選択すると、すべてのインターフェイスで MLD クエリアが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の MLD プロキシを設定するには、スタティック VLAN を選択して [編集] をクリックします。次のフィールドを入力します。

- [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。デバイスでネットワーク トラフィックが監視され、マルチキャスト トラフィックの受信を要求したホストが特定されます。デバイスで MLD スヌーピングが実行されるのは、MLD スヌーピングとブリッジ マルチキャスト フィルタリングの両方の機能が有効になっている場合だけです。
- [マルチキャストルータポート自動学習]: これを選択すると、マルチキャスト ルータの自動学習が有効になります。

- [即時脱退]: これを選択すると、スイッチは、脱退メッセージを送信してきたインターフェイスを転送テーブルから削除する際、まず最初に MAC に基づく一般クエリーをそのインターフェイスに送らなくても削除できるようになります。ホストから MLD グループ脱退メッセージを受け取った場合、システムはテーブル エントリからそのホストのポートを削除します。マルチキャスト ルータからの MLD クエリーを中継した後、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。
- [最終メンバー クエリー カウンタ]: このデバイスがクエリアとして選出されている場合に、グループ メンバーがこれ以上存在しないとデバイスが判断する基準となる、MLD グループ固有のクエリーの送信回数。この値に達すると、デバイスはグループ メンバーがこれ以上存在しないと見なします。
  - [クエリーロバストネスの使用(x)]: この値は、[MLD インターフェイス設定] ページで設定されます。括弧内の数字は現在のクエリー ロバストネス値です。
  - [ユーザ定義]: ユーザ定義値を入力します。
- [MLD クエリア ステータス]: 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 クエリア選出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 で指定された標準的な MLD クエリア選出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ー メッセージの送信を 60 秒間遅らせ、他のクエリアがなければ一般クエリー メッセージを送信し始めます。他のクエリアを検出すると、一般クエリー 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、次に示すクエリー パッシブ間隔で別のクエリアの機能を検出した場合、一般クエリー メッセージの送信を再開します。ロバストネス * (クエリー間隔) + 0.5 * クエリー応答間隔
- [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される 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。それ以外の場合は MLDv1 を選択します。

ステップ 4 [適用] 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 MLD スヌーピング タイマー設定(クエリー ロバストネス(堅牢性)、クエリー間隔など)を変更しても、すでに作成済みのタイマーに対しては影響を及ぼしません。

MLD インターフェイス設定

マルチキャスト ルータ ポートとして定義されたインターフェイスは、すべての MLD パケット(報告とクエリー)およびすべてのマルチキャスト データを受信します。

インターフェイスをマルチキャスト ルータ インターフェイスとして設定するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPv6マルチキャストコンフィギュレーション] > [MLDインターフェイス設定] をクリックします。

MLD が有効になっているそれぞれの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。

- [ルータMLDバージョン]:マルチキャスト ルータの MLD バージョン。
- [クエリー ロバストネス]:リンクで想定されるパケット損失数を入力します。
- [クエリー間隔](秒):このデバイスがクエリアとして選出された場合に使用される、一般クエリーの送信間隔。
- [クエリー最大応答間隔](秒):定期的な一般クエリーに挿入される最大応答コードを計算するために使われる遅延時間。
- [最終メンバー クエリー間隔(ミリ秒)]:選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延。
- [マルチキャストTTLしきい値]: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)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。

  値 256 は、どのマルチキャスト パケットもインターフェイスで転送されないことを意味します。

  境界ルータでのみ TTL しきい値を設定してください。逆に言うと、TTL しきい値が設定されたルータは自動的に境界ルータになります。

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 [編集] をクリックします。上記で説明されているフィールドに入力します。

ステップ 3 [適用] 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、次のようにします。

ステップ 1 [マルチキャスト] > [IPv6マルチキャストコンフィギュレーション] > [MLD VLAN設定] をクリックします。

MLD が有効になっているそれぞれの VLAN について、次のフィールドが表示されます。

- [インターフェイス名]:MLD 情報が表示されている対象の VLAN。
- [ルータ MLD バージョン]:MLD ルータのバージョン。
- [クエリー ロバストネス]:リンクで想定されるパケット損失数を入力します。
- [クエリー間隔](秒):このデバイスがクエリアとして選出された場合に使用される、一般クエリーの送信間隔。
- [クエリー最大応答間隔](秒):定期的な一般クエリーに挿入される最大応答コードを計算するために使われる遅延時間。
- [最終メンバー クエリー間隔(ミリ秒)]:選出されたクエリアから送られたグループ固有のクエリーの最大応答時間値をデバイスが読み込めない場合に使用される最大応答遅延を入力します。
- [マルチキャストTTLしきい値]: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)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。

  値 256 は、どのマルチキャスト パケットもインターフェイスで転送されないことを意味します。

  境界ルータでのみ TTL しきい値を設定してください。逆に言うと、TTL しきい値が設定されたルータは自動的に境界ルータになります。

ステップ 2 VLAN を設定するには、それを選択して [編集] をクリックします。上記に説明されているフィールドに入力します。

ステップ 3 [適用] 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

ステップ 4 MLD プロキシを構成するには、次のようにします。

ステップ 1 [マルチキャスト] > [IPv6マルチキャストコンフィギュレーション] > [MLDプロキシ] をクリックします。

ステップ 2 次のフィールドを入力します。

- [MLDマルチキャストルーティング]: これを選択すると、IPv6 マルチキャスト ルーティングが有効になります。
- [ダウンストリーム保護]: これを選択すると、デバイスに必要でないダウンストリーム パケットが破棄されます。
- [ソース固有マルチキャスト]: これを選択すると、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 パケットを送信できるようになります。
- [SSM IPv6アクセスリスト]: マルチキャスト パケット送信の送信元アドレスを含むリストを定義します。
  - [デフォルトリスト]: SSM 範囲アクセス リストを FF3E::/32 に定義します。
  - [ユーザ定義アクセスリスト]: SSM 範囲を定義する標準的な 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、[アクセス リスト] で定義されます。

ステップ 3 [適用] 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、[追加] 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]: 発信インターフェイスを選択します。
- [ダウンストリームインターフェイス]: 着信インターフェイスを選択します。
- [ダウンストリーム保護]: 次のいずれかのオプションを選択します。
  - [グローバルの使用]: グローバル ブロックで設定されたステータスを使用します。
  - [無効]: ダウンストリーム インターフェイスからの IPv6 マルチキャスト トラフィックの転送が可能になります。
  - [有効]: ダウンストリーム インターフェイスからの転送が不可になります。

ステップ 5 [適用] 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。

IP マルチキャスト ルートごとに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。
- [グループアドレス]:マルチキャスト宛先 IPv4 アドレス。
- [入力インターフェイス]:送信元からのマルチキャスト パケットに期待されるインターフェイス。このインターフェイスで受信されないパケットは、破棄されます。
- [出力インターフェイス]:パケットの転送に使われるインターフェイス。
- [アップタイム]:アイテムが IP マルチキャスト ルーティング テーブルに存在している経過時間の長さ(時間、分、秒)。
- [期限切れ時間]:アイテムが 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)。

IGMP/MLD スヌーピング IP マルチキャスト グループ

[IGMP/MLDスヌーピングIPマルチキャストグループ] ページには、IGMP/MLD メッセージから学習された IPv4 および IPv6 のグループ アドレスが表示されます。

このページに表示される情報は、[MAC グループ アドレス] ページの情報と異なる場合があります。たとえば、システムが MAC に基づくグループに従ってフィルタリングを行っている状況で、あるポートがマルチキャスト グループ 224.1.1.1 および 225.1.1.1 への参加を要求していて、その両方のグループが同じ MAC マルチキャスト アドレス 01:00:5e:01:01:01にマップされているとします。この場合、MAC マルチキャストのページにはエントリが 1 つしか表示されませんが、[IGMP/MLD IP マルチキャストグループ] ページにはエントリが 2 つ表示されます。

IP マルチキャスト グループを照会するには、次のようにします。

ステップ 1 [マルチキャスト] > [IGMP/MLDスヌーピングIPマルチキャスト グループ] をクリックします。

ステップ 2 検索するスヌーピング グループのタイプを設定します(IGMP または MLD)。

ステップ 3 次のクエリー フィルタ基準の一部または全部を指定します。

- [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 アドレスを定義します。
- [送信元アドレスが次に等しい]:照会する送信側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 [実行] をクリックします。マルチキャスト グループごとに次のフィールドが表示されます。

- [VLAN ID]:VLAN の ID。
- [グループアドレス]:マルチキャスト グループの MAC アドレスまたは IP アドレス。
- [送信元アドレス]:指定したすべてのグループ ポートに対する送信側アドレス。
- [含まれるポート]:マルチキャスト ストリームの宛先ポートのリスト。
- [除外ポート]:このグループに含まれないポートのリスト。
- [互換モード]:IP グループ アドレスに関してデバイスが受信したホスト登録情報の最も古い 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 ポートとは、マルチキャスト ルータが接続されているポートのことです。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 ルータ上でマルチキャスト ストリームを順次転送し、登録メッセージを他のサブネットに伝達するには、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 ポートの静的な設定、または動的な設定の確認を行うには、次のようにします。

ステップ 1 [マルチキャスト] > [マルチキャストルータポート] をクリックします。

ステップ 2 次のクエリー フィルタ基準の一部または全部を指定します。

- [VLAN IDが次に等しい]:記述されるルータ ポートの VLAN ID を選択します。

- [IPバージョンが次に等しい]:マルチキャスト ルータでサポートされている IP バージョンを選択します。
- [インターフェイスタイプが次に等しい]:ポートまたは LAG のどちらを表示するかを選択します。

ステップ 3 [実行] をクリックします。クエリー基準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、関連付けタイプを選択します。選択項目は次のとおりです。

- [スタティック]:このポートをマルチキャスト ルータ ポートとして静的に設定します。
- [ダイナミック]:(表示のみ) このポートは MLD/IGMP クエリー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 スヌーピング] ページ、または、[MLD スヌーピング] ページを使用します。
- [禁止]:このポートで IGMP/MLD クエリーが受信された場合でも、このポートをマルチキャスト ルータ ポートとして設定しません。ポートで [禁止] 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)。
- [なし]: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 [適用] をクリックしてデバイスを更新します。

すべて転送

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は、登録済みマルチキャスト グループへのマルチキャスト パケットが IGMP スヌーピングと MLD スヌーピングに基づいてポートに転送されます。ブリッジ マルチキャスト フィルタリングが無効になっている場合は、すべてのマルチキャスト パケットが対応する VLAN にフラッディングされます。

[すべて転送] ページでは、特定の VLAN からマルチキャスト ストリームを受信するポートや 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 アドレスの特徴 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。無効になっている場合、すべてのマルチキャスト トラフィックがデバイス上のポートにフラッディングされます。

ポートに接続されているデバイスで IGMP または MLD がサポートされていない場合、そのポートに対して全マルチキャスト転送を静的に(手動で)設定できます。

IGMP メッセージと MLD メッセージを除くマルチキャスト パケットは、必ず、[すべて転送] として定義された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にのみ影響を与えます。

全マルチキャスト転送を設定するには、次のようにします。

ステップ 1 [マルチキャスト] > [すべて転送] をクリックします。

ステップ 2 次の項目を定義します。

- [VLAN IDが次に等しい]: 表示するポート/LAG の VLAN ID。
- [インターフェイスタイプが次に等しい]: ポートまたは LAG のどちらを表示するかを定義します。

ステップ 3 [実行] 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 以下を使用して、「すべて転送」として設定するポート/LAG を選択します。

- [スタティック]: このポートはすべてのマルチキャスト ストリームを受信します。
- [禁止]: IGMP/MLD スヌーピングにより、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。
- [なし]: このポートは現在、「すべて転送」ポートではありません。

ステップ 5 [適用] 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。

未登録マルチキャスト

この機能を使用すると、要求(登録)されたマルチキャスト グループだけを受信することができます。ネットワークで送信されるその他の(未登録の)マルチキャストは受信されません。

未登録マルチキャスト フレームは、通常 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 ストリームを受信または拒否(フィルタリング)するポートを選択できます。この設定は、そのポートがメンバーである(またはメンバーになる予定の)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、次のようにします。

ステップ 1 [マルチキャスト] > [登録解除済みマルチキャスト] をクリックします。

ステップ 2 [インターフェイスタイプが次に等しい] を選択して、ポートまたは LAG を表示します。

ステップ 3 [実行] をクリックします。

ステップ 4 次の項目を定義します。

- [ポート/LAG]: ポートまたは LAG の ID を表示します。
- 選択したインターフェイスの転送ステータスが表示されます。表示される値は次のとおりです。
  - [フォワーディング]: 選択したインターフェイスへの、未登録マルチキャスト フレームのフォワーディングを有効にします。
  - [フィルタリング]: 選択したインターフェイスでの、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 [適用] をクリックします。設定値が保存され、実行コンフィギュレーション ファイルが更新されます。

16

IP コンフィギュレーション

IP インターフェイスのアドレスは、ユーザが手動で割り当てるか、または、DHCP サーバ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 IP 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。

ここで説明する内容は次のとおりです。

- 概要
- ループバック インターフェイス
- IPv4 の管理およびインターフェイス
- IPv6 の管理およびインターフェイス
- ポリシーベースのルーティング
- ドメイン ネーム システム

概要

ジャンボ フレームが無効である場合、トラフィックに関する L3 トラフィック MTU は 1518 バイトに制限されます。

ジャンボ フレームが有効である場合、トラフィックに関する L3 トラフィック MTU は 9000 バイトに制限されます。

工場出荷時の IPv4 インターフェイス設定では、デフォルト VLAN は *DHCPv4* です。つまり、デバイスは DHCPv4 クライアントとして動作し、起動時にデバイスから DHCPv4 要求が送信されます。

DHCPv4 サーバから、IPv4 アドレスが含まれている DHCPv4 応答が受信された場合、デバイスから Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットが送信されます。これにより、一意の IP アドレスが割り当てられます。「IPv4 アドレスが使用中である」という内容の DHCP 応答が受信された場合は、デバイスからその DHCP サーバに DHCPDECLINE メッセージが送信され、続いて、DHCPDISCOVER パケットが再度送信され、DHCP サーバ検出プロセスがやり直されます。

60 秒以内に DHCPv4 応答が受信されなかった場合、デバイスから DHCPDISCOVER クエリーが引き続き送信されると共に、デフォルトの IPv4 アドレス192.168.1.254/24 が使用されます。

同じ IP サブネット上で複数のデバイスによって同じ IP アドレスが使用されている場合、IP アドレス衝突が発生します。IP アドレス衝突が発生した場合、DHCP サーバ上、または、IP アドレスがデバイスと衝突するデバイス上、あるいはその両方で、管理作業を行う必要があります。

デフォルト VLAN に関する IP アドレス割り当てルールは次のとおりです。

- デバイスにスタティック IPv4 アドレスが設定されていない場合、DHCPv4 サーバから応答が受信されるまで、デバイスから DHCPv4 クエリーが送信され続けます。
- デバイスの IP アドレスが変更された場合、Gratuitous ARP パケットがデバイスから VLAN に送信され、IP アドレスが衝突していないかどうかが検査されます。このルールは、デバイスの IP アドレスがデフォルト値に戻された場合にも適用されます。
- DHCP サーバから新しい一意の IP アドレスが割り当てられると、システム ステータス LED が緑で点灯します。スタティック IP アドレスを割り当てた場合も、システム ステータス LED は緑で点灯します。IP アドレス割り当て処理中、および出荷時設定の IP アドレス（192.168.1.254）が使用されている場合、システム ステータス LED は点滅します。
- リース期間終了前にクライアントが DHCPREQUEST メッセージを送信してリース期間を更新しなければならない場合、同様のルールが適用されます。
- 出荷時設定では、スタティック IP アドレスも DHCP サーバから割り当てられた IP アドレスも使用できない場合、デフォルトの IP アドレスが使用されます。デフォルト以外の IP アドレスが使用可能になると、その IP アドレスが自動的に使用されます。デフォルトの IP アドレスは、常に管理 VLAN 上にあります。

デバイスには複数の IP アドレスを設定できます。各 IP アドレスを、指定されたポート、LAG、または VLAN に割り当てることができます。これらの IP アドレスは [IPv4 インターフェイス] ページと [Ipv6 インターフェイス] ページで設定します。デバイスには、対応するインターフェイスからそのすべての IP アドレスにアクセスできます。

事前に定義されたデフォルト ルートは提供されません。デバイスをリモート管理するには、デフォルト ルートを定義する必要があります。DHCP 割り当てのすべてのデフォルト ゲートウェイがデフォルト ルートとして保存されます。さらに、デフォルト ルートを手動で定義することもできます。これは、[IPv4 スタティック ルート] ページと [IPv6 ルータ] ページで定義します。

このガイドでは、デバイスに設定または割り当てられている IP アドレスは、すべて、管理 IP アドレスとして参照しています。

ループバック インターフェイス

概要

ループバック インターフェイスは、動作状態が常にオンになっている仮想インターフェイスです。リモート IP アプリケーションと通信する際にこの仮想インターフェイスで設定されている IP アドレスがローカル アドレスとして使用される場合、リモート アプリケーションまでの実際のルートが変更されたとしても、通信は中断されません。

ループバック インターフェイスの動作状態は常にオンです。IP アドレス（IPv4 か IPv6 のいずれか）を定義し、その IP アドレスを、リモート IP アプリケーションとの IP 通信のローカル IP アドレスとして使用します。リモート アプリケーションが、スイッチのアクティブ（ループバック以外の）IP インターフェイスのいずれか 1 つからアクセス可能である限り、通信はそのまま維持されます。一方、リモート アプリケーションとの通信でいずれかの IP インターフェイスの IP アドレスが使用される場合、その IP インターフェイスがダウンすると通信が終了することになります。

ループバック インターフェイスではブリッジ機能がサポートされておらず、VLAN のメンバーになることはできませんし、レイヤ 2 プロトコルを有効にすることもできません。

IPv6 リンクのローカル インターフェイス ID は 1 です。

ループバック インターフェイスの設定

IPv4 ループバック インターフェイスを設定するには、IPv4 インターフェイスでループバック インターフェイスを追加します。

IPv6 ループバック インターフェイスを設定するには、IPv6 アドレスでループバック インターフェイスを追加します。

IPv4 の管理およびインターフェイス

ここで説明する内容は次のとおりです。

- IPv4 インターフェイス
- IPv4 スタティック ルート
- IPv4 転送テーブル
- RIPv2

- VRRP
- ARP
- ARP プロキシ
- UDP リレー/IP ヘルパー
- DHCP スヌーピング/リレー
- DHCP サーバ

IPv4 インターフェイス

Web ベースのコンフィギュレーション ユーティリティを使用してデバイスを管理するには、IPv4 デバイス管理 IP アドレスが定義されていて、かつ、その IP アドレスを知っている必要があります。デバイスの IP アドレスは、手動で割り当てることも、DHCP サーバから自動的に割り当てることもできます。

[IPv4インターフェイス] ページは、デバイス管理用の IP アドレスを設定するために使用します。この IP アドレスは、ポート、LAG、VLAN、ループバック インターフェイス、またはアウトオブバンド インターフェイスに対して設定できます。

注 デバイスのソフトウェアは、1 つのポートまたは LAG に設定されているすべての IP アドレスに 1 つずつ VLAN ID (VID) を割り当てます。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、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス]> [IPv4インターフェイス] をクリックします。

IPv4 ルーティングを有効にするには、[有効] ボックスをオンにします。

ステップ 2 [適用] 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。

[IPv4インターフェイステーブル] に次のフィールドが表示されます。

- [インターフェイス]: IP アドレスが定義されているユニット/インターフェイス。これはアウトオブバンド ポートにすることもできます。
- [IPアドレスタイプ]: 使用可能なオプションを以下に示します。
  - [DHCP]: DHCP サーバから受信したもの。
  - [スタティック]: 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非 DHCP インターフェイスです。

- [デフォルト]:設定の実行前からデフォルトでデバイス上に存在するデフォルト アドレス。

- [IP アドレス]:インターフェイスに設定されている IP アドレス。
- [マスク]:設定されている IP アドレス マスク。
- [ステータス]:IP アドレス重複チェックの結果。
  - [暫定]:IP アドレス重複チェックの最終結果はありません。
  - [有効]:IP アドレスのコリジョン チェックが完了しており、IP アドレスのコリジョンは検出されませんでした。
  - [妥当な重複]:IP アドレス重複チェックが完了しており、IP アドレスの重複が検出されました。
  - [重複]:デフォルト IP アドレスの、IP アドレスの重複が検出されました。
  - [遅延]:DHCP クライアントが始動時に有効なら、DHCP アドレス検出のための時間を取るため、IP アドレスの割り当ては 60 秒間遅延されます。
  - [未受信]:DHCP アドレス関連。DHCP クライアントによる検出プロセスの開始時には、実アドレス取得の前にダミー IP アドレス 0.0.0.0 が割り当てられます。このダミー アドレスのステータスは「未受信」です。

ステップ 3 [追加] をクリックします。

ステップ 4 次のいずれかのフィールドを選択します。

- [インターフェイス]:この IP コンフィギュレーションに関連するインターフェイスとしてポート、OOB ポート、LAG、ループバック、または VLAN を選択し、リストからインターフェイスを選択します。
- [IPアドレスタイプ]:次のいずれかのオプションを選択します。
  - [ダイナミック IP アドレス]:IP アドレスを DHCP サーバから受け取ります。
  - [スタティック IP アドレス]:IP アドレスを入力します。

ステップ 5 [スタティック IP アドレス] が選択されている場合は、[マスク] フィールドに入力します。

- [IPアドレス]:インターフェイスの IP アドレスを入力します。
- [ネットワークマスク]:このアドレスの IP マスク。
- [プレフィックス長]:IPv4 プレフィックスの長さ。

ステップ 6 [適用] 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、バックアップ マスター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、スタッキング マスター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。バックアップ マスター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、スタックの元のマスター対応ユニットで受信したものとは異なる IP アドレスを受信する可能性があります。

IPv4 スタティック ルート

このページでは、デバイス上の IPv4 スタティック ルートの設定と表示を実行できます。トラフィックのルーティング時、ネクスト ホップはプレフィックスの最長一致に従って決定されます（LPM アルゴリズム）。1 つの宛先 IPv4 アドレスが、IPv4 スタティック ルート テーブルの複数のルートに一致する可能性があります。デバイスで使用されるのは、サブネット マスクが最も高いルート、つまりプレフィックス最長一致です。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、設定されているすべてのデフォルト ゲートウェイのうち最も低い 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、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [IPv4 スタティック ルート] の順にクリックします。

IPv4 スタティック ルート テーブルが表示されます。エントリごとに次のフィールドが表示されます。

- [送信先 IP プレフィックス]: 宛先 IP アドレス プレフィックス。
- [プレフィックス長]: 宛先 IP の IP ルート プレフィックス。
- [ルート タイプ]: ルートは拒否ルート、リモート ルートのうちどれか。
- [ネクスト ホップ ルータ IP アドレス]: ルート上のネクスト ホップ IP アドレスまたは IP エイリアス。
- [メトリック]: このホップのコスト（低い値ほど良い）。
- [送信インターフェイス]: このルートの送信インターフェイス。

- [トラッキング オブジェクト ID]:(550 ファミリでのみサポートされます)このエントリに関連付けられた IP SLA トラック オブジェクト ID。このフィールドと次のフィールドは、SLA が存在する場合にのみ表示されます。
- [トラック ステータス]:(550 ファミリでのみサポートされます)追跡するオブジェクトのステータス(アップまたはダウン)。

注 ルーティング エントリの IP SLA オブジェクト トラッキング ID を定義すると、指定されたネクスト ホップ経由でリモート ネットワークへの接続がチェックされます。接続が存在しない場合は、オブジェクト トラック ステータスがダウンに設定され、ルータが転送テーブルから削除されます(「IP 設定:SLA」の項で詳細を確認してください)。

ステップ 2 [追加] 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。

- [送信先 IP プレフィックス]:宛先 IP アドレス プレフィックスを入力します。
- [マスク]:以下を選択して入力します。
  - [ネットワーク マスク]: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)。
  - [プレフィックス長]:IP アドレス形式の、宛先 IP の IP ルート プレフィックス。
- [ルート タイプ]:ルート タイプを選択します。
  - [拒否]: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、以下の制御が無効になります。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。
  - [リモート]:このルートがリモート パスであることを示します。
- [ネクストホップルータIPアドレス]:ルート上のネクスト ホップ 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 サーバから IP アドレスを取得する場合、直接接続 IP サブネットを通じてスタティック ルートを設定することはできません。
- [メトリック]: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。
- [IP SLA トラック]:(550 ファミリのみ)このエントリと IP SLA オブジェクトの関連付けを有効にする場合に選択します。このフィールドと次のフィールドは、SLA が存在する場合にのみ表示されます。

- [トラッキング オブジェクト ID]:(550 ファミリのみ)オブジェクト ID を入力します。このフィールドと次のフィールドは、SLA が存在する場合にのみ表示されます。

ステップ 4 [適用] をクリックします。IP スタティック ルートが、実行コンフィギュレーション ファイルに保存されます。

IPv4 転送テーブル

IPv4 転送テーブルを表示するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [IPv4 転送テーブル] の順にクリックします。

IPv4 転送テーブルが表示されます。エントリごとに次のフィールドが表示されます。

- [送信先 IP プレフィックス]:宛先 IP アドレス プレフィックス。
- [プレフィックス長]:宛先 IP の IP ルート プレフィックスの長さ。
- [ルート タイプ]:ルートはローカル ルート、拒否ルート、リモート ルートのうちどれか。
- [ネクスト ホップ ルータ IP アドレス]:ネクスト ホップ IP アドレス。
- [ルート オーナー]:以下のオプションのうちのいずれか 1 つ。
  - [デフォルト]:デフォルト システム コンフィギュレーションによって設定されたルート。
  - [スタティック]:手動で作成されたルート。
  - [ダイナミック]:IP ルーティング プロトコルによって作成されたルート。
  - [DHCP]:DHCP サーバから受け取ったルート。
  - [直接接続]:デバイスが接続されるサブネット。
- [メトリック]:このホップのコスト(低い値ほど良い)。
- [管理ステータス]:ネクスト ホップまでの管理距離(低い値ほど良い)。これは、スタティック ルートには関係ありません。
- [送信インターフェイス]:このルートの送信インターフェイス。

RIPv2

IP 設定:RIPv2を参照してください。

VRRP

IP 設定:VRRPを参照してください。

ARP

このデバイスには、直接接続されている IP サブネット上にある既知のデバイスがすべて登録された、Address Resolution Protocol(ARP)テーブルが保持されています。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。デバイスでローカル デバイスにパケットを送信またはルーティングすることが必要な場合、ARP テーブルが検索され、そのデバイスの MAC アドレスが取得されます。ARP テーブルには、スタティック アドレスとダイナミック アドレスの両方が登録されます。スタティック アドレスとは、手動で割り当てられたアドレスのことであり、有効期間がありません。デバイス上では、受信された ARP パケットからダイナミック アドレスが生成されます。ダイナミック アドレスには有効期間が設定されています。

注 生成されたトラフィックの転送に加えて、ルーティングでもマッピング情報が使用されます。

ARP テーブルを定義するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス]> [ARP] をクリックします。

ステップ 2 パラメータを入力します。

- [ARP エントリのエージング アウト]:ARP テーブル内でダイナミック アドレスを保持する期間(単位:秒)を入力します。テーブルに登録されている期間が ARP エントリのエージング アウトの時間を超えると、そのダイナミック アドレスは期限切れになります。期限切れになったダイナミック アドレスは ARP テーブルから削除されます。再学習された場合のみ、再登録されます。
- [ARP テーブル エントリのクリア]:システムから削除する ARP エントリのタイプを選択します。
  - [すべて]:すべてのスタティック アドレスとすべてのダイナミック アドレスを今すぐ削除します。
  - [ダイナミック]:すべてのダイナミック アドレスを今すぐ削除します。

- [スタティック]:すべてのスタティック アドレスを今すぐ削除します。
- [標準エージング アウト]:[ARP エントリのエージング アウト] で指定した期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 [適用] 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 テーブルに表示されるフィールドは次のとおりです。

- [インターフェイス]:IP デバイスが存在する直接接続されている IP サブネットに対する、IPv4 インターフェイス。
- [IP アドレス]:IP デバイスの IP アドレス。
- [MAC アドレス]:IP デバイスの MAC アドレス。
- [ステータス]:エントリが手動で入力されたか、動的に学習されたか。

ステップ 4 [追加] をクリックします。

ステップ 5 パラメータを入力します。

- [IP バージョン]:このホストでサポートされている IP アドレス形式。サポートされているのは IPv4 だけです。
- [インターフェイス]:IPv4 インターフェイスをポート、LAG、または VLAN 上に設定することができます。デバイス上で設定されている IPv4 インターフェイスのリストから、目的のインターフェイスを選択します。
- [IP アドレス]:ローカル デバイスの IP アドレスを入力します。
- [MAC アドレス]:ローカル デバイスの MAC アドレスを入力します。

ステップ 6 [適用] 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 のテクニックは、特定の IP サブネット上のデバイスにより、ネットワーク上にないネットワーク アドレスについて問い合わせる ARP クエリーに応答するために使用されます。

注 ARP プロキシ機能は、デバイスが L3 モードの場合にのみ使用できます。

ARP プロキシでは、トラフィックの宛先が認識されており、応答で別の MAC アドレスが提供されます。別のホストの ARP プロキシとして動作すると、LAN トラフィックの宛先を効率的にそのホストに向けられます。一般的には、そのようにして検出されたトラフィックは、別のインターフェイスを使用して、またはトンネルを使用して、プロキシによって意図された宛先へルーティングされます。

プロキシの動作のために異なる IP アドレスを求める ARP クエリー要求が出されて、ノードが自分の MAC アドレスで応答するというプロセスは、パブリッシングと呼ばれることがあります。

すべての IP インターフェイス上で ARP プロキシを有効にするには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス]> [ARPプロキシ] をクリックします。

ステップ 2 [ARP プロキシ] を選択することにより、リモート ノードを求める ARP 要求に対してデバイスが、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 [適用] 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。しかし、この機能によりデバイスは、IPv4 インターフェイスから受け取った特定の 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るようになります。

特定の UDP ポートを宛先とする UDP パケットを特定の IPv4 インターフェイスから受け取った場合のリレー処理を設定するには、UDP リレーを追加します。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス] > [UDPリレー/IPヘルパー] をクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 デバイスが UDP ブロードキャスト パケットを、設定されている UDP 宛先ポートに基づいてリレーする先の [送信元 IP インターフェイス] を選択します。そのインターフェイスは、デバイス上で設定されている IPv4 インターフェイスのうちの 1 つでなければなりません。

ステップ 4 デバイスがリレーするパケットの [UDP 宛先ポート] の番号を入力します。ドロップダウン リストからウェルノウン ポートを 1 つ選択するか、またはポート ラジオ ボタンをクリックして手動で番号を入力します。

ステップ 5 UDP パケット リレーを受信する [宛先 IP アドレス] を入力します。このフィールドが 0.0.0.0 の場合、UDP パケットは破棄されます。このフィールドが 255.255.255.255 の場合、UDP パケットはすべての IP インターフェイスにフラッディングされます。

ステップ 6 [適用] をクリックします。UDP リレー設定が実行コンフィギュレーション ファイルに書き込まれます。

DHCP スヌーピング/リレー

ここで説明する内容は次のとおりです。

- 概要
- プロパティ
- インターフェイス設定
- DHCP スヌーピングで信頼されたインターフェイス
- DHCP スヌーピング バインディング データベース

概要

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ぎ、DHCP アドレスのログを記録するセキュリティ メカニズムを提供します。これは、デバイス上のポートを、信頼できるものと信頼できないもののいずれかとして処理することにより実現されます。

信頼できるポートは、DHCP サーバに接続されているポートであり、DHCP アドレス割り当てが許可されます。信頼できるポート上で受信した DHCP メッセージは、このデバイスの通過が許可されます。

信頼できないポートは、DHCP アドレス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([インターフェイス設定] ページで)信頼できるものとして宣言されるまで、信頼できないものと見なされます。

DHCPv4 リレーの概要

DHCP リレーは、DHCP パケットを DHCP サーバにリレーします。

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 メッセージをリレーすることができます。IP アドレスのない VLAN 上で DHCP リレーが有効になっているなら、常にオプション 82 が自動的に挿入されます。この挿入は特定の VLAN においてなされるものであり、オプション 82 挿入のグローバル管理状態には影響しません。

トランスペアレント DHCP リレー

外部 DHCP リレー エージェントが使用されているトランスペアレント DHCP リレーの場合、以下のことを実行します。

- DHCP スヌーピングを有効にします。
- オプション 82 挿入を有効にします。
- DHCP リレーを無効にします。

正規の DHCP リレーの場合、

- DHCP リレーを有効にします。
- オプション 82 挿入を有効にする必要はありません。

オプション 82

オプション 82（DHCP リレー エージェント情報オプション）は、ポートとエージェントの情報を中央 DHCP サーバに渡して、割り当てられている IP アドレスが物理的にネットワークに接続されている場所を示します。

オプション 82 の主要な目的は、DHCP サーバが、IP アドレス取得元となる最適な 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。

デバイス上では、以下のオプション 82 オプションが利用可能です。

- [DHCP 挿入]：オプション 82 情報を、外部オプション 82 情報のないパケットに追加します。
- [DHCP パススルー]：信頼できないポートから来たオプション 82 情報を含む DHCP パケットを転送または拒否します。信頼できるポートの場合、オプション 82 情報を含む DHCP パケットは常に転送されます。

DHCP リレー、DHCP スヌーピング、およびオプション 82 の各モジュールでのパケットの流れを以下の表に示します。

次のそれぞれの場合が考えられます。

- DHCP クライアントと DHCP サーバとが同じ VLAN に接続されている場合。この場合、正規のブリッジ機能により、DHCP クライアントと DHCP サーバの間で DHCP メッセージがやり取りされます。
- DHCP クライアントと DHCP サーバとが異なる VLAN に接続されている場合。この場合、DHCP リレーのみが、DHCP クライアントと DHCP サーバの間の DHCP メッセージのブロードキャストを実行可能であり、実際にそれを実行します。ユニキャスト DHCP メッセージは正規のルータによって渡されるため、IP アドレスのない VLAN 上で DHCP リレーが有効である場合は、外部ルータが必要になります。

DHCP リレーは、DHCP メッセージを DHCP サーバにリレーします。これを実行するのは、DHCP リレーのみです。

DHCPv4 スヌーピング、DHCPv4 リレー、およびオプション 82 の相互作用

以下の表は、DHCP スヌーピング、DHCP リレー、およびオプション 82 のさまざまな組み合わせに対してデバイスの動作がそれぞれどうなるかを示しています。

DHCP スヌーピングが有効でなく、かつ DHCP リレーが有効である場合に DHCP 要求パケットがどのように処理されるかを以下で示します。

	DHCP リレー IP アドレスのある VLAN		DHCP リレー IP アドレスのない VLAN	
	オプション 82 なしのパケットが着信	オプション 82 ありのパケットが着信	オプション 82 なしのパケットが着信	オプション 82 ありのパケットが着信
オプション 82 挿入無効	オプション 82 なしのパケットを送信	元のオプション 82 が指定されたパケットを送信	リレー:オプション 82 挿入 ブリッジ:オプション 82 挿入なし	リレー:パケットを破棄 ブリッジ:元のオプション 82 が指定されたパケットを送信

	DHCP リレー IP アドレスのある VLAN		DHCP リレー IP アドレスのない VLAN	
オプション 82 挿入有効	リレー:オプション 82 付きで送信 ブリッジ:オプション 82 なしで送信	元のオプション 82 が指定されたパケットを送信	リレー:オプション 82 付きで送信 ブリッジ:オプション 82 なしで送信	リレー:パケットを破棄 ブリッジ:元のオプション 82 が指定されたパケットを送信

DHCP スヌーピングと DHCP リレーの両方が有効である場合に DHCP 要求パケットがどのように処理されるかが以下に示されています。

	DHCP リレー IP アドレスのある VLAN		DHCP リレー IP アドレスのない VLAN	
	オプション 82 なしのパケットが着信	オプション 82 ありのパケットが着信	オプション 82 なしのパケットが着信	オプション 82 ありのパケットが着信
オプション 82 挿入無効	オプション 82 なしのパケットを送信	元のオプション 82 が指定されたパケットを送信	リレー:オプション 82 挿入 ブリッジ:オプション 82 挿入なし	リレー:パケットを破棄 ブリッジ:元のオプション 82 が指定されたパケットを送信
オプション 82 挿入有効	リレー:オプション 82 付きで送信 ブリッジ:オプション 82 追加 (信頼できるポートでは DHCP スヌーピングが無効であるかのように動作)	元のオプション 82 が指定されたパケットを送信	リレー:オプション 82 付きで送信 ブリッジ:オプション 82 挿入 (信頼できるポートでは DHCP スヌーピングが無効であるかのように動作)	リレー:パケットを破棄 ブリッジ:元のオプション 82 が指定されたパケットを送信

DHCP スヌーピングが無効になっている場合に DHCP リレー パケットがどのように処理されるかが以下に示されています。

	DHCP リレー IP アドレスのある VLAN		DHCP リレー IP アドレスのない VLAN	
	オプション 82 なしのパケットが着信	オプション 82 ありのパケットが着信	オプション 82 なしのパケットが着信	オプション 82 ありのパケットが着信
オプション 82 挿入無効	オプション 82 なしのパケットを送信	元のオプション 82 が指定されたパケットを送信	リレー:オプション 82 を破棄 ブリッジ:オプション 82 なしのパケットを送信	リレー: 1応答がデバイス由来の場合、オプション 82 なしのパケットを送信 2応答がデバイス由来でない場合、パケットを破棄 ブリッジ:元のオプション 82 が指定されたパケットを送信
オプション 82 挿入有効	オプション 82 なしのパケットを送信	リレー:オプション 82 なしのパケットを送信 ブリッジ:オプション 82 が指定されたパケットを送信	リレー:オプション 82 を破棄 ブリッジ:オプション 82 なしのパケットを送信	リレー:オプション 82 なしのパケットを送信 ブリッジ:オプション 82 が指定されたパケットを送信

DHCP スヌーピングと DHCP リレーの両方が有効である場合に DHCP 応答パケットがどのように処理されるかが以下に示されています。

	DHCP リレー IP アドレスのある VLAN		DHCP リレー IP アドレスのない VLAN	
	オプション 82 なしのパケットが着信	オプション 82 ありのパケットが着信	オプション 82 なしのパケットが着信	オプション 82 ありのパケットが着信
オプション 82 挿入無効	オプション 82 なしのパケットを送信	元のオプション 82 が指定されたパケットを送信	リレー:オプション 82 を破棄 ブリッジ:オプション 82 なしのパケットを送信	リレー 1応答がデバイス由来の場合、オプション 82 なしのパケットを送信 2応答がデバイス由来でない場合、パケットを破棄 ブリッジ:元のオプション 82 が指定されたパケットを送信
オプション 82 挿入有効	オプション 82 なしのパケットを送信	オプション 82 なしのパケットを送信	リレー:オプション 82 を破棄 ブリッジ:オプション 82 なしのパケットを送信	オプション 82 なしのパケットを送信

DHCP スヌーピング バインディング データベース

DHCP スヌーピングにより、信頼できるポート経由でデバイスに入ってくる DHCP パケットの情報から派生するデータベース(DHCP スヌーピング バインディング データベース)が作成されます。

DHCP スヌーピング バインディング データベースには、以下のデータが含まれています。入力ポート、入力 VLAN、クライアントの MAC アドレス、およびクライアントの IP アドレス(存在する場合)。

また、DHCP スヌーピング バインディング データベースは、正当なパケット送信元を判別するため、IP ソース ガード機能およびダイナミック ARP インスペクション機能によっても使用されます。

DHCP 信頼済みポート

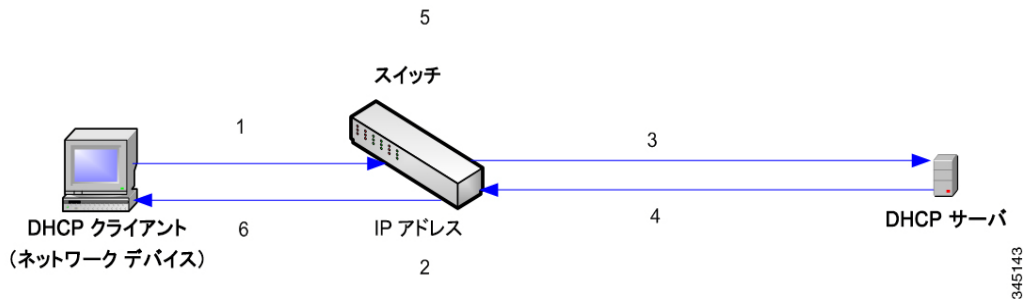
ポートには、DHCP 信頼済みと非信頼とがあります。デフォルトでは、すべてのポートは非信頼です。ポートを信頼済みとして作成するには、[インターフェイス設定] ページを使用します。それらのポートからのパケットは、自動的に転送されます。信頼済みポートからのパケットは、バインディング データベースを作成するために使用され、後述のようにして処理されます。

DHCP スヌーピングが有効になっていない場合、すべてのポートはデフォルトで信頼済みです。

DHCP スヌーピング バインディング データベースの作成方法

DHCP クライアントと DHCP サーバとが両方とも信頼済みの場合、デバイスで DHCP パケットがどう処理されるかを以下に説明します。このプロセスで、DHCP スヌーピング バインディング データベースが作成されます。

DHCP 信頼済みパケットの処理



アクションは次のとおりです。

ステップ 1 デバイスが DHCPDISCOVER を送信して IP アドレスを要求するか、または DHCPREQUEST を送信して IP アドレスを受け入れてリースします。

ステップ 2 デバイスがパケットをスヌープし、IP-MAC 情報を DHCP スヌーピング バインディング データベースに追加します。

ステップ 3 デバイスが DHCPDISCOVER または DHCPREQUEST パケットを転送します。

ステップ 4 DHCP サーバが、DHCPOFFER パケットを送信して IP アドレスを提供するか、DHCPACK を送信してそれを割り当てるか、または DHCPNAK を送信してアドレス要求を拒否します。

ステップ 5 デバイスによりパケットがスヌープされます。パケットに一致する DHCP スヌーピング バインディング テーブルの中にエントリが存在する場合、DHCPACK 受信時にデバイスによりそれが IP-MAC バインディングに置き換えられます。

ステップ 6 デバイスが DHCPOFFER、DHCPACK、または DHCPNAK を転送します。

信頼済みと非信頼のポートから来た DHCP パケットがそれぞれどう処理されるのかを以下に要約します。DHCP スヌーピング バインディング データベースは、不揮発メモリ内に保存されます。

DHCP スヌーピング パケットの処理

パケットのタイプ	非信頼入力インターフェイスから着信	信頼済み入力インターフェイスから着信
DHCPDISCOVER	信頼済みインターフェイスにのみ転送。	信頼済みインターフェイスにのみ転送。
DHCPOFFER	フィルタ。	DHCP 情報に従ってパケットを転送。宛先アドレスが未知なら、パケットはフィルタ処理されます。
DHCPREQUEST	信頼済みインターフェイスにのみ転送。	信頼済みインターフェイスにのみ転送。
DHCPACK	フィルタ。	DHCPOFFER と同じ。エントリが DHCP スヌーピング バインディング データベースに追加されます。
DHCPNAK	フィルタ。	DHCPOFFER と同じ。存在する場合、エントリを削除します。
DHCPDECLINE	データベース中に情報があるかどうかを調べます。情報は存在するものの、メッセージを受信したインターフェイスに一致しない場合、パケットはフィルタ処理されます。そうでない場合、パケットは信頼済みインターフェイスにのみ転送され、データベースからエントリが削除されます。	信頼済みインターフェイスにのみ転送

パケットのタイプ	非信頼入力インターフェイスから着信	信頼済み入力インターフェイスから着信
DHCPRELEASE	DHCPDECLINE と同じ。	DHCPDECLINE と同じ。
DHCPINFORM	信頼済みインターフェイスにのみ転送。	信頼済みインターフェイスにのみ転送。
DHCPLEASEQUERY	フィルタ処理。	転送。

DHCP スヌーピングと DHCP リレー

DHCP スヌーピングと DHCP リレーの両方がグローバルに有効になっている場合、クライアントの VLAN 上で DHCP スヌーピングが有効になっているなら、リレーされるパケットに関し、DHCP スヌーピング バインディング データベース内に含まれている DHCP スヌーピング ルールが適用され、クライアントと DHCP サーバの VLAN において、DHCP スヌーピング バインディング データベースが更新されます。

DHCP デフォルト コンフィギュレーション

以下では、DHCP スヌーピングおよび DHCP リレー デフォルト オプションについて説明します。

オプション	デフォルト状態
DHCP スヌーピング	無効
オプション 82 挿入	無効
オプション 82 パススルー	無効
MAC アドレスの確認	有効
DHCP スヌーピング バインディング データベースのバックアップ	無効
DHCP リレー	無効

DHCP ワークフローの設定

DHCP リレーおよび DHCP スヌーピングを設定するには、次のようにします。

ステップ 1 [プロパティ] ページで、DHCP スヌーピングまたは DHCP リレーを有効にします。

ステップ 2 [インターフェイス設定] ページで、DHCP スヌーピングを有効にするインターフェイスを定義します。

ステップ 3 [DHCP スヌーピングで信頼されたインターフェイス] ページで、インターフェイスを信頼済みまたは信頼されていないに設定します。

ステップ 4 オプション。[DHCP スヌーピング バインディング データベース] ページで、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します。

プロパティ

DHCP リレー、DHCP スヌーピング、およびオプション 82 を設定するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス] > [DHCPスヌーピング/リレー] > [プロパティ] をクリックします。

次のフィールドを入力します。

- [オプション82]:オプション 82 情報をパケット中に挿入する場合、[オプション 82] を選択します。
- [DHCPリレー]:DHCP リレーを有効にする場合に選択します。
- [DHCPスヌーピングステータス]:DHCP スヌーピングを有効にする場合に選択します。
- [オプション 82 パススルー]:パケット転送時に外部オプション 82 情報をそのままにする場合に選択します。
- [MAC アドレスの確認]:DHCP 非信頼ポートにおいて、レイヤ 2 ヘッダーの送信元 MAC アドレスが、DHCP ヘッダーの中で(ペイロードの一部として)現れるクライアント ハードウェア アドレスに一致することを確認する場合に選択します。
- [バックアップデータベース]:デバイスのフラッシュ メモリ上で 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する場合に選択します。

ステップ 2 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

ステップ 3 DHCP サーバを定義するには、[追加] をクリックします。

ステップ 4 DHCP サーバの IP アドレスを入力し、[適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

インターフェイス設定

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 リレーを機能させるには、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。

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、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [DHCP スヌーピング/リレー] > [インターフェイス設定]をクリックします。

ステップ 2 インターフェイス上で DHCP リレーまたは DHCP スヌーピングを有効にするには、[追加] をクリックします。

ステップ 3 有効にするインターフェイスと機能を選択します。[DHCPリレー] と [DHCPスヌーピング] のどちらかまたはその両方。

ステップ 4 [適用] 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 データベースページを参照)。

デフォルトでは、インターフェイスは信頼済みです。

インターフェイスを信頼できないものとして指定するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス] > [DHCPスヌーピング/リレー] > [DHCPスヌーピングで信頼されたインターフェイス] 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、[編集] をクリックします。

ステップ 3 [信頼できるインターフェイス] を選択します([はい] または [いいえ])。

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

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 データベースにダイナミック エントリが追加される方法については、「DHCP スヌーピング バインディング データベースの作成方法」を参照してください。

DHCP スヌーピング バインディング データベースのメンテナンスについては、以下の点に注意してください。

- 端末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っている場合、その VLAN について収集されたバインディング エントリは削除されます。
- データベースが一杯になった場合、DHCP スヌーピングはパケットの転送を続行しますが、新しいエントリは作成されません。IP ソース ガードや ARP インスペクションの機能がアクティブの場合、DHCP スヌーピング バインディング データベースに書き込まれていないクライアントは、ネットワークに接続できません。

DHCP スヌーピング バインディング データベースにエントリを追加するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス]> [DHCP スヌーピング/リレー] > [DHCP スヌーピング バインディング データベース] をクリックします。

DHCP スヌーピング バインディング データベースの中のエントリのサブセットを表示するには、フィルタで該当する検索条件を入力して、[実行] をクリックします。

DHCP スヌーピング バインディング データベースの中のフィールドが表示されます。それらのうち [IP ソース ガード] フィールド以外については、[追加] ページで説明されています。

- **ステータス:**
  - [アクティブ]:デバイス上で IP ソース ガードがアクティブです。
  - [非アクティブ]:デバイス上で IP ソース ガードがアクティブではありません。

- **理由:**
  - *問題なし*
  - *リソースなし*
  - *スヌープ VLAN なし*
  - *ポートを信頼*

ステップ 2 エントリを追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [VLAN ID]:パケットを受信すると予想される VLAN。
- [MAC アドレス]:パケットの MAC アドレス。
- [IP アドレス]:パケットの IP アドレス。
- [インターフェイス]:パケットが予期されているユニット/スロット/インターフェイス。
- [タイプ]:フィールドで可能な値は、次のとおりです。
  - [ダイナミック]:エントリのリース時間は制限されています。
  - [スタティック]:エントリは静的に設定されています。
- [リース時間]:エントリがダイナミックの場合、DHCP データベースの中でそのエントリがアクティブになる時間の長さを入力します。リース時間がない場合、[無制限] をチェックします。

ステップ 4 [適用] をクリックします。設定値が定義され、デバイスが更新されます。

DHCP サーバ

ここで説明する内容は次のとおりです。

- 概要
- プロパティ
- ネットワーク プール
- 除外されるアドレス
- スタティックホスト

- DHCP のオプション
- アドレス バインディング

概要

DHCPv4 サーバ機能により、デバイスを DHCPv4 サーバとして設定することができます。DHCPv4 サーバは、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 サーバは、IPv4 アドレスを、IPv4 アドレスのユーザ定義プールから割り当てます。

それらのモードとしては、以下のものが可能です。

- **スタティック割り当て**：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 1 つの IP アドレスにマッピングされます。これは、[スタティック ホスト] ページで実行します。
- **ダイナミック割り当て**：クライアントは、指定された時間（無制限の場合もある）、リースされる IP アドレスを取得します。割り当てられた IP アドレスを DHCP クライアントが更新しない場合、その期間の終了後にその 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。この作業は [ネットワーク プール] ページで行います。

機能間の依存関係

- システム上に DHCP サーバと DHCP クライアントを同時に設定することは不可能です。つまり、1 つのインターフェイスが DHCP クライアント対応である場合、グローバルに DHCP サーバを有効にすることは不可能です。
- DHCPv4 リレーが有効な場合、デバイスを DHCP サーバとして設定することはできません。

デフォルトの設定値とコンフィギュレーション

- デバイスは、デフォルトでは DHCPv4 サーバとして設定されません。
- デバイスが DHCPv4 サーバとして有効な場合、デフォルトで定義されたアドレスのネットワーク プールはありません。

DHCP サーバ機能を有効にする際のワークフロー

デバイスを DHCPv4 サーバとして設定するには、次のようにします。

ステップ 1 [プロパティ] ページを使用して、デバイスを DHCP サーバとして有効にします。

ステップ 2 割り当てないようにする IP アドレスがある場合は、[除外されるアドレス] ページを使用して設定します。

ステップ 3 [ネットワーク プール] ページを使用して、IP アドレスのネットワーク プールを 16 個まで定義します。

ステップ 4 [スタティックホスト] ページを使用して、固定 IP アドレスを割り当てるクライアントを設定します。

ステップ 5 [DHCP オプション] ページで必須 DHCP オプションを設定します。これにより、関係するあらゆる DHCP オプションについて返される値が設定されます。

ステップ 6 [ネットワーク プール] ページで、設定されている DHCP プールの 1 つの範囲内の IP インターフェイスを追加します。デバイスは、その IP インターフェイスからの DHCP クエリーに応答します。たとえば、プールの範囲が 1.1.1.1～1.1.1.254 の場合、直接接続クライアントが、設定されているプールから IP アドレスを受信するようにするには、その範囲内の IP アドレスを追加します。これは、[IPv4 インターフェイス] ページで行います。

ステップ 7 [アドレスバインディング] ページを使用して、割り当てられている IP アドレスを表示します。IP アドレスは、そのページで削除できます。

プロパティ

デバイスを DHCPv4 サーバとして設定するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス] > [DHCPサーバ] > [プロパティ] をクリックして、[プロパティ] ページを表示します。

ステップ 2 [有効] を選択して、デバイスを DHCP サーバとして設定します。

ステップ 3 [適用] をクリックします。ただちにデバイスは、DHCP サーバとして機能し始めます。しかし、プールを作成するまで、IP アドレスがクライアントに割り当てられることはありません。

ネットワーク プール

デバイスが DHCP サーバとして機能している場合、IP アドレスの 1 つ以上のプールを定義する必要があります。デバイスは、そこから IP アドレスを DHCP クライアントに割り当てます。各ネットワーク プールには、特定のサブネットに属するアドレス範囲が含まれています。それらのアドレスが、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 サーバのデバイスが、以下のようにして IP アドレスを割り当てます。

- **直接接続クライアント**: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 プールからのアドレスが、デバイスにより割り当てられます。

  メッセージが(DHCP リレー経由ではなく)直接に着信した場合、プールはローカル プールであり、入力レイヤ 2 インターフェイスで定義されている IP サブネットの 1 つに属します。その場合、プールの IP マスクは IP インターフェイスの IP マスクと等しくなり、プールの最小および最大の IP アドレスは IP サブネットに属します。

- **リモート クライアント**:デバイスは、DHCP リレー エージェントの IP アドレスと一致する IP サブネットを含むネットワーク プールから IP アドレスを取得します。

  メッセージが DHCP リレー経由で着信した場合は、使用されるアドレスはプールの最小 IP アドレスと IP マスクによって指定される IP サブネットに属し、プールはリモート プールです。

定義できるネットワーク プールは最大 16 個です。

IP アドレスのプールを作成し、それらのリース期間を定義するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4管理およびインターフェイス] > [DHCPサーバ] > [ネットワークプール] をクリックします。

それまでに定義済みのネットワーク プールが表示されます。[追加] ページ内のフィールドについては以下で説明します。次のフィールドが表示されます(ただし、[追加] ページには表示されません)。

- [リースされたアドレスの数]:割り当てられた(リースされた)プール内のアドレスの数。

ステップ 2 [追加] 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。サブネットの IP アドレスとマスクを入力するか、またはマスク、アドレス プールの開始とアドレス プールの終了を入力するかのいずれかであることに注意してください。

ステップ 3 次のフィールドを入力します。

- [プール名]:プール名を入力します。
- [サブネット IP アドレス]:ネットワーク プールの属するサブネットを入力します。
- [マスク]:以下のうちの 1 つを入力します。
  - [ネットワーク マスク]:これをオンにし、プールのネットワーク マスクを入力します。
  - [プレフィックス長]:これをオンにし、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。
- [アドレスプールの開始]:ネットワーク プールの範囲のうち最初の IP アドレスを入力します。
- [アドレス プールの終了]:ネットワーク プールの範囲のうち最後の IP アドレスを入力します。
- [リース期間]:DHCP クライアントがこのプールからの IP アドレスを使用できる期間の長さを入力します。49,710 日間以下のリース期間、または無制限の期間を設定することができます。
  - [無制限]:リースの期間は無制限です。
  - [日間]:リースの期間(日数)。範囲は 0 ～ 49710 日間です。
  - [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。
- [デフォルト ルータ IP アドレス(オプション 3)]:DHCP クライアントのデフォルト ルータを入力します。
- [ドメイン ネーム サーバ IP アドレス(オプション 6)]:デバイス DNS サーバ(設定済みの場合)の 1 つを選択するか、または [その他] を選択して DHCP クライアントから利用可能な DNS サーバの IP アドレスを入力します。
- [ドメイン名(オプション 15)]:DHCP クライアントのドメイン名を入力します。
- [NetBIOS WINS サーバ IP アドレス(オプション 44)]:DHCP クライアントから利用可能な NetBIOS WINS ネーム サーバを入力します。

- [NetBIOS ノード タイプ(オプション 46)]:NetBIOS 名の解決方法を選択します。有効なノード タイプは、次のとおりです。
  - [ハイブリッド]:b ノードと p ノードのハイブリッド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されている場合、常に p ノードの使用が最初に試され、p ノードが失敗した場合にのみ b ノードが使用されます。これはデフォルトです。
  - [混合]:b ノードと p ノードの混合通信を使用して、NetBIOS 名が登録および解決されます。M ノードでは最初に b ノードが使用された後、必要なら p ノードが使用されます。多くの場合、大規模なネットワークにおいては M ノードは最適な選択ではありません。その場合、b ノード ブロードキャストが好んで使用されてネットワーク トラフィックが増加することになるからです。
  - [ピアツーピア]:NetBIOS ネーム サーバによるポイントツーポイント通信を使用して、コンピュータ名が登録され、IP アドレスに解決されます。
  - [ブロードキャスト]:IP ブロードキャスト メッセージを使用して、NetBIOS 名が登録され、IP アドレスに解決されます。
- [SNTP サーバ IP アドレス(オプション 4)]:デバイスの SNTP サーバ(設定済みの場合)の 1 つを選択するか、または [その他] を選択して DHCP クライアントのタイム サーバの IP アドレスを入力します。
- [ファイル サーバ IP アドレス(siaddr)]:コンフィギュレーション ファイルのダウンロード元 TFTP/SCP サーバの IP アドレスを入力します。
- [ファイル サーバ ホスト名(sname/オプション 66)]:TFTP/SCP サーバの名前を入力します。
- [コンフィギュレーション ファイル名(ファイル/オプション 67)]:コンフィギュレーション 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 [適用] 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 サーバでは、プール内のすべてのプール アドレスがクライアントに割り当て可能であることが想定されています。単一 IP アドレスまたはある範囲の IP アドレスを除外することが可能です。除外されたアドレスは、すべての DHCP プールから除外されます。

除外アドレス範囲を定義するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4管理およびインターフェイス] > [DHCPサーバ] > [除外されるアドレス] をクリックします。

それまでに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 除外される IP アドレスの範囲を追加するには、[追加] をクリックして、以下のフィールドを入力します。

- [開始 IP アドレス]:除外される IP アドレスの範囲の中の最初の IP アドレス。
- [終了 IP アドレス]:除外される IP アドレスの範囲の中の最後の IP アドレス。

ステップ 3 [適用] 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

いくつかの DHCP クライアントを、決して変更されない固定 IP アドレスに割り当てることが望ましい場合があるかもしれません。この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 120 台まで定義できます。

固定 IP アドレスを手動で特定のクライアントに割り当てるには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4管理およびインターフェイス] > [DHCPサーバ] > [スタティックホスト] をクリックします。

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は [追加] ページで説明されます。ただし、次のフィールドを除きます。

- [MACアドレス/クライアント識別子]:。

ステップ 2 スタティック ホストを追加するには、[追加] をクリックして、以下のフィールドを入力します。

- [IP アドレス]:スタティックにホストに割り当てられた IP アドレスを入力します。
- [ホスト名]:ホスト名を入力します。これは、シンボルの文字列、または整数です。
- [マスク]:スタティック ホストのネットワーク マスクを入力します。
  - [ネットワーク マスク]:オンにして、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。

- [プレフィックス長]: これをオンにし、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。

- [識別子タイプ]: 特定のスタティック ホストを識別する方法を設定します。
  - [クライアント識別子]: クライアントの固有識別子を 16 進数表記で入力します。例: 01b60819681172。

または

  - [MAC アドレス]: クライアントの MAC アドレスを入力します。

  選択したタイプに応じて、クライアント識別子または MAC アドレスのどちらかを入力します。

- [クライアント名]: ASCII モードの標準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。クライアント名にドメイン名を含めることはできません。
- [デフォルト ルータ IP アドレス (オプション 3)]: スタティック ホストのデフォルト ルータを入力します。
- [ドメイン ネーム サーバ IP アドレス (オプション 6)]: デバイス DNS サーバ (設定済みの場合) の 1 つを選択するか、または [その他] を選択して DHCP クライアントから利用可能な DNS サーバの IP アドレスを入力します。
- [ドメイン名 (オプション 15)]: スタティック ホストのドメイン名を入力します。
- [NetBIOS WINS サーバ IP アドレス (オプション 44)]: スタティック ホストから利用可能な NetBIOS WINS ネーム サーバを入力します。
- [NetBIOS ノード タイプ (オプション 46)]: NetBIOS 名の解決方法を選択します。有効なノード タイプは、次のとおりです。
  - [ハイブリッド]: b ノードと p ノードのハイブリッド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されている場合、常に p ノードの使用が最初に試され、p ノードが失敗した場合にのみ b ノードが使用されます。これはデフォルトです。
  - [混合]: b ノードと p ノードの混合通信を使用して、NetBIOS 名が登録および解決されます。M ノードでは最初に b ノードが使用された後、必要なら p ノードが使用されます。多くの場合、大規模なネットワークにおいては M ノードは最適な選択ではありません。その場合、b ノード ブロードキャストが好んで使用されてネットワーク トラフィックが増加することになるからです。
  - [ピアツーピア]: NetBIOS ネーム サーバによるポイントツーポイント通信を使用して、コンピュータ名が登録され、IP アドレスに解決されます。
  - [ブロードキャスト]: IP ブロードキャスト メッセージを使用して、NetBIOS 名が登録され、IP アドレスに解決されます。

- [SNTP サーバ IP アドレス(オプション 4)]:デバイスの SNTP サーバ(設定済みの場合)の 1 つを選択するか、または [その他] を選択して DHCP クライアントのタイム サーバの IP アドレスを入力します。
- [ファイル サーバ IP アドレス(siaddr)]:コンフィギュレーション ファイルのダウンロード元 TFTP/SCP サーバの IP アドレスを入力します。
- [ファイル サーバ ホスト名(sname/オプション 66)]:TFTP/SCP サーバの名前を入力します。
- [コンフィギュレーション ファイル名(ファイル/オプション 67)]:コンフィギュレーション 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 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

DHCP のオプション

デバイスが DHCP サーバとして動作している場合、DHCP のオプションは HEX オプションを使用して設定できます。それらのオプションについては、RFC2131 の中で説明されています。

それらのオプションのコンフィギュレーションにより、設定済み DHCP オプションの要求(オプション 55 を使用)がパケットに含まれる DHCP クライアントに対して送信される応答が決まります。

例:DHCP オプション 66 は、[DHCP オプション] ページで TFTP サーバの名前により設定されています。クライアント DHCP パケットが受信され、それにオプション 66 が含まれている場合、オプション 66 の値として TFTP サーバが返されます。

1 つ以上の DHCP オプションを設定するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4管理およびインターフェイス] > [DHCPサーバ] > [DHCPオプション] をクリックします。

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 まだ設定されていないオプションを設定して、フィールドに入力するには、次のようにします。

- [DHCPサーバ プール名が次に等しい]:[ネットワーク プール] 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 つを選択します。

ステップ 3 [追加] をクリックして、以下のフィールドに入力します。

- [プール名]: コードが定義されているプール名を表示します。
- [コード]: DHCP オプション コードを入力します。
- [タイプ]: このフィールドのラジオ ボタンは、DHCP オプションのパラメータのタイプに従って変わります。以下のコードのうちの 1 つを選択し、DHCP オプション パラメータの値を入力します。
  - [16 進]: DHCP オプションのパラメータの 16 進値を入力する場合に選択します。16 進値は、他の任意のタイプの値の代わりに指定することができます。たとえば、IP アドレス自体の代わりに IP アドレスの 16 進値を指定することができます。

    16 進値については何も検証がなされないため、入力する HEX 値が正しくない場合もエラーは表示されず、クライアントがサーバからの DHCP パケットを処理できなくなる可能性があります。
  - [IP]: 選択した DHCP オプションに関係する IP アドレスを入力する場合に選択します。
  - [IP リスト]: 複数の IP アドレスをカンマで区切ったリストを入力します。
  - [整数]: 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場合に選択します。
  - [ブーリアン]: 選択した DHCP オプションのパラメータがブーリアンの場合に選択します。
- [ブール値]: タイプがブーリアンの場合、返す値を選択します。[True] または [False]。
- [値]: タイプがブーリアンでない場合に、このコードについて送信する値を入力します。
- [説明]: ドキュメンテーションのためのテキストによる説明を入力します。

ステップ 4 [適用] 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

[アドレス バインディング] ページは、デバイスによって割り当てられている IP アドレス、およびそれらに対応する MAC アドレスを表示したり削除したりするために使用します。

アドレス バインディングを表示したり削除したりするには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4管理およびインターフェイス] > [DHCPサーバ] > [アドレスバインディング] をクリックします。

アドレス バインディングの以下のフィールドが表示されます。

- [IP アドレス]:DHCP クライアントの IP アドレス。
- [アドレス タイプ]: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。
- [MACアドレス/クライアント識別子]:MAC アドレスとして、または 16 進表記（例:01b60819681172）として指定される、クライアントの固有識別子。
- [リース期限切れ]:ホストの IP アドレスのリース期限の日時、またはリース期間が無制限として定義されている場合は [無制限]。
- [タイプ]:IP アドレスがクライアントに割り当てられている方法。次のオプションがあります。
  - [スタティック]:ホストのハードウェア アドレスが 1 つの IP アドレスにマッピングされている場合。
  - [ダイナミック]: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。その期間が終わると IP アドレスは無効になり、その時点で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。
- [状態]:次のオプションがあります。
  - [割り当て済み]:IP アドレスは割り当て済みです。スタティック ホストが設定されている場合、その状態は割り当て済みです。
  - [拒否済み]:IP アドレスは提供されているものの受け付けられていないため、割り当てられていません。
  - [期限切れ]:IP アドレスのリースが期限切れです。
  - [事前割り当て済み]: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、エントリは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 [削除] 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 の管理およびインターフェイス

ここで説明する内容は次のとおりです。

概要

Internet Protocol version 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、広く普及している IPv4 の後継プロトコルとして策定されました。

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、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、FE80:0000:0000:0000:0000:9C00:876A:130B）。すべての桁が 0 であるグループを「::」に置き換えた、短縮形で記述することもできます（たとえば、FE80::9C00:876A:130B）。

IPv4 しか使用できないネットワーク上で IPv6 ノードどうしが通信するには、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上で他の IPv6 ノードと通信できます。

トンネルでは、ISATAP または手動メカニズムのどちらかが使用されます（IPv6 トンネルを参照）。トンネルでは、IPv4 ネット ワークが仮想 IPv6 ローカル リンクとして扱われ、各 IPv4 アドレスがこのローカル リンク上の IPv6 アドレスにマッピングされます。

このデバイスでは、IPv6 フレームを検出する際、フレームの EtherType が IPv6 であるかどうかが検査されます。

IPv4 ルーティングの場合と同じ方法で、デバイスの MAC アドレスに宛てられたものの、デバイスには認識されていない IPv6 アドレスに宛てられたフレームは、ネクスト ホップ デバイスに転送されます。そのデバイスは、ターゲット端末であるか、または宛先により近いルータの場合があります。転送メカニズムにより、（実質的に）未変更の受信された L3 パケットを含む L2 フレームが再構築され、ネクスト ホップ デバイスの MAC アドレスが宛先 MAC アドレスとなります。

システムによりスタティック ルーティングおよびネイバー ディスカバリのメッセージ（IPv4 ARP メッセージに類似のもの）が使用されて、適切な転送テーブルとネクスト ホップ アドレスが構築されます。

ルートは、2 つのネットワーク デバイスの間の経路を定義するものです。ユーザによって追加されるルーティング エントリはスタティックであり、ユーザが明示的に削除するまでシステムによって保持されて使用されます。それらは、ルーティング プロトコルでは変更されません。スタティック ルートを更新する必要がある場合、それはユーザによって明示的に実行されなければなりません。ネットワーク内にルーティング ループが発生しないようにすることはユーザの責任です。

スタティック IPv6 ルートは、以下のいずれかです。

- 直接接続。この場合、宛先はデバイス上のインターフェイスに直接接続され、パケット宛先（インターフェイス）がネクスト ホップ アドレスとして使用されます。
- 再帰的。ネクスト ホップのみ指定され、発信インターフェイスはそのネクスト ホップから派生します。

同じように、ネクスト ホップ デバイス（直接接続エンド システムを含む）の MAC アドレスは、ネットワーク ディスカバリを使用して自動的に派生します。しかしこれは、ネイバー テーブルに手動でエントリを追加することにより、ユーザによってオーバーライドおよび補足されることがあります。

IPv6 グローバル コンフィギュレーション

IPv6 グローバル パラメータおよび DHCPv6 クライアントの設定値を定義するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理とインターフェイス] > [IPv6グローバルコンフィギュレーション] 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。

- [IPv6ルーティング]: これを選択すると、IPv6 ルーティングが有効になります。これが有効になっていない場合、デバイスは(ルータではなく)ホストとして動作し、管理パケットは受信できますが、パケットの送信はできなくなります。ルーティングが有効の場合、デバイスによる IPv6 パケット送信が可能です。

  IPv6 ルーティングを有効にすると、ネットワーク内のルータから送信された RA からオートコンフィグ操作を介してデバイス インターフェイスに割り当てられたすべてのアドレスが削除されます。

- [ICMPv6 レート制限間隔]: ICMP エラー メッセージの生成頻度を入力します。
- [ICMPv6 レート制限バケットサイズ]: 間隔ごとにデバイスから送信できる ICMP エラー メッセージの最大件数を入力します。
- [IPv6ホップ制限]: パケットを渡す先となる最終宛先までの途上にある中間ルータの最大数を入力します。パケットが別のルータに転送されるたびに、ホップ制限が小さくなっていきます。ホップ制限がゼロになった時点で、パケットが破棄されます。これにより、パケットが無限に転送され続ける事態が回避されます。
- **DHCPv6 クライアント設定**
  - [固有 ID (DUID) 形式]: これは、DHCP サーバによりクライアントを検索するために使用される DHCP クライアントの識別子です。以下の形式のいずれかを使用できます。

    [リンク レイヤ]: (デフォルト)。このオプションを選択した場合、デバイスの MAC アドレスが使用されます。

    [エンタープライズ番号]: このオプションを選択した場合、以下のフィールドを入力します。

  - [エンタープライズ番号]: ベンダーにより IANA によって管理されている民間企業番号が登録されています。
  - [ID]: ベンダー定義の 16 進ストリング(16 進文字 64 桁以下)。文字数が偶数でない場合、右端にゼロが追加されます。16 進文字は、2 文字ごとにピリオドまたはコロンで区切ることができます。
- [DHCPv6 固有 ID (DUID)]: 選択されている識別子が表示されます。

ステップ 3 [適用] をクリックします。IPv6 グローバル パラメータおよび DHCPv6 クライアントの設定値が更新されます。

Ipv6 インターフェイス

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。

他のタイプのインターフェイスとは異なり、トンネル インターフェイスは [IPv6 トンネル] ページで最初に作成された後、そのページの中でトンネルに IPv6 インターフェイスが設定されます。

IPv6 インターフェイスを定義するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [IPv6インターフェイス] をクリックします。

ステップ 2 パラメータを入力します。

- [IPv6リンクローカルのデフォルトゾーン]:デフォルト ゾーンを定義する機能を有効にする場合に選択します。これは、指定されたインターフェイスなしで、またはデフォルト ゾーン 0 で着信するリンク ローカル パケットを発信するために使用するインターフェイスです。
- [IPv6リンク ローカルのデフォルトゾーンインターフェイス]: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、それ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することが可能です。

ステップ 3 [適用] 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一緒に表示されます。

- [トンネル タイプ]:[手動]、[6 to 4]、および [ISATAP] 。

ステップ 4 [追加] をクリックして、インターフェイス IPv6 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 次のフィールドを入力します。

- [IPv6インターフェイス]:IPv6 アドレスの特定のユニット、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SNTP コンフィギュレーションや DNS 情報などの情報を受信できるようにするには、以下の **DHCPv6 クライアント** フィールドを入力します。

- [DHCPv6 クライアント]: インターフェイス上で DHCPv6 クライアント（ステートレスおよびステートフル）を有効にする場合に選択します。
- [高速コメント]: アドレス割り当てとその他の設定に対する 2 メッセージ交換の使用を有効にする場合に選択します。これが有効になっている場合は、クライアントが要請メッセージに高速コミット オプションを含めます。
- [情報の最小更新時間]: この値は、更新時間値の最小値を規定するために使用されます。サーバから送信される更新時間オプションがこの値未満の場合、この値が使用されることになります。[無制限]（サーバがこのオプションを送信するのでない限り更新されない）を選択するか、または [ユーザ定義] を選択して値を設定します。
- [情報更新時間]: 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す。[無制限]（サーバがこのオプションを送信するのでない限り更新されない）を選択するか、または [ユーザ定義] を選択して値を設定します。

ステップ 7 付加的な IPv6 パラメータを設定するには、以下のフィールドを入力します。

- [IPv6 アドレス自動コンフィギュレーション]: 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 コンフィギュレーションを有効にする場合に選択します。
- [DAD 試行回数]: このインターフェイスのユニキャスト IPv6 アドレスに対して Duplicate Address Detection（DAD; 重複アドレス検出）処理を実行しているときに送信する、ネイバー送信要求メッセージの件数を入力します。DAD は、ユニキャスト IPv6 アドレスを新規に割り当てる前に、そのアドレスが重複していないかどうかを検査する処理です。DAD 処理中、新規アドレスは仮割り当て状態になります。「**0**」を入力した場合、このインターフェイスに対する DAD 処理は無効になります。「**1**」を入力した場合、メッセージは 1 回だけ送信されます。
- [ICMPv6 メッセージの送信]: 宛先到達不能メッセージを生成します。
- [MLDバージョン]: IPv6 MLD バージョン。
- [IPv6リダイレクト]: ICMP IPv6 リダイレクト メッセージの送信を有効にする場合に選択します。それらのメッセージは、他のデバイスに対して、そのデバイスにはトラフィックを送信せず、別のデバイスに送信するように通知します。

ステップ 8 [適用] をクリックし、選択したインターフェイス上での IPv6 処理を有効にします。正規の IPv6 インターフェイスには、次のアドレスが自動的に割り当てられます。

- リンク ローカル アドレス。インターフェイス ID 部はデバイスの MAC アドレスから生成され、EUI-64 形式になっています。
- 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」)。
- 送信要求ノード マルチキャスト アドレス。形式は「FF02::1:FFXX:X」です。

ステップ 9 [再起動] ボタンを押して、DHCPv6 サーバから受信されるステートレス情報の更新を開始します。

ステップ 10 必要なら [IPv6 アドレス テーブル] をクリックし、インターフェイスに IPv6 アドレスを手動で割り当てます。このページについては、IPv6 アドレスセクションで説明されています。

ステップ 11 トンネルを追加するには、IPv6 トンネル テーブルの中で([Ipv6 インターフェイス] ページでトンネルとして定義されている)インターフェイスを選択して、[IPv6 トンネル テーブル] をクリックします。「IPv6 トンネル」を参照してください。

DHCPv6 クライアント詳細

[詳細] ボタンを押すと、インターフェイスで DHCPv6 サーバから受信する情報が表示されます。

これは、選択されているインターフェイスが DHCPv6 ステートレス クライアントとして定義されている場合にアクティブです。

ボタンが押された場合、以下のフィールドが表示されます(DHCP サーバから受信された情報の場合)。

- [DHCP動作モード]: ここには、以下の条件が満たされている場合に [有効] と表示されます。
  - インターフェイスが有効。
  - その上で IPv6 が有効。
  - その上で DHCPv6 クライアントが有効。
- [ステートフル サービス状態]: クライアントで DHCP サーバからステートフル コンフィギュレーション情報を受信するようにします。
- [ステートレス サービス状態]: クライアントで DHCP サーバからステートレス コンフィギュレーション情報を受信するようにします。

- [IPv6 アドレス IA NA]:IA ID にタグの C/IANAID、T1-C/T1、T2、- C/T2 の値が設定されます。T1 と T2 は、少なくとも 1 つのアドレスがインターフェイス上で受信されたときに使用可能になります。
- [DHCP サーバ アドレス]:DHCPv6 サーバのアドレス。
- [DHCPサーバDUID]:DHCPv6 サーバの固有識別子。
- [DHCPサーバプリファレンス]:この DHCPv6 サーバの優先度。
- [情報の最小更新時間]:上記参照。
- [情報更新時間]:上記参照。
- [受信した情報更新時間]:DHCPv6 サーバから受信した更新時間。
- [残りの情報更新時間]:次の更新までの残り時間。
- [DNSサーバ]:DHCPv6 サーバから受信した DNS サーバのリスト。
- [DNS ドメイン検索リスト]:DHCPv6 サーバから受信したドメインのリスト。
- [SNTP サーバ]:DHCPv6 サーバから受信した SNTP サーバのリスト。
- [POSIXタイムゾーン文字列]:DHCPv6 サーバから受信したタイムゾーン。
- [コンフィギュレーション サーバ]:DHCPv6 サーバから受信したコンフィギュレーション ファイルを含むサーバ。
- [コンフィギュレーション ファイル名]:DHCPv6 サーバから受信したコンフィギュレーション サーバ上のコンフィギュレーション ファイルのパス。

IPv6 トンネル

トンネルにより、IPv4 ネットワークを通じた IPv6 パケットの転送が可能になります。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。それらのアドレスの間では、IPv6 パケットが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。送信元アドレスは、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際、宛先 IPv4 アドレスがルータにより提供されます。次のことに注意してください。

- リンク ローカル IPv6 アドレスが、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 ISATAP インターフェイスに割り当てられると、その ISATAP 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化されている場合、ISATAP と IPv4 がマッピングされ、DNS プロセスによって ISATAP ルータの IPv4 アドレスが解決されます。ISATAP DNS レコードが解決されない場合、ホスト マッピング テーブル内の、ISATAP ホストの名前とアドレスのマッピングが検索されます。
- ISATAP ルータの IPv4 アドレスが DNS プロセスで解決されない場合、ISATAP IP インターフェイスはアクティブ化されたままになります。DNS プロセスでアドレスが解決されるまで、ISATAP トラフィックを処理するためのデフォルト ルータは設定されません。

追加的なトンネル タイプ

このデバイスでは、以下の追加的なタイプのトンネルを設定できます。

- **手動トンネル**
  - リンク ローカル IPv6 アドレスが、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 ISATAP インターフェイスに割り当てられると、その ISATAP 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化されている場合、ISATAP と IPv4 がマッピングされ、DNS プロセスによって ISATAP ルータの IPv4 アドレスが解決されます。ISATAP DNS レコードが解決されない場合、ホスト マッピング テーブル内の、ISATAP ホストの名前とアドレスのマッピングが検索されます。
  - ISATAP ルータの IPv4 アドレスが DNS プロセスで解決されない場合、ISATAP IP インターフェイスはアクティブ化されたままになります。DNS プロセスでアドレスが解決されるまで、ISATAP トラフィックを処理するためのデフォルト ルータは設定されません。

  これは、ポイントツーポイント定義です。手動トンネルを作成する際、送信元 IP アドレス（デバイスの IP アドレスの 1 つ）と宛先 IPv4 アドレスの両方を入力します。
- **6 to 4 トンネル**

  6 to 4 は、基礎となる IPv4 ネットワークを、IPv6 のための非ブロードキャスト複数アクセス リンク レイヤとして使用する自動トンネル メカニズムです。1 つのデバイスでは、1 つの 6 to 4 トンネルのみサポートされます。

  6to4 トンネルがサポートされるのは、IPv6 転送機能がサポートされる場合だけです。

6to4 トンネル インターフェイスでは、IPv6 マルチキャストはサポートされません。

6to4 トンネル上の 2002::/16 オンリンク プレフィックスは、スイッチにより自動作成されます。オンリンク プレフィックス作成の結果として、トンネルで接続されている 2002::/16 ルートがルーティング テーブルに追加されます。

トンネル モードが 6to4 から別のモードに変わると、オンリンク プレフィックスおよび接続されているルートは削除されます。

ネクスト ホップ発信インターフェイスが 6to4 トンネルの場合、ネクスト ホップ ノードの IPv4 アドレスは、それがグローバルの場合は IPv6 ネクスト ホップ IPv6 アドレスのプレフィックス 2002:WWXX:YYZZ::/48 から、およびそれがリンク ローカルの場合は IPv6 ネクスト ホップ IPv6 アドレスのインターフェイス識別子の最後の 32 ビットから取られます。

次の表に、さまざまなデバイスによるトンネル サポートを示します。

トンネル タイプ	Sx350	SG350x	SG350XG	SG550X	SG550XG
ISATAP	サポート済み	サポート済み	サポート済み	サポート済み	サポート済み
手動	未サポート	未サポート	ネイティブ モード : サポート済み - 最大 16 トンネル。ハイブリッド スタックではサポートされない。	最大 16 トンネル（全部で）	最大 16 トンネル（全部で）
自動 6to4 トンネル	未サポート	未サポート	ネイティブ モード : 1 X 4-6 トンネル（全部で最大 16 トンネル） ハイブリッド スタック : 未サポート。	1 X 4-6 トンネル（全部で最大 16 トンネル）	1 X 4-6 トンネル（全部で最大 16 トンネル）

トンネルの設定

IPv6 トンネルを設定するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [IPv6トンネル] 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。

- [ISATAP 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。**デフォルト値**をそのまま使用するか、または**ユーザ定義値**を使用することができます。
- [ISATAP 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。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**ユーザ定義値**を使用することができます。

  注 IPv4 インターフェイスが動作していない場合、ISATAP トンネルは機能しません。

注 手動トンネルと 6to4 トンネルは、SG350XG デバイスと Sx550 ファミリ デバイスにのみ該当します。これらのデバイスの場合、IPv6 トンネルを示す [**IPv6** トンネル テーブル] がページに表示され、ここでトンネルを作成または設定できます（下記の手順を参照）。

Sx350 および Sx350X では ISATAP トンネルのみがサポートされます。これらのデバイスで ISATAP トンネルを設定するには、[ISATAP トンネルの作成] ボタンをクリックして [送信元 IPv4 アドレス] および [ISATAP ルータ名] フィールドに情報を入力します。これらのフィールドについては、以下の説明を参照してください。

ステップ 3 次のフィールドを入力します。

- [トンネル番号]: トンネルの番号を選択します。
- [トンネルタイプ]: トンネル タイプ（[手動]、[6 から 4]、または [ISATAP]）を選択します。
- [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 アドレス]:トンネルの送信元アドレスとして使用す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。
  - [デフォルトを使用]:常に ISATAP です。
  - [ユーザ定義]:ルータのドメイン名を入力します。

ステップ 4 [適用] をクリックします。トンネルが、実行コンフィギュレーション ファイルに保存されます。

注 350XG デバイスとデバイスの 550 ファミリの場合、トンネルをシャットダウンするには、[編集] をクリックして、[トンネル状態] をオフにします。トラップを無効にするには、[編集] をクリックし、[リンク ステータス SNMP トラップ] をオフにします。

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、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [IPv6アドレス] をクリックします。

ステップ 2 テーブルに対してフィルタ処理を実行するには、インターフェイス名を選択してから、[実行] をクリックします。このインターフェイスが [IPv6 アドレス テーブル] に表示されます。これらのフィールドは [追加] ページで説明されます。ただし、次のフィールドを除きます。

- [アドレス ソース]: アドレス ソース タイプのいずれかが表示されます。DHCP、システム、またはスタティック。
- [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。
- [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。
- [有効期限]: 有効期限が表示されます。

ステップ 3 [追加] をクリックします。

ステップ 4 フィールドに値を入力します。

- [IPv6 インターフェイス]: IPv6 アドレスを定義するインターフェイスが表示されます。* が表示されている場合、それは、IPv6 インターフェイスが有効になっていないにもかかわらず、設定されていることを意味します。
- [IPv6 アドレス タイプ]: 追加する IPv6 アドレスのタイプを選択します。
  - [リンクローカル]: 単一ネットワーク 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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]: 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 タイプである IPv6 アドレス。

- [エニーキャスト]:IPv6 アドレスはエニーキャスト アドレスです。これは、多くの場合、異なる複数のノードに属する一連のインターフェイスに割り当てられるアドレスです。エニーキャスト アドレスに送信されるパケットは、エニーキャスト アドレスによって識別される最近接インターフェイス(使用されているルーティング プロトコルで定義)に配布されます。

注 IPv6 アドレスが ISATAP インターフェイス上にある場合、エニーキャストは使用できません。

- [IPv6 アドレス]: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。1 つのインターフェ イスに割り当て可能なアドレスは最大 128 個です。各アドレスは、16 ビット値をコロンで区切った 16 進表記で入力する必要があります。

  さまざまなタイプのトンネルに、以下のタイプのアドレスを追加することができます。

  - [手動トンネルに]:グローバル アドレスまたはエニーキャスト アドレス
  - [ISATAPトンネルに]:EUI-6 によるグローバル アドレス
  - [6 to 4 トンネル]:なし

- [プレフィックス長]:グローバル IPv6 プレフィックス部の長さ。0 ～ 128 の範囲の値を入力します。この値は、プレフィックス(アドレスのネットワーク部)を構成する、アドレスの上位ビットの数を意味します。
- [EUI-64]:EUI-64 パラメータを使用して、デバイスの MAC アドレスに基づく EUI-64 形式を使用することによりグローバル IPv6 アドレスのインターフェイス ID 部を識別する場合に選択します。

ステップ 5 [適用] をクリックします。実行コンフィギュレーション ファイルが更新されます。

IPv6 ルータの設定

以下のセクションでは、IPv6 ルータの設定方法について説明します。具体的な内容は、次のとおりです。

- ルータ アドバタイズメント
- IPv6 プレフィックス

ルータ アドバタイズメント

IPv6 ルータは、そのプレフィックスを隣接デバイスにアドバタイズできます。この機能は、次のようにして、インターフェイスごとに有効にしたり抑止したりできます。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [IPv6ルータコンフィギュレーション] > [ルータアドバタイズメント] 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 テーブルに示されているインターフェイスを構成するには、それを選択してから [編集] をクリックします。

ステップ 3 次のフィールドを入力します。

- [ルータ アドバタイズメントの抑制]: インターフェイス上で IPv6 ルータ アドバタイズメントの伝送を抑制する場合は、[はい] を選択します。この機能が抑制されていない場合は、以下のフィールドを入力します。
- [ルータ プリファレンス]:ルータのプリファレンスとして、[低]、[中] または [高] 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、このフィールドで設定されているプリファレンスで送信されます。プリファレンスが設定されていない場合、[中] プリファレンスで送信されます。

プリファレンスとルータとの関連付けは、たとえば、1 つのリンク上の 2 つのルータが同等ではあるもののコストの異なるルーティングを提供し、ホストがルータの 1 つを優先することがポリシーで述べられている場合に便利です。

- [アドバタイズメント間隔オプションを含める]: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ることを指示する場合に選択します。このオプションは、アクセスしてくるモバイル ノードに対して、そのノードがルータ アドバタイズメントを受け取る間隔を示します。ノードでは、移動検出アルゴリズムの中でこの情報を使用することがあります。
- [ホップ限度]: 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。
- [マネージド アドレス コンフィギュレーション フラグ]:接続されているホストに対して、アドレスを取得するためステートフル自動コンフィギュレーションを使用するよう指示する場合、このフラグを選択します。ホストでは、ステートフルとステートレスのアドレス自動コンフィギュレーションを同時に使用する可能性があります。
- [他のステートフル コンフィギュレーション フラグ]:接続されているホストに対して、その他の(アドレス以外の)情報を取得するためステートフル自動コンフィギュレーションを使用するよう指示する場合、このフラグを選択します。

注 マネージド アドレス コンフィギュレーション フラグが設定されている場合、接続されているホストでは、ステートフル自動コンフィギュレーションを使用することにより、このフラグの設定には関係なく、その他の（アドレス以外の）情報を取得することができます。

- [ネイバー要求再送信間隔]:アドレスを解決する場合、またはあるネイバーに到達可能であるかどうかを試す場合に、ネイバー送信要求メッセージをネイバーに送信する際の再送信と再送信の間の時間を決定します。
- [最大ルータ アドバタイズメント間隔]:ルータ アドバタイズメントの時間間隔の合計の最大値を入力します。

このコマンドを使用してルータをデフォルト ルータとして設定する場合、送信間隔は、IPv6 ルータ アドバタイズメントのライフタイム以下でなければなりません。他の IPv6 ノードとの同期を回避するため、実際に使用される間隔は、最小値と最大値の間の値からランダムに選択されます。

- [最小ルータアドバタイズメント間隔]:ルータ アドバタイズメントの時間間隔の合計の最小値を入力するか（[ユーザ定義]）、またはシステム デフォルトを使用する場合は [デフォルトを使用] を選択します。

  注 最小ルータ アドバタイズメント間隔は、最大ルータ アドバタイズメント間隔の 75% 以下でなければならず、かつ 3 秒以上でなければなりません。
- [ルータ アドバタイズメント ライフタイム]:このルータがデフォルト ルータとして有用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 ルータとして有用でなくなったことを示します。
- [到達可能時間]:リモート IPv6 ノードが到達可能であると見なされる時間の合計をミリ秒単位で入力するか（[ユーザ定義]）、またはシステム デフォルトを使用する場合は [デフォルトを使用] オプションを選択します。

ステップ 4 [適用] をクリックし、実行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クスを定義するには

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [IPv6ルータ コンフィギュレーション] > [IPv6プレフィクス] の順にクリックします。

ステップ 2 必要なら、[フィルタ] フィールドを有効にし、[実行] をクリックします。フィルタにマッチ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、[追加] 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 次のフィールドを入力します。

- [プレフィックス アドレス]:IPv6 ネットワーク。この引数は、RFC 4293 で説明されている形式になっていなければならず、アドレスは、コロンとコロンの間に 16 ビット値を使用した 16 進数で指定します。
- [プレフィックス長]:IPv6 プレフィックスの長さ。アドレスのうち何桁の高次連続ビットがプレフィックス(アドレスのネットワーク部分)となるかを示す 10 進値。10 進値の前には、スラッシュ記号を付ける必要があります。
- [プレフィックス アドバタイズメント]:このプレフィックスをアドバタイズする場合に選択します。
- [有効なライフタイム]:このプレフィックスが有効であり続ける時間、つまり無効になるまでの残り時間(秒数)。無効になったプレフィックスから生成されるアドレスは、パケットの宛先または送信元アドレスになってはなりません。
  - [無制限]:フィールドを、無制限を表す 4,294,967,295 に設定する場合、この値を選択します。
  - [ユーザ定義]:値を入力します。
- [優先ライフタイム]:このプレフィックスが優先であり続ける残りの時間(秒数)。この時間が経過した後、プレフィックスは、新たな通信において送信元アドレスとして使用されなくなります。しかし、そのようなインターフェイスで受信されるパケットは期待どおりに処理されます。優先ライフタイムは、有効なライフタイム以下でなければなりません。
  - [無制限]:フィールドを、無制限を表す 4,294,967,295 に設定する場合、この値を選択します。
  - [ユーザ定義]:値を入力します。
- [自動コンフィギュレーション]:インターフェイス上でステートレス自動コンフィギュレーションを使用して IPv6 アドレスの自動コンフィギュレーションを有効にし、そのインターフェイス上で 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るプレフィックスに応じて設定されます。

- [プレフィックス ステータス]:次のいずれかのオプションを選択します。
  - [オンリンク]:指定されたプレフィックスをオンリンクとして設定します。指定され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では、宛先が、リンクでローカルに到達可能であると見なします。オンリンク プレフィックスは、接続プレフィックス(L ビット設定)としてルーティング テーブル中に挿入されます。
  - [オンリンクなし]:指定され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。オンリンクなしのプレフィックスは、接続プレフィックスとしてルーティング テーブル中に挿入されますが、L ビットがクリアされてアドバタイズされます。
  - [オフリンク]: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 ビットをクリアした状態でアドバタイズされます。プレフィックスは、接続プレフィックスとしてルーティング テーブル中に挿入されません。プレフィックスが接続プレフィックスとしてルーティング テーブル中にすでに存在する場合(たとえばプレフィックスが IPv6 アドレスの追加でも設定されていた場合)、それは削除されます。

ステップ 6 [適用] をクリックし、実行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を保存します。

IPv6 デフォルト ルータ リスト

[IPv6 デフォルト ルータ リスト] ページでは、デフォルトの IPv6 ルータの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)。このリスト内のルータが無作為に選択されます。このデバイスでは、スタティック IPv6 デフォルト ルータを 1 台使用できます。ダイナミック デフォルト ルータとは、ルータ アドバタイズメントをこのデバイスの IPv6 インターフェイスに送信したルータのことです。

IP アドレスを追加または削除すると、次の処理が実行されます。

- IP インターフェイスを削除すると、デフォルト ルータの IP アドレスがすべて削除されます。ダイナミック IP アドレスを削除することはできません。
- ユーザ定義アドレスを複数個挿入しようとすると、アラート メッセージが表示されます。
- リンク ローカル アドレス(プレフィックスが「fe80:」)でないアドレスを挿入しようとすると、アラート メッセージが表示されます。

デフォルト ルータを定義するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理とインターフェイス] > [IPv6デフォルト ルータリスト] をクリックします。

このページには、次のフィールドがデフォルト ルータごとに表示されます。

- [発信インターフェイス]:デフォルト ルータが接続されている発信 IPv6 インターフェイス。
- [デフォルト ルータ IPv6 アドレス]:デフォルト ルータのリンク ローカル IP アドレス。
- [タイプ]:以下のオプションを含むデフォルト ルータ コンフィギュレーション。
  - [スタティック]:デフォルト ルータは、[追加] ボタンで手動でこのテーブルに追加されました。
  - [ダイナミック]:デフォルト ルータは動的に設定されました。
- [メトリック]:このホップのコスト。

ステップ 2 [追加] をクリックし、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 次のフィールドを入力します。

- [ネクストホップタイプ]:パケット送信先となる次の宛先の IP アドレス。これは、以下のもので構成されます。
  - [グローバル]: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 タイプである IPv6 アドレス。
  - [リンク ローカル]:単一ネットワーク 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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [ポイントツーポイント]:ポイントツーポイント トンネル。IPv6 ルーティング トンネルがサポートされる場合には、これがサポートされます。
- [発信インターフェイス]: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 ルータ IPv6 アドレス]:スタティック デフォルト ルータの IP アドレス。

- [メトリック]: このホップのコストを入力します。

ステップ 4 [適用] 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 ネイバー] ページでは、IPv6 インターフェイス上の 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（別名：IPv6 近隣探索キャッシュ）には、デバイスと同じ IPv6 サブネット上にある IPv6 ネイバーの MAC アドレスが表示されます。いわば、IPv4 の ARP テーブルの IPv6 版です。デバイスがネイバーと通信する際、この IPv6 ネイバー テーブルが使用され、その IPv6 アドレスに基づいて MAC アドレスが特定されます。

このページには、自動検出されたエントリと手動設定されたエントリが表示されます。エントリごとに、ネイバーが接続されているインターフェイス、ネイバーの IPv6 アドレスと MAC アドレス、エントリ タイプ（スタティックまたはダイナミック）、およびネイバーの状態が表示されます。

IPv6 ネイバーを定義するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [IPv6ネイバー] をクリックします。

[テーブルのクリア] オプションを選択することにより、IPv6 ネイバーテーブル内の IPv6 アドレスの全部または一部を消去することができます。

- [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。

隣接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。

- [インターフェイス]: 隣接 IPv6 インターフェイス 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 アドレスにマップされる 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 ネイバーの状態を指定します。値は次のとおりです。
  - [未完了]:アドレス解決中です。ネイバーからの応答はまだありません。
  - [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性が生じるまで、このネイバーの到達可能性は検査されません。
  - [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。このインターフェイスは、事前定義された遅延時間の間、[遅延] 状態になります。到達可能性確認応答が受信されない場合、状態が [プローブ] に変わります。
  - [プローブ]:ネイバーが到達不能になっており、到達可能性を検査するためのユニキャスト ネイバー宛送信要求プローブを送信中です。
- [ルータ]:ネイバーがルータかどうかを指定します([はい] または [いいえ])。

ステップ 2 ネイバーをテーブルに追加するには、[追加] 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。

- [インターフェイス]:追加する隣接 IPv6 インターフェイスが表示されます。
- [IPv6 アドレス]:インターフェイスに割り当てられた IPv6 ネットワーク アドレスを入力します。このアドレスは、有効な IPv6 アドレスでなければなりません。
- [MAC アドレス]:指定された IPv6 アドレスにマップされる MAC アドレスを入力します。

ステップ 4 [適用] 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 IP アドレスのタイプを [スタティック] から [ダイナミック] に変更するには、アドレスを選択し、[編集] をクリックし、[IPv6ネイバーの編集] ページを使用します。

IPv6 プレフィックス リスト

最初のホップ セキュリティが設定されている場合、IPv6 プレフィックスに基づくフィルタリングのルールを定義することが可能です。それらのリストは、[IPv6プレフィックスリスト] ページで定義できます。

プレフィックス リストは、**permit** または **deny** キーワードにより、マッチング条件に基づいてプレフィックスを許可するか拒否するように設定することができます。暗黙の拒否は、どのプレフィックス リスト エントリにもマッチしないトラフィックに適用されます。

プレフィクス リスト エントリは、IP アドレスとビット マスクとで構成されます。IP アドレスとしては、クラスフル ネットワーク、サブネット、あるいは単一ホスト ルートのためのものが可能です。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、プレフィックス長の等号マッチ、または ge および le キーワード使用する場合の範囲内のマッチに基づいてトラフィックをフィルタ処理するように設定されています。

[より大きい] および [より小さい] のパラメータは、プレフィックス長の範囲を指定するために使用され、ネットワーク/長さ引数のみ使用する場合に比べてコンフィギュレーションの柔軟性が高くなります。[より大きい] と [より小さい] のどちらのパラメータも指定されていない場合、プレフィックス リストは等号マッチを使用して処理されます。[より大きい] パラメータのみ指定されている場合、範囲は [より大きい] に入力された値から 32 ビット長さの最大値までです。[より小さい] のみ指定されている場合、範囲はネットワーク/長さ引数に入力されている値から、[より小さい] までです。[より大きい] と [より小さい] の両方の引数が入力された場合、範囲は、[より小さい] と [より大きい] で使用されている値の間になります。

プレフィックス リストを作成するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [IPv6プレフィックスリスト] の順にクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [リスト名]:次のいずれかのオプションを選択します。
  - [既存のリストの使用]:プレフィックスの追加先となる定義済みリストを選択します。
  - [新しいリストの作成]:作成する新しいリストの名前を入力します。
- [連続番号]: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。次のいずれかのオプションを選択します。
  - [自動番号付与]:新しい IPv6 プレフィックスを、プレフィックス リストの最後のエントリの後に入れます。連続番号は、最後の連続番号に 5 を加えたものと等しくなります。リストが空の場合、最初のプレフィックス リスト エントリに番号 5 が割り当てられ、それ以降のプレフィックス リスト エントリはそれぞれ 5 ずつインクリメントしていきます。
  - [ユーザ定義]:新しい IPv6 プレフィックスを、パラメータで指定される場所に入れます。その番号のエントリが存在する場合、新しいものによって置換されます。

- [ルール タイプ]:プレフィックス リストのためのルールを入力します。
  - [許可]:条件に一致するネットワークを許可します。
  - [拒否]:条件に一致するネットワークを拒否します。
  - [説明]:テキスト。
- [IPv6 プレフィックス]:IP ルート プレフィックス。
- [プレフィックス長]:IP ルート プレフィックス長。
- [より大きい]:マッチングに使用するプレフィックスの最小長。次のいずれかのオプションを選択します。
  - [限度なし]:マッチングにプレフィックスの最小長を使用しません。
  - [ユーザ定義]:マッチングするプレフィックス最小長。
- [より小さいい]:マッチングに使用するプレフィックスの最大長。次のいずれかのオプションを選択します。
  - [限度なし]:マッチングにプレフィックスの最大長を使用しません。
  - [ユーザ定義]:マッチングするプレフィックス最大長。
- [説明]:プレフィックス リストの説明を入力します。

ステップ 4 [適用] をクリックし、実行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を保存します。

IPv6 アクセス リスト

IPv6 アクセス リストは、[MLDプロキシ] > [グローバルMLDプロキシ設定] > [SSM IPv6アクセスリスト] ページで使用できます。

アクセス リストを作成するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [IPv6アクセスリスト] 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、[追加] をクリックして、次のフィールドに入力します。

- [アクセスリスト名]:次のいずれかを選択します。
  - [既存のリストの使用]:既存のアクセス リストを選択します。

- [新しいリストの作成]:新しいアクセス リストの名前を入力します。

- [送信元IPv6アドレス]:送信元 IP アドレスを入力します。次のオプションが選択できます。
  - [任意]:すべての IP アドレスが含まれます。
  - [ユーザ定義]:IP アドレスを入力します。
- [プレフィックス長]:送信元 IPv6 プレフィックス長を入力します。
- [アクション]:アクセス リストに対するアクションを選択します。次のオプションが選択できます。
  - [許可]: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]: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 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

IPv6 ルータ

IPv6 転送テーブルには、設定されているさまざまなルートが含まれています。それらのルートの 1 つはデフォルト ルート(IPv6 アドレスは「0」)です。このルートは、IPv6 デフォルト ルータ リストから選択されたデフォルト ルータを使用して、デバイスと同じ IPv6 サブネット上にない宛先デバイスにパケットを送信するものです。このテーブルには、デフォルト ルートの他に、ダイナミック ルートも登録されています。ダイナミック ルートとは、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 ルートのことです。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、次のようにします。

[IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [IPv6ルート] 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。

- [IPv6 プレフィックス]:宛先 IPv6 サブネット アドレスの IP ルート アドレス プレフィックス。
- [プレフィックス長]:宛先 IPv6 サブネット アドレスの IP ルート プレフィックス長。数値の前にスラッシュ(/)が付加されています。

- [発信インターフェイス]:パケットの転送に使用されるインターフェイス。
- [ネクスト ホップ]:パケット転送先アドレスのタイプ。通常は、隣接ルータのアドレスです。以下のタイプのいずれかです。
  - [リンク ローカル]:単一ネットワーク 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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]: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 タイプである IPv6 アドレス。
  - [ポイントツーポイント]:ポイントツーポイント トンネル。
- [メトリック]: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。デフォルト ルートにはすべて同じ値が設定されています。
- [ライフタイム]:パケットの送信および再送信のタイムアウト時間。この時間内に送信または再送信されなかったパケットは破棄されます。
- [ルート タイプ]:宛先の接続方法、およびエントリの取得に使用される方式。値は次のとおりです。
  - S(スタティック):エントリは、ユーザによって手動で設定されました。
  - I(ICMP リダイレクト):エントリは、ICMP リダイレクト メッセージを使用して IPv6 ルータから受信された ICMP リダイレクト ダイナミック ルートです。
  - ND(ルータ アドバタイズメント):エントリは、ルータ アドバタイズメント メッセージから取得されます。

ステップ 1 新しいルートを追加するには、[追加] をクリックして、前述のフィールドに値を入力します。加えて、次のフィールドに値を入力します。

- [IPv6アドレス]:新しいルートの IPv6 アドレスを追加します。

ステップ 2 [適用] をクリックし、変更を保存します。

DHCPv6 リレー

ここで説明する内容は次のとおりです。

- グローバル宛先
- インターフェイス設定

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 クライアントの直接接続先の DHCPv6 リレー エージェント（デバイス）により、直接接続されている DHCPv6 クライアントから受信するメッセージがカプセル化され、それらが DHCPv6 サーバに転送されます。

その反対方向では、リレー エージェントにより、DHCPv6 からの受信パケットがカプセルから取り出され、DHCPv6 クライアントに向けてそれらが転送されます。

ユーザは、パケット転送先となるリスト DHCP サーバのリストを設定する必要があります。DHCPv6 サーバの 2 つのセットを設定できます。

- [グローバル宛先]: パケットは、常にそれらの DHCPv6 サーバにリレーされます。
- [インターフェイス リスト]: これは、DHCPv6 サーバのインターフェイスごとのリストです。あるインターフェイスで DHCPv6 パケットが受信された場合、その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。

他の機能との依存関係

DHCPv6 クライアントと DHCPv6 リレー機能は、1 つのインターフェイス上では相互に排他的です。

グローバル宛先

すべての DHCPv6 パケットのリレー先 DHCPv6 サーバのリストを設定するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [DHCPv6 リレー] > [グローバル宛先] をクリックします。

ステップ 2 デフォルト DHCPv6 サーバを追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [IPv6 アドレス タイプ]: クライアント メッセージ転送先の宛先アドレスのタイプを入力します。アドレス タイプは、[リンク ローカル]、[グローバル]、または [マルチキャスト]（All_DHCP_Relay_Agents_and_Servers）のいずれかです。
- [DHCPv6 サーバ IP アドレス]: パケット転送先の DHCPv6 サーバのアドレスを入力します。
- [IPv6インターフェイス]: 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 [適用] 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。

インターフェイス設定

あるインターフェイス上で DHCPv6 リレーを有効にし、そのインターフェイス上で DHCPv6 パケット受信時にそれらのリレー先となる DHCPv6 サーバのリストを設定するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv6の管理およびインターフェイス] > [DHCPv6 リレー] > [インターフェイス設定] の順にクリックします。

ステップ 2 あるインターフェイス上で DHCPv6 を有効にし、オプションとして、インターフェイスの DHCPv6 サーバを追加するには、[追加] をクリックします。

次のフィールドを入力します。

- [送信元インターフェイス]: DHCPv6 リレーを有効にするインターフェイス（ポート、LAG、VLAN、またはトンネル）を選択します。
- [グローバル宛先のみ使用]: パケットの転送先が DHCPv6 グローバル宛先サーバのみの場合に選択します。
- [IPv6 アドレス タイプ]: クライアント メッセージ転送先の宛先アドレスのタイプを入力します。アドレス タイプは、[リンク ローカル]、[グローバル]、または [マルチキャスト]（All_DHCP_Relay_Agents_and_Servers）のいずれかです。
- [DHCPv6 サーバ IP アドレス]: パケット転送先の DHCPv6 サーバのアドレスを入力します。
- [宛先IPv6インターフェイス]: 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インターフェイスを入力します。

ステップ 3 [適用] 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。

ポリシーベースのルーティング

ポリシーベース ルーティング(PBR)は、分類用の ACL を利用し、パケット フィールドに基づいて、選択され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 はルーティング プロトコルから導き出されるルータへの依存度を軽減します。

ルート マップ

ルート マップは PBR を設定するために使用される手段です。

ルートマップを追加するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [ポリシーベースルーティング] > [ルートマップ] の順にクリックします。

ステップ 2 [追加] をクリックして、以下のパラメータを入力します。

- [ルートマップ名]:ルートマップを定義するオプションとして、次のいずれか 1 つを選択します。
  - [既存のマップの使用]:以前に新しいルールの追加用に定義されたルートマップを選択します。
  - [新しいマップの作成]:新しいルート マップの名前を入力します。
- [連続番号]:指定したルート マップ内の位置または優先度を示す番号。ルートマップに複数のルール(ACL)が定義されている場合、連続番号により、パケットが ACL と照合される順序が決まります(数字が小さい方から大きい方へ)。
- [ルートマップIPタイプ]:ネクスト ホップ IP アドレスのタイプに応じて、IPv6 または IPv4 のどちらかを選択します。
- [一致ACL]:以前に定義された 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]:ネクスト ホップ アドレスが IPv6 アドレスの場合、次のいずれかの特性を選択します。
  - [グローバル]: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 タイプである IPv6 アドレス。
  - [リンク ローカル]:単一ネットワーク 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。

- [ポイントツーポイント]:ポイントツーポイント トンネル。

- [インターフェイス]: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]:ネクスト ホップ ルータの IP アドレス。

ステップ 3 [適用] 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、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [ポリシーベースルーティング] > [ルートマップバインディング] の順にクリックします。

ステップ 2 [追加] をクリックして、以下の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(IP アドレスが付帯)を選択します。
- [バインドされるIPv4ルートマップ]:インターフェイスフェイスにバインドする IPv4 ルート マップを選択します。
- [バインドされるIPv6ルートマップ]: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 [適用] 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。

ポリシーベースのルート

定義されているルート マップを表示するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [ポリシーベースルーティング] > [ポリシーベースのルート] の順にクリックします。

ステップ 2 以前に定義されたルート マップが次のように表示されます。

- [インターフェイス名]:ルート マップが定義されるインターフェイス。
- [ルートマップ名]:ルート マップの名前。

- [ルートマップステータス]:次に示すインターフェイスの状態。
  - [アクティブ]:インターフェイスは起動しています。
  - [インターフェイスダウン]:インターフェイスは停止しています。
- [ACL名]:ルート マップに関連付けられた ACL。
- [ネクストホップ]:ルート マップに一致すパケットのルーティング先。
- [ネクストホップステータス]:次に示すネクスト ホップの到達可能性。
  - [アクティブ]:ネクスト ホップ IP アドレスは到達可能です。
  - [到達不能]: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。
  - [非直接]: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

Domain Name System(DNS; ドメイン ネーム システム)は、ドメイン名を IP アドレスに変換するものです。これにより、ホストを探したりホストのアドレス指定をしたりすることができます。

このデバイスは、DNS クライアントとして、1 台以上の設定済み DNS サーバを使用することによってドメイン名を IP アドレスに変換します。

DNS 設定

[DNS 設定] ページを使用して、DNS 機能を有効にしたり、DNS サーバを設定したり、デバイスによって使用されるデフォルト ドメインを設定したりできます。

ステップ 1 [IP コンフィギュレーション] > [ドメイン ネーム システム] > [DNS 設定] の順にクリックします。

ステップ 2 基本モードでは、次のパラメータを入力します。

- [サーバ指定方法]:DNS サーバを定義するオプションとして、次のいずれか 1 つを選択します。
  - [IPアドレス別]:IP アドレスが DNS サーバに入力されます。
  - [無効]:DNS サーバが定義されません。

- [サーバIPアドレス]:前述の [IPアドレス別] を選択した場合は、DNS サーバの IP アドレスを入力します。
- [デフォルト ドメイン名]:非修飾ホスト名を完成させるために使用する DNS ドメイン名を入力します。デバイスによりこれがすべての非完全修飾ドメイン名(NFQDN)に付加されて、それらが 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 拡張モードでは、次のパラメータを入力します。

- [DNS]:デバイスを DNS クライアントとして指定し、1 台以上の設定済み DNS サーバを使用して DNS 名を IP アドレスに解決できるようにする場合に選択します。
- [ポーリング再試行回数]:デバイスが DNS サーバが存在しないと判断するまで、DNS クエリーを DNS サーバに送信する回数を入力します。
- [ポーリング タイムアウト]:DNS クエリー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]:再試行回数に達した後、DNS クエリー パケットをデバイスが送信する頻度を秒数として入力します。
  - [デフォルトを使用]:デフォルト値を使用する場合に選択します。

    この値 = 2*(ポーリング再試行回数 + 1)* ポーリング タイムアウト
  - [ユーザ定義]:ユーザ定義値を入力する場合に選択します。
- [デフォルト パラメータ]: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]:非修飾ホスト名を完成させるために使用する DNS ドメイン名を入力します。デバイスによりこれがすべての非完全修飾ドメイン名(NFQDN)に付加されて、それらが 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 ドメイン検索リスト]:[詳細] をクリックして、デバイス上で設定されている DNS サーバのリストを表示します。

ステップ 4 [適用] 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サーバテーブル] には、設定された DNS サーバごとに次の情報が表示されます。

- [DNS サーバ]:DNS サーバの IP アドレスを入力します。
- [プリファレンス]:サーバごとにプリファレンス値があります。その値が低いほど、使用される確率が高くなります。

- [送信元]:サーバの 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]:サーバの IP アドレスのインターフェイス。

ステップ 5 定義できる DNS サーバは最大 8 台です。DNS サーバを追加するには、[追加] をクリックします。

ステップ 6 パラメータを入力します。

- [IP バージョン]:IPv6 の場合は [バージョン 6]、IPv4 の場合は [バージョン 4] を選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:IPv6 アドレス タイプがリンク ローカルである場合、その受信元のインターフェイスを選択します。
- [DNS サーバ IP アドレス]:DNS サーバの IP アドレスを入力します。
- [プリファレンス]:ドメインの使用順序を決定する値を選択します。低い値から高い値へという順序で使用されます。これにより、DNS クエリー中に非修飾名が完成される順序が効率的に決定されます。

ステップ 7 [適用] 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、[DNS 設定] ページ、および DHCPv4 と DHCPv6 のサーバ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、[IPコンフィギュレーション] > [ドメインネームシステム] > [検索リスト] の順にクリックします。

デバイスに設定されている 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]: デバイスで使用できるドメインの名前。
- [送信元]: このドメインのサーバの 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]: 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。
- [プリファレンス]: これは、ドメインの使用順序です。低い値から高い値へという順序で使用されます。これにより、DNS クエリー中に非修飾名が完成される順序が効率的に決定されます。

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）に保存されています。

そのキャッシュには、以下のタイプのエントリが含まれる可能性があります。

- [スタティックエントリ]: これらは、手動でキャッシュに追加されたマッピング ペアです。スタティック エントリは 64 個まで可能です。
- [ダイナミックエントリ]: これらは、ユーザによって使用された結果として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。ダイナミック エントリは 256 個まで可能です。

名前解決処理では必ず、最初にこれらのスタティック エントリが検査されます。一致するエントリがない場合は、ダイナミック エントリが検査されます。ここでも一致するエントリがない場合は、外部 DNS サーバに要求が送信されます。

1 つの DNS サーバの 1 つのホスト名に対して 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、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [ドメインネームシステム] > [ホストマッピング] の順にクリックします。

ステップ 2 必要なら、[テーブルのクリア] オプションを選択して、ホスト マッピング テーブル内のエントリの全部または一部を消去できます。

- [スタティックのみ]: スタティック ホストを削除します。
- [ダイナミックのみ]: 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およびスタティック]: スタティック ホストおよびダイナミック ホストを削除します。

ホスト マッピング テーブルに表示されるフィールドは次のとおりです。

- [ホスト名]: ユーザ定義ホスト名または完全修飾名。
- [IPアドレス]: ホスト IP アドレス。
- [IPバージョン]: ホスト IP アドレスの IP バージョン。
- [タイプ]: このエントリがキャッシュに対して [ダイナミック] かそれとも [スタティック] か。
- [ステータス]: 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)]: これがダイナミック エントリの場合、これがキャッシュ内に保持される長さ。
- [残りのTTL(秒)]: これがダイナミック エントリの場合、これがキャッシュ内に保持される残りの長さ。

ステップ 3 ホスト マッピングを追加するには、[追加] 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 バージョン]:IPv6 の場合は [バージョン 6]、IPv4 の場合は [バージョン 4] を選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:IPv6 アドレス タイプがリンク ローカルである場合、その受信元のインターフェイスを選択します。
- [ホスト名]::ユーザ定義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(大文字と小文字は区別しない)、数字 0～9、下線文字、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ています。
- [IPアドレス]: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 5 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

17

IP 設定：RIPv2

ここでは、Routing Information Protocol（RIP）バージョン 2 の機能について説明します。

注 この機能は、デバイスの 550 ファミリ上でのみサポートされます。

具体的な内容は、次のとおりです。

- 概要
- デバイス上での RIP の動作
- RIP の設定
- アクセス リスト

概要

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 ネットワーク用のディスタンス ベクター プロトコルの実装です。このプロトコルは、ルータを *アクティブ*と *パッシブ*(サイレント）に分類します。アクティブ ルータは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ルートをリッスンしたり、更新したりしますが、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、コンフィギュレーションで有効になっている場合は他のすべてのスタティック ルータと同じように RIP 経由でアドバタイズされます。

IP ルーティングが有効になっている場合は、RIP が完全に動作します。IP ルーティングが無効になっている場合は、RIP がパッシブ モードで動作します。これは、RIP が、受信した RIP メッセージからしかルートを学習せず、それらを送信しないことを意味します。

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、次の標準に基づく RIP バージョン 2 をサポートします。

- 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 MIB 拡張

受信した RIPv1 パケットはドロップされます。

デバイス上での RIP の動作

以降の項では、RIP の有効化、オフセット コンフィギュレーション、パッシブ モード、認証、統計情報カウンタ、およびピア データベースについて説明します。

RIP の有効化

RIP の有効化

- RIP はグローバルに有効にしたうえで、インターフェイス単位でも有効にする必要があります。
- RIP を設定できるのは有効になっている場合だけです。
- RIP をグローバルに無効にすると、システム上の RIP コンフィギュレーションが削除されます。
- インターフェイス上で RIP を無効にすると、そのインターフェイス上の RIP コンフィギュレーションが削除されます。
- IP ルーティングが無効になっている場合は、RIP メッセージが送信されませんが、受信された RIP メッセージはルーティング テーブル情報の更新に使用されます。

注 RIP は、手動で設定された IP インターフェイス上でしか定義できません。これは、IP アドレスが DHCP サーバから受信されたインターフェイス上、または、IP アドレスがデフォルト IP アドレスのインターフェイス上では RIP を定義できないことを意味します。

オフセット コンフィギュレーション

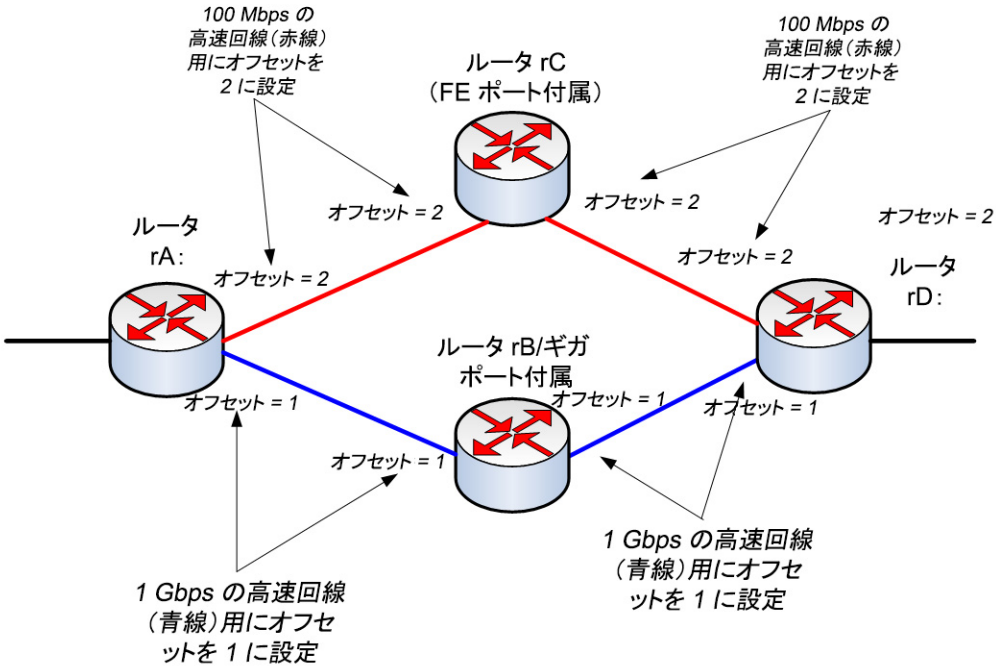
RIP メッセージには、ルートごとのメトリック（ホップ数）が含まれています。

オフセットは、メトリックに追加され、パスのコストに影響を与える数値です。また、オフセットは、インターフェイス単位で設定され、たとえば、特定のインターフェイスの速度、遅延、またはその他の品質を反映させることができます。このように、必要に応じて、インターフェイスの相対的コストを調整することができます。

各インターフェイスのオフセット（デフォルトで 1）を設定するのはユーザの責任です。

ポート速度に基づく、さまざまなインターフェイスのメトリック オフセットのコンフィギュレーションを以下に示します。

オフセットの設定（ポート速度に基づく）



ルータ rD は rB または rC 経由で rA にデータを送信できます。rC はファスト イーサネット（FE）ポートのみをサポートし、rB はギガビット イーサネット（GE）ポートをサポートするため、ルータ rD からルータ rA までのパス コストはルータ rB 経由（コスト パスが 2 増える）よりもルータ rC 経由（コスト パスが 4 増える）の方が高くなります。そのため、トラフィックはルーティング rB 経由で転送する方が望ましいことになります。これを実現するには、回線速度に基づいてインターフェイスごとに別々のオフセット（メトリック値）を設定します。

詳細については、「オフセット コンフィギュレーション」を参照してください。

パッシブ モード

特定の IP インターフェイス上でのルーティング アップデート メッセージの伝送を無効にすることができます。その場合、ルータはパッシブになり、そのインターフェイス上で更新された RIP 情報しか受信しません。デフォルトで、IP インターフェイスのルーティング アップデートの伝送は有効になっています。

詳細については、「RIPv2 設定」を参照してください。

ルーティング アップデートのフィルタリング

2 つの標準アクセス リスト(入力用と出力用)を使用して、特定の IP インターフェイスの着信ルートと発信ルートをフィルタリングすることができます。

標準アクセス リストは、IP プレフィックス(IP アドレスと IP マスク長)とアクションのペアの名前および順序付きリストです。アクションは拒否または許可のどちらかです。

アクセス リストが定義されている場合は、RIP メッセージ内の各ルートが、最初のペアから始まるリストに照らしてチェックされます。それが最初のペアと一致し、アクションが許可だった場合は、そのルートが採用されます。アクションが拒否だった場合は、そのルートが採用されません。ルートが一致しなかった場合は、次のペアが考慮されます。

ルートが一致するペアが見つからなかった場合は、拒否アクションが適用されます。

IP インターフェイス上でのデフォルト ルート エントリのアドバタイズ

デフォルト ルートの記述には特殊なアドレス 0.0.0.0 が使用されます。デフォルト ルートは、システム内の 1 つ以上の密接に接続されたルータが、明示的に列挙されていないネットワークへのトラフィックの転送に使用可能な場合に、使用可能なすべてのネットワークをルーティング アップデート内に列挙するのを避けるために使用されます。これらのルータは、接続先のネットワークであるかのように、アドレス 0.0.0.0 用の RIP エントリを作成します。

デフォルト ルート アドバタイズメントを有効にして、それを特定のメトリックで設定することができます。

再配布機能

次のタイプのルートが存在し、RIP 経由で配布することができます。

- [接続済み]: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。デフォルトで、RIP ルーティング テーブルには、RIP が有効になっている IP インターフェイスに対応するルートだけが含まれています。
- [スタティック]:手動で定義された(リモート)ルート。

[スタティックルートの再配布] 機能または [接続済みルートの再配布] 機能を設定することによって、RIP 経由で再配布されるのがスタティック ルートか接続済みルートかを特定することができます。

これらの機能はデフォルトで無効になっており、グローバルに有効にすることができます。

これらの機能が有効になっている場合は、拒否されたルートが、メトリックが 16 のルートとしてアドバタイズされます。

ルート コンフィギュレーションは、次のオプションのいずれかを使用して伝達することができます。

- [デフォルトメトリック]

  RIP で、伝達するルート コンフィギュレーション用の事前定義のデフォルト メトリック値を使用できるようにします。

- [トランスペアレント](デフォルト)

  RIP で、伝達するルート コンフィギュレーション用の RIP メトリックとして ルーティング テーブル メトリックを使用できるようにします。

  その結果、次のように動作します。

  - ルートのメトリック値が 15 以下の場合は、ルートのアドバタイズ時にこの値が 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 を超えている場合は、そのルートが RIP 経由で他のルータにアドバタイズされません。

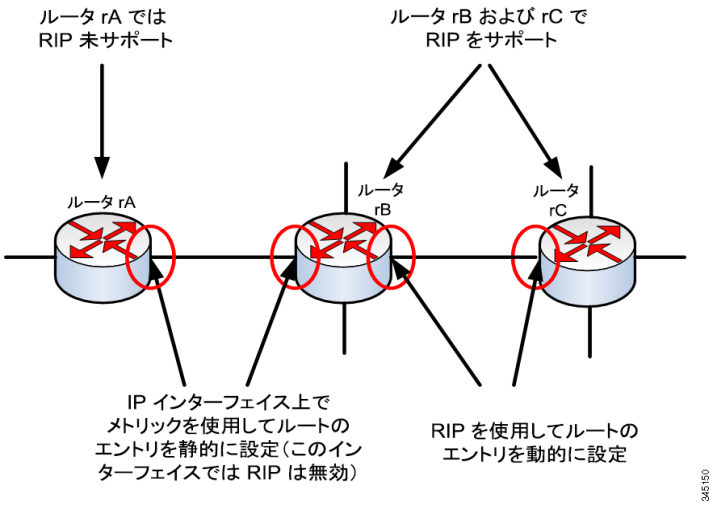
- [ユーザ定義メトリック]

  RIP で、ユーザが入力したメトリック値を使用できるようにします。

非 RIP デバイスを含むネットワークでの RIP の使用

RIP を使用する場合は、スタティック ルート コンフィギュレーションと接続先のインターフェイスを考慮に入れる必要があります。次の図は、一部のルータだけが RIP をサポートしているネットワークを示しています。

RIP ルータと非 RIP ルータで構成されたネットワーク



ルータ rA は RIP をサポートしていません。そのため、このルータ上では適切なメトリックを含むルーティング エントリが静的に設定されます。ルータ rB 上では、ルータ rA へのルートが接続済みルートと見なされます。一方、ルータ rB と rC は RIP を使用してルーティング エントリを抽出して配布します。

ルータ rB の接続済みルート コンフィギュレーションは、デフォルト メトリックとトランスペアレント システムのどちらかを使用してルータ rC に伝達することができます。スタティック/接続済みルートは、ルートのメトリック(トランスペアレント メトリック)または default-metric コマンドで定義されたメトリックのどちらかを使用して*再配布*されます。

詳細については、「再配布機能」を参照してください。

RIP 認証

RIP メッセージの認証を IP インターフェイス単位で無効にすることも、次の認証タイプのいずれかを有効にすることもできます。

- **平文またはパスワード**:ルートと一緒に他のルータに送信されたキー パスワード(文字列)を使用します。受信側のルータは、このキーと独自の設定済みキーを比較します。それらが同じであれば、そのルートが受け入れられます。
- MD5:MD5 ダイジェスト認証を使用します。それぞれのルータが秘密キーのセットで設定されます。このセットは**キー チェーン**と呼ばれています。それぞれのキー チェーンが 1 つ以上のキーで構成されます。それぞれのキーに、識別番号(**キー識別子**)、**キー ストリング**、およびオプションで **send-lifetime** 値と **accept-lifetime** 値が割り当てられます。Send-lifetime は、キー チェーン上の認証キーを送信可能な期間です。accept-lifetime は、キー チェーン上の認証キーが受信可能な期間です。

  送信された RIP メッセージのそれぞれに、メッセージの計算された MD5 ダイジェスト(キー チェーンを含む)と使用されたキー ストリングのキー識別子が含まれています。受信者にもキー チェーンが設定されます。キー識別子は、受信者が MD5 ダイジェストを検証するためのキーを選択するときに使用されます。

RIP 統計情報カウンタ

RIP の動作は、IP インターフェイス単位で統計情報カウンタをチェックすることによって監視できます。これらのカウンタの説明については、「RIPv2 統計情報」を参照してください。

RIP ピア データベース

RIP ピア データベースは IP インターフェイス単位で監視できます。これらのカウンタの説明については、「RIPv2 ピア データベース」を参照してください。

RIP の設定

次のアクションを実行することができます。

- 必須アクション:
  - [RIPv2 プロパティ] ページを使用して、RIP プロトコルをグローバルに有効/無効にします。
  - [RIPv2 設定] ページを使用して、IP インターフェイス上の RIP プロトコルを有効/無効にします。
- 任意アクション(実行されなかった場合は、デフォルト値が使用されます)
  - [RIPv2 プロパティ] ページを使用して、IP インターフェイス上のスタティックまたは接続済みルートとそのメトリックの RIP 経由のアドバタイズを有効/無効にします。
  - [RIPv2 設定] ページを使用して、IP インターフェイス上の着信ルートに関するメトリックに追加するオフセットを設定します。
  - [RIPv2 設定] ページを使用して、IP インターフェイス上のパッシブ モードを有効にします。
  - IP インターフェイス上の IP アドレス一覧を指定することによって、着信/発信ルーティング アップデートで処理するルートを制御します(「アクセス リスト」を参照)。
  - [RIPv2 設定] ページを使用して、IP インターフェイス上のデフォルト ルート エントリをアドバタイズします。
  - [RIPv2 設定] ページを使用して、IP インターフェイス上の RIP 認証を有効にします。

次のページについて説明します。

- RIPv2 プロパティ
- RIPv2 設定
- RIPv2 統計情報
- RIPv2 ピア データベース

RIPv2 プロパティ

注 この機能は、Sx550X/SG550XG デバイスの場合のみサポートされます。

デバイス上で RIP を有効/無効にするには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス] > [RIPv2] > [RIPv2プロパティ] 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。
  - [有効]:RIP を有効にします。
  - [無効]:RIP を無効にします。RIP を無効にすると、システム上の RIP コンフィギュレーションが削除されます。
  - [シャットダウン]:RIP グローバル状態をシャットダウンに設定します。
- [RIPアドバタイズメント]:すべての RIP IP インターフェイス上のルーティング アップデートの送信を有効にする場合に選択します。
- [デフォルトルートアドバタイズメント]:RIP ドメインへのデフォルト ルートの送信を有効にする場合に選択します。このルートがデフォルト ルートとして機能します。
- [デフォルト メトリック]:デフォルト メトリックの値を入力します(再配布機能を参照)。

ステップ 3 [スタティック ルートの再配布]:この機能を有効にする場合に選択します(再配布機能を参照)。

ステップ 4 [スタティックルートの再配布] が有効になっている場合は、[固定メトリックの再配布] フィールド用のオプションを選択します。次のオプションが選択できます。

- [デフォルト メトリック]:RIP で、伝達するスタティック ルート コンフィギュレーション用のデフォルト メトリック値を使用できるようにします(「再配布機能」を参照)。
- [トランスペアレント]:RIP で、伝達するスタティック ルート コンフィギュレーション用の RIP メトリックとしてルーティング テーブル メトリックを使用できるようにします。その結果、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 以下の場合は、そのスタティック ルートのアドバタイズ時にこの値が 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 を超えている場合は、そのスタティック ルートが RIP 経由で他のルータにアドバタイズされません。

- [ユーザ定義メトリック]: メトリックの値を入力します。

ステップ 5 [接続済みルートの再配布]: この機能を有効にする場合に選択します(「スタティック ルート コンフィギュレーションの再配布」を参照)。

ステップ 6 [接続済みルートの再配布] が有効になっている場合は、[接続済みメトリックの再配布] フィールド用のオプションを選択します。次のオプションが選択できます。

- [デフォルト メトリック]:RIP で、伝達するスタティック ルート コンフィギュレーション用のデフォルト メトリック値を使用できるようにします(「再配布機能」を参照)。

- [トランスペアレント]:RIP で、伝達するスタティック ルート コンフィギュレーション用の RIP メトリックとしてルーティング テーブル メトリックを使用できるようにします。その結果、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 以下の場合は、そのスタティック ルートのアドバタイズ時にこの値が 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 を超えている場合は、そのスタティック ルートが RIP 経由で他のルータにアドバタイズされません。

- [ユーザ定義メトリック]: メトリックの値を入力します。

ステップ 7 [適用] 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、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [RIPv2] > [RIPv2設定] の順にクリックします。

ステップ 2 RIP パラメータが IP インターフェイス単位で表示されます。新しい IP インターフェイスを追加するには、[追加] をクリックして、次のフィールドに値を入力します。

- [IPアドレス]: レイヤ 2 インターフェイス上で定義された IP インターフェイスを選択します。

- [シャットダウン]: インターフェイス上の RIP コンフィギュレーションを維持しますが、インターフェイスを非アクティブに設定します。

- [パッシブ]:指定された IP インターフェイス上で RIP ルート アップデート メッセージの送信を許可するかどうかを指定します。このフィールドが有効になっていない場合は、RIP アップデートが送信されません(パッシブ)。
- [オフセット]:指定された IP インターフェイスのメトリック番号を指定します。これにより、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追加のコストが考慮されます。
- [デフォルトルートアドバタイズメント]:このオプションは、[RIPv2 プロパティ] ページでグローバルに定義されます。グローバル定義を使用することも、特定のインターフェイス用にこのフィールドを定義することもできます。次のオプションが選択できます。
  - [グローバル]:[RIPv2プロパティ] 画面で定義されたグローバル設定を使用します。
  - [有効]:この RIP インターフェイス上でデフォルト ルートをアドバタイズします。
  - [無効]:この RIP インターフェイス上でデフォルト ルートをアドバタイズしません。
- [デフォルトルートアドバタイズメント メトリック]:このインターフェイスのデフォルト ルートに関するメトリックを入力します。
- [認証モード]:指定された IP インターフェイス上の RIP 認証状態(有効/無効)。次のオプションが選択できます。
  - [なし]:認証が実行されません。
  - [テキスト]:下で入力されたキー パスワードが認証に使用されます。
  - [MD5]:下で選択されたキー チェーンの MD5 ダイジェストが認証に使用されます。
- [キーパスワード]:[テキスト] が認証タイプとして選択された場合に、使用するパスワードを入力します。
- [キーチェーン]:[MD5] が認証タイプとして選択された場合に、ダイジェストするキー チェーンを入力します。このキー チェーンは、「キー管理」に記載されているように作成されます。
- [Distribute-list In]:[アクセスリスト名] で指定された IP アドレスの RIP 着信ルート上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になっている場合は、下の [アクセス リスト名] を選択します。

- [アクセスリスト名]:指定された IP インターフェイスに対する RIP 着信ルートフィルタリングのアクセス リスト名(IP アドレスの一覧を含む)を選択します。アクセス リストの説明については、「アクセス リスト設定」を参照してください。
- [Distribute-list Out]:[アクセスリスト名] で指定された IP アドレスの RIP 発信ルート上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になっている場合は、下の [アクセス リスト名] を選択します。
- [アクセスリスト名]:指定された IP インターフェイスに対する RIP 発信ルートフィルタリングのアクセス リスト名(IP アドレスの一覧を含む)を選択します。アクセス リストの説明については、「アクセス リスト設定」を参照してください。

ステップ 3 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

RIPv2 統計情報

IP アドレスごとの RIP 統計情報カウンタを表示するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [RIPv2] > [RIPv2統計情報] の順にクリックします。

次のフィールドが表示されます。

- [IPインターフェイス]:レイヤ 2 インターフェイス上で定義された IP インターフェイス。
- [不正なパケットを受信しました]:IP インターフェイス上の RIP によって識別された不正パケットの数を示します。
- [不正なルートを受信しました]:IP インターフェイス上の RIP によって受信および識別された不正ルートの数を示します。不正ルートは、ルート パラメータが間違っていることを意味します。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。
- [更新が送信されました]:IP インターフェイス上の RIP によって送信されたパケットの数を示します。

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、[すべてのインターフェイス カウンタのクリア] をクリックします。

RIPv2 ピア データベース

RIP ピア(ネイバー)データベースを表示するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [RIPv2] > [RIPv2ピアルータデータベース] の順にクリックします。

ピア ルータ データベースに関する次のフィールドが表示されます。

- [ルータIPアドレス]:レイヤ 2 インターフェイス上で定義された IP インターフェイス。
- [不正なパケットを受信しました]:IP インターフェイス上の RIP によって識別された不正パケットの数を示します。
- [不正なルートを受信しました]:IP インターフェイス上の RIP によって受信および識別された不正ルートの数を示します。不正ルートは、ルート パラメータが間違っていることを意味します。たとえば、IP 宛先がブロードキャストになっていたり、メトリックが 0 または 16 を超えていたりした場合です。
- [最終更新]: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刻を示します。

ステップ 2 すべてのカウンタをクリアするには、[すべてのインターフェイスカウンタのクリア] をクリックします。

アクセス リスト

アクセス リストの説明については、「ルーティング アップデートのフィルタリング」を参照してください。

アクセス リストを作成するには、次のようにします。

1. [アクセス リスト] ページを使用して、単一の IP アドレスを含むアクセス リストを作成します。
2. 必要に応じて、[送信元 IPv4 アクセス リスト] ページを使用して、新しい IP アドレスを追加します。

アクセス リスト設定

アクセス リストのグローバル コンフィギュレーションを設定するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス] > [アクセスリスト] > [アクセスリスト設定] 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、[追加] をクリックして [アクセスリストの追加] ページを開き、次のフィールドに値を入力します。

- [名前]:アクセス リストの名前を定義します。
- [送信元IPv4アドレス]:送信元 IPv4 アドレスを入力します。次のオプションが選択できます。
  - [任意]:すべての IP アドレスが含まれます。
  - [ユーザ定義]:IP アドレスを入力します。
- [送信元IPv4マスク]:送信元 IPv4 アドレス マスクのタイプと値を入力します。次のオプションが選択できます。
  - [ネットワークマスク]:ネットワーク 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入力します。
- [アクション]:アクセス リストに対するアクションを選択します。次のオプションが選択できます。
  - [許可]: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]: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 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

送信元 IPv4 アクセス リスト

アクセス リストに IP アドレスを設定するには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス] > [アクセスリスト] > [送信元IPv4アドレスリスト] の順にクリックします。

ステップ 2 アクセス リストのパラメータを変更するには、[追加] をクリックして、次のフィールドのいずれかを変更します。

- [アクセスリスト名]:アクセス リストの名前。
- [送信元IPv4アドレス]:送信元 IPv4 アドレス。次のオプションが選択できます。
  - [任意]:すべての IP アドレスが含まれます。
  - [ユーザ定義]:IP アドレスを入力します。
- [送信元IPv4マスク]:送信元 IPv4 アドレス マスクのタイプと値。次のオプションが選択できます。
  - [ネットワークマスク]:ネットワーク マスク(255.255.0.0 など)を入力します。
  - [プレフィックス長]:プレフィックス長を入力します。
- [アクション]:アクセス リストに対するアクション。次のオプションが選択できます。
  - [許可]: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]: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 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

18

IP 設定：VRRP

注　この機能は、スイッチの 550 ファミリ上でのみサポートされます。

この章では、Virtual Router Redundancy Protocol（VRRP）の機能と WEB GUI 経由で VRRP を実行する仮想ルータを設定する方法について説明します。

具体的な内容は、次のとおりです。

- 概要
- VRRP トポロジ
- VRRP の設定可能要素
- VRRP の設定

概要

VRRP は、仮想ルータの責任を LAN 上の物理ルータの 1 つに動的に割り当てる選択および冗長プロトコルです。これにより、ネットワーク内のルーティング パスの可用性と信頼性が向上します。

VRRP では、仮想ルータ内の 1 台の物理ルータがマスターとして選択されます。マスターで障害が発生した場合は同じ仮想ルータ内の別の物理ルータがバックアップとして機能します。物理ルータは VRRP ルータと呼ばれます。

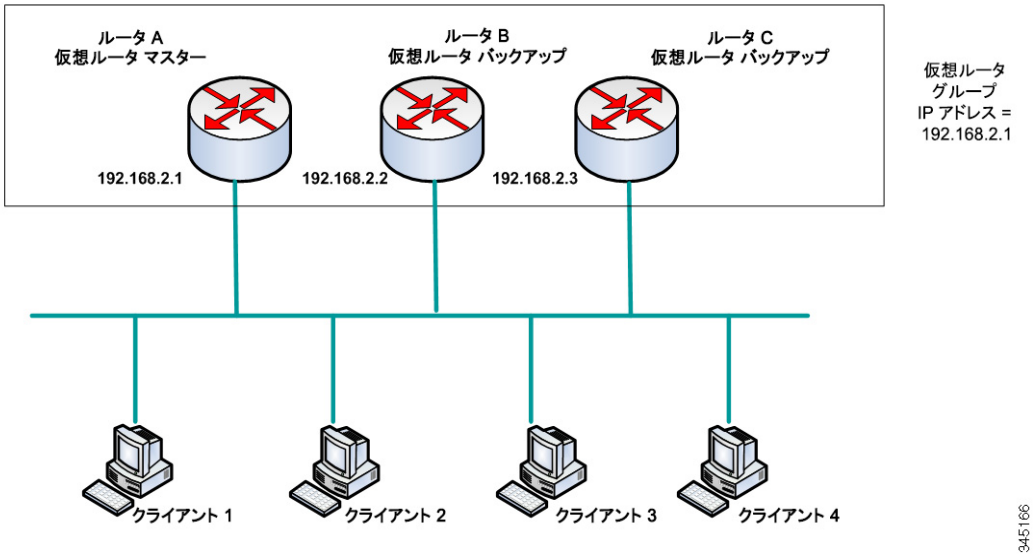
参加しているホストのデフォルト ゲートウェイは、物理ルータではなく、仮想ルータに割り当てられます。仮想ルータの代わりにパケットをルーティングしている物理ルータで障害が発生した場合は、別の物理ルータが選択され、自動的に置き換えらます。いつもパケットを転送している物理ルータがマスター ルータと呼ばれます。

VRRP はトラフィックのロード シェアリングも可能にします。LAN クライアントとやり取りするトラフィックを複数のルータで共有するように VRRP を設定することによって、使用可能なルータ間でトラフィックを公平に分配することができます。

VRRP トポロジ

VRRP が設定された LAN トポロジを以下に示します。この例では、ルータ A、B、および C が VRRP で、仮想ルータを構成しています。仮想ルータの IP アドレスは、ルータ A のイーサネット インターフェイス用に設定されたものと同じです(198.168.2.1)。

基本 VRRP トポロジ



仮想ルータはルータ A の物理イーサネット インターフェイスの IP アドレスを使用するため、ルータ A は*仮想ルータ マスター*の役割を引き受け、*IP アドレス オーナー*とも呼ばれます。仮想ルータ マスターとしてルータ A は、仮想ルータの IP アドレスを制御し、仮想ルータの代わりにパケットをルーティングする責任があります。クライアント 1 ～ 3 は、198.168.2.1 のデフォルト ゲートウェイ IP アドレスに設定されます。クライアント 4 は、198.168.2.2 のデフォルト ゲートウェイ IP アドレスに設定されます。

注 IP アドレス オーナーである VRRP ルータは、その IP アドレス宛てのパケットに応答/処理します。仮想ルータ マスターだが、IP アドレス オーナーではない VRRP ルータは、そのようなパケットに応答/処理しません。

ルータ B と C は、*仮想ルータ バックアップ*として機能します。仮想ルータ マスターで障害が発生した場合は、次にプライオリティの高いルータが仮想ルータ マスターになって、最小限の中断で LAN ホストにサービスを提供します。

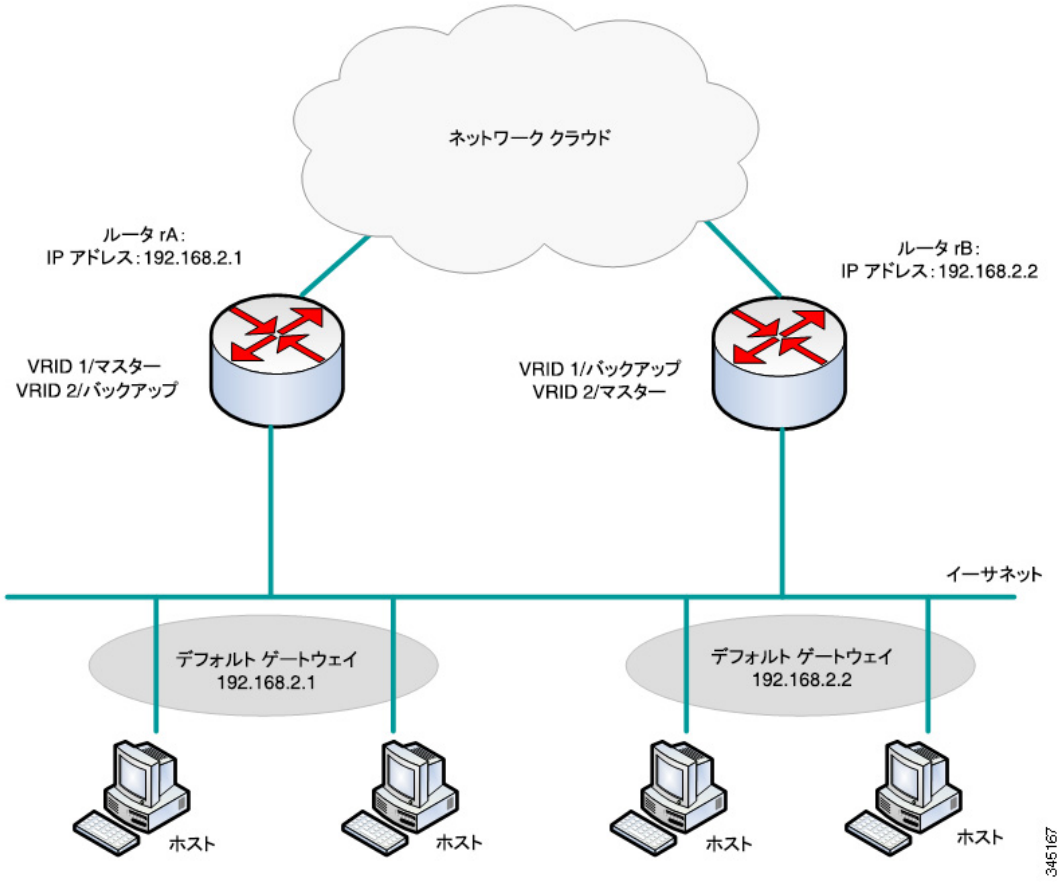
注 VRRP ルータのプライオリティは次によって決まります:VRRP ルータがオーナーの場合は、プライオリティが 255(最高)になります。オーナーでない場合は、プライオリティが手動で設定されます(必ず 255 未満)。

ルータ A が復旧したら、再び仮想ルータ マスターになります。マスターの復旧中は、両方のマスターがパケットを転送するため、重複(通常の動作)が発生しますが、中断はありません。

VRRP ルータが果たす役割と仮想ルータ マスターで障害が発生した場合の動作の詳細については、「VRRP ルータのプライオリティとプリエンプション」を参照してください。

VRRP が設定された LAN トポロジを以下に示します。ルータ A と B がクライアント 1 ～ 4 との間のトラフィックを共有し、どちらか一方のルータで障害が発生すると、もう一方が仮想ルータ バックアップとして機能します。

VRRP トポロジのロード シェアリング



このトポロジでは、2 台の仮想ルータが設定されています。仮想ルータ 1 では、rA が IP アドレス 192.168.2.1 のオーナーで仮想ルータ マスターです。また、rB が rA に対する仮想ルータ バックアップです。クライアント 1 と 2 は、192.168.2.1 のデフォルト ゲートウェイ IP アドレスに設定されています。

仮想ルータ 2 では、rB が IP アドレス 192.168.2.2 のオーナーで仮想ルータ マスターです。また、rA が rB に対する仮想ルータ バックアップです。クライアント 3 と 4 は、192.168.2.2 のデフォルト ゲートウェイ IP アドレスに設定されています。

VRRP の設定可能要素

仮想ルータには、同じ LAN 上のすべての仮想ルータ間で一意の仮想ルータ識別子（VRID）を割り当てる必要があります。同じ仮想ルータをサポートするすべての VRRP ルータを、VRID を含む仮想ルータに関するすべての情報を使って設定する必要があります。デバイス上で仮想ルータを有効にするには、そのデバイス上で IP ルーティングも有効にする必要があります。

VRRP ルータは、CLI コマンドを使用するか、「VRRP の設定」に記載されているように Web GUI を経由して、1 台以上の仮想ルータに参加するように設定できます。

仮想ルータを設定するには、それをサポートするすべての VRRP ルータ上で仮想ルータ ID や IP アドレスなどの情報を設定します。次の要素を設定してカスタマイズすることができます。

仮想ルータの識別

仮想ルータには、識別子（VRID）を割り当てる必要があり、説明を付加することもできます。以下の項で、仮想ルータのさまざまな属性について説明します。

VRRP は最大 255 台の仮想ルータ（VRRP グループ）をサポートします。

VRRP のバージョン

このデバイスは、次の VRRP バージョン タイプをサポートします。

- RFC5798 に基づく IPv4 VRRPv3。VRRPv3 メッセージが送信されます。
- RFC5798 に基づく IPv4 VRRPv3 および VRRPv2。VRRPv3 メッセージと VRRPv2 メッセージが送信されます。
- RC3768 に基づく IPv4 VRRPv2。VRRPv2 メッセージが送信されます。

VRRP バージョンの設定は仮想ルータ単位に行います。デフォルトは VRRPv2 です。

仮想ルータを設定するときの状態を以下に示します。

- 仮想ルータの既存の VRRP ルータのすべてが VRRPv3 で動作している。この場合は、新しい VRRP ルータを VRRPv3 で動作するように設定します。
- 仮想ルータの既存の VRRP ルータのすべてが VRRPv2 で動作している。この場合は、新しい VRRP ルータを VRRPv2 で動作するように設定します。
- VRRPv2 と VRRPv3 の両方で動作している仮想ルータの VRRP ルータが 1 台以上存在している。この場合は、VRRPv2 が相互運用可能であっても、VRRP ルータを VRRPv3 で動作するように設定します。

  注 仮想ルータ内に VRRPv2 専用のルータと VRRPv3 専用のルータが存在する場合は、VRRPv2 ルータと VRRPv3 ルータを 1 台以上設定する必要があります。

注 VRRPv2 と VRRPv3 の両方が VRRP ルータ上で有効になっている場合は、VRRP ルータが VRRPv2 パケットと VRRPv3 パケットの両方を送信します。VRRPv3 標準によれば、v2 から v3 にアップグレードするときに、VRRPv2 と VRRPv3 の両方を有効にする必要があります。2 つのバージョンの混在を恒久的なソリューションと考えないでください。VRRPv2 と VRRPv3 の相互運用の詳細については、VRRPv3 標準を参照してください。

仮想ルータIPアドレス

仮想ルータごとに、現在のマスターが責任を負っている 1 つ以上の IP アドレスが割り当てられます。

仮想ルータをサポートする VRRP ルータは、仮想ルータ上に設定された IP アドレスに対応する、同じ IP サブネット上の IP インターフェイスを備えている必要があります。

仮想ルータへの IP アドレスの割り当ては、次のルールに従って行われます。

- 仮想ルータをサポートするすべての VRRP ルータを仮想ルータのコンフィギュレーション内の同じ仮想ルータ IP アドレスに設定する必要があります。
- 別の仮想ルータ内の IP アドレスや仮想ルータをサポートしない VRRP ルータ内の IP アドレスは使用できません。
- 仮想ルータをサポートする VRRP ルータのいずれかを仮想ルータのすべての IP アドレスのオーナーにする必要があります。IP アドレスが VRRP ルータの IP インターフェイス上で設定された実アドレスの場合は、VRRP ルータがその IP アドレスのオーナーです。

- VRRP ルータ(物理ルータ)が仮想ルータの IP アドレスのオーナーの場合は、仮想ルータの IP アドレスを DHCP 経由ではなく、VRRP ルータ上で手動で設定する必要があります。
- VRRP ルータが仮想ルータの IP アドレスのオーナーでない場合:
  - オーナー以外の VRRP ルータは、仮想ルータの IP アドレスと同じ IP サブネット上の IP インターフェイスで設定する必要があります。
  - 対応する IP サブネットは、DHCP 経由ではなく、VRRP ルータ内で手動で設定する必要があります。

同じ仮想ルータをサポートするすべての VRRP ルータを同じコンフィギュレーションにする必要があります。コンフィギュレーションが異なる場合は、マスターのコンフィギュレーションが使用されます。バックアップ VRRP ルータは、コンフィギュレーションがマスターのものと異なる場合に、メッセージを syslog に書き込みます。

VRRP ルータの送信元 IP アドレス

仮想ルータをサポートする各 VRRP ルータは、仮想ルータ宛ての発信 VRRP メッセージ内の送信元 IP アドレスとして個別の IP アドレスを使用します。同じ仮想ルータの VRRP ルータは、VRRP メッセージで相互に通信します。VRRP ルータが仮想ルータの IP アドレスのオーナーの場合は、IP アドレスが仮想ルータ IP アドレスのいずれかになります。VRRP ルータが仮想ルータの IP アドレスのオーナーでない場合は、IP アドレスが仮想ルータの同じ IP サブネットへの VRRP ルータ インターフェイスの IP アドレスになります。

送信元 IP アドレスが手動で設定された場合は、そのコンフィギュレーションが削除され、デフォルト送信元 IP アドレス(インターフェイス上で定義された VRRP ルータの最小の IP アドレス)が取得されます。送信元 IP アドレスがデフォルトだった場合は、新しいデフォルト送信元 IP アドレスが取得されます。

VRRP ルータのプライオリティとプリエンプション

VRRP 冗長スキームの重要な側面は、VRRP ルータごとに VRRP プライオリティを割り当てることができることです。VRRP プライオリティは、VRRP ルータがその中で定義された仮想ルータに対するバックアップとしてどれほど効率的に動作するかを表している必要があります。仮想ルータのバックアップ VRRP ルータが複数存在する場合は、現在のマスターで障害が発生した場合にマスターとして割り当てられるバックアップ VRRP ルータがプライオリティで決定されます。

仮想ルータが IP アドレスのオーナーの場合は、その VRRP プライオリティがシステムによって自動的に 255 に設定され、VRRP ルータ(この仮想ルータが割り当てられる)がアップしている場合は自動的に仮想ルータ マスターとして機能します。

図「基本 VRRP トポロジ」では、仮想ルータ マスターのルータ A で障害が発生すると、仮想ルータ バックアップの B と C のどちらが引き継ぐかを決定する選択プロセスが実行されます。ルータ B と C のプライオリティがそれぞれ 101 と 100 に設定されている場合は、プライオリティの高いルータ B が選ばれて仮想ルータ マスターになります。両方のプライオリティが同じ場合は、IP アドレス値の高い方が選ばれて仮想ルータ マスターになります。

デフォルトで、プリエンプティブ機能が有効になっており、次のように動作します。

- 有効:現在のマスターより高いプライオリティに設定された VRRP ルータがアップしている場合は、それが現在のマスターに取って代わります。
- 無効:現在のマスターより高いプライオリティに設定された VRRP ルータがアップしている場合でも、それが現在のマスターに取って代わることはありません。オリジナルのマスター(使用可能な場合)だけがバックアップに取って代わります。

VRRP アドバタイズメント

仮想ルータ マスターは、同じグループ内のルータ(同じ仮想ルータ識別を使用して設定されている)に VRRP アドバタイズメントを送信します。

VRRP アドバタイズメントは、IP パケット内にカプセル化され、VRRP グループに割り当てられた IPv4 マルチキャスト アドレスに送信されます。アドバタイズメントはデフォルトで 1 秒間隔で送信されます。このアドバタイズメント間隔は設定可能です。

アドバタイズメント間隔はミリ秒単位(範囲:50 ～ 40950、デフォルト:1000)です。値なしは無効です。

- VRRPバージョン3では、動作アドバタイズ間隔は10ミリ秒の丸め単位で直近の値に丸められます。
- VRRP バージョン 2 では、動作アドバタイズメント間隔が最も近い秒数に切り捨てられます。最小動作値は 1 秒です。

VRRP の設定

仮想ルータ

VRRP プライオリティは、VRRP 仮想ルータ ページで設定してカスタマイズすることができます。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス] > [VRRP] > [仮想ルータ] の順にクリックします。

仮想ルータが表示されます。フィールドは [追加] ページで説明されます。ただし、システムで生成されるフィールドを除きます。

- [マスター/バックアップステータス]:仮想ルータがマスターなのか、バックアップなのか、そのどちらでもないのかが表示されます。
- [マスタープライマリアドレス]:マスター ルータの IP アドレスが表示されます。
- [プリエンプトモード]:プリエンプティブ機能が有効になっているか無効になっているか。

ステップ 2 仮想ルータを追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [インターフェイス]:仮想ルータが定義されるインターフェイス。
- [仮想ルータ識別子]:仮想ルータを識別するユーザ定義の番号。
- [説明]:仮想ルータを識別するユーザ定義の文字列。
- [ステータス]:デバイス上で VRRP を有効にする場合に選択します。
- [バージョン]:このルータで使用する VRRP のバージョンを選択します。
- [IPアドレスオーナー]:[はい] がオンになっている場合は、デバイスの IP アドレスが仮想ルータの IP アドレスであることを示します。[使用可能な IP アドレス] リストからオーナーの IP アドレスを選択して、それを [オーナー IP アドレス] リストに移動します。

  [いいえ] がオンになっている場合は、[仮想ルータIPアドレス] フィールドに仮想ルータのアドレスを入力する必要があります。ここで複数の IP ドレスを追加する場合は、「1.1.1.1, 2.2.2.2」のように区切って入力します。
- [送信元IPアドレス]:VRRP メッセージ内で使用される IP アドレスを選択します。デフォルト送信元 IP アドレスは、インターフェイス上で定義された最小の IP アドレスです。

- [プライオリティ]:このデバイスがオーナーの場合は、このフィールドに 255 の値が設定され、この値を変更することはできません。そうでない場合は、マスターにどれほど適しているかに基づいて、このデバイスのプライオリティを入力します。100 がオーナー以外のデバイスのデフォルトです。
- [プリエンプト モード]:次のオプションのいずれかを選択します。
  - [True]:現在のマスターより高いプライオリティに設定された VRRP ルータがアップしている場合は、それが現在のマスターに取って代わります。
  - [False]:現在のマスターより高いプライオリティに設定された VRRP ルータがアップしている場合でも、それが現在のマスターに取って代わることはありません。オリジナルのマスター(使用可能な場合)だけがバックアップに取って代わります。
- [許可制御モード]:次のオプションのいずれかを選択します。
  - [許可]:マスター状態の仮想ルータは、アドレス オーナーでない場合でも、仮想ルータの IP アドレス宛てのパケットをそのまま受け入れます。
  - [ドロップ]:マスター状態の仮想ルータは、アドレス オーナーでない場合、仮想ルータの IP アドレス宛てのパケットをドロップします。
- [IP SLA トラック]:ルータからデフォルト ルートのネクスト ホップへの接続のトラッキングを有効にする場合に選択します。
- [トラッキング オブジェクト]:接続を検証する SLA トラックの番号を入力します。この値は、[SLA トラック] ページで入力されたものです。
- [デクリメント]:トラック オブジェクトの状態がダウンの場合は、ルータの VRRP プライオリティがこの値だけ下げられます。
- [アドバタイズメント間隔]:アドバタイズメント パケットの送信頻度を入力します。

  注 これらのパラメータが変更([編集])された場合は、仮想ルータが変更され、新しいパラメータを含む新しいメッセージが送信されます。

ステップ 4 仮想ルータの詳細を確認するには、[詳細] をクリックします。

選択された仮想ルータに関する次のフィールドが表示されます。

- [インターフェイス]:仮想ルータが定義されたレイヤ 2 インターフェイス(ポート、LAG、または VLAN)。
- [仮想ルータ識別子]:仮想ルータの識別番号。
- [仮想ルータMACアドレス]:仮想ルータの仮想 MAC アドレス。
- [仮想ルータIPアドレステーブル]:この仮想ルータに関連付けられた IP アドレス。
- [説明]:仮想ルータの名前。

- [追加ステータス]
  - [バージョン]:仮想ルータのバージョン。
  - [ステータス]:VRRP が有効かどうか。
  - [IPアドレスオーナー]:仮想ルータの IP アドレスのオーナー。
  - [スキュー時間]:マスター ダウン時間の計算に使用される時間。
  - [マスター ダウン間隔]:マスター ユニットがダウンしていた時間。
  - [マスター/バックアップステータス]:仮想ルータがマスターかバックアップか。
  - [プリエンプトモード]:プリエンプト モードが有効かどうか。
  - [許可/制御モード]:ドロップ/許可のどちらかが表示されます。
- **トラック パラメータ**
  - [トラッカー オブジェクト]:接続を検証する SLA トラックの番号が表示されます。
  - [デクリメント]:トラック オブジェクトの状態がダウンの場合は、ルータの VRRP プライオリティがこの値だけ下げられます。
  - [状態]:ルータがアップ状態なのかダウン状態なのかが表示されます。
  - [現在のプライオリティ]:ルータのプライオリティが表示されます。
- **選択された仮想ルータの [マイ パラメータ]**
  - [プライオリティ]:マスターにどれほど適しているかに基づく、この仮想ルータのデバイスのプライオリティ。
  - [アドバタイズメント間隔]:VRRP アドバタイズメントで記述されている時間間隔。
  - [送信元IPアドレス]:VRRP メッセージ内で使用される IP アドレス。
- [マスターパラメータ]
  - [プライオリティ]:255
  - [アドバタイズメント間隔]:VRRP アドバタイズメントで記述されている時間間隔。
  - [送信元IPアドレス]:VRRP メッセージ内で使用される IP アドレス。

VRRP 統計情報

VRRP 統計情報を表示してインターフェイス カウンタをクリアするには、次のようにします。

ステップ 1 [IPコンフィギュレーション] > [IPv4の管理およびインターフェイス] > [VRRP] > [VRRP統計情報] の順にクリックします。

VRRP が有効になっているすべての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。

- [インターフェイス]:VRRP が有効になっているインターフェイスが表示されます。
- [無効なチェックサム]:無効なチェックサムを含むパケットの数が表示されます。
- [無効なパケット長]:無効なパケット長を含むパケットの数が表示されます。
- [無効なTTL]:無効な存続可能時間値を含むパケットの数が表示されます。
- [無効なVRRPパケットタイプ]:無効な VRRP パケット タイプを含むパケットの数が表示されます。
- [無効なVRRP ID]:無効な VRRP ID を含むパケットの数が表示されます。
- [無効なプロトコル番号]:無効なプロトコル番号を含むパケットの数が表示されます。
- [無効なIPリスト]:無効な IP リストを含むパケットの数が表示されます。
- [無効な間隔]:無効な間隔を含むパケットの数が表示されます。
- [無効な認証]:認証に失敗したパケットの数が表示されます。

ステップ 2 インターフェイスを選択します。

ステップ 3 特定のインターフェイスのカウンタをクリアするには、[インターフェイスカウンタのクリア] をクリックします。

ステップ 4 すべてのカウンタをクリアするには、[すべてのインターフェイスカウンタのクリア] をクリックします。

19

IP 設定：SLA

注　この機能は、スイッチの 550 ファミリ上でのみサポートされます。

この章では、サービス レベル アグリーメント（SLA）機能の動作について説明します。

具体的な内容は、次のとおりです。

- 概要
- SLA の使用

概要

VRRP の IP SLA トラッキング

VRRP は、仮想ルータの責任をネットワーク内のルータの 1 つに動的に割り当てる選択プロトコルです。VRRP 優先順位が最も高いルータがネットワーク マスター ルータとして選択され、他のすべてのルータはバックアップ ルータになります。マスター ルータで障害が発生すると、VRRP 優先順位が最も高いバックアップ ルータがマスター ルータになります。

VRRP プロトコルは、ルータ自体の状態に関する情報は提供しますが、ルータによって使用されるルートの状態に関する情報は提供しません。そのため、スタティック ルーティングが使用されている場合は、マスター ルータは引き続きマスター ルータとして機能しますが、そのルータから（デフォルト ルートの）ネクスト ホップへの接続が失われることがあります。IP VRRP SLA は、VRRP ルータへの接続を追跡するためのメカニズムをデフォルト ルート ネクスト ホップに提供します。ネクスト ホップへの接続が失われた場合は、マスター ルータの VRRP 優先順位が下げられるため、（その下げられた値より）優先順位がより高いバックアップ ルータが引き継いで、マスター ルータになることができます。これにより、新しく選択されたマスター ルータ経由のネクスト ホップへの接続が可能になります。RIP などのダイナミック ルーティング プロトコルが使用されている場合、IP SLA は必要ありません。

IP SLA のオブジェクト トラッキングは、特定のネットワーク宛先への接続を検出する IP SLA オペレーションに依存します。IP SLA オペレーションは、ICMP パケットをユーザによって定義されたアドレス(必要なネクスト ホップ)に送信し、ホストからの応答で成功または失敗をモニタします。トラック オブジェクトを使用して、オペレーション結果を追跡します。ICMP 宛先の成功または失敗に基づいてステータスがアップまたはダウンに設定されます。

トラック オブジェクトのステータスは、さまざまなアプリケーションが、ネットワーク接続の情報が必要な決定をする際に使用できます。このようなアプリケーションの 1 つが VRRP です。トラック オブジェクトは VRRP ルータに割り当てられます。トラック ステータスがダウンの場合は、ルータの VRRP 優先順位がユーザによって定義された値だけ下げられます。トラック ステータスがアップの場合は、ルータのオリジナルの VRRP 優先順位が維持されます。

IPv4 スタティック ルートの IP SLA トラッキング

スタティック ルーティングが使用されている場合は、スタティック ルートがアクティブになっていても、指定されたネクスト ホップ経由で宛先ネットワークに到達できないことがあります。たとえば、問題のスタティック ルートで宛先ネットワークに最低のメトリックが設定されており、ネクスト ホップへの発信インターフェイスはアップ状態だが、宛先ネットワークへのパスに沿ったどこかで接続が「切断」されている場合です。このケースでは、デバイスがスタティック ルートを使用することはできますが、宛先ネットワークへの接続を確立できません。スタティック ルートの IP SLA オブジェクト トラッキングは、スタティック ルートで指定されたネクスト ホップ経由の宛先ネットワークへの接続を追跡するメカニズムを提供します。宛先ネットワークへの接続が失われた場合は、ルート状態がダウンに設定され、使用可能であれば、別のスタティック ルート(アップ状態になっている)をトラフィックのルーティング用として選択できます。

VRRP の IP SLA トラッキングと同様に、スタティック ルートの IP SLA オブジェクト トラッキングも宛先ネットワークへの接続の検出を IP SLA オペレーションに依存します。IP SLA オペレーションは、ICMP パケットをユーザによって定義されたアドレス(必要な宛先ネットワーク上のホスト)に送信し、ping 操作に使用するネクスト ホップも定義します。その後で、IP SLA オペレーションは、ホストからの応答で成功または失敗をモニタします。トラック オブジェクトを使用して、オペレーション結果を追跡します。ICMP 宛先の成功または失敗に基づいてステータスがアップまたはダウンに設定されます。トラック オペレーションはスタティック ルートに割り当てられます。トラック ステータスがダウンの場合は、スタティック ルート状態がダウンに設定されます。トラック ステータスがアップの場合は、スタティック ルート状態がアップに設定されます。

ここで、このセクションで使用される主な用語について説明します。

- **オペレーション**:各 IP SLA のエコー オペレーションは、単一の ICMP エコー要求を設定された頻度でターゲット アドレスに送信します。その後で、応答を待機します。
- **トラック オブジェクト ステータス**:各トラッキング オブジェクトは、オペレーション ステータスを維持します。ステータスは次のどちらかです。アップまたはダウン。オブジェクトが作成されると、その状態はアップに設定されます。次の表に、IP SLA オペレーション リターン コードとオブジェクト ステータスの対応を示します。

オペレーション リターン コード	トラック オペレーション ステータス
OK	アップ
エラー	ダウン

注 トラック引数で指定された IP SLA オペレーションが設定されていない、または、そのスケジュールが保留中になっている場合、その状態は OK になります。

注 存在しないトラッキング オブジェクトにバインドされたアプリケーションはアップ状態を受け取ります。

- **SLA オペレーション ステータス**:これは、オペレーションが間もなく始まることを意味する**スケジュール済み**と、作成されているがアクティブになっていないことを意味する**保留中**のどちらかです。
- **タイムアウト値**:ICMP エコー応答メッセージまたは ICMP エラー メッセージを待機する時間間隔を指定します。
- **リターン コード**:オペレーションの終了後に、オペレーション リターン コードが以下に基づいて設定されます。
  - ICMP エコー応答が受信された - リターン コードが **OK** に設定されます。
  - ICMP エラー応答が受信された - リターン コードが **error** に設定されます。
  - どの ICMP 応答も受信されなかった - リターン コードが **error** に設定されます。
  - 設定された送信元 IP アドレスまたは送信元インターフェイスにアクセスできない - リターン コードが **error** に設定されます。
- **トラッカー**:オペレーションの結果を追跡します。

- **遅延**:IP SLA オペレーションの結果がトラッキング オブジェクトの状態を X から Y に変更する必要があることを示している場合に、トラッキング オブジェクトが以下のアクションを実行します。
  - トラッキング オブジェクトの状態は変化せず、トラッキング オブジェクトにより、時間間隔が設定された遅延タイマーが起動します。
  - タイマーがセットされた時間内にオリジナルの状態(Y)が再度受信されれば、タイマーはキャンセルされて、状態が Y のまま維持されます。
  - 遅延タイマーが切れると、トラッキング オブジェクトの状態が X に変化し、X 状態が関連するアプリケーションに渡されます。

SLA の使用

ICMP エコー オペレーション

IP SLA ICMP エコー オペレーションはこのページで設定することができます。このオペレーションは、入力された頻度に基づいて実行されます。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [SLA] > [ICMP エコー オペレーション] の順にクリックします。

ICMP エコー オペレーションが表示されます(一部のフィールドの説明が [追加] ページにあります)。

- [ステータス]:上記概要で説明したように、保留中とスケジュール済みのどちらかが表示されます。
- [リターン コード]:上記概要で説明したように、OK とエラーのどちらかが表示されます。

ステップ 2 新しいオペレーションを追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [オペレーション番号]:未使用の番号を入力します。
- [オペレーション ステータス]:次のオプションのいずれかを選択します。
  - [保留中]:オペレーションがアクティブになっていません。
  - [スケジュール済み]:オペレーションがアクティブになっています。

ICMP エコー パラメータ

- [オペレーション ターゲット]:オペレーション ターゲットの定義方法を選択します。
  - [IP 指定]:オペレーション ターゲットの IP アドレスを入力します。
  - [ホスト名指定]:オペレーション ターゲットのホスト名を入力します。

  注 IP SLA オペレーションがスタティック ルート機能に対して行われる場合、オペレーション ターゲットはスタティック ルートによって定義されたリモート ネットワーク内のホストの IP アドレスになります。
- [送信元定義]:このフィールドが定義されていない場合は、オペレーションが宛先に最も近い送信元 IP アドレスを選択します。このフィールドを定義するには、次のオプションのいずれかを選択します。
  - [自動]:送信元インターフェイスが転送テーブル情報に基づきます。
  - [アドレス指定]:別の送信元 IP アドレスを指定します。
- [ネクスト ホップ IP アドレス]:[なし] または [ユーザ定義] を選択します。[ユーザ定義] を選択した場合は、ネクスト ホップ IP アドレスを入力します。このパラメータは、IP SLA 処理でスタティック ルートを使用する場合にのみ定義する必要があります。
- [要求データ サイズ]:ICMP エコー オペレーションの要求パケット データ サイズを入力します。このデータ サイズは、64 バイトの IP パケットを構成する ICMP パケットのペイロード部分です。
- [頻度]:SLA オペレーションを実行する(パケットが送信される)頻度を入力します。この値は、[タイムアウト] より大きくする必要があります。
- [タイムアウト]:IP SLA オペレーションが要求パケットに対する応答を待機する時間を入力します。パケットの最大往復時間(RTT)値と IP SLA オペレーションの処理時間の合計に基づくミリ秒引数の値にすることをお勧めします。

ステップ 4 [適用] をクリックし、設定を保存します。

SLA トラック

SLA トラックは、このページで設定できます。SLA トラックは、IP SLA リターン コードを追跡し、それに応じて、アップまたはダウンの状態を設定するために使用されます。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [SLA] > [SLA トラック] の順にクリックします。

SLA トラック オブジェクトが表示されます(一部のフィールドの説明が [追加] ページにあります)。

- [ステータス]:次の状態のいずれかが表示されます。
  - [ダウン]:ルートへの接続が存在しません(パケットがエラー リターン コードを返しました)。
  - [アップ]:ルートへの接続が存在します(パケットが OK リターン コードを返しました)。
- [オペレーション タイプ]:[ICMP エコー] しか表示できません。
- [残りの遅延間隔(秒)]:どのくらいの遅延期間が残っているか。

ステップ 2 新しいオブジェクトを追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [トラック番号]:未使用の番号を入力します。
- [オペレーション番号]:リストから SLA オペレーションを選択します。
- [アップ遅延]:ダウンからアップへの状態変化を遅らせる時間を秒単位で指定します。
  - [なし]:トラックの状態をただちに変更します。
  - [遅延期間]:この遅延期間後にトラックの状態を変更します。
- [ダウン遅延]:アップからダウンへの状態変化を遅らせる時間を秒単位で指定します。
  - [なし]:トラックの状態をただちに変更します。
  - [遅延期間]:この遅延期間後にトラックの状態を変更します。

ステップ 4 [適用] をクリックし、設定を保存します。

ICMP エコー統計情報

SLA 統計情報を表示するには、次のようにします。

ステップ 1 [IP コンフィギュレーション] > [IPv4 の管理およびインターフェイス] > [SLA] > [ICMP エコー統計情報] の順にクリックします。

ステップ 2 次のフィールドを入力します。

- [SLA オペレーション]:事前に定義されたオペレーションのいずれかを選択します。
- [リフレッシュ レート]:統計情報の更新頻度を選択します。オプションは次のとおりです。
  - [リフレッシュなし]:統計情報はリフレッシュされません。
  - [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 秒ごとにリフレッシュされます。
  - [60 秒]:統計情報は 60 秒ごとにリフレッシュされます。

ステップ 3 次のフィールドを表示します。

- [オペレーション成功]:SLA トラック エコーが成功した回数。
- [オペレーション失敗]:SLA トラック エコーが失敗した回数。
- [ICMP エコー要求]:送信された要求パケットの数。
- [ICMP エコー応答]:受信された応答パケットの数。
- [ICMP エコー エラー]:受信されたエラー パケットの数。

これらのカウンタをリフレッシュするには、以下をクリックします。

- [カウンタのクリア]:選択されたオペレーションのカウンタをクリアします。
- [すべてのオペレーション カウンタのクリア]:すべてのオペレーションのカウンタをクリアします。
- [リフレッシュ]:カウンタをリフレッシュします。

20

セキュリティ

ここでは、デバイスのセキュリティとアクセス コントロールについて説明します。このシステムにはさまざまなセキュリティ機能が備わっています。

ここで説明する各種のセキュリティ機能は、以下のとおりです。一部の機能は、複数の種類のセキュリティまたはアクセス コントロールに対して利用されています。そのため、このような機能は以下の一覧に 2 回出現します。

デバイスを管理する権限については、次の各項で説明します。

- TACACS+ の設定
- パスワード強度
- 管理アクセス方式
- 管理アクセス認証
- キー管理
- セキュア機密データ管理
- SSL サーバ
- SSH サーバ
- SSH クライアント

デバイスの CPU を標的にした攻撃を防ぐ方法については、次の各項で説明します。

- TCP/UDP サービス
- ストーム制御
- アクセス制御

エンドユーザによるデバイス経由でのネットワーク アクセスを制御する方法については、次の各項で説明します。

- 管理アクセス方式
- TACACS+ の設定

- RADIUS
- ポート セキュリティ
- 802.1X 認証

その他のネットワーク ユーザからの攻撃を防ぐ方法については、次の各項で説明します。これらの攻撃はデバイスを通過するものであり、デバイスを標的にしたものではありません。

- サービス拒絶防御
- SSL サーバ
- ストーム制御
- ポート セキュリティ
- IP ソース ガード
- ARP インスペクション
- アクセス制御
- ファースト ホップのセキュリティ

TACACS+ の設定

組織のすべてのデバイスのセキュリティを一元管理するために、Terminal Access Controller Access Control System（TACACS+）サーバを設置できます。この方法により、組織内のすべてのデバイスに関する認証と認可を 1 つのサーバで扱うことができます。

デバイスは、次のサービスを提供する TACACS+ サーバを使用する TACACS+ クライアントとして機能できます。

- 認証：ユーザ名およびユーザ定義のパスワードを使用して、デバイスにログオンするユーザを認証する機能を提供します。
- [承認]：ログイン時に実行されます。認証セッションが完了した後、認証済みのユーザ名を使って承認セッションが開始します。次に、TACACS+ サーバはユーザの特権を確認します。
- [アカウンティング]：TACACS+ サーバを使用したログイン セッションのアカウンティングを有効にします。これにより、システム管理者は TACACS+ サーバからアカウンティング レポートを生成できます。

認証/承認サービスを提供することに加えて、TACACS+ プロトコルは、暗号化 TACACS 本文メッセージを使って TACACS メッセージを確実に保護するうえでも役立ちます。

TACACS+ は IPv4 にのみ対応しています。

一部の TACACS+ サーバは単一接続をサポートします。この場合、デバイスはすべての情報を単一の接続で受信します。TACACS+ サーバ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。

TACACS+ サーバを使用したアカウンティング

ユーザは RADIUS または TACACS+ サーバを使用したログイン セッションのアカウンティング機能を有効にすることができます。

TACACS+ サーバ アカウンティングに使用されるユーザ定義可能な TCP ポートは、TACACS+ サーバ認証および承認に使われる TCP ポートと同じです。

ユーザがログインまたはログアウトすると、デバイスは次の情報を TACACS+ サーバに送ります。

「表」1:

引数	説明	開始メッセージに含まれるか	停止メッセージに含まれるか
task_id	一意のアカウンティング セッション ID。	はい	はい
user	ログイン認証で入力されたユーザ名。	はい	はい
rem-addr	ユーザの IP アドレス。	はい	はい
elapsed-time	ユーザがログインしている時間の長さを示します。	いいえ	はい
reason	セッションが終了した理由を報告します。	いいえ	はい

デフォルト

この機能には、次のデフォルト設定が適用されます。

- デフォルトでは、デフォルト TACACS+ サーバが定義されていません。
- TACACS+ サーバを設定するとき、デフォルトではアカウンティング機能が無効になります。

他の機能との連携

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

ワークフロー

TACACS+ サーバを使用するには、次の手順を実行します。

ステップ 1 TACACS+ サーバ上でユーザのアカウントを開きます。

ステップ 2 [TACACS+ クライアント] ページで、そのサーバおよび他のパラメータを設定します。

ステップ 3 [管理アクセス認証] ページで TACACS+ を選択します。これにより、ユーザがデバイスにログオンしたときにローカル データベースではなく TACACS+ サーバで認証が実行されるようになります。

注 複数の TACACS+ サーバがすでに構成されている場合、デバイスは、使用可能な TACACS+ サーバに関する構成済みの優先度に基づき、デバイスで使用する TACACS+ サーバを選択します。

TACACS+ クライアント

[TACACS+] ページでは、TACACS+ サーバの設定を行うことができます。

TACACS+ サーバに対する特権レベル 15 を持つユーザだけが、デバイスを管理できます。ユーザまたはグループの定義で次の文字列を使用すると、TACACS+ サーバに対する特権レベル 15 がユーザまたはユーザ グループに付与されます。

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

TACACS+ サーバ パラメータを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [TACACS+] をクリックします。

ステップ 2 必要に応じて [TACACS+アカウンティング] を有効にします。TACACS+ サーバを使用したアカウンティングセクションの説明を参照してください。

ステップ 3 次のデフォルト パラメータを入力します。

- [キーストリング]: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+ サーバとの通信に使用されるデフォルトのキー ストリングを入力します。このキーを使用するか、([TACACS+ サーバの追加] ページで入力される)特定のサーバ用のキーを使用するよう、デバイスを設定できます。

  このフィールドにキー ストリングを入力しない場合、[TACACS+サーバの追加] ページで入力されるサーバ キーは、TACACS+ サーバで使用される暗号キーに一致する必要があります。

  ここでキー ストリングを入力し、しかも個別の TACACS+ サーバのキー ストリングも入力した場合、個別の TACACS+ サーバに設定されたキー ストリングが優先されます。

- [応答タイムアウト]:デバイスと TACACS+ サーバ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。特定のサーバに関する値が [TACACS+サーバの追加] ページで入力されない場合、このフィールドの値が採用されます。

- [送信元IPv4インターフェイス]:TACACS+ サーバとの通信のために送られるメッセージで使用されるデバイス IPv4 送信元インターフェイスを選択します。

- [送信元IPv6インターフェイス]:TACACS+ サーバ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] オプションが選択されている場合、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。

ステップ 4 [適用] をクリックします。TACACS+ 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。対応するパラメータが [追加] ページで定義されない場合に、これらが使用されます。

各 TACACS サーバに関する情報が TACACS+ サーバ テーブルに表示されます。このテーブル内のフィールドは [追加] ページで入力されます。ただし、[ステータス] フィールドを除きます。このフィールドは、サーバ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、[追加] をクリックします。

ステップ 6 パラメータを入力します。

- [サーバ指定方法]:TACACS+ サーバを識別する方法として、次のいずれか 1 つを選択します。

  - [IPアドレス]:これを選択した場合は、[サーバのIPアドレス/名前] フィールドにサーバの IP アドレスを入力してください。

  - [名前]:これが選択されている場合、[サーバの IP アドレス/名前] フィールドにサーバの名前を入力します。

- [IPバージョン]:送信元アドレスとしてサポートされる IP バージョンを選択します(IPv6 または IPv4)。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 アドレス タイプとしてリンク ローカルが選択されている場合)。
- [サーバのIPアドレス/名前]:TACACS+サーバの IP アドレスまたはドメイン名を入力します。
- [プライオリティ]:この TACACS+ サーバの使用順序を入力します。ゼロは最も高いプライオリティの TACACS+ サーバを示し、これが使用される最初のサーバです。プライオリティの高いサーバとのセッションを確立できない場合、デバイスは次に高いプライオリティのサーバを試します。
- [キーストリング]:デバイスと TACACS+ サーバの間の認証と暗号化に使用されるデフォルトのキー ストリングを入力します。このキーは、TACACS+ サーバで設定されるキーと一致する必要があります。

  キーは、MD5 を使用して送信データを暗号化する際に使用されます。デバイスでデフォルト キーを選択することも、[暗号化] 形式または [プレーンテキスト] 形式でキーを入力することもできます。(別のデバイスからの)暗号化キー ストリングがない場合は、プレーンテキスト モードでキー ストリングを入力して [適用] をクリックします。暗号化キー ストリングが生成されて、表示されます。

  キーを入力した場合、メイン ページでデバイスのデフォルト キー ストリングが定義済みであれば、それがオーバーライドされます。
- [応答タイムアウト]:[ユーザ定義] を選択して、デバイスと TACACS+ サーバ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。ページに表示されるデフォルト値を使用するには、[デフォルトを使用] 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 [適用] 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 このページで機密データをプレーンテキスト形式で表示するには、[機密データを平文で表示] をクリックします。

RADIUS

Remote Authorization Dial-In User Service(RADIUS)サーバは、802.1x または MAC に基づいてネットワーク アクセスを制御します。

デバイスは、RADIUS サーバを使用してセキュリティを一元管理できる RADIUS クライアントか、または RADIUS サーバとして設定できます。

RADIUS クライアント

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、デバイスを使用して Remote Authorization Dial-In User Service(RADIUS)サーバを設置することができます。この方法により、組織内のすべてのデバイスに関する認証と認可を 1 つのサーバで扱うことができます。

デバイスを RADIUS クライアントとして設定すると、次のサービスのために RADIUS サーバを使用できます。

- 認証:ユーザ名およびユーザ定義のパスワードを使用して、デバイスにログオンする通常のユーザおよび 802.1X ユーザを認証する機能を提供します。
- 承認:ログイン時に実行されます。認証セッションが完了した後、認証済みのユーザ名を使って承認セッションが開始します。次に、RADIUS サーバはユーザの特権を確認します。

アカウンティング:RADIUS サーバを使用したログイン セッションのアカウンティングを有効にします。これにより、システム管理者は RADIUS サーバからアカウンティング レポートを生成できます。RADIUS サーバ アカウンティングに使用されるユーザ定義可能な TCP ポートは、RADIUS サーバ認証および承認に使われる TCP ポートと同じです。

デフォルト

この機能には、次のデフォルト設定が適用されます。

- デフォルトでは、デフォルト RADIUS サーバが定義されていません。
- RADIUS サーバを設定するとき、デフォルトではアカウンティング機能が無効になります。

他の機能との連携

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

RADIUS の手順

RADIUS サーバを使用するには、次のようにします。

ステップ 1 RADIUS サーバ上でデバイスのアカウントを開きます。

ステップ 2 [RADIUS] ページと [RADIUSサーバの追加] ページで、そのサーバおよび他のパラメータを設定します。

注 複数の RADIUS サーバがすでに構成されている場合、デバイスは、使用可能な RADIUS サーバに関する構成済みの優先度に基づき、デバイスで使用する RADIUS サーバを選択します。

RADIUS サーバのパラメータ値を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [RADIUSクライアント] 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。次のオプションが選択できます。

- [ポートベースのアクセスコントロール(802.1X、MACベース、Web認証)]: 802.1x ポート アカウンティングに RADIUS サーバが使用されることを指定します。
- [管理アクセス]: ユーザ ユーザ ログイン アカウンティングに RADIUS サーバが使用されることを指定します。
- [ポートベースのアクセスコントロールと管理アクセスの両方]: ユーザ ログイン アカウンティングと 802.1x ポート アカウンティングの両方に RADIUS サーバが使用されることを指定します。
- [なし]: アカウンティングに RADIUS サーバが使用されないことを指定します。

ステップ 3 必要に応じてデフォルト RADIUS パラメータを入力します。[デフォルトパラメータ] で入力した値は、すべての RADIUS サーバに適用されます。([RADIUSサーバの追加] ページで) 特定の RADIUS サーバに関する値が入力されない場合、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失敗する場合は、エラーが発生したと見なされます。
- [応答タイムアウト]:RADIUS サーバからの応答をデバイスが待つ時間 (単位:秒) を入力します。この時間が経過した後、クエリーを再試行するか、または次のサーバに切り替えます。
- [デッドタイム]:応答のない RADIUS サーバへのサービス要求がバイパスされるようになるまでの経過時間 (単位:分) を入力します。「0」を入力した場合、この RADIUS サーバはバイパスされません。
- [キーストリング]:デバイスと RADIUS サーバの間の認証と暗号化に使用されるデフォルトのキー ストリングを入力します。このキーは、RADIUS サーバ側で設定されているキーと一致していなければなりません。キーは、MD5 を使用して送信データを暗号化する際に使用されます。暗号化またはプレーンテキストのいずれかの形式でキーを入力できます。(別のデバイスからの) 暗号化キー ストリングがない場合は、プレーンテキスト モードでキー ストリングを入力して [適用] をクリックします。暗号化キー ストリングが生成されて、表示されます。

デフォルト キー ストリングが定義済みであれば、それがオーバーライドされます。

- [送信元IPv4インターフェイス]:RADIUS サーバとの通信のためのメッセージで使用されるデバイス IPv4 送信元インターフェイスを選択します。
- [送信元IPv6インターフェイス]:RADIUS サーバとの通信のための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] オプションが選択されている場合、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。

ステップ 4 [適用] をクリックします。実行コンフィギュレーション ファイル内で、デバイスの RADIUS デフォルト設定が更新されます。

RADIUS サーバを追加するには、[追加] をクリックします。

ステップ 5 RADIUS サーバごとに、フィールドに値を入力します。[RADIUS] ページで入力したデフォルト値を使用するには、[デフォルトを使用] を選択します。

- [サーバ指定方法]:RADIUS サーバを 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]:RADIUS サーバの IP アドレスのバージョンを選択します。

- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 アドレス タイプとしてリンク ローカルが選択されている場合)。
- [サーバのIPアドレス/名前]:RADIUS サーバを IP アドレスまたは名前で入力します。
- [プライオリティ]:サーバのプライオリティを入力します。プライオリティにより、デバイスがユーザ認証のためにサーバと通信を試みる際の順序が決まります。デバイスは、プライオリティが最も高い RADIUS サーバを最初に試します。プライオリティは 0 が最高です。
- [キーストリング]:デバイスと RADIUS サーバとの間の通信を認証および暗号化するために使われるキー ストリングを入力します。このキーは、RADIUS サーバ側で設定されているキーと一致していなければなりません。**暗号化**または**プレーンテキスト**のいずれかの形式で入力できます。[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キー ストリングを使用して RADIUS サーバへの認証を試みます。
- [応答タイムアウト]:[ユーザ定義] を選択して、RADIUS サーバからの応答をデバイスが待つ時間(単位:秒)を入力します。この時間が経過した後、デバイスはクエリーを再試行するか、または(最大再試行回数に達していれば)次のサーバに切り替えます。[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。
- [認証ポート]: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]: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。

- [リトライ回数]:[ユーザ定義] を選択して、RADIUS サーバに要求を送る最大試行回数を入力します。この回数送信しても失敗する場合は、エラーが発生したと見なされます。[デフォルトを使用] を選択した場合、デバイスはリトライ回数のデフォルト値を使用します。
- [デッド タイム]:[ユーザ定義] を選択して、応答のない RADIUS サーバへのサービス要求がバイパスされるようになるまでの経過時間(単位:分)を入力します。[デフォルトを使用] を選択した場合、デバイスはデッド タイムのデフォルト値を使用します。「0」と入力した場合、デッド タイムは設定されません。
- [使用タイプ]:RADIUS サーバ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]:RADIUS サーバは、デバイスの管理を希望するユーザを認証する目的で使用されます。
  - [802.1X]:RADIUS サーバは 802.1x 認証用に使用されます。
  - [すべて]:RADIUS サーバは、デバイスの管理を希望するユーザの認証、および 802.1X 認証に使用されます。

ステップ 6 [適用] をクリックします。RADIUS サーバ定義が、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 7 ページ上で機密データをプレーンテキスト形式で表示するには、[機密データを平文で表示] をクリックします。

RADIUS サーバ

デバイスを DHCP サーバとして設定できます。そのためには、以下に説明する GUI ページを使用します。

RADIUS サーバ グローバル設定

RADIUS サーバ グローバル パラメータを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [RADIUSサーバ] > [RADIUSサーバグローバル設定] をクリックします。

ステップ 2 次のパラメータを指定します。

- [RADIUSサーバステータス]:RADIUS サーバ機能の状態を有効にする場合はチェックボックスをオンにします。

- [認証ポート]: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]: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。

トラップ設定

- [RADIUSアカウンティングトラップ]: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チェックボックスをオンにします。
- [RADIUS認証失敗トラップ]:失敗したログインのトラップを生成する場合はチェックボックスをオンにします。
- [RADIUS認証成功トラップ]:成功したログインのトラップを生成する場合はチェックボックスをオンにします。

ステップ 3 [適用] をクリックします。実行コンフィギュレーション ファイル内で、デバイスの RADIUS デフォルト設定が更新されます。

RADIUS サーバ キー

RADIUS サーバ キーを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [RADIUSサーバ] > [RADIUSサーバキー] をクリックします。

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。[デフォルトキー] に入力した値はデフォルト キーを使用するように設定された([RADIUSサーバの追加] ページ内)すべてのサーバに適用されます。

- [デフォルトキー] :デバイスと RADIUS クライアントの間の認証と暗号化に使用されるデフォルトのキー ストリングを入力します。次のいずれかのオプションを選択します。
  - [既存のデフォルトキーを維持]: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 ストリングを使用して、RADIUS クライアントの認証を試行します。
  - [暗号化]:MD5 を使用して通信を暗号化するために、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]:プレーンテキスト モードでキー ストリングを入力します。
- [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 [適用] をクリックします。実行コンフィギュレーション ファイル内で、デバイスのRADIUS デフォルト設定が更新されます。

ステップ 4 秘密キーを追加するには、[追加] をクリックして、以下のフィールドに入力します。

- [NASアドレス]:RADIUS クライアントを含むスイッチのアドレス。
- [秘密キー]:RADIUS クライアントを含むスイッチのアドレス。
  - [デフォルトキーを使用]: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 ストリングを使用して、RADIUS クライアントの認証を試行します。
  - [暗号化]:MD5 を使用して通信を暗号化するために、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]:プレーンテキスト モードでキー ストリングを入力します。

ステップ 5 [適用] をクリックします。実行コンフィギュレーション ファイル内で、デバイスのキーが更新されます。

RADIUS サーバ グループ

デバイスを RADIUS サーバとして使用するユーザのグループをセットアップするには、次のようにします。

ステップ 1 [セキュリティ] > [RADIUSサーバ] > [RADIUSサーバグループ] をクリックします。

ステップ 2 [追加] をクリックして、以下のフィールドに入力します。

- [グループ名]:グループの名前を入力します。
- [特権レベル]:グループの管理アクセス特権レベルを入力します。
- [時間範囲]:このグループに時間範囲を適用する場合はチェックボックスをオンにします。
- [時間範囲名]:[時間範囲] 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」の項の時間範囲を定義するには、[編集] をクリックします。このフィールドは、[時間範囲] が事前に定義されている場合にのみ表示されます。
- [VLAN]:ユーザの VLAN を選択します。
  - [なし]:VLAN ID は送信されません。
  - [VLAN ID]:送信される VLAN ID。
  - [VLAN名]:送信される VLAN 名。

ステップ 3 [適用] をクリックします。RADIUS グループ定義が、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 ユーザ

ユーザを追加するには、次のようにします。

ステップ 1 [セキュリティ] > [RADIUSサーバ] > [RADIUSサーバ ユーザ] をクリックします。

現在のユーザが表示されます。

ステップ 2 [追加] をクリックします。

- [ユーザ名]:ユーザの名前を入力します。
- [グループ名]:以前に定義されたグループを選択します。
- [パスワード]:次のいずれかのオプションを入力します。
  - [暗号化]:キー ストリングは 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、キーを暗号化された形式で入力します。
  - [プレーンテキスト]:(別のデバイスからの)暗号化キー ストリングがない場合は、プレーンテキスト モードでキー ストリングを入力します。暗号化キー ストリングが生成されて、表示されます。

ステップ 3 [適用] 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、フラッシュ上の循環ファイルに最後のアカウンティング ログを保存します。これらを表示できます。

RADIUS サーバ アカウンティングを表示するには、次のようにします。

ステップ 1 [セキュリティ] > [RADIUSサーバ] > [RADIUSサーバ アカウンティング] 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。

- [ユーザ名]:ユーザの名前。

- [イベント タイプ]:次のいずれかの値。
  - [開始]:セッションが開始されました。
  - [停止]:セッションが停止されました。
  - [日付/時刻変更]:デバイスの日付/時刻が変更されました。
  - [リセット]:デバイスが指定時刻にリセットされました。
- [認証方式]:ユーザにより使用される認証方式。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] が表示されます。
- [NASアドレス]:RADIUS クライアントを含む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] が表示されます。
- [ユーザアドレス]: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 IP アドレスです。ユーザがステーションの場合、これはその 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] が表示されます。
- [イベント時間]:イベントの時間。

ステップ 2 ユーザ/イベントの追加詳細を確認するには、[詳細] をクリックします。

次のフィールドが表示されます。

注 このページ内のフィールドは、表示されるアカウントのタイプとそのために受信される詳細に依存します。すべてのフィールドが常に表示されるとは限りません。

- [イベント時間]:上記参照。
- [イベントタイプ]:上記参照。
- [ユーザ名]:上記参照。
- [認証方式]:上記参照。
- [NAS IPv4アドレス]:上記の [NASアドレス] 参照。
- [NASポート]:NAS アドレスのスイッチで使用されるポート。
- [ユーザアドレス]:上記参照。
- [アカウンティングセッション時間]:上記の [イベント時間] 参照。
- [セッション終了理由]:セッション終了の理由(ユーザ要求など)が表示されます。

RADIUS サーバ 拒否 ユーザ

RADIUS サーバを使用して認証を試行し、拒否されたユーザを表示するには、次のようにします。

ステップ 1 [セキュリティ] > [RADIUSサーバ] > [RADIUS拒否ユーザ] 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。

- [イベント タイプ]: 次のいずれかのオプションが表示されます。
  - [拒否]: ユーザは拒否されました。
  - [時間変更]: デバイス上のクロックは管理者によって変更されました。
  - [リセット]: 管理者によってデバイスがリセットされました。
- [ユーザ名]: 拒否されたユーザの名前。
- [ユーザタイプ]: 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。
  - [ログイン]: 管理アクセス ユーザ。
  - [802.1x]: 802.1x ネットワーク アクセス ユーザ。
  - [N/A]: リセット イベント用。
- [理由]: ユーザが拒否された理由。
- [時間]: ユーザが拒否された時間。

ステップ 2 拒否されたユーザの追加詳細を確認するには、ユーザを選択して、[詳細] をクリックします。

次のフィールドが表示されます。

注 このページ内のフィールドは、表示されるアカウントのタイプとそのために受信される詳細に依存します。すべてのフィールドが常に表示されるとは限りません。

- [イベント時間]: 上記参照。
- [ユーザ名]: 上記参照。
- [ユーザ タイプ]: 上記参照。
- [拒否理由]: ユーザが拒否された理由。
- [NAS IP アドレス]: 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、[クリア] をクリックします。

RADIUS サーバ不明 NAS エントリ

NAS が RADIUS サーバ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、次のようにします。

ステップ 1 [セキュリティ] > [RADIUS サーバ] > [RADIUS サーバ不明 NAS エントリ] をクリックします。

次のフィールドが表示されます。

- **(ログ)イベント タイプ**
  - [不明な NAS]:発生した不明な NAS イベント。
  - [時間変更]:デバイス上のクロックは管理者によって変更されました。
  - [リセット]:管理者によってデバイスがリセットされました。
- [IP アドレス]:不明な NAS の IP アドレス。
- [時間]:イベントのタイムスタンプ。

RADIUS サーバ統計情報

RADIUS サーバ統計情報を表示するには、次のようにします。

ステップ 1 [セキュリティ] > [RADIUSサーバ] > [RADIUSサーバ統計情報] をクリックします。

次のフィールドが表示されます。

- **統計情報源**
  - [グローバル]:すべてのユーザの統計情報
  - [特定のNAS]:特定の NAS の NAS の統計情報。
- [リフレッシュレート]:統計情報がリフレッシュされるまでの時間を示すリフレッシュ レートを選択します。
- [認証ポート上の着信パケット]:認証ポートで受信したパケットの数。
- [不明アドレスからの着信アクセス要求]:不明な NAS アドレスからの着信アクセス要求の数。
- [重複着信アクセス要求]:受信した再送信パケットの数。
- [送信済みアクセス承認]:送信したアクセス承認の数。

- [送信済みアクセス拒否]:送信したアクセス拒否の数。
- [送信済みアクセスチャレンジ]:送信したアクセス チャレンジの数。
- [着信不正アクセス要求]:受信した不正アクセス要求の数。
- [不良オーセンティケータを含む着信認証要求]:不良なパスワードを含む着信パケットの数。
- [その他の間違いを含む着信認証パケット]:その他の間違いを含む受信済み着信認証パケットの数。
- [不明タイプの着信認証パケット]:不明なタイプの受信済み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]:アカウンティングポート上の着信パケットの数。
- [不明アドレスからの着信認証要求]:不明なアドレスからの着信認証要求の数。
- [着信重複アカウンティング要求]: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]:送信したアカウンティング応答の数。
- [着信不正アカウンティング要求]:不正アカウンティング要求の数。
- [不良オーセンティケータを含む着信アカウンティング要求]:不良なオーセンティケータを含む着信アカウンティング要求の数。
- [その他の間違いを含む着信アカウンティングパケット]:その他の間違いを含む着信アカウンティングパケットの数。
- [着信非記録アカウンティング要求]:記録されない着信アカウンティング要求の数。
- [不明タイプの着信アカウンティングパケット]:不明なタイプの着信アカウンティングパケットの数。

カウンタをクリアするには、[カウンタのクリア] をクリックします。

カウンタを更新するには、[更新] をクリックします。

パスワード強度

デフォルトのユーザ名とパスワードは **cisco** および **cisco** です。デフォルトのユーザ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。パスワード複雑度は、デフォルトで有効になっています。([パスワード強度] ページの [パスワードの複雑度の設定] が有効になっていて)パスワードの複雑さが不十分な場合は、別のパスワードを作成するように求められます。

ユーザ アカウントの作成方法については、「ユーザ アカウント」を参照してください。

デバイスにアクセスするユーザの認証にパスワードが使用されるため、単純なパスワードはセキュリティを危険にさらす可能性があります。そのため、パスワード複雑度要件がデフォルトで適用されており、必要に応じて設定を変更できます。

パスワード複雑度ルールを定義するには、次のようにします。

ステップ 1 [セキュリティ] > [パスワード強度] をクリックします。

ステップ 2 パスワードに関する次のエージング パラメータを入力します。

- [パスワードエージング]: これを選択した場合、[パスワードエージング時間] で指定した日数が経過するとユーザはパスワードを変更するよう要求されます。
- [パスワードエージング時間]: パスワードの有効日数を入力します。この日数が経過すると、パスワードを変更するよう要求されます。

  注 パスワード エージングは、長さゼロのパスワード(つまりパスワードなし)にも適用されます。

ステップ 3 パスワードの複雑度ルールを有効にするには、[パスワードの複雑度の設定] を選択します。

パスワード複雑度が有効な場合、新しいパスワードは次のデフォルト設定に従う必要があります。

- 長さは 8 文字以上にする。
- 3 つ以上の文字クラスの文字を含む(大文字、小文字、数字、標準キーボードで使用可能な特殊文字)。
- 現在のパスワードとは異なるパスワードにする。
- 同じ文字を 3 回以上続けて使用しない。
- ユーザ名や、その大文字小文字を入れ替えただけの派生形を繰り返したり逆にしたりして使用しない。
- 製造業者名や、その大文字小文字を入れ替えただけの派生形を繰り返したり逆にしたりして使用しない。

ステップ　4　[パスワードの複雑度の設定] が有効な場合は、次のパラメータを設定できます。

- [最小パスワード長]:パスワードの最小文字数を入力します。

  注　長さをゼロのパスワード（つまりパスワードなし）を使用できます。また、この場合でもパスワード エージングを割り当てることができます。

- [許容される文字の繰り返し]:1 つの文字を繰り返すことのできる回数を入力します。
- [文字クラスの最小数]:パスワードに含まれる必要のある文字クラスの数を入力します。文字クラスは、小文字（1）、大文字（2）、数字（3）、および記号または特殊文字（4）です。
- [新規パスワードは現在のパスワードとは異なっている必要があります]:これを選択した場合、パスワードの変更時に、新しいパスワードを現在のパスワードと同じ値にすることはできません。

ステップ　5　[適用] をクリックします。パスワード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　ユーザ名/パスワード同等値の設定、および製造業者/パスワード同等値の設定は CLI で可能です。詳細については、*『CLI Reference Guide』*を参照してください。

キー管理

注　この項は 550 ファミリのみに関連します。

ここでは、アプリケーションやプロトコル（RIP など）のためのキー チェーンを設定する方法について説明します。RIP が認証用にキー チェーンをどのように使用するかについては、「IP 設定:RIPv2」を参照してください。

具体的な内容は、次のとおりです。

- キー チェーン
- キー設定

キー チェーン

注 この機能は、Sx550X/SG550XG デバイスの場合のみサポートされます。

新しいキー チェーンを作成するには、次のようにします。

ステップ 1 [セキュリティ] > [キー管理] > [キーチェーン設定] の順にクリックします。

ステップ 2 新しいキー チェーンを追加するには、[追加] をクリックして [キーチェーンの追加] ページを開き、次のフィールドに入力します。

- [キーチェーン]:キー チェーンの名前。
- [キー識別子]:キー チェーンを識別する整数の ID。
- [キーストリング]: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。
  - [ユーザ定義(暗号化)]:暗号化バージョンを入力します。
  - [ユーザ定義(プレーンテキスト)]:プレーンテキスト バージョンを入力します。

  注 [受け入れライフタイム] および [送信ライフタイム] の両方の値を入力できます。受け入れライフタイムは、パケット受信用のキー識別子がいつ有効であるかを示します。送信ライフタイムは、パケット送信用のキー識別子がいつ有効であるかを示します。
- [受け入れライフタイム/送信ライフタイム]: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。次のいずれかのオプションを選択します。
  - [常に有効]:キー識別子の存続期間に制限はありません。
  - [ユーザ定義]: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、次のフィールドに値を入力します。

  注 [ユーザ定義] を選択した場合、手動で、または SNTP からシステム時間を設定する必要があります。こうしないと、受け入れライフタイムおよび送信ライフタイムに常に問題が発生します。

次のフィールドが、[受け入れライフタイム] フィールドと [送信ライフタイム] フィールドに関係します。

- [開始日]:キー識別子が有効になる最も早い日付を入力します。
- [開始時刻]:[開始日] 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。

- [終了時間]:キー識別子が有効である最後の日付を指定します。次のいずれかのオプションを選択します。
  - [無制限]:キー識別子の存続期間に制限はありません。
  - [期間]:キー識別子の存続期間には制限があります。このオプションを選択した場合は、次のフィールドに値を入力します。
- [期間]:キー識別子が有効である時間の長さ。次のフィールドを入力します。
  - [日間]:キー識別子が有効である日数。
  - [時間]:キー識別子が有効である時間数。
  - [分]:キー識別子が有効である分数。
  - [秒]:キー識別子が有効である秒数。

ステップ 3 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

キー設定

キーを既存のキー チェーンに追加するには、次のようにします。

ステップ 1 [セキュリティ] > [キー管理] > [キー設定] の順にクリックします。

ステップ 2 新しいキー ストリングを追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [キーチェーン]:キー チェーンの名前。
- [キー識別子]:キー チェーンを識別する整数の ID。
- [キーストリング]: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。
  - [ユーザ定義(暗号化)]:暗号化バージョンを入力します。
  - [ユーザ定義(プレーンテキスト)]:プレーンテキスト バージョンを入力します。

注 [受け入れライフタイム] および [送信ライフタイム] の両方の値を入力できます。[受け入れライフタイム] は、パケット受信用のキー識別子がいつ有効であるかを示します。[送信ライフタイム] は、パケット送信用のキー チェーンがいつ有効であるかを示します。[受け入れライフタイム] のフィールドについてのみ説明します。[送信ライフタイム] にも同じフィールドがあります。

- [受け入れライフタイム]: 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。次のいずれかのオプションを選択します。
  - [常に有効]: キー識別子の存続期間に制限はありません。
  - [ユーザ定義]: 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、次のフィールドに値を入力します。
- [開始日]: キー識別子が有効になる最も早い日付を入力します。
- [終了日]: キー識別子が有効である最後の日付を指定します。
- [開始時刻]: [開始日] 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。
- [終了時刻]: キー識別子が有効である最後の時刻を指定します。次のいずれかのオプションを選択します。
  - [無制限]: キー識別子の存続期間に制限はありません。
  - [期間]: キー識別子の存続期間には制限があります。このオプションを選択した場合は、次のフィールドに値を入力します。
- [期間]: キー識別子が有効である時間の長さ。次のフィールドを入力します。
  - [日間]: キー識別子が有効である日数。
  - [時間]: キー識別子が有効である時間数。
  - [分]: キー識別子が有効である分数。
  - [秒]: キー識別子が有効である秒数。

ステップ 4 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

ステップ 5 ページ上で機密データを常に(暗号化形式ではなく)プレーンテキストで表示するには、[機密データを平文で表示] をクリックします。

管理アクセス方式

ここでは、さまざまな管理方式に関するアクセス ルールについて説明します。

具体的な内容は、次のとおりです。

- アクセス プロファイル
- プロファイル ルール

アクセス プロファイルによって、さまざまなアクセス方法でデバイスにアクセスするユーザを認証および承認する方法が決まります。アクセスプロファイルを使用して、特定のソースからの管理アクセスを制限することができます。

アクティブ アクセス プロファイルと管理アクセス認証方式の両方に合格したユーザだけが、デバイスに管理アクセスできます。

デバイス上では、一度に 1 つのアクセス プロファイルだけをアクティブにすることができます。

アクセス プロファイルは、1 つ以上のルールから構成されています。各ルールは、アクセス プロファイル内のプライオリティ順に（上から順に）実行されます。

各ルールはフィルタで構成されており、各フィルタは次の要素で構成されています。

- [アクセス方式]: デバイスにアクセスして管理するための方式。
  - Telnet
  - Secure Telnet（SSH）
  - Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）
  - Secure HTTP（HTTPS）
  - Simple Network Management Protocol（SNMP; シンプル ネットワーク管理プロトコル）
  - 上記すべて
- [アクション]: 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。
- [インターフェイス]: 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（OOB ポートを含む）、LAG、または VLAN。

- [送信元 IP アドレス]:IP アドレスまたはサブネット。ユーザ グループによって、管理方式へのアクセスが異なる可能性があります。たとえば、あるユーザ グループは HTTPS セッションのみを使ってデバイス モジュールにアクセスでき、別のユーザ グループは HTTPS および Telnet の両方のセッションを使ってデバイス 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

[アクセスプロファイル] 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、アクティブにする 1 つのアクセス プロファイルを選択できます。

ユーザがあるアクセス方式でデバイスにアクセスしようとすると、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 アクセス プロファイルで明示的に許可されているかどうかを確認します。合致するルールが見つからない場合、アクセスは拒否されます。

アクティブ アクセス プロファイルに違反するデバイス アクセスが試行された場合、デバイスで SYSLOG メッセージが生成され、システム管理者にそのアクセス試行が通知されます。

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」を参照してください。

[アクセスプロファイル] ページを使用してアクセス プロファイルを作成し、その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、[プロファイルルール]ページを使用します。

ステップ 1 [セキュリティ] > [管理アクセス方式] > [アクセスプロファイル]をクリックします。

このページには、アクティブ アクセス プロファイルと非アクティブ アクセス プロファイルを含むすべてのアクセス プロファイルが表示されます。

ステップ 2 アクティブなアクセス プロファイルを切り替えるには、[アクティブアクセスプロファイル] ドロップダウン メニューからプロファイルを選択し、[適用] をクリックします。選択したプロファイルがアクティブ アクセス プロファイルになります。

注 [コンソールのみ] を選択した場合、注意を促すメッセージが表示されます。そのまま続行すると、Web ベースの設定ユーティリティからただちに切断されて、デバイスはコンソール ポートからでなければアクセスできなくなります。これは、コンソール ポートを備えたデバイス タイプにのみ該当します。

他のいずれかのアクセス プロファイルを選択した場合、「選択したアクセスプロファイルによっては Web ベースのデバイス設定ユーティリティから切断される可能性がある」という内容の注意メッセージが表示されます。

ステップ 3 アクティブ アクセス プロファイルを選択するには [OK] をクリックします。操作を中止するには、[キャンセル] をクリックします。

ステップ 4 [追加] をクリックして、[アクセスプロファイルの追加] ページを開きます。このページでは、新しいアクセス プロファイルとルール 1 つを設定できます。

ステップ 5 [アクセスプロファイル名] を入力します。この名前には最大で 32 文字を含めることができます。

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。パケットがルールの条件に一致した場合、ユーザ グループはデバイスへの管理アクセスを許可または拒否されます。プライオリティの高いルールから順に適用されるため、ルールのプライオリティは非常に重要です。最高のプライオリティは「1」です。
- [管理方式]:ルールを定義する対象となる管理方式を選択します。次のオプションがあります。
  - [すべて]:すべての管理方式をこのルールに割り当てます。
  - [Telnet]:デバイスへのアクセスを要求しているユーザが Telnet アクセス プロファイル基準を満たす場合、そのユーザはアクセスを許可または拒否されます。
  - [Secure Telnet(SSH)]:デバイスへのアクセスを要求しているユーザが SSH アクセス プロファイル基準を満たす場合、そのユーザはアクセスを許可または拒否されます。
  - [HTTP]: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。
  - [Secure HTTP(HTTPS)]:デバイスへのアクセスを要求しているユーザが HTTPS 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。
  - [SNMP]:デバイスへのアクセスを要求しているユーザが SNMP 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。

- [アクション]: このルールに関連付けられる処理を選択します。次のオプションがあります。
  - [許可]: ユーザがこのプロファイルの設定に一致した場合、デバイスへのアクセスを許可します。
  - [拒否]: ユーザがこのプロファイルの設定に一致した場合、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]: このルールに関連付けられ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。
  - [すべて]: すべてのポート、VLAN、および LAG に適用されます。
  - [ユーザ定義]: 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 プロファイルの適用対象となる送信元 IP アドレスのタイプを選択します。[送信元IPアドレス] フィールドにはサブネットワークを入力できます。次のいずれかを選択します。
  - [すべて]: すべてのタイプの IP アドレスに適用されます。
  - [ユーザ定義]: フィールドで定義されたタイプの IP アドレスだけに適用されます。
- [IPバージョン]: 送信元 IP アドレスのバージョンを入力します(バージョン 6 またはバージョン 4)。
- [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。
  - [ネットワーク マスク]: 送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをピリオド区切りの 10 進表記で入力します。
  - [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 7 [適用] 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 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 プロファイルには最大 128 個のルールを含めることができます。これにより、デバイスにアクセスして管理することを許可されるユーザ、および使用できるアクセス方式を定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、1 つのアクションおよび照合する基準（1 つ以上のパラメータ）が含まれます。各ルールにはプライオリティが設定されています。プライオリティが最も高いルールが最初に適用されます。入力パケットがルールの条件に合致した場合、そのルールの処理が実行されます。アクティブ アクセス プロファイル内のどのルールの条件にも合致しなかったパケットは、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た IP アドレス以外のすべての IP アドレスからデバイスにアクセスできないように制限できます。このようにして、さらにデバイスを管理できるので、セキュリティの層を追加できます。

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、次のようにします。

ステップ 1 [セキュリティ] > [管理アクセス方式] > [プロファイルルール] をクリックします。

ステップ 2 [フィルタ] フィールドを選択し、次にアクセス プロファイルを選択します。[実行] 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 [追加] 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。パケットがルールの条件に一致した場合、ユーザ グループはデバイスへの管理アクセスを許可または拒否されます。プライオリティの高いルールから順に適用されるため、ルールのプライオリティは非常に重要です。
- [管理方式]: ルールを定義する対象となる管理方式を選択します。次のオプションがあります。
  - [すべて]: すべての管理方式をこのルールに割り当てます。
  - [Telnet]: デバイスへのアクセスを要求しているユーザが Telnet アクセス プロファイル基準を満たす場合、そのユーザはアクセスを許可または拒否されます。
  - [Secure Telnet（SSH）]: デバイスへのアクセスを要求しているユーザがTelnet アクセス プロファイル基準を満たす場合、そのユーザはアクセスを許可または拒否されます。

- [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。
- [Secure HTTP(HTTPS)]:デバイスへのアクセスを要求しているユーザが HTTPS 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。
- [SNMP]:デバイスへのアクセスを要求しているユーザが SNMP 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。

- [アクション]:次のいずれかのオプションを選択します。
  - [許可]:このルールで定義されたインターフェイスおよび IP ソースからのユーザに対してデバイス アクセスを許可します。
  - [拒否]:このルールで定義されたインターフェイスおよび IP ソースからのユーザに対してデバイス アクセスを拒否します。
- [インターフェイスに適用]:このルールに関連付けられ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。
  - [すべて]:すべてのポート、VLAN、および LAG に適用されます。
  - [ユーザ定義]:選択したポート、VLAN、または LAG のみに適用されます。
- [インターフェイス]:インターフェイス番号を入力します。OOB ポートも入力できます。
- [送信元IPアドレスに適用]:このアクセス プロファイルの適用対象となる送信元 IP アドレスのタイプを選択します。[送信元IPアドレス] フィールドにはサブネットワークを入力できます。次のいずれかを選択します。
  - [すべて]:すべてのタイプの IP アドレスに適用されます。
  - [ユーザ定義]:フィールドで定義されたタイプの IP アドレスだけに適用されます。
- [IPバージョン]:送信元アドレスとしてサポートされる IP バージョンを選択します(IPv6 または IPv4)。
- [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。
  - [ネットワーク マスク]:送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをピリオド区切りの 10 進表記で入力します。

- [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 5 [適用] をクリックすると、このルールがアクセス プロファイルに追加されます。

管理アクセス認証

SSH、コンソール、Telnet、HTTP、HTTPS など、さまざまな管理アクセス方式に承認方式と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、あるいは TACACS+ または RADIUS サーバで実行可能です。

承認処理が有効になっている場合、ユーザの ID と読み取り/書き込み特権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、ユーザの ID だけが検証されます。

使用される承認/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]、[ローカル] の順に認証方式を選択した場合、設定されたすべての RADIUS サーバに対してプライオリティ順にクエリーが送られて応答がなければ、ユーザはローカルに承認/認証されます。

承認処理が有効になっている場合、認証方式が失敗するか、またはユーザの特権レベルが十分でないと、デバイスへのアクセスを拒否されます。言い換えると、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。

アクセス方式に割り当てる認証方式を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [管理アクセス認証] をクリックします。

ステップ 2 管理アクセス方式の [アプリケーション](タイプ)を入力します。

ステップ 3 [承認] を選択すると、下記で説明する方式のリストに従ってユーザの認証および承認の両方が有効になります。このフィールドを選択しない場合は、認証だけが実行されます。[承認] が有効になっている場合、ユーザの読み取り/書き込み特権が検査されます。この特権レベルは [ユーザ アカウント] ページで設定されます。

ステップ 4 矢印を使用して、[オプションの方式] 列と [選択した方式] 列の間で認証方式を移動します。最初に選択した認証方式が最初に使用されます。

- [RADIUS]:ユーザは RADIUS サーバで承認/認証されます。RADIUS サーバが 1 つ以上定義されている必要があります。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「cisco-avpair = shell:priv-lvl=15」を返す必要があります。
- [TACACS+]:ユーザは TACACS+ サーバで承認/認証されます。TACACS+ サーバが 1 つ以上設定されている必要があります。
- [なし]:ユーザは承認/認証なしでデバイスへのアクセスを許可されます。
- [ローカル]:ユーザ名とパスワードは、ローカル デバイスに格納されているデータと照合されます。これらのユーザ名とパスワードは、[ユーザアカウント] ページで定義されます。

  注 [ローカル] または [なし] は、必ず最後の認証方式として選択する必要があります。[ローカル] または [なし] の後に選択した認証方式はすべて無視されます。

ステップ 5 [適用] をクリックします。選択した認証方式が、そのアクセス方式に割り当てられます。

セキュア機密データ管理

「セキュリティ:セキュア機密データ管理」を参照してください。

SSL サーバ

ここではセキュア ソケット レイヤ(SSL)機能について説明します。

具体的な内容は、次のとおりです。

- SSL の概要
- SSL サーバ認証設定

SSL の概要

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されます。

デバイス上に存在するデフォルト証明書を使って HTTPS セッションを開くことができます。

デフォルト証明書を使用するとき、ブラウザによっては、証明書が証明機関(CA)によって署名されていないという理由で警告が発生することがあります。信頼されている CA によって署名された証明書を使用するのがベスト プラクティスです。

ユーザ作成の証明書を使って HTTPS セッションを開くには、次のようにします。

1. 証明書を生成します。
2. 証明書を認定するよう CA に要請します。
3. 署名された証明書をデバイスにインポートします。

デフォルトでは、変更可能な証明書がデバイスに含まれています。

HTTPS はデフォルトで有効になっています。

SSL サーバ認証設定

デバイスにあるデフォルトの証明書を置換するために、新しい証明書を生成する必要が生じることがあります。

新しい証明書を作成するには、次のようにします。

ステップ 1 [セキュリティ] > [SSLサーバ] > [SSLサーバ認証設定] をクリックします。

SSL サーバ キー テーブル内に **SSL アクティブ証明書番号** 1 および 2 に関する情報が表示されます。次のフィールドのいずれかを選択します。

これらのフィールドは [編集] ページで定義されます。ただし次のフィールドを除きます。

- [有効期限の開始]:証明書が有効になる最初の日付を指定します。
- [有効期限の終了]:証明書が有効である最後の日付を指定します。
- [証明書ソース]:証明書がシステムによって生成されたか(自動生成)、それともユーザによって生成されたか(ユーザ定義)を指定します。

ステップ 2 アクティブな証明書を選択します。

ステップ 3 [証明書要求の生成] 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。

- [証明書ID]:アクティブな証明書を選択します。
- [共通名]:完全修飾デバイス URL または IP アドレスを指定します。これを指定しない場合、デフォルトとして(証明書の生成時に)最も低いデバイス IP アドレスになります。
- [組織単位]:組織単位または部署の名前を指定します。
- [組織名]:組織の名前を指定します。
- [ロケーション]:場所または市町村名を指定します。
- [都道府県]:州または都道府県の名前を指定します。
- [国]:国名を指定します。
- [期間]:証明書を有効にする日数を入力します。
- [証明書要求]:[証明書要求の生成] ボタンを押したときに作成されるキーを表示します。

ステップ 5 [証明書要求の生成] をクリックします。これにより、証明機関(CA)で入力する必要のあるキーが作成されます。[証明書要求] フィールドからこれをコピーします。

証明書をインポートするには、次のようにします。

ステップ 1 [セキュリティ] > [SSLサーバ] > [SSLサーバ認証設定] をクリックします。

ステップ 2 [証明書のインポート] をクリックします。

ステップ 3 次のフィールドを入力します。

- [証明書ID]:アクティブな証明書を選択します。
- [証明書ソース]:ユーザ定義の証明書であることを表示します。
- [証明書]:受信される証明書にコピーします。
- [RSAキーペアのインポート]:新しい RSA キーペアへのコピーを有効にするには、このフォールドを選択します。
- [公開キー]:RSA 公開キーにコピーします。
- [秘密キー(暗号化)]:暗号化形式で RSA 秘密キーにコピーするには、このフィールドを選択します。

- [秘密キー(プレーンテキスト)]:プレーンテキスト形式で RSA 秘密キーにコピーするには、このフィールドを選択します。

ステップ 4 [適用] をクリックして、実行コンフィギュレーションに変更を適用します。

ステップ 5 このキーを暗号化して表示するには、[機密データを暗号化して表示] をクリックします。このボタンをクリックした場合、暗号化形式で秘密キーが([適用] をクリックしたときに)コンフィギュレーション ファイルに書き込まれます。テキストが暗号化形式で表示されているときには、ボタンが [機密データを平文で表示] 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。

[詳細] ボタンをクリックすると、証明書と RSA キーペアが表示されます。これを使用して、証明書および RSA キーペアを他のデバイスにコピーします(コピー/貼り付けを使用)。[機密データを暗号化して表示] をクリックすると、秘密キーが暗号化形式で表示されます。

証明書を編集するには、次のようにします。

ステップ 1 [セキュリティ] > [SSLサーバ] > [SSLサーバ認証設定] をクリックします。

ステップ 2 証明書を選択して [編集] をクリックします。

ステップ 3 必要に応じて次のフィールドに入力します。

- [RSA キーの再生成]:RSA キーを再生成する場合に選択します。
- [キーの長さ]:[デフォルトを使用]を選択するか、[ユーザ定義]を選択して長さを入力します。
- [共通名]:を入力します。
- [組織単位]:証明書の組織単位の名前を入力します。
- [場所]:証明書の組織単位の場所を入力します。
- [都道府県/州]:証明書の組織単位の都道府県/州を入力します。
- [国]:証明書の組織単位の国を入力します。
- [期間]:証明書を有効にする時間の長さを入力します。

SSH サーバ

「セキュリティ:SSH サーバ」を参照してください。

SSH クライアント

「セキュリティ:SSH クライアント」を参照してください。

TCP/UDP サービス

[TCP/UDPサービス] ページで、主にセキュリティを強化する目的で、デバイスのさまざまな TCP/UDP サービスを有効にすることができます。

デバイスで提供される TCP/UDP サービスは次のとおりです。

- **HTTP**:工場出荷時に有効に設定されています
- **HTTPS**:工場出荷時に有効に設定されています
- **SNMP**:工場出荷時に無効に設定されています
- **Telnet**:工場出荷時に無効に設定されています
- **SSH**:工場出荷時に無効に設定されています

このウィンドウには、アクティブな TCP 接続も表示されます。

TCP/UDP サービスを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [TCP/UDPサービス] をクリックします。

ステップ 2 サービスが表示されたら、次の TCP/UDP サービスを有効または無効にします。

- [HTTP サービス]: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サービス]: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 サービス]: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** サービス]:**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 サービス]:SSH サーバ 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 [適用] 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、各サービスについて次のフィールドが表示されます。

- [サービス名]: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。
- [タイプ]:サービスが使用する IP プロトコル。
- [ローカルIPアドレス]: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。
- [ローカルポート]: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。
- [リモートIPアドレス]: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。
- [リモートポート]:サービスを要求しているリモート デバイスの TCP ポート。
- [状態]:サービスのステータス。

UDP サービス テーブルに表示される情報は次のとおりです。

- [サービス名]: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。
- [タイプ]:サービスが使用する IP プロトコル。
- [ローカルIPアドレス]: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。
- [ローカルポート]: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。
- [アプリケーションインスタンス]:UDP サービスのサービス インスタンス。(たとえば 2 つの送信元が同じ宛先にデータを送る場合。)

ストーム制御

ここでは、ストーム制御について説明します。具体的な内容は、次のとおりです。

- ストーム制御
- ストーム制御統計情報

ブロードキャスト フレーム、マルチキャスト フレーム、または Unknown ユニキャスト フレームが受信された場合、そのフレームが複製され、フレームのコピーがすべての該当出力ポートに送信されます。つまり実際には、該当 VLAN に属するすべてのポートに送信されます。このように、1 つの入力フレームに対して多数のコピーが生成されるので、トラフィック ストームが発生するおそれがあります。

ストーム防止機能を利用すると、デバイスに入ってくるフレームの数を制限し、この制限の対象としてカウントされるフレームのタイプを指定することができます。

ブロードキャスト フレーム、マルチキャスト フレーム、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高い場合、しきい値を超えて受信されたフレームは破棄されます。

ストーム制御

ストーム制御を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [ストーム制御] > [ストーム制御設定] の順にクリックします。

ステップ 2 ポートを選択して [編集] をクリックします。

ステップ 3 パラメータを入力します。

- [インスタンス]: ストーム制御を有効にする対象の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]: ユニキャスト パケットのストーム制御を有効にする場合に選択します。
- [レートしきい値]: 不明なパケットを転送できるように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。
- [トラップオンストーム]: ポート上でストームが発生したときにトラップを送信する場合に選択します。これが選択されていない場合は、トラップが送信されません。

- [シャットダウンオンストーム]:ポート上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]:マルチキャスト パケットのストーム制御を有効にする場合に選択します。
- [マルチキャストタイプ]:ストーム制御を実装する次のタイプのマルチキャスト パケットのいずれかを選択します。
  - [すべて]: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。
  - [登録済みマルチキャスト]: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。
  - [登録解除済みマルチキャスト]: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]:不明なパケットを転送できるように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。
- [トラップオンストーム]:ポート上でストームが発生したときにトラップを送信する場合に選択します。これが選択されていない場合は、トラップが送信されません。
- [シャットダウンオンストーム]:ポート上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]:ブロードキャスト パケットのストーム制御を有効にする場合に選択します。
- [レートしきい値]:不明なパケットを転送できるように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。
- [トラップオンストーム]:ポート上でストームが発生したときにトラップを送信する場合に選択します。これが選択されていない場合は、トラップが送信されません。
- [シャットダウンオンストーム]:ポート上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 [適用] をクリックします。ストーム制御が変更され、実行コンフィギュレーション ファイルが更新されます。

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、次のようにします。

ステップ 1 [セキュリティ] > [ストーム制御] > [ストーム制御統計情報] 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 [リフレッシュレート] を入力します。統計情報の更新頻度を選択します。オプションは次のとおりです。

- [リフレッシュなし]:統計情報はリフレッシュされません。
- [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 秒ごとにリフレッシュされます。
- [60 秒]:統計情報は 60 秒ごとにリフレッシュされます。

不明なユニキャスト、マルチキャスト、およびブロードキャスト ストーム制御に関する次の統計情報が表示されます。

- [マルチキャストトラフィックタイプ]:(マルチキャスト トラフィックの場合のみ):[登録済み] または [未登録]。
- [通過したバイト数]:受信バイト数。
- [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のカウンタを完全にクリアするには、[すべてのインターフェイスカウンタのクリア] をクリックします。1 つ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、そのインターフェイスを選択し、[インターフェイス カウンタのクリア] 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。

特定の MAC アドレスからのポート アクセスを制限することにより、ネットワークのセキュリティを強化できます。アクセスを制限したい送信元 MAC アドレスは、動的（ダイナミック）に学習させることも、静的（スタティック）に設定することもできます。

ポート セキュリティを設定すると、受信された MAC アドレスと学習された MAC アドレスが照合されます。ロックされているポートには、特定の MAC アドレスからのみアクセスできます。

ポート セキュリティには次の 4 つのモードがあります。

- [クラシックロック]：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。また、学習済み MAC アドレスがエージングしたり再学習されたりすることはありません。
- [限定ダイナミックロック]：デバイスは、許容最大アドレス数として設定された制限に達するまで MAC アドレスを学習します。制限に達すると、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 MAC アドレスがエージングしたり再学習されたりすることがあります。
- [無期限セキュア]：ポートに関連している現在のダイナミック MAC アドレスを保持し、（[アドレスの最大許容数] で設定される）ポートの許容最大アドレス数に達するまで学習します。再学習とエージングは無効です。
- [リセット時にセキュア削除]：リセット後に、ポートに関連している現在のダイナミック MAC アドレスを削除します。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「リセット時に削除」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です。

新しい MAC アドレスから届いたフレームがポート上で検出され、かつ、その MAC アドレスが承認されていない場合、（つまり、ポート セキュリティがクラシック ロック モードであり、届いた MAC アドレスがロックされている場合、または、ポート セキュリティが限定ダイナミック ロック モードであり、学習済み MAC アドレスが上限数に達している場合）、防御機構が働き、次のいずれかの処理が実行されます。

- フレームが廃棄される
- フレームが転送される
- ポートが停止する

安全な 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。

これらの処理のいずれかを実行するのに加え、トラップを生成することができます。その際、トラップの生成頻度を下げて回数を減らし、スイッチが過負荷状態になるのを回避することができます。

ポート セキュリティを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [ポートセキュリティ] をクリックします。

ステップ 2 変更対象となるインターフェイスを選択して、[編集] 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には、このフィールドを選択します。
- [学習モード]: ポートのロックの種類を選択します。このフィールドの値を指定するには、[インターフェイスステータス]のロックを解除する必要があります。[学習モード] フィールドは、[インターフェイスステータス] 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。[学習モード]の値を変更するには、[インターフェイスステータス]のロックをいったん解除する必要があります。変更後、[インターフェイスステータス]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]: すでに学習済みのアドレス数にかかわらず、ポートをただちにロックします。
  - [限定ダイナミックロック]: ポートに関連付けられている現在のダイナミック MAC アドレスを削除することで、ポートをロックします。このポートに対して設定した上限数に達するまで MAC アドレスが学習されます。また、MAC アドレスはエージングしたり再学習されたりすることがあります。
  - [無期限セキュア]: ポートに関連している現在のダイナミック MAC アドレスを保持し、([アドレスの最大許容数] で設定される) ポートの許容最大アドレス数に達するまで学習します。再学習とエージングは有効です。
  - [リセット時にセキュア削除]: リセット後に、ポートに関連している現在のダイナミック MAC アドレスを削除します。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「リセット時に削除」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です。

- [アドレスの最大許容数]:学習モードとして [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 アドレスの最大数を入力します。数値 0 は、このポート上でスタティック MAC アドレスだけを設定できることを意味します。
- [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。
  - [廃棄]:学習されていない送信元から届いたパケットを廃棄します。
  - [転送]:不明な送信元からのパケットを転送します。MAC アドレスは学習されません。
  - [シャットダウン]:学習されていない送信元からのパケットを廃棄し、ポートをシャットダウンします。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、ポートはシャットダウンしたままになります。
- [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には、このフィールドを選択します。トラップは、ロックが侵害されようとしたことを通知するものです。クラシック ロック モードの場合、トラップの内容は、新たに受信された MAC アドレスです。限定ダイナミック ロック モードの場合、トラップの内容は、上限数を超過した分の新しい MAC アドレスです。
- [トラップ間隔]:トラップとトラップの間の最短経過時間を入力します(単位:秒)。

ステップ 4 [適用] をクリックします。ポート セキュリティが変更され、実行コンフィギュレーション ファイルが更新されます。

802.1X 認証

802.1X 認証については、「セキュリティ:802.1X 認証」という章の情報を参照してください。

IP ソース ガード

IP ソース ガードというセキュリティ機能を使用すると、ホストが自分のネイバーの 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止できます。

IP ソース ガードを有効にすると、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る IP アドレス向けのクライアント IP トラフィックだけを伝送します。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、および手動で追加されたエントリが含まれます。

パケットがデータベース内のエントリに一致する場合、デバイスはそれを転送します。そうでない場合はドロップします。

ここでは、IP ソース ガード機能について説明します。具体的な内容は、次のとおりです。

- 他の機能との連携
- フィルタリング
- IP ソース ガードの作業フロー
- プロパティ
- インターフェイス設定
- バインディング データベース

他の機能との連携

IP ソース ガードには、次の点が当てはまります。

- インターフェイスで IP ソース ガードを有効にするには、DHCP スヌーピングがグローバルに有効になっている必要があります。
- インターフェイスで IP ソース ガードをアクティブ化できるのは、次の場合だけです。
  - ポートの VLAN の少なくとも 1 つで DHCP スヌーピングが有効になっている
  - インターフェイスが DHCP 非信頼である。信頼されているポートではすべてのパケットが転送されます。
- ポートが DHCP 信頼である場合、この状況ではポートの IP ソース ガードを有効化することで IP ソース ガードがアクティブにはなりませんが、スタティック IP アドレスのフィルタリングを設定できます。

- ポートのステータスが DHCP 非信頼から DHCP 信頼に変化すると、スタティック IP アドレス フィルタリング エントリはバインディング データベースに残りますが、非アクティブになります。
- 送信元 IP および MAC アドレス フィルタリングがポートで設定されている場合、ポート セキュリティを有効にすることはできません。
- IP ソース ガードは TCAM リソースを使用し、IP ソース ガード アドレス エントリごとに 1 つの TCAM ルールを必要とします。IP ソース ガード エントリの数が使用可能な TCAM ルールの数を超えた場合、余分なアドレスは非アクティブになります。

フィルタリング

ポートでの 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 フィルタリングが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 アドレスを含むトラフィックだけが許可されます。
  - IPv4 以外のトラフィック：許可されます（ARP パケットを含む）。

IP ソース ガードの作業フロー

IP ソース ガードを設定するには、次のようにします。

ステップ 1 （DHCP スヌーピング）[プロパティ] ページを有効にします。

ステップ 2 （DHCP スヌーピング）[インターフェイス設定] ページで、DHCP スヌーピングを有効にする VLAN を定義します。

ステップ 3 （DHCP スヌーピング）[インターフェイス設定] ページで、インターフェイスを信頼または非信頼に設定します。

ステップ 4 （IP ソースガード）[プロパティ] ページで IP ソース ガードを有効にします。

ステップ 5 必要に応じて、（IP ソース ガード）[インターフェイス設定] ページで、非信頼インターフェイスでの IP ソース ガードを有効にします。

ステップ 6 （IP ソースガード）[バインディング データベース] ページで、バインディング データベースへのエントリを確認します。

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、次のようにします。

ステップ 1 [セキュリティ] > [IPソースガード] > [プロパティ] をクリックします。

ステップ 2 IP ソース ガードをグローバルに有効にするには、[有効] を選択します。

ステップ 3 [適用] を選択すると、IP ソース ガードが有効になります。

インターフェイス設定

非信頼ポート/LAG 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 パケットが伝送されます。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、次のようにパケット伝送が許可されます。

- [IPv4 トラフィック]: 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。
- [IPv4 以外のトラフィック]: 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の IP ソース ガードの有効化について、詳しくは「他の機能との連携」を参照してください。

インターフェイスで IP ソース ガードを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [IPソースガード] > [インターフェイス設定] をクリックします。

ステップ 2 [フィルタ] フィールドからポート/LAG を選択して、[実行] をクリックします。このユニット上のポート/LAG、および次の情報が表示されます。

- [IPソースガード]: 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スヌーピングで信頼されたインターフェイス]: これが DHCP 信頼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/LAG を選択して [編集] をクリックします。[IPソースガード] フィールドの [有効] 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 [適用] をクリックすると、実行コンフィギュレーション ファイルに設定がコピーされます。

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検査するために DHCP スヌーピング バインディング データベースを使用します。デバイスが DHCP スヌーピング バインディング データベースに書き込もうとするエントリの数が多すぎる場合、余分なエントリが非アクティブ ステータスで維持されます。エントリのリース時間が期限切れになるとエントリは削除され、非アクティブ エントリがアクティブになります。

「DHCP スヌーピング/リレー」を参照してください。

注 [バインディングデータベース] 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 バインディング データベースを表示して TCAM 使用状況を確認するには、[挿入非アクティブ] を次のように設定します。

ステップ 1 [セキュリティ] > [IPソースガード] > [バインディングデータベース] をクリックします。

ステップ 2 DHCP スヌーピング バインディング データベースは、データベース管理用に TCAM リソースを使用します。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。オプションは、次のとおりです。

- [再試行頻度]: TCAM リソースが検査される頻度。
- [無期限]: 非アクティブ アドレスを一度も再アクティブ化しようとしません。

ステップ 3 [適用] 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 [今すぐ再試行] をクリックすると TCAM リソースが検査されます。

バインディング データベースのエントリが次のように表示されます。

- [VLAN ID]: パケットを受信すると予想される VLAN。
- [MACアドレス]: 照合される MAC アドレス。
- [IP アドレス]: 照合される IP アドレス。
- [インターフェイス]: パケットを受信すると予想されるインターフェイス。
- [ステータス]: 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]: エントリがダイナミックまたはスタティックのどちらであるかを表示します。

- [理由]: 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。可能性のある理由は次のとおりです。
  - [問題なし]: インターフェイスはアクティブです。
  - [スヌープVLANなし]: VLAN で DHCP スヌーピングが有効になっていません。
  - [信頼できるポート]: ポートが信頼されるようになりました。
  - [リソースの問題]: TCAM リソースを使い尽くしました。

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、該当する検索条件を入力して [実行] をクリックします。

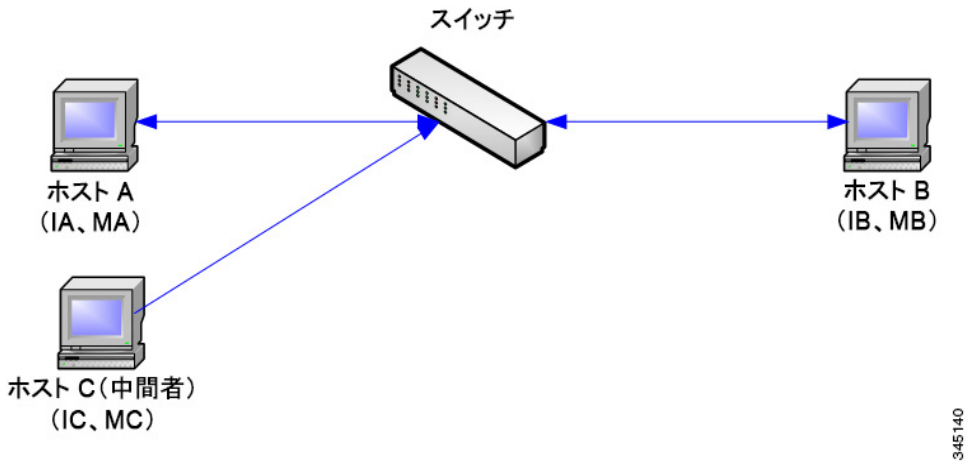
ARP インスペクション

ARP では、IP アドレスを MAC アドレスにマップすることでレイヤ 2 ブロードキャスト ドメイン内の IP 通信が可能です。

悪意のあるユーザは、サブネットに接続されたシステムの ARP キャッシュをポイズニングし、サブネット上の他のホストに向かうトラフィックをインターセプトすることにより、レイヤ 2 ネットワークに接続されたホスト、スイッチ、ルータを攻撃することができます。ARP では、ARP 要求を受け取らなくてもホストからの Gratuitous 応答が可能なため、このような状況が発生する可能性があります。攻撃の後、標的となったデバイスからのすべてのトラフィックは攻撃者のコンピュータを通過してルータ、スイッチ、またはホストに流れます。

ARP キャッシュ ポイズニングの例を次に示します。

ARP キャッシュ ポイズニング



ホスト A、B、C がインターフェイス A、B、C 上でスイッチに接続され、これらはすべて同じサブネットにあります。IP アドレスと MAC アドレスは括弧で示されています。たとえばホスト A は IP アドレス IA および MAC アドレス MA を使用します。ホスト A が IP レイヤでホスト B と通信する必要がある場合、IP アドレス IB に関連付けられた MAC アドレスに対する ARP 要求をブロードキャストします。これに対してホスト B は ARP 応答を送ります。スイッチおよびホスト A は、ホスト B の MAC と IP を使って ARP キャッシュを更新します。

ホスト C は、IP アドレス IA(または IB)と MAC アドレス MC のホスト バインディングを使って偽造 ARP 応答をブロードキャストして、スイッチ、ホスト A、ホスト B の ARP キャッシュをポイズニングできます。ポイズニングされた ARP キャッシュを使用するホストは、IA または IB 向けのトラフィックの宛先 MAC アドレスとして MC を使用し、これによりホスト C はこのトラフィックをインターセプトできます。ホスト C は IA および IB に関連付けられた本当の MAC アドレスを知っているため、インターセプトしたトラフィックを、宛先として正しい MAC アドレスを使ってそれらのホストに転送できます。こうしてホスト C はホスト A からホスト B に向かうトラフィック ストリームの中に自分を挿入し、典型的な中間者攻撃を行います。

ここでは、ARP インスペクションと以下のトピックについて説明します。

- ARP でキャッシュ ポイズニングを防ぐ方法
- ARP インスペクションと DHCP スヌーピングとの連携
- ARP デフォルト

ARP でキャッシュ ポイズニングを防ぐ方法

ARP インスペクション機能は、インターフェイスの信頼/非信頼に関連しています([インターフェイス設定] ページを参照)。

インターフェイスは、ユーザによって次のように分類されます。

- [信頼済み]:パケットは検査されません。
- [信頼されていない]:パケットは上記のように検査されます。

ARP インスペクションは、信頼されていないインターフェイスに対してのみ実行されます。信頼できるインターフェイスで受信される ARP パケットは単純に転送されます。

信頼されていないインターフェイスにパケットが到着すると、次のロジックが実施されます。

- パケットの IP/MAC アドレスの ARP アクセス コントロール ルールを検索します。IP アドレスが見つかった場合、リスト内の MAC アドレスとパケットの MAC アドレスが一致すれば、それは正当なパケットです(そうでなければ不正パケットです)。
- パケットの IP アドレスが見つからない場合、パケットの VLAN の 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 データベース内でパケットの「VLAN と IP アドレス」ペアを探します。「VLAN と IP アドレス」のペアが見つかった場合、データベース内の MAC アドレスとインターフェイスがパケットの MAC アドレスと入力インターフェイスに一致すれば、パケットは正当です。
- パケットの IP アドレスが ARP アクセス コントロール ルールと DHCP スヌーピング バインディング データベースのどちらにも見つからない場合、それは不正パケットとしてドロップされます。SYSLOG メッセージが生成されます。

- パケットが正当である場合、パケットは転送されて ARP キャッシュが更新されます。

([プロパティ] ページで) ARP パケット検証オプションを選択した場合、次に示す追加的な検証が実行されます。

- [送信元MAC]: イーサネット ヘッダー内のパケット送信元 MAC アドレスを、ARP 要求内の送信者 MAC アドレスと比較します。この検査は ARP 要求と応答の両方に対して行われます。
- [宛先MAC]: イーサネット ヘッダー内のパケット宛先 MAC アドレスを、宛先インターフェイスの MAC アドレスと比較します。この検査は ARP 応答に対して行われます。
- [IPアドレス]: ARP 本文を比較して不正な IP アドレスと予期されない IP アドレスを検査します。アドレスには、0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。

不正な ARP インスペクション バインディングを含むパケットはログに記録され、ドロップされます。

ARP アクセス コントロール テーブルには最大で 1024 個のエントリを定義できます。

ARP インスペクションと DHCP スヌーピングとの連携

DHCP スヌーピングが有効になっている場合、ARP インスペクションでは ARP アクセス コントロール ルールに加えて DHCP スヌーピング バインディング データベースも使用します。DHCP スヌーピングが有効になっていない場合、ARP アクセス コントロール ルールだけが使用されます。

ARP デフォルト

次の表は ARP のデフォルトを示しています。

オプション	デフォルト状態
ダイナミック ARP インスペクション	無効。
ARP パケット検証	無効
VLAN での ARP インスペクション有効化	無効
ログバッファ間隔	ドロップされたパケットに関する SYSLOG メッセージの生成は 5 秒間隔で有効

ARP インスペクションの作業フロー

ARP インスペクションを設定するには、次のようにします。

ステップ 1 ARP インスペクションを有効にして、さまざまなオプションを設定します([プロパティ] ページ)。

ステップ 2 [インターフェイス設定] ページで、インターフェイスを ARP 信頼または非信頼に設定します。

ステップ 3 [ARP アクセス コントロール ルール] ページでルールを追加します。

ステップ 4 ARP インスペクションが有効になる VLAN、および各 VLAN のアクセス コントロール ルールを定義します([VLAN 設定] ページ)。

プロパティ

ARP インスペクション プロパティを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [ARPインスペクション] > [プロパティ] をクリックします。

次のフィールドを入力します。

- [ARPインスペクションステータス]:ARP インスペクションを有効にする場合に選択します。
- [ARPパケット検証]:検証チェックを有効にする場合に選択します。
- [ログ バッファ間隔]:次のいずれかのオプションを選択します。
  - [再試行頻度]:ドロップされたパケットに関す SYSLOG メッセージの送信を有効にします。メッセージが送信される頻度を入力してください。
  - [無期限]: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 [適用] をクリックします。設定値が定義され、実行コンフィギュレーション ファイルが更新されます。

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 テーブルに照らして検査され、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 データベースに照らして検査されます（[DHCP スヌーピング バインディング データベース] ページを参照）。

デフォルトで、ポート/LAG は ARP インスペクション非信頼になっています。

ポート/LAG の ARP 信頼ステータスを変更するには、次のようにします。

ステップ 1 [セキュリティ] > [ARP インスペクション] > [インターフェイス設定] をクリックします。

ポート/LAG と、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「信頼されない」に設定するには、そのポート/LAG を選択して [編集] をクリックします。

ステップ 3 [信頼済み] または [信頼されていない] を選択して [適用] 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。

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、次のようにします。

ステップ 1 [セキュリティ] > [ARP インスペクション] > [ARP アクセス コントロール] をクリックします。

ステップ 2 エントリを追加するには、[追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [ARP アクセス コントロール名]: ユーザ作成の名前を入力します。
- [IP アドレス]: パケットの IP アドレス。
- [MAC アドレス]: パケットの MAC アドレス。

ステップ 4 [適用] をクリックします。設定値が定義され、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、次のようにします。

ステップ 1 [セキュリティ] > [ARP インスペクション] > [ARP アクセス コントロール ルール] をクリックします。

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、フィルタを選択して、コントロール名を選択し、[実行] をクリックします。

ステップ 2 グループにルールを追加するには、[追加] をクリックします。

ステップ 3 [ARPアクセスコントロール名] を選択して、次のフィールドに値を入力します。

- [IP アドレス]:パケットの IP アドレス。
- [MAC アドレス]:パケットの MAC アドレス。

ステップ 4 [適用] をクリックします。設定値が定義され、実行コンフィギュレーション ファイルが更新されます。

VLAN 設定

VLAN で ARP インスペクションを有効にしてアクセス コントロール グループを VLAN に関連付けるには、次のようにします。

ステップ 1 [セキュリティ] > [ARP インスペクション] > [VLAN 設定] をクリックします。

ステップ 2 VLAN で ARP インスペクションを有効にするには、[使用可能なVLAN] リストにある VLAN を [有効なVLAN] リストに移動します。

ステップ 3 ARP アクセス コントロール グループを VLAN に関連付けるには、[追加] をクリックします。VLAN 番号を選択して、定義済みの [ARPアクセスコントロール名] を選択します。

ステップ 4 [適用] をクリックします。設定値が定義され、実行コンフィギュレーション ファイルが更新されます。

ファースト ホップのセキュリティ

セキュリティ:IPv6 ファースト ホップ セキュリティ

サービス拒絶防御

サービス妨害(DoS)攻撃は、デバイスをユーザにとって使用不能にしようとするハッカーの妨害行為です。

DoS 攻撃は、大量の外部要求通信でデバイスを飽和させて、正当なトラフィックに応答できないようにします。このような攻撃により、デバイス CPU オーバーロードがよく発生します。

- Martian アドレス
- 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 フィルタリング

セキュア コア テクノロジー(SCT)

DoS 攻撃への対抗策としてデバイスで採用できる方式の 1 つは、SCT の使用です。デバイスでは SCT はデフォルトで有効になっており、無効にできません。

シスコ デバイスは拡張機能を備えたデバイスであり、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 トラフィックを扱います。

SCT を使用すると、受信されるトラフィックの総量にかかわらず、デバイスは管理トラフィックとプロトコル トラフィックを確実に受け取って処理することができます。これを実現するために、CPU への TCP トラフィックがレート制限されます。

他の機能との干渉は発生しません。

SCT は [セキュリティ スイート設定] ページ([詳細] ボタン)で監視できます。

DoS 攻撃の種類

DoS 攻撃には、次のような種類のパケットまたは他の戦略が使われる可能性があります。

- **TCP SYN パケット**：このようなパケットはしばしば、送信者アドレスを偽装します。それぞれのパケットは接続要求として扱われ、サーバは TCP/SYN-ACK パケット（確認応答）を送り返し、送信者アドレスからの応答パケット（ACK パケットに対する応答）を待機することにより、ハーフオープン接続を生成します。しかし送信者アドレスが偽装されているため、応答は決して届きません。このようなハーフオープン接続のために、デバイスで作成できる接続数が飽和し、正当な要求への応答が妨げられます。
- TCP SYN-FIN パケット：新しい TCP 接続を作成するために SYN パケットが送られます。接続を閉じるために TCP FIN パケットが送られます。通常、1 つのパケット内に SYN と FIN の両方のフラグが設定されることは決してありません。したがって、そのようなパケットはデバイスに対する攻撃である可能性があり、ブロックすべきです。
- **Martian アドレス**：IP プロトコルの観点から言うと、Martian アドレスは不正なアドレスです。詳細については、「Martian アドレス」を参照してください。
- **ICMP 攻撃**：不適切な形式の ICMP パケットまたは膨大な数の ICMP パケットが攻撃の標的に送られると、システム クラッシュが発生する可能性があります。
- **IP フラグメンテーション**：重複する、サイズが大きすぎるペイロードを含む細切れの IP フラグメントがデバイスに送られます。その結果、TCP/IP フラグメンテーション再構築コードのバグが原因で、さまざまなオペレーティング システムがクラッシュする可能性があります。Windows 3.1x、Windows 95 および Windows NT オペレーティング システム、さらにバージョン 2.0.32 および 2.1.63 より前の Linux バージョンは、この攻撃に対して脆弱です。
- **Stacheldraht（分散型）**：攻撃者はクライアント プログラムを使ってハンドラに接続します。そのハンドラのシステムは侵害され、エージェントをゾンビ化するコマンドを発行して、それを利用した DoS 攻撃が可能になります。攻撃者により、ハンドラを介してエージェントが侵害されます。

  自動化されたルーチンを使用して、リモート接続を受け入れる標的のリモートホストで実行されるプログラムの脆弱性を悪用します。各ハンドラは最大で 1000 個のエージェントを制御できます。

- **Invasor（トロイの木馬）**：トロイの木馬を介して攻撃者はゾンビ エージェントをダウンロードできます（トロイの木馬にゾンビが含まれていることもあります）。また、リモート ホストからの接続をリッスンするプログラム内の欠陥を悪用する自動化ツールを使用して、攻撃者はシステムに不正侵入できます。特に Web 上でサーバとして機能するデバイスには、このような攻撃の標的となる危険があります。
- **Back Oriface（トロイの木馬）**：このトロイの木馬の亜種は、Back Oriface ソフトウェアを使ってトロイの木馬を注入します。

DoS 攻撃に対する防御

サービス妨害（DoS）防御機能により、システム管理者は次のような方法でこのような攻撃に対抗できます。

- TCP SYN 保護の有効化。この機能を有効にすると、SYN パケット攻撃が検出されたときにレポートが発行され、攻撃を受けたポートを一時的にシャットダウンできます。1 秒あたりの SYN パケット数が、ユーザ設定しきい値を超えた場合に、SYN 攻撃であると識別されます。
- SYN-FIN パケットのブロック。
- 予約済みの Martian アドレスを含むパケットをブロックする（[Martian アドレス] ページ）
- 特定のインターフェイスからの TCP 接続を防止し（[SYN フィルタリング] ページ）、パケットをレート制限する（[SYN レート保護] ページ）
- 特定の ICMP パケットのブロックを設定する（[ICMP フィルタリング] ページ）
- 特定のインターフェイスからのフラグメント化された IP パケットを破棄する（[IP フラグメント フィルタリング] ページ）
- Stacheldraht Distribution、Invasor Trojan、Back Orifice Trojan からの攻撃を拒否する（[セキュリティ スイート設定] ページ）

機能間の依存関係

ポートで DoS 防止機能が有効化されている間、ACL および拡張 QoS ポリシーは非アクティブになります。インターフェイスで ACL が定義されている場合に DoS 防止機能を有効にしようとすると、エラー メッセージが表示されます。また、DoS 防止機能が有効になっているインターフェイスで ACL を定義しようとした場合にも、エラーが表示されます。

アクティブな ACL がインターフェイスに存在する場合、SYN 攻撃をブロックすることはできません。

デフォルト コンフィギュレーション

DoS 防御機能のデフォルトは次のとおりです。

- DoS 防御機能はデフォルトで無効になっています。
- SYN-FIN 保護機能はデフォルトで有効です(DoS 防御機能が無効になっている場合でも)。
- SYN 保護が有効になっている場合、デフォルトの保護モードは [ブロックとレポート] です。デフォルトのしきい値は 1 秒あたり 30 SYN パケットです。
- その他のすべての DoS 防御機能はデフォルトで無効になっています。

セキュリティ スイート設定

注 DoS 攻撃防止機能をアクティブ化するには、その前に、すべての Access Control List (ACL; アクセス コントロール リスト)および拡張 QoS ポリシーをポートからアンバインドしておく必要があります。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 防御機能のグローバル設定および SCT の監視を行うには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [セキュリティスイート設定] をクリックします。

[CPU 保護メカニズム]:[有効] は、SCT が有効になっていることを示します。

ステップ 2 [CPU 利用率] の横の [詳細] をクリックすると [CPU 利用率] 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保護] の横にある [編集] をクリックします。

ステップ 4 [DoS 防御] を選択するとこの機能が有効になります。

- [無効]: この機能が無効になります。
- [システムレベルの防御]: Stacheldraht(分散型)、Invasor(トロイの木馬)、および Back Orifice(トロイの木馬)による攻撃を防ぐ機能が有効になります。
- [システムレベルおよびインターフェイスレベルの防御]: Stacheldraht(分散型)、Invasor(トロイの木馬)、および Back Orifice(トロイの木馬)による攻撃を防ぐ機能が有効になります。

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（分散型）]：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（トロイの木馬）]：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（トロイの木馬）]：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 必要に応じて次の項目をクリックします。

- [Martianアドレス]：[編集] をクリックすると [Martian アドレス] ページに移動します。
- [SYNフィルタリング]：[編集] をクリックすると [SYN フィルタリング] ページに移動します。
- [SYNレート保護]：（レイヤ 2 のみ）[編集] をクリックすると [SYN レート保護] ページに移動します。
- [ICMPフィルタリング]：[編集] をクリックすると [ICMP フィルタリング] ページに移動します。
- [IIPフラグメント化]：[編集] をクリックすると [IP フラグメント フィルタリング] ページに移動します。

ステップ 7 [適用] をクリックします。サービス拒絶防御のセキュリティ スイート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

デバイスを攻撃するためにハッカーがネットワーク ポートを使用して SYN 攻撃を仕掛け、結果として TCP リソース（バッファ）と CPU パワーが消費される可能性があります。

CPU は SCT を使って保護されるため、CPU への TCP トラフィックは制限されます。しかし、高いレートの SYN パケットによって 1 つ以上のポートが攻撃された場合、CPU は攻撃者のパケットだけを受け取り、こうしてサービス拒否が発生します。

SYN 保護機能を使用すると、CPU は各ネットワーク ポートから CPU に入ってくる 1 秒ごとの SYN パケット数をカウントします。

この数が、ユーザ定義の特定のしきい値よりも大きい場合には、「自分への MAC を含む SYN を拒否」ルールがポートで適用されます。ユーザ定義の間隔（SYN 保護期間）ごとに、このルールはポートからバインド解除されます。

SYN 保護を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [SYN保護] をクリックします。

ステップ 2 パラメータを入力します。

- [SYN-FIN パケットのブロック]：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保護モード]：次の 3 つのモードから選択します。
  - [無効]：特定のインターフェイスでこの機能が無効になります。
  - [レポート]：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 [攻撃済み] に変わります。
  - [ブロックとレポート]：TCPSYN 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 [ブロック済み] に変わります。
- [SYN保護しきい値]：（「自分への MAC を含む SYN を拒否」ルールがポートで適用されて）SYN パケットをブロックするようになる、1 秒あたりの SYN パケット数。
- [SYN保護期間]：（「自分への MAC を含む SYN を拒否」ルールがポートからバインド解除されて）SYN パケットのブロックを解除するまでの秒数。

ステップ 3 [適用] 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 テーブルには、(ユーザからの要求に従って)ポートまたは LAG ごとに次のフィールドが表示されます。

- [現在のステータス]: インターフェイスのステータス。表示される値は次のとおりです。
  - [ノーマル]: このインターフェイスで攻撃は検出されませんでした。
  - [ブロック済み]: このインターフェイスではトラフィックが転送されません。
  - [攻撃済み]: このインターフェイスで攻撃が検出されました。
- [最新の攻撃]: システムで最後に検出された SYN-FIN 攻撃の日付とシステム アクション(**レポート済み**、または**ブロックおよびレポート済み**)。

Martian アドレス

[Martianアドレス] ページでは、ネットワークで検出されると攻撃と見なされる IP アドレスを入力できます。このような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言うと不正なアドレスであるいくつかの予約済み Martian アドレスをサポートしています。サポートされる予約済み Martian アドレスは、

- [Martianアドレス] 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不正と見なされるアドレス。次の範囲内のアドレスを含みます。
  - **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 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。

さらに、DoS 防御用に新しい 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、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [Martianアドレス] をクリックします。

ステップ 2 [予約済みのMartianアドレス] を選択して [適用] をクリックすると、システム レベル防御リストに予約済みの Martian アドレスが含まれるようになります。

ステップ 3 Martian アドレスを追加するには、[追加] 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バージョン]: サポートされる IP バージョンを示します。現在、IPv4 のみがサポートされています。
- [IPアドレス]: 拒否する IP アドレスを入力します。表示される値は次のとおりです。
  - [予約済みリストから]: 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。
  - [新規IPアドレス]: IP アドレスを入力します。
- [マスク]: 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。
  - [ネットワークマスク]: ドット付き 10 進表記でのネットワーク マスク。
  - [プレフィックス長]: 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 [適用] をクリックします。Martian アドレ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。

SYN フィルタリング

[SYNフィルタリング] ページでは、SYN フラグを含む、1 つ以上のポート宛ての 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、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [SYNフィルタリング] をクリックします。

ステップ 2 [追加] 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]: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]:IP アドレス形式で、フィルタを有効にする対象のネットワーク マスクを入力します。次のいずれかを入力します。
  - [マスク]: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]: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。
- [TCPポート]:フィルタされる宛先 TCP ポートを次のように選択します。
  - [既知のポート]:リストからポートを選択します。
  - [ユーザ定義]: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 [適用] をクリックします。SYN フィルタが定義され、実行コンフィギュレーション ファイルが更新されます。

SYN レート保護

[SYNレート保護] ページでは、入力ポートで受信される SYN パケットの数を制限できます。これにより、パケット処理のために開かれる新しい接続の数をレート制限することで、サーバに対する SYN フラッドの影響を軽減できる可能性があります。

SYN レート保護を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [SYNレート保護] をクリックします。

このページには、インターフェイスごとに、現在定義されている SYN レート保護が表示されます。

ステップ 2 [追加] 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]:レート保護を定義するインターフェイスを選択します。
- [IPアドレス]:SYN レート保護を定義する対象の IP アドレスを入力するか、[すべてのアドレス] を選択します。IP アドレスを入力する場合には、マスクまたはプレフィックス長のいずれかを入力してください。
- [ネットワークマスク]: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]:送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをドット区切り 10 進表記で入力します。
  - [プレフィックス長]:[プレフィックス長] を選択し、送信元 IP アドレス プレフィックスを構成するビット数を入力します。
- [SYNレート制限]:受信してもよい SYN パケットの数を入力します。

ステップ 4 [適用] をクリックします。SYN レート保護が定義され、実行コンフィギュレーションが更新されます。

ICMP フィルタリング

[ICMPフィルタリング] 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。これにより、ICMP 攻撃が発生した場合にネットワークの負荷を減らすことができます。

ICMP フィルタリングを定義するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [ICMPフィルタリング] をクリックします。

ステップ 2 [追加] 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]:ICMP フィルタリングを定義す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には、マスクまたはプレフィックス長のいずれかを入力してください。

- [ネットワークマスク]: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]:送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをドット区切り 10 進表記で入力します。
  - [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 [適用] をクリックします。ICMP フィルタリングが定義され、実行コンフィギュレーションが更新されます。

IP フラグメント フィルタリング

[IPフラグメント化] ページでは、フラグメント化された IP パケットをブロックできます。

フラグメント化された IP をブロックする機能を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [サービス拒絶防御] > [IPフラグメントフィルタリング] をクリックします。

ステップ 2 [追加] 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]:IP フラグメンテーションを定義するインターフェイスを選択します。
- [IPアドレス]:フラグメント化された 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には、マスクまたはプレフィックス長のいずれかを入力してください。
- [ネットワークマスク]: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]:送信元 IP アドレスが属するサブネットを選択し、サブネット マスクをドット区切り 10 進表記で入力します。
  - [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 [適用] 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。

21

セキュリティ:802.1X 認証

ここでは、802.1X 認証について説明します。

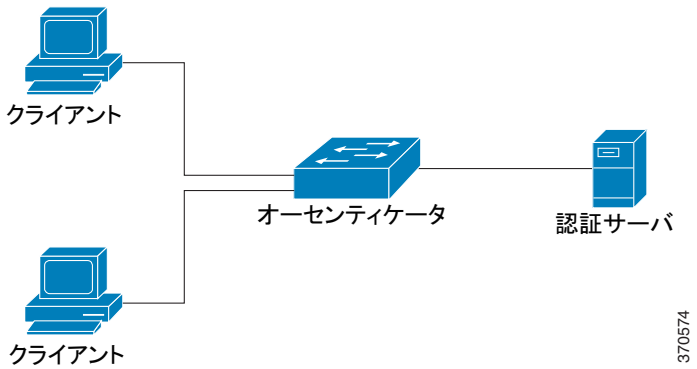
具体的な内容は、次のとおりです。

概要

802.1X 認証を使用すると、権限がないクライアントは、公衆アクセス可能なポート経由での接続が制限されます。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 デバイスは次の特定の役割を果たします。

- クライアントまたはサプリカント
- オーセンティケータ
- 認証サーバ

次の図で説明します。



ネットワーク デバイスは、ポートごとにクライアント/サプリカント、オーセンティケータ、またはその両方として使用することができます。

クライアントまたはサプリカント

クライアントまたはサプリカントとは、LAN へのアクセスを要求するネットワーク デバイスです。このクライアントはオーセンティケータに接続されます。

クライアントが認証に 802.1x プロトコルを使用する場合、クライアントは、802.1x プロトコルのサプリカントの部分と EAP プロトコルのクライアントの部分を実行します。

MAC ベースまたは Web ベースの認証を使用するために、クライアント上で特別なソフトウェアは必要ありません。

オーセンティケータ

オーセンティケータは、サプリカント ポートの接続先となる、ネットワーク サービスを提供するネットワーク デバイスです。

次の認証方式がサポートされています。

- 802.1x ベース:すべての認証モードでサポートされています。
- MAC ベース:すべての認証モードでサポートされています。
- Web ベース:複数セッション モードでのみサポートされています。

802.1x ベース認証では、オーセンティケータが 802.1x メッセージ(EAPOL パケット)から EAP メッセージを抽出し、RADIUS プロトコルを使用してこれを認証サーバに渡します。

MAC ベース、または Web ベースの認証では、ネットワーク アクセスを探索しているクライアントに代わって、オーセンティケータ自体がソフトウェアの EAP クライアント部分を実行します。

ポートは認証モードに設定されます。詳細については、「ポート ホスト モード」を参照してください。

認証サーバ

認証サーバは、クライアントの実際の認証を実行します。デバイス用の認証サーバは、EAP 拡張機能を備えた RADIUS 認証サーバです。

オープンアクセス

オープン(モニタリング)アクセス機能は、実際の認証失敗と、802.1x 環境のコンフィギュレーションの誤りやリソース不足が原因で生じる失敗を区別するのに役立ちます。

オープン アクセスを使用することにより、システム管理者はネットワークに接続しているホストのコンフィギュレーション上の問題を容易に把握できるようになります。さらにこの機能は、不適切な状態を監視して、これらの問題を修正できるようにします。

オープン アクセスがインターフェイスで有効になっている場合、スイッチは RADIUS サーバから受け取った失敗をすべて成功と見なし、認証結果にかかわらず、インターフェイスに接続しているステーションにネットワークへのアクセスを許可します。

通常の動作では、認証が有効なポート上のトラフィックは認証と承認が正常に完了するまでブロックされますが、オープン アクセスにより、その動作が変更されます。デフォルトの認証動作では、Extensible Authentication Protocol over LAN(EAPoL)を除くすべてのトラフィックがブロックされます。ただし、オープン アクセスでは、認証(802.1X ベース、MAC ベース、および WEB ベース)が有効になっている場合でも、すべてのトラフィックに対する無制限のアクセスを許可するオプションが管理者に提供されます。

RADIUS アカウンティングが有効になっている場合、認証試行をログに記録し、監査証跡を使用して、ネットワークに接続しているユーザやシステムを把握できます。

エンド ユーザや、ネットワークに接続されたホストへの影響はありません。オープンアクセスは、[ポート認証] ページから有効化できます。

ポート認証状態

ポート認証状態により、クライアントにネットワークへのアクセス権が付与されるかどうかが決まります。

ポートの管理状態は [ポート認証] ページで設定できます。

次の値のいずれかを使用できます。

- [強制許可]

  ポート認証は無効で、ポートはスタティック設定に従い、認証を行わずにすべてのトラフィックを送信します。スイッチは、802.1x EAPOL 開始メッセージを受信すると、EAP 成功メッセージを格納した 802.1x EAP パケットを送信します。

  デフォルトでは、この状態です。

- [強制無許可]

  ポート認証は無効で、ポートはゲスト VLAN および非認証 VLAN 経由ですべてのトラフィックを送信します。詳細については、「ホストおよびセッション認証」を参照してください。スイッチは、802.1x EAPOL 開始メッセージを受信すると、EAP 失敗メッセージを格納した 802.1x EAP パケットを送信します。

- [自動]

  ポート認証は、設定済みのポート ホスト モードおよびポートに設定されている認証方式に従って有効になります。

ポート ホスト モード

ポートは、次のポート ホストモードに設定できます([ホストおよびセッション認証] ページで設定)。

- [単一ホスト モード]

  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 つのポートには 1 つのホストのみ許可されます。

  ポートが許可されておらず、ゲスト VLAN が有効な場合、タグのないトラフィックはゲスト VLAN に再マッピングされます。タグ付きトラフィックは、ゲスト VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポートでゲスト VLAN が無効な場合、非認証 VLAN に所属するタグ付きトラフィックのみがブリッジされます。

ポートが許可されると、許可されたホストからのトラフィックは、タグなしのものもタグ付きのものも、スタティック VLAN メンバーシップ ポート設定に従ってブリッジされます。その他のホストからのトラフィックはドロップされます。

ユーザは、許可されたホストからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによる割り当て済み VLAN に再マッピングされるように指定することもできます。タグ付きトラフィックは、RADIUS による割り当て済み VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポート上の RADIUS VLAN 割り当ては、[ポート認証] ページで設定します。

- [複数ホスト モード]

  許可されたクライアントが少なくとも 1 つ存在する場合にポートが許可されます。

  ポートが許可されておらず、ゲスト VLAN が有効な場合、タグのないトラフィックはゲスト VLAN に再マッピングされます。タグ付きトラフィックは、ゲスト VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポートでゲスト VLAN が無効な場合、非認証 VLAN に所属するタグ付きトラフィックのみがブリッジされます。

  ポートが許可されると、そのポートに接続されたすべてのホストからのトラフィックは、タグなしのものもタグ付きのものも、スタティック VLAN メンバーシップ ポート設定に従ってブリッジされます。

  許可されたポートからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによる割り当て済み VLAN に再マッピングされるように指定することもできます。タグ付きトラフィックは、RADIUS による割り当て済み VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポート上の RADIUS VLAN 割り当ては、[ポート認証] ページで設定します。

- [複数セッション モード]

  単一ホスト モードや複数ホスト モードとは異なり、複数セッション モードのポートには認証ステータスがありません。認証ステータスは、ポートに接続している各クライアントに対して割り当てられます。

  非認証 VLAN に所属するタグ付きトラフィックは、ホストが許可されているどうかにかかわらず、常にブリッジされます。

  非認証 VLAN に所属していない未許可のホストのトラフィックは、タグ付きのものもタグなしのものも、VLAN で定義され有効な場合はゲスト VLAN に再マッピングされ、ゲスト VLAN がポートで無効な場合はドロップされます。

許可されたポートからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによる割り当て済み VLAN に再マッピングされるように指定することもできます。タグ付きトラフィックは、RADIUS による割り当て済み VLAN か非認証 VLAN に所属する場合以外は、ドロップされます。ポート上の RADIUS VLAN 割り当ては、[ポート認証] ページで設定します。

複数の認証方式

スイッチで複数の認証方式が有効な場合、次の階層の認証方式が適用されます。

- 802.1x 認証:最高
- Web ベース認証
- MAC ベース認証:最低

複数の方式を同時に実行できます。1 つの方式が正常に終了すると、そのクライアントは許可され、プライオリティが低い方式が停止し、プライオリティが高い方式での処理が続行されます。

同時に実行している認証方式のいずれかで失敗した場合、その他の方式での処理が続行されます。

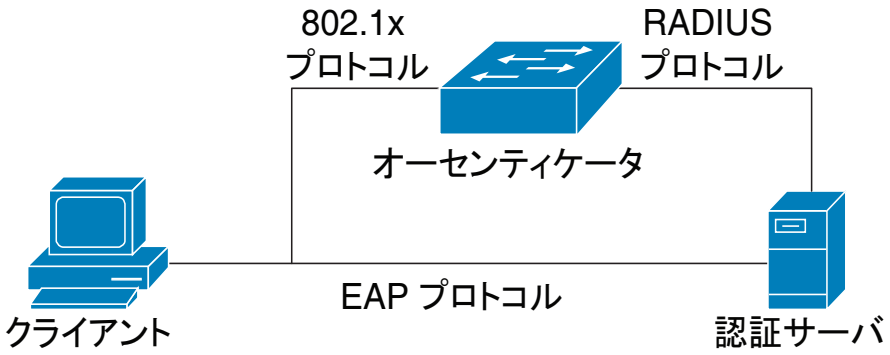
ある認証方式が、プライオリティが低い認証方式で認証済みのクライアントにおいて正常に終了すると、新しい認証方式の属性が適用されます。新しい方式で失敗した場合、クライアントに対する元の方式での許可が引き続き有効になります。

802.1x ベース認証

802.1x ベースのオーセンティケータは、透過的な EAP メッセージを 802.1x サプリカントと認証サーバ間でリレーします。サプリカントとオーセンティケータ間の EAP メッセージは 802.1x メッセージ内にカプセル化され、オーセンティケータと認証サーバ間の EAP メッセージは RADIUS メッセージ内にカプセル化されます。

次の図で説明します。

図 1　802.1x ベース認証

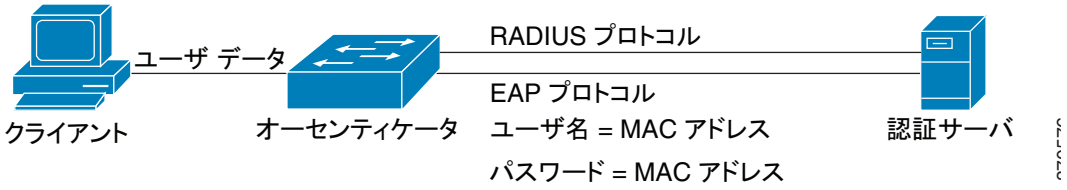


MAC ベース認証

MAC ベース認証は 802.1X 認証の代替方式です。この方式は、802.1x サプリカント機能を持たないデバイス(プリンタや IP 電話など)にネットワーク アクセスを許可するのに使用できます。MAC ベース認証では、接続デバイスの MAC アドレスを使用して、ネットワーク アクセス権を付与または拒否します。

この場合、スイッチはクライアントの MAC アドレスと同じ値をユーザ名およびパスワードとして使用し、EAP MD5 機能をサポートします。次の図で説明します。

図 2　MAC ベース認証



この方式には特定のコンフィギュレーションはありません。

Web ベース認証

Web ベース認証は、スイッチ経由でのネットワーク アクセスを要求するエンド ユーザの認証に使用します。スイッチに直接接続しているクライアントの場合、この認証方式を使用すると、クライアントに対してネットワーク アクセスを許可する前に、キャプティブ ポータル機能を使用してクライアントの認証を実行できます。Web ベース認証は、クライアント ベースの認証方式で、レイヤ 2 およびレイヤ 3 両方の複数セッション モードでサポートされます。

この認証方式はポートごとに有効にすることが可能で、あるポートが有効な場合、ネットワークにアクセスするには各ホストが自身を認証する必要があります。そのため、有効なポートでは、認証済みのホストと非認証ホストが混在する場合があります。

あるポートで Web ベース認証が有効な場合、そのポートが未許可のクライアントから受信したトラフィックは、すべてスイッチによりドロップされます。ただし、ARP、DHCP、および DNS パケットは例外で、ドロップされません。これらのパケットは、未許可のクライアントも IP アドレスを取得してホスト名やドメイン名を解決できるように、スイッチによる転送が許可されます。

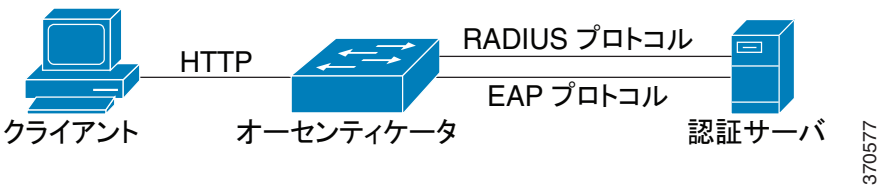
未許可のクライアントから受信した IPv4 の HTTP および HTTPS パケットはすべて、スイッチの CPU にトラップされます。Web ベース認証がポートで有効な場合は、要求されたページが表示される前にログイン ページが表示されます。ユーザは自身のユーザ名とパスワードを入力する必要があり、RADIUS サーバによって EAP プロトコルを使用した認証が実行されます。認証が成功すると、ユーザに通知されます。

これで、ユーザは認証済みセッションを使用できます。そのセッションは、使用中に開いたままになります。使用しない時間が特定の間隔になると、セッションは閉じます。この時間間隔は「待機時間」と呼ばれ、システム管理者によって設定されます。セッションがタイムアウトになると、ユーザ名とパスワードは破棄されます。ゲストが新しいセッションを開くには、それらを再入力する必要があります。

「認証方式とポート モード」を参照してください。

認証が完了すると、そのポートのクライアントから受信したトラフィックはすべてスイッチにより転送されます。次の図で説明します。

図 3　Web ベース認証



ゲスト VLAN が有効になっているポートや、RADIUS による割り当て済み VLAN が有効になっているポートには、Web ベース認証を設定することはできません。

Web ベース認証は次のページをサポートします。

- [ログイン] ページ
- [ログイン成功] ページ

これらのページには、あらかじめ定義された組み込み済みのセットがあります。

これらのページは、[Web ベース認証] ページで変更できます。

カスタマイズした各ページはプレビューできます。設定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。

非認証 VLAN およびゲスト VLAN

非認証 VLAN およびゲスト VLAN は、サプリカント デバイスやポートを認証して許可する必要のないサービスへのアクセスを提供します。

ゲスト VLAN とは、未許可のクライアントに割り当てられている VLAN のことです。ゲスト VLAN、および非認証にする 1 つ以上の VLAN を、[プロパティ] ページから設定できます。

非認証 VLAN とは、許可済みのデバイスやポートだけでなく未許可のデバイスやポートからもアクセス可能な VLAN のことです。

非認証 VLAN には次の特徴があります。

- 非認証 VLAN はスタティック VLAN である必要があり、ゲスト VLAN やデフォルトの VLAN にすることはできません。
- メンバー ポートは、タグ付きのメンバーとして手動で設定する必要があります。
- メンバー ポートは、トランク ポートか一般ポート、またはその両方に指定する必要があります。アクセス ポートを非認証 VLAN のメンバーにすることはできません。

ゲスト VLAN は、設定されている場合、次の特徴を持つスタティック VLAN です。

- ゲスト VLAN は、既存のスタティック VLAN から手動で定義する必要があります。
- ゲスト VLAN は、音声 VLAN や非認証 VLAN としては使用できません。

ゲスト VLAN がサポートされるモードの概要については、「RADIUS VLAN 割り当てのサポート」を参照してください。

ゲスト VLAN におけるホスト モード

ホスト モードは、ゲスト VLAN において次のように作動します。

- **単一ホスト モードと複数ホスト モード**

  未許可のポートで受信する、ゲスト VLAN に所属するトラフィックは、タグなしのものもタグ付きのものも、ゲスト VLAN 経由でブリッジされます。その他のトラフィックはすべて破棄されます。非認証 VLAN に所属するトラフィックは、この VLAN 経由でブリッジされます。

- **複数セッション モード**

  非認証 VLAN に所属せず、未許可のクライアントから受信したトラフィックは、タグなしのものもタグ付きのものも、TCAM ルールを使用してゲスト VLAN に割り当てられ、ゲスト VLAN 経由でブリッジされます。非認証 VLAN に所属するタグ付きトラフィックは、この VLAN 経由でブリッジされます。

  このモードは、ポリシーベース VLAN を持つ同一のインターフェイスには設定できません。

RADIUS VLAN 割り当て、またはダイナミック VLAN 割り当て

[ポート認証] ページでこのオプションが有効になっている場合、許可されたクライアントには RADIUS サーバで VLAN を割り当てることができます。これは、ダイナミック VLAN 割り当て(DVA)、または RADIUS VLAN 割り当てと呼ばれます。このガイドでは、RADIUS による割り当て済み VLAN という用語を使用します。

クライアントから受信した、非認証 VLAN に所属しないトラフィックは、タグなしのものもタグ付きのものも、TCAM ルールを使用して RADIUS による割り当て済み VLAN に割り当てられ、この VLAN 経由でブリッジされます。

RADIUS による割り当て済み VLAN がデバイスで有効な場合の各モードの動作については、「RADIUS VLAN 割り当てのサポート」を参照してください。

DVA が有効なポートでデバイスを認証して許可するために、次のようにしてください。

- RADIUS サーバでそのデバイスを認証し、デバイスに VLAN をダイナミックに割り当てる必要があります。[ポート認証] ページで、[RADIUS VLAN 割り当て] フィールドを [スタティック] に設定できます。このように設定すると、スタティック設定に従ってホストをブリッジできます。
- RADIUS サーバは、RADIUS 属性を次のように指定した DVA をサポートする必要があります:tunnel-type (64) = VLAN (13)、tunnel-media-type (65) = 802 (6)、および tunnel-private-group-id = VLAN ID。

VLAN 名として tunnel-private-group ID 属性を指定する場合、この名前の VLAN をデバイス上で静的に設定する必要があります。この属性内の VLAN ID(2-4094)が使用された場合、サプリカントが認証された後で、VLAN が動的に作成されます。

RADIUS による割り当て済み VLAN が有効な場合、ホスト モードは次のように動作します。

- **単一ホスト モードと複数ホスト モード**

  RADIUS による割り当て済み VLAN に所属するトラフィックは、タグなしのものもタグ付きのものも、この VLAN 経由でブリッジされます。非認証 VLAN に所属していないその他のトラフィックはすべて破棄されます。

- **複数セッション モード**

  クライアントから受信した、非認証 VLAN に所属しないトラフィックは、タグなしのものもタグ付きのものも、TCAM ルールを使用して RADIUS による割り当て済み VLAN に割り当てられ、この VLAN 経由でブリッジされます。

ゲスト VLAN および RADIUS VLAN 割り当てのサポート状況を、認証方式とポート モード別に次の表で示します。

RADIUS VLAN 割り当てのサポート

認証方式	単一ホスト	複数ホスト	複数セッション
802.1x	†	†	†
MAC	†	†	†
Web	**N/S**	**N/S**	**N/S**

凡例:

†: このポート モードは、ゲスト VLAN および RADIUS VLAN 割り当てをサポートします。

N/S: このポート モードは、その認証方式をサポートしません。

違反モード

単一ホスト モードでは、許可済みのポート上の未許可ホストがインターフェイスにアクセスしようとしたときに実行するアクションを設定できます。この作業は [ホストおよびセッション認証] ページで行います。

次のオプションが選択できます。

- [制限]:サプリカント MAC アドレスとは異なる MAC アドレスを持つステーションがインターフェイスにアクセスしようとすると、トラップを生成します。トラップ間の最小時間は 1 秒です。これらのフレームは転送されますが、送信元アドレスは学習されません。
- [保護]:サプリカント アドレスとは異なる送信元アドレスを持つフレームを破棄します。
- [シャットダウン]:サプリカント アドレスとは異なる送信元アドレスを持つフレームを破棄し、ポートをシャットダウンします。

SNMP トラップを、設定可能な最小の時間間隔で送信するようにデバイスを設定することもできます。[秒] に 0 を指定すると、トラップは無効になります。最小の時間を指定しない場合、[制限] モードではデフォルトで 1 秒に設定され、その他のモードでは 0 に設定されます。

待機期間

待機時間とは、認証失敗情報交換後に、ポート(単一ホスト モードまたは複数ホスト モード)またはクライアント(複数セッション モード)が認証の試行を実行できない期間を指します。単一ホスト モードと複数ホスト モードの場合、この期間はポートごとに定義され、複数セッション モードの場合、この期間はクライアントごとに定義されます。待機時間中、スイッチは認証要求を承諾も開始もしません。

この期間は、802.1x ベース認証と Web ベース認証にのみ適用されます。

待機時間に入る前のログインの最大試行回数を指定することもできます。値として 0 を指定すると無制限にログインを試行できるようになります。

待機時間の長さとログインの最大試行回数は、[ポート認証] ページで設定できます。

認証方式とポート モードのサポート

次の表で、サポートされている認証方式とポート モードの組み合わせを示します。

認証方式とポート モード

認証方式	単一ホスト	複数ホスト	複数セッション	
			L3 のデバイス	L2 のデバイス
802.1x	†	†	†	†
MAC	†	†	†	†
Web	N/S	N/S	N/S	†

凡例:

†:このポート モードは、ゲスト VLAN および RADIUS VLAN 割り当てもサポートします。

N/S:この認証方式は、そのポート モードをサポートしません。

注 [ポート認証] ページで [最大ホスト数] パラメータを 1 に設定すると、単一ホスト モードをシミュレートできます。

モードの動作

さまざまな状況で認証済みトラフィックと非認証トラフィックがどのように処理されるかを次の表で説明します。

	非認証トラフィック				認証済みトラフィック			
	ゲスト VLAN を使用		ゲスト VLAN を使用しない		RADIUS VLAN を使用		RADIUS VLAN を使用しない	
	タグなし	タグ付き	タグなし	タグ付き	タグなし	タグ付き	タグなし	タグ付き
単一ホスト	フレームはゲスト VLAN に再マッピングされます	フレームは、ゲスト VLAN か非認証 VLAN に所属する場合を除き、ドロップされます	フレームはドロップされます	フレームは、非認証 VLAN に所属する場合を除き、ドロップされます	フレームは RADIUS による割り当て済み VLAN に再マッピングされます	フレームは、RADIUS VLAN か非認証 VLAN に所属する場合を除き、ドロップされます	フレームはスタティック VLAN 設定に基づいてブリッジされます	フレームはスタティック VLAN 設定に基づいてブリッジされます
複数ホスト	フレームはゲスト VLAN に再マッピングされます	フレームは、ゲスト VLAN か非認証 VLAN に所属する場合を除き、ドロップされます	フレームはドロップされます	フレームは、非認証 VLAN に所属する場合を除き、ドロップされます	フレームは RADIUS による割り当て済み VLAN に再マッピングされます	フレームは、RADIUS VLAN か非認証 VLAN に所属する場合を除き、ドロップされます	フレームはスタティック VLAN 設定に基づいてブリッジされます	フレームはスタティック VLAN 設定に基づいてブリッジされます
ライト複数セッション	N/S	N/S	フレームはドロップされます	フレームは、非認証 VLAN に所属する場合を除き、ドロップされます	N/S	N/S	フレームはスタティック VLAN 設定に基づいてブリッジされます	フレームはスタティック VLAN 設定に基づいてブリッジされます

	非認証トラフィック				認証済みトラフィック			
	ゲスト VLAN を使用		ゲスト VLAN を使用しない		RADIUS VLAN を使用		RADIUS VLAN を使用しない	
	タグなし	タグ付き	タグなし	タグ付き	タグなし	タグ付き	タグなし	タグ付き
完全複数セッション	フレームはゲスト VLAN に再マッピングされます	フレームは、非認証 VLAN に所属する場合を除き、ゲスト VLAN に再マッピングされます	フレームはドロップされます	フレームは、非認証 VLAN に所属する場合を除き、ドロップされます	フレームは RADIUS による割り当て済み VLAN に再マッピングされます	フレームは、非認証 VLAN に所属する場合を除き、RADIUS VLAN に再マッピングされます	フレームはスタティック VLAN 設定に基づいてブリッジされます	フレームはスタティック VLAN 設定に基づいてブリッジされます

802.1x サプリカントとしてのスイッチ

スイッチの 802.1x オーセンティケータとしての機能に加えて、スイッチ自体を、ネイバーからのポート アクセス許可を探索する 802.1x サプリカントとして設定することができます。サプリカントは、RFC3748 で指定されている EAP MD5-Challenge 方式をサポートします。この方式は、名前とパスワードでクライアントを認証します。

インターフェイス上でサプリカントを有効にすると、そのインターフェイスは未承認の状態になります。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承認済みに変わります。

次のようなイベントで、ポート上の 802.1X サプリカント認証が開始されます。

- サプリカントがアップ ステータスのポート上で有効になった。
- ポートのステータスがアップに変わり、サプリカントがそのポート上で有効になった。
- ポート上で EAP 識別子要求メッセージが受信され、サプリカントがそのポート上で有効になった。

802.1x オーセンティケータとサプリカントを単一のインターフェイス上で同時に設定することはできません。

一般的な作業

ワークフロー 1:ポート上で 802.1x 認証を有効にするには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [プロパティ] の順にクリックして、802.1x 認証をグローバルに有効にします。

ステップ 2 ポートベース認証を有効にします。

ステップ 3 [認証方式] を選択します。

ステップ 4 [適用] 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 [セキュリティ] > [802.1x 認証] > [ホストとセッション] **の順にクリックします。**

ステップ 6 必要なポートを選択し、[編集] をクリックします。

ステップ 7 ホストの [認証モード] を設定します。

ステップ 8 [適用] 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 9 [セキュリティ] > [802.1x 認証] > [ポート認証] の順にクリックします。

ステップ 10 ポートを選択して、[編集] をクリックします。

ステップ 11 [管理ポート制御] フィールドを [自動] に設定します。

ステップ 12 認証方式を定義します。

ステップ 13 [適用] 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。

ワークフロー 2:トラップを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [プロパティ] の順にクリックします。

ステップ 2 必要なトラップを選択します。

ステップ 3 [適用] 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。

ワークフロー 3:802.1x ベース認証、MAC ベース認証、または Web ベース認証を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [ポート認証] の順にクリックします。

ステップ 2 必要なポートを選択し、[編集] をクリックします。

ステップ 3 ポートに必要なフィールドを入力します。

このページのフィールドについては、「ポート認証」の説明を参照してください。

ステップ 4 [適用] 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。

ポート間で設定をコピーするには、[設定のコピー] ボタンを使用します。

ワークフロー 4:待機期間を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [ポート認証] の順にクリックします。

ステップ 2 ポートを選択して、[編集] をクリックします。

ステップ 3 [待機期間] フィールドに待機時間を入力します。

ステップ 4 [適用] 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。

ワークフロー 5:ゲスト VLAN を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [プロパティ] の順にクリックします。

ステップ 2 [ゲスト VLAN] フィールドで [有効] を選択します。

ステップ 3 [ゲスト VLAN ID] フィールドでゲスト VLAN を選択します。

ステップ 4 [ゲスト VLAN タイムアウト] を [即時] に設定するか、[ユーザ定義] フィールドに値を入力します。

ステップ 5 [適用] 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。

ワークフロー 6:非認証 VLAN を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [プロパティ] の順にクリックします。

ステップ 2 VLAN を選択して、[編集] をクリックします。

ステップ 3 VLAN を選択します。

ステップ 4 必要に応じて、[認証] をオフにすると、その VLAN は非認証 VLAN に設定されます。

ステップ 5 [適用] 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。

ワークフロー 7:インターフェイス上でサプリカント 802.1x を設定するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x] > [サプリカント クレデンシャル] の順にクリックして、サプリカント クレデンシャルを設定します。

ステップ 2 [セキュリティ] > [802.1x] > [ポート認証] の順にクリックします。

ステップ 3 必要なポートを選択し、[編集] をクリックします。

ステップ 4 サプリカント サポートを有効にして、使用するクレデンシャルを指定します。

このページのフィールドについては、「**ポート認証**」の説明を参照してください。

ステップ 5 [適用] 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。

プロパティ

[プロパティ] ページを使用して、ポートまたはデバイスの認証をグローバルに有効にします。認証を使用するには、各ポートでグローバルにも個別にも認証を有効化する必要があります。

ポートベース認証を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [プロパティ] 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。

  この認証を無効にすると、802.1x、MAC ベース、および Web ベース認証と 802.1x サプリカントが無効になります。

- [認証方式]:ユーザの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 サーバを使用してポート認証を実行します。RADIUS サーバから応答がない場合(例:サーバが停止している場合)、認証処理は実行されず、セッションが許可されます。サーバが利用可能でもユーザのクレデンシャルが正しくない場合は、アクセスが拒否され、セッションは終了します。

  - [RADIUS]:RADIUS サーバ上でユーザを認証します。認証処理が実行されなかった場合、セッションは許可されません。

  - [なし]:ユーザを認証しません。セッションは許可されます。

- [ゲスト 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。ゲスト VLAN が有効な場合、未許可のポートはすべて、[ゲスト VLAN ID] フィールドで選択した VLAN に自動的に参加します。後で許可されたポートはゲスト 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た)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。

- [ゲスト VLAN ID]:VLAN の一覧からゲスト VLAN を選択します。

- [ゲスト VLAN タイムアウト]:期間を [即時] として定義するか、[ユーザ定義] に値を入力します。この値は次にように使用されます。

  リンクアップ後にソフトウェアで 802.1x サプリカントが検出されない場合、または認証に失敗した場合、[ゲスト VLAN タイムアウト] で設定した時間の経過後に、そのポートがゲスト VLAN に追加されます。

  ポートの状態が許可から未許可に変わると、ゲスト VLAN タイムアウトが発生してから、そのポートがゲスト VLAN 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認証失敗トラップ]: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認証成功トラップ]:選択すると、802.1X 認証が成功したときにトラップが生成されます。
  - *[MAC認証失敗トラップ]*:選択すると、MAC 認証が失敗したときにトラップが生成されます。
  - [MAC認証成功トラップ]:選択すると、MAC 認証が成功したときにトラップが生成されます。
  - [サプリカント認証失敗トラップ]:選択すると、サプリカント認証が失敗したときにトラップが生成されます。
  - [サプリカント認証成功トラップ]:選択すると、サプリカント認証が成功したときにトラップが生成されます。
  - [Web認証失敗トラップ]:選択すると、Web 認証が失敗したときにトラップが生成されます。
  - [Web認証成功トラップ]:選択すると、Web 認証が成功したときにトラップが生成されます。
  - [Web認証待機トラップ]:選択すると、待機期間が開始したときにトラップが生成されます。

VLAN 認証テーブルにすべての VLAN が表示され、認証が有効になっているかどうかが表示されます。

ステップ 3 [適用] をクリックします。802.1x 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。

VLAN での認証の有効/無効を変更するには、VLAN を選択し、[編集] をクリックして、[有効] または [無効] のいずれかを選択します。

ポート認証

[ポート認証] 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 [強制許可] 状態の間しか変更できないため、ポート制御を [強制許可] 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 が設定されているポートを LAG のメンバーにすることはできません。802.1x とポート セキュリティは同じポート上で同時に有効にできません。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、[管理ポート制御] を [自動] モードに変更できません。

802.1X 認証を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [ポート認証] の順にクリックします。

このページには、すべてのポートに対する認証設定情報が表示されます。[追加] ページで説明したフィールドに加えて、以下のフィールドがポートごとに表示されます。

- [サプリカント ステータス]:802.1x サプリカントが有効になっているインターフェイスについて、許可または未許可のいずれか。
- [クレデンシャル]:サプリカント インターフェイスに使用されるクレデンシャル構造の名前。使用可能な値は、任意の名前か、サプリカントが有効になっていない場合の N/A です。ポートにサプリカント クレデンシャル名が設定されている場合は、ポート制御パラメータの値がサプリカントになります。この値によって、ポートから受信された他のポート制御情報がオーバーライドされます。

ステップ 2 ポート(OOB ポートを除く)を選択し、[編集] をクリックします。

ステップ 3 パラメータを入力します。

- [インターフェイス]:ポート(OOB ポートを除く)を選択します。
- [現在のポート制御]:現在のポート許可状態が表示されます。状態が [許可] の場合は、そのポートが認証されているか、[管理ポート制御] が [強制許可] に設定されています。一方、状態が [無許可] の場合は、ポートが認証されていないか、[管理ポート制御] が [強制無許可] に設定されています。サプリカントをインターフェイス上で有効にすると、現在のポート制御がサプリカントになります。
- [管理ポート制御]: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。
  - [強制無許可]:インターフェイスの状態を未許可に移行して、インターフェイス アクセスを拒否します。デバイスが、このインターフェイスを介してクライアントに認証サービスを提供することはありません。

- [自動]:そのデバイス上でのポートベースの認証と許可を有効にします。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許可になったり未許可になったりします。
- [強制許可]:認証せずにインターフェイスを許可します。

- [RADIUS VLAN割り当て]: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。
  - [無効]:機能が有効になっていません。
  - [拒否]:RADIUS サーバがサプリカントを許可したのにサプリカント VLAN を提供しなかった場合、そのサプリカントは拒否されます。
  - [スタティック]:RADIUS サーバがサプリカントを許可したのにサプリカント VLAN を提供しなかった場合、そのサプリカントは許可されます。
- [ゲストVLAN]:未許可のポートに対するゲスト VLAN の使用を可能にする場合に選択します。ゲスト VLAN が有効な場合、未許可のポートは、[ポート認証] ページの [ゲストVLAN ID] フィールドで選択した VLAN に自動的に参加します。認証の失敗後、指定したポート上でゲスト VLAN がグローバルに有効になっている場合は、このゲスト VLAN がタグなし VLAN としてその未許可のポートに自動的に割り当てられます。
- [オープンアクセス]: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。「オープンアクセス」を参照してください。
- [802.1xベース認証]:選択すると、そのポートで 802.1X 認証が有効になります。
- [MACベース認証]:選択すると、サプリカント MAC アドレスに基づくポート認証を有効になります。このポートでは 8 個の MAC ベース認証のみ使用できます。

  注 MAC ベース認証が成功するには、RADIUS サーバのサプリカントのユーザ名とパスワードが、サプリカント MAC アドレスである必要があります。MAC アドレスは、小文字で、ピリオドやハイフン(":" や "-")の区切り文字を使用せずに入力する必要があります。例:0020aa00bbcc。
- [Webベース認証]:選択すると、サプリカント MAC アドレスに基づく Web ベース認証が有効になります。
- [定期再認証]:選択すると、[再認証期間] で指定した間隔で、ポートの再認証試行が有効になります。
- [再認証期間]:選択したポートを再認証する間隔を入力します(単位:秒)。
- [即時再認証]:選択すると、ポートの再認証がすぐに有効になります。

- [認証状態]: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。
  - [強制許可]:ポート制御状態が [強制許可](トラフィックの転送)に設定されています。
  - [強制無許可]:ポート制御状態が [強制無許可](トラフィックの廃棄)に設定されています。

  注 [強制許可] でも [強制無許可] でもない場合、ポートは [自動] モードになっており、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。ポートが認証されたら、その状態が [認証済み] と表示されます。
- [時間範囲]:選択すると、認証が指定した時間範囲に制限されます。
- [時間範囲名]:[時間範囲] 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。
- [WBAログインの最大試行回数]: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] を選択して無制限にするか、[ユーザ定義] を選択して制限を設定します。
- [最大WBAサイレンス期間]:そのインターフェイスで許可される Web ベース認証の最大サイレンス期間を入力します。[無制限] を選択して無制限にするか、[ユーザ定義] を選択して制限を設定します。
- [最大ホスト数]:このインターフェイスで使用できる、許可されたホストの最大数を入力します。[無制限] を選択して無制限にするか、[ユーザ定義] を選択して制限を設定します。

  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。
- [待機期間]:待機期間の長さを入力します。
- [EAPの再送信]:サプリカント(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。
- [最大 EAP 要求]: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(サプリカント タイムアウト)場合は、認証プロセスが再開されます。
- [最大 EAP 再試行]:送信可能な EAP 再試行の最大数を入力します。

- [EAP タイムアウト]: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入力します。
- [サプリカントタイムアウト]:EAP 要求がサプ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)。
- [サーバタイムアウト]:デバイスが認証サーバに要求を再送信するまでの経過時間を入力します(単位:秒)。
- [サプリカント]:802.1X を有効にする場合に選択します。
- [クレデンシャル]:このサプリカントに使用するクレデンシャルをドロップダウン リストから選択します。このパラメータは、サプリカントがインターフェイス上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可能な [サプリカント クレデンシャル] ページへのリンクを**編集**します。
- [サプリカント保留タイムアウト]:サプリカントが RADIUS サーバから FAIL 応答を受信してから認証を再始動するまで待機する期間を入力します。

ステップ 4 [適用] をクリックします。ポート設定が、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。

ホストおよびセッション認証

[ホストおよびセッション認証] ページでは、ポート上での 802.1X の動作モード、および違反検出時に実行する処理を設定できます。

これらのモードに関する説明は、「ポート ホスト モード」を参照してください。

ポートの 802.1X 詳細設定を定義するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [ホストおよびセッション認証] の順にクリックします。

このページには、すべてのポートの認証パラメータが表示されます。次のフィールドを除くすべてのフィールドは、[編集] ページに表示されます。

- [違反の数]:単一ホスト モードで、そのインターフェイスが、サプリカントの MAC アドレスとは異なる MAC アドレスを持つホストから受信したパケット数が表示されます。

ステップ 2 ポートを選択して、[編集] 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。OOB ポートは含まれません。
- [ホスト認証]:いずれかのモードを選択します。これらのモードについては、上記の「ポート ホスト モード」の説明を参照してください。

[単一ホストの違反設定](ホスト認証が [単一ホスト] の場合にのみ表示されます)。

- [違反時アクション]:サプリカントの MAC アドレスとは異なる MAC アドレスを持つホストから、単一セッション モードか単一ホスト 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]:パケットを破棄し、ポートをシャットダウンします。ポートは、再アクティブ化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。
- [トラップ間隔]: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指定できるのは、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 [適用] をクリックします。設定が実行コンフィギュレーション ファイルに書き込まれます。

認証済みホスト

認証済みユーザの詳細を表示するには、[セキュリティ] > [802.1x 認証] > [認証済みホスト] 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。

- [ユーザ名]:各ポートで認証されたサプリカント名。
- [ポート]:ポートの数。
- [セッション時間 (DD:HH:MM:SS)]:そのポートでのアクセスをサプリカントが認証および許可されていた時間の長さ。
- [認証方式]:最後のセッションが認証された方式。

- [認証サーバ]:RADIUS サーバ。
- [MACアドレス]:サプリカントの MAC アドレスが表示されます。
- [VLAN ID]:ポートの VLAN。

ロック済みクライアント

ログインに失敗した結果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、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [ロック済みクライアント] の順にクリックします。

次のフィールドが表示されます。

- [インターフェイス]:ロックされたポート。
- [MACアドレス]:現在のポート許可状態が表示されます。状態が [許可] の場合は、そのポートが認証されているか、[管理ポート制御] が [強制許可] に設定されています。一方、状態が [無許可] の場合は、ポートが認証されていないか、[管理ポート制御] が [強制無許可] に設定されています。
- [残り時間(秒)]:ポートがロックされる残り時間。

ステップ 2 ポートを選択します。

ステップ 3 [ロック解除] をクリックします。

Web 認証のカスタマイズ

このページでは、さまざまな言語で Web ベース認証ページをデザインできます。

最大 4 つの言語を追加できます。

注 最大で、HTTP ユーザ 5 名と HTTPS ユーザ 1 名まで、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れば、他のユーザが認証を要求できます。

Web ベース認証に言語を追加するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [Web 認証のカスタマイズ] の順にクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 [言語] 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 選択した言語をデフォルトの言語に設定するには、[デフォルトの表示言語として設定] を選択します。エンド ユーザが言語を選択しない場合は、[デフォルトの言語] ページが表示されます。

ステップ 5 [適用] をクリックすると、設定が実行コンフィギュレーション ファイルに書き込まれます。

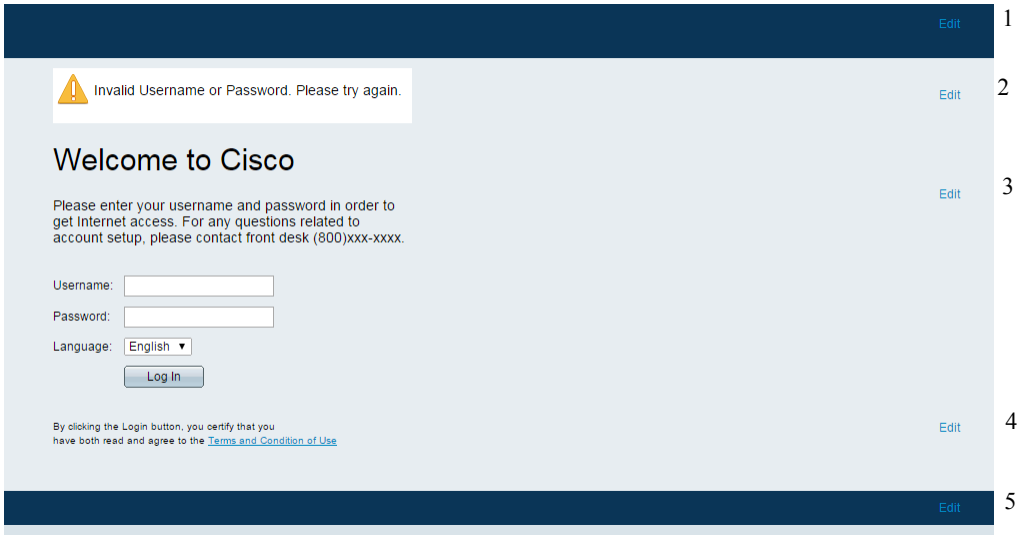
Web 認証ページをカスタマイズするには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [Web 認証のカスタマイズ] の順にクリックします。

このページに、カスタマイズできる言語が表示されます。

ステップ 2 [ログインページの編集] をクリックします。

次のページが表示されます



ステップ 3 [ラベル1を編集] 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。
- [配色]:コントラストのオプションの中からいずれかを選択します。

  [カスタム] 配色を選択した場合は、次のオプションを使用できます。

  - [ページの背景色]:背景色の 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。
  - [ページのテキスト色]:テキスト色の 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。
  - [ヘッダーおよびフッタの背景色]:ヘッダーおよびフッタの背景色の 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。
  - [ヘッダーおよびフッタのテキスト色]:ヘッダーおよびフッタのテキスト色の 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。
  - [ハイパーリンク色]:ハイパーリンク色の ASCII コードを入力します。選択した色が [テキスト] フィールドに表示されます。
- [現在のロゴ画像]:現在のログ画像を含むファイルの名前が表示されます。
- [ロゴ画像]:次のいずれかのオプションを選択します。
  - [なし]: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。
  - [その他]:これを選択すると、カスタマイズしたロゴを入力できます。

  [その他] のロゴ オプションを選択した場合は、次のオプションを使用できます。

  - [ロゴ画像ファイル名]:ロゴのファイル名を入力するか、画像を [参照] します。
  - [アプリケーションテキスト]:ログと一緒に表示するテキストを入力します。
  - [ウィンドウタイトルテキスト]:ログイン ページのタイトルを入力します。

ステップ 4 [適用] をクリックすると、設定が実行コンフィギュレーション ファイルに書き込まれます。

ステップ 5 [ラベル2を編集] をクリックします。次のフィールドが表示されます。

- [無効なユーザ資格情報]: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。
- [サービス使用不可]: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 6 [適用] をクリックすると、設定が実行コンフィギュレーション ファイルに書き込まれます。

ステップ 7 [ラベル3を編集] をクリックします。次のフィールドが表示されます。

- [ウェルカムメッセージ]: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。
- [指示メッセージ]:エンド ユーザに表示される指示を入力します。
- [RADIUS認証]:RADIUS 認証が有効かどうかを表示します。有効な場合は、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。
- [ユーザ名テキストボックス]:表示されるユーザ名テキストボックスを選択します。
- [ユーザ名テキストボックスラベル]:ユーザ名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。
- [パスワードテキストボックス]:表示されるパスワードテキストボックスを選択します。
- [パスワードテキストボックスラベル]:パスワード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。
- [言語選択]: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。
- [言語ドロップダウンラベル]:[言語選択] ドロップダウンのラベルを入力します。
- [ログインボタンラベル]:[ログイン] ボタンのラベルを入力します。
- [ログイン進捗ラベル]: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 8 [適用] をクリックすると、設定が実行コンフィギュレーション ファイルに書き込まれます。

ステップ 9 [ラベル4を編集] をクリックします。次のフィールドが表示されます。

- [使用条件]:選択すると、[使用条件] テキスト ボックスが有効になります。
- [使用条件の警告]:使用条件の入力を指示するために表示されるメッセージのテキストを入力します。
- [使用条件の内容]:使用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 10 [適用] をクリックすると、設定が実行コンフィギュレーション ファイルに書き込まれます。

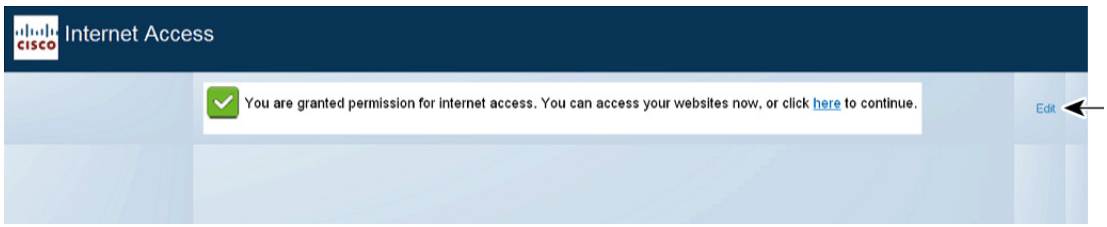
ステップ 11 [ラベル5を編集]。次のフィールドが表示されます。

- [著作権]:選択すると、著作権のテキストが表示されるようになります。
- [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 12 [適用] をクリックすると、設定が実行コンフィギュレーション ファイルに書き込まれます。

ステップ 13 [成功ページの編集] をクリックします。

図 4 次のページが表示されます



ステップ 14 ページの右側にある [編集] ボタンをクリックします。

ステップ 15 [成功メッセージ] を入力します。エンド ユーザがログインに成功すると、このテキストが表示されます。

ステップ 16 [適用] をクリックすると、設定が実行コンフィギュレーション ファイルに書き込まれます。

ログイン画面または成功メッセージをプレビューするには、[プレビュー] をクリックします。

GUI インターフェイスのデフォルトの言語を Web ベース認証のデフォルトの言語に設定するには、[デフォルトの表示言語の設定] をクリックします。

サプリカント クレデンシャル

このページでは、802.1x サプリカントとして設定されたインターフェイスで使用可能なクレデンシャルの作成と設定が可能です。

サプリカントのクレデンシャルを追加するには、次のようにします。

ステップ 1 [セキュリティ] > [802.1x 認証] > [サプリカント クレデンシャル] の順にクリックします。

ステップ 2 [追加] をクリックします。

ステップ 3 次のフィールドを入力します。

- [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。
- [ユーザ名]: クレデンシャル名に関連付けられたユーザ名を入力します。
- [説明]: ユーザに関するテキストを入力します。
- [パスワード]: パスワードのタイプ([暗号化済み] または [プレーンテキスト])を選択して、パスワードを追加します。

ステップ 4 [適用] をクリックすると、設定が実行コンフィギュレーション ファイルに書き込まれます。

22

セキュリティ:セキュア機密データ管理

セキュア機密データ(SSD)とは、デバイスの機密データ(パスワードやキーなど)の保護を実現するためのアーキテクチャです。SSD では、機密データを管理するセキュアなソリューションを提供するために、パスフレーズ、暗号化、アクセス制御、およびユーザ認証を使用します。

SSD は、コンフィギュレーション ファイルの整合性を守り、設定プロセスを保護し、さらに SSD ゼロタッチ自動コンフィギュレーションをサポートするために拡張されています。

はじめに

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、機密データを含むコンフィギュレーション ファイルのセキュアなバックアップと共有を可能にします。

SSD は、機密データの保護を目的のレベルに設定する柔軟性を提供します。機密データの保護レベルには、保護のないプレーンテキストから、デフォルトのパスフレーズによる暗号化に基づく最小限の保護、ユーザ定義のパスフレーズによる暗号化に基づくより良好な保護まであります。

SSD は、認証および承認されたユーザに限り、SSD ルールに従って、機密データの読み取り権限を付与します。デバイスは、ユーザ認証プロセスを通して、ユーザの管理アクセスの認証と承認を行います。

管理者には、SSD を使用しているかどうかにかかわらず、ローカルの認証データベースを使用して認証プロセスを安全にすること、または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を安全にすること、あるいはその両方を行うことをお勧めします。

すなわち SSD は、SSD ルール、SSD プロパティ、およびユーザ認証を使用してデバイスの機密データを保護するものです。またデバイスの SSD ルール、SSD プロパティ、およびユーザ認証の設定は、それ自体が SSD で守られた機密データです。

SSD 管理

SSD 管理には、機密データの処理およびセキュリティを定義するコンフィギュレーション パラメータのコレクションが含まれます。SSD コンフィギュレーション パラメータ自体は、機密データであり SSD によって守られています。

SSD のすべてのコンフィギュレーションは、適正な権限でのみユーザが利用できる SSD ページ経由で実行されます(「SSD ルール」を参照)。

SSD ルール

SSD ルールは、管理チャネル上のユーザ セッションに付与される読み取り権限およびデフォルトの読み取りモードを定義します。

SSD ルールは、ユーザおよび SSD 管理チャネルで一意に決まります。同一のユーザに異なる SSD ルールが存在する可能性がありますが、異なるチャネル向けです。逆に、同一のチャネルに異なるルールが存在する可能性がありますが、異なるユーザ向けです。

読み取り権限は、機密データを表示する方法を決定します。表示方法には、暗号化形式のみ、プレーンテキスト形式のみ、暗号化形式とプレーンテキスト形式の両方、または機密データを表示する権限なしがあります。SSD ルールは、それ自身を機密データとして保護するよう規定します。

デバイスは、合計で 32 の SSD ルールをサポートすることができます。

デバイスはユーザに、ユーザ ID/ユーザ資格情報およびユーザが機密データにアクセスする管理チャネルのタイプの組み合わせに最も良く適合する SSD ルールの SSD 読み取り権限を付与します。

デバイスには、一連の SSD ルールがデフォルトで付属します。管理者は、必要に応じて SSD ルールの追加、削除、および変更ができます。

注 デバイスは、SSD で定義されたすべてのチャネルをサポートしていない場合があります。

SSD ルールの要素

SSD ルールは次の要素を含みます。

- [ユーザタイプ]:サポートされるユーザ型を望ましい順に並べると次のようになります。(ユーザが複数の SSD ルールに一致する場合は、最も望ましいユーザ タイプが適用されます)。
  - [特定]:このルールは特定のユーザに適用されます。
  - [デフォルトユーザ(cisco)]:このルールはデフォルト ユーザ(cisco)に適用されます。
  - [レベル 15]:このルールは特権レベル 15 のユーザに適用されます。
  - [すべて]:このルールはすべてのユーザに適用されます。
- [ユーザ名]:ユーザ タイプが [特定] の場合、ユーザ名が必要です。
- [チャネル]。ルールが適用される SSD 管理チャネルのタイプ。サポートされるチャネルのタイプは次のとおりです。
  - [セキュア]:このルールがセキュアなチャネルのみに適用されるように指定します。デバイスによっては、次のセキュアなチャネルの一部またはすべてをサポートします。
    コンソール ポート インターフェイス、SCP、SSH、および HTTPS。
  - [セキュアでない]:このルールがセキュアでないチャネルのみに適用されるように指定します。デバイスによっては、次のセキュアでないチャネルの一部またはすべてをサポートします。
    Telnet、TFTP、および HTTP。
  - [セキュア XML SNMP]:このルールが XML over HTTPS またはプライバシー機能のある SNMPv3 のみに適用されるように指定します。デバイスが、セキュアな XML および SNMP チャネルのすべてをサポートする場合と一部しかサポートしない場合があります。

- [セキュアでないXML SNMP]:このルールが XML over HTTPS または SNMPv1/v2 およびプライバシー機能のない SNMPv3 のみに適用されるように指定します。デバイスが、セキュアな XML および SNMP チャネルのすべてをサポートする場合と一部しかサポートしない場合があります。

- [読み取り権限]:ルールと関連付けられた読み取り権限。次のものがあります。
  - (最低)[除外]:ユーザはあらゆる形式の機密データへのアクセスを許可されません。
  - (中間)[暗号化のみ]:ユーザ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。
  - (高)[プレーンテキストのみ]:ユーザ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。ユーザに、SSD パラメータへの読み取り権限と書き込み権限がある場合もあります。
  - (最高)[両方]:ユーザは、暗号化およびプレーンテキストの権限の両方を持ち、暗号化された機密データおよびプレーンテキストの機密データへのアクセスが許可されます。ユーザに、SSD パラメータへの読み取り権限と書き込み権限がある場合もあります。

  各管理チャネルは特定の読み取り権限を許可します。これらを次にまとめます。

管理チャネル	許可される読み取り権限オプション
セキュア	両方、暗号化のみ
セキュアでない	両方、暗号化のみ
セキュア XML SNMP	除外、プレーンテキストのみ
セキュアでない XML SNMP	除外、プレーンテキストのみ

- [デフォルトの読み取りモード]:すべてのデフォルトの読み取りモードは、ルールの読み取り権限に従属します。次のオプションが存在しますが、読み取り権限によっては拒否されることがあります。ユーザのユーザ定義済み読み取り権限が、たとえば [除外] であり、さらにデフォルトの読み取りモードが [暗号化] の場合、ユーザ定義済みの読み取り権限が優先します。
  - [除外]:機密データの読み取りを許可しない。
  - [暗号化]:機密データは暗号化形式で提示されます。
  - [プレーンテキスト]:機密データはプレーンテキストで提示されます。

各管理チャネルは特定の読み取り推定を許可します。これらを次にまとめます。

読み取り権限	許可されるデフォルトの読み取りモード
除外	除外
暗号化のみ	*暗号化
プレーンテキストのみ	*プレーンテキスト
両方	*プレーンテキスト、暗号化

* セッションの読み取りモードは、新しい読み取りモードが読み取り権限に違反しない場合には、[SSD プロパティ] ページで一時的に変更することができます。

注　次の点に注意してください。

- [セキュア XML SNMP] および [セキュアでない XML SNMP] 管理チャネルのデフォルトの読み取りモードは、読み取り権限と同じでなければなりません。
- 読み取り権限 [除外] は、[セキュアXML SNMP] および [セキュアでないXML SNMP] 管理チャネルにのみ許可されます。[除外] は、通常のセキュアなチャネルおよびセキュアでないチャネルには許可されません。
- セキュアおよびセキュアでない XML-SNMP 管理チャネルで機密データが [除外] になっている場合、機密データは 0 (null 文字列または数値 0) として提示されます。ユーザが機密データを表示させたい場合は、ルールをプレーンテキストに変更する必要があります。
- デフォルトでは、プライバシー機能のある SNMPv3 のユーザおよび XML-over-secure チャネル権限がある SNMPv3 ユーザは、レベル 15 ユーザと見なされます。
- セキュアでない XML および SNMP (SNMPv1、v2、およびプライバシー機能のない v3) チャネルの SNMP ユーザは、[すべて] のユーザと見なされます。
- SNMP コミュニティ名は、SSD ルールに一致するユーザ名としては使用されません。
- 特定の SNMPv3 ユーザによるアクセスは、SNMPv3 ユーザ名に一致するユーザ名で SSD ルールを設定することで制御できます。
- 読み取りアクセス許可 (プレーンテキストのみまたは両方) 付きのルールを 1 つ以上設置する必要があります。これは、このようなアクセス許可を持っているユーザだけが SSD ページにアクセスできるためです。

- ルールのデフォルトの読み取りモードおよび読み取り権限に対する変更が有効となると、すべてのアクティブな管理セッションの対象ユーザおよびチャネルには直ちに適用されます(変更を加えたセッションは、そのルールが適用可能な場合でも除外されます)。ルールが変更された場合(追加、削除、編集)、システムは対象となるすべての CLI/GUI セッションを更新します。

注 セッションに SSD ルールが適用されると、ログインはそのセッションから変更されます。そのユーザはログアウトしてから再度ログインして変更を確認する必要があります。

注 XML または SNMP コマンドが開始するファイル転送を実行している場合、使用されている基礎となるプロトコルは TFTP です。そのため、セキュアでないチャネル用の SSD ルールが適用されます。

SSD ルールおよびユーザ認証

SSD は、認証および承認されたユーザに限り、SSD ルールに従って SSD 権限を付与します。デバイスは、管理アクセスの認証と承認をユーザ認証プロセスに依存しています。不正アクセスからデバイスや機密データおよび SSD 設定を含むデータを守るために、デバイスのユーザ認証プロセスをセキュアにすることをお勧めします。ユーザ認証プロセスをセキュアにするために、ローカルの認証データベースを使用したり、RADIUS サーバなどの外部認証サーバを経由して通信をセキュアにできます。外部認証サーバとのセキュア通信の設定は機密データであり、SSD によって保護されています。

注 ローカルの認証データベースにあるユーザの資格情報は、すでに SSD と関係のない仕組みによって保護されています。

代替チャネルを使用するアクションをチャネルからユーザが発行した場合、デバイスは SSD ルールから、ユーザの資格情報および代替チャネルに一致する読み取り権限およびデフォルトの読み取りモードを適用します。たとえば、ユーザがセキュアなチャネルからログインして TFTP のアップロード セッションを開始した場合、セキュアでないチャネル(TFTP)上のユーザの SSD 読み取り権限が適用されます。

デフォルトの SSD ルール

デバイスには次の工場出荷時ルールがあります。

ルール キー		ルール アクション	
ユーザ	チャネル	読み取り権限	デフォルトの読み取りモード
レベル 15	セキュア XML SNMP	プレーンテキストのみ	プレーンテキスト
レベル 15	セキュア	両方	暗号化
レベル 15	セキュアでない	両方	暗号化
すべて	セキュアでない XML SNMP	除外	除外
すべて	セキュア	暗号化のみ	暗号化
すべて	セキュアでない	暗号化のみ	暗号化

デフォルト ルールは変更することができますが、削除することはできません。SSD のデフォルト ルールが変更されている場合には、復元することが可能です。

SSD デフォルト読み取りモード セッションのオーバーライド

システムは、ユーザの読み取り権限およびデフォルトの読み取りモードに基づいて、暗号化またはプレーンテキストとして機密データをセッションに含めます。

デフォルトの読み取りモードは、セッションの SSD 読み取り権限と競合しない限り、一時的にオーバーライドできます。この変更は、現在のセッションでただちに有効となり、次のいずれかが発生するまで有効です。

- ユーザが再度変更した。
- セッションが終了した。
- セッションのユーザに適用される SSD ルールの読み取り権限が変更され、セッションの現在の読み取りモードと互換性がなくなった。この場合、セッションの読み取りモードは SSD ルールのデフォルトの読み取りモードに戻ります。

SSD プロパティ

SSD プロパティは、SSD ルールと連動しながら、デバイスの SSD 環境を定義して制御する一連のパラメータです。SSD 環境は、次のプロパティから構成されます。

- 機密データの暗号化を制御するプロパティ。
- 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プロパティ。
- 機密データが現在のセッション内でどのように表示されるかを制御するプロパティ。

パスフレーズ

パスフレーズは、SSD 機能におけるセキュリティの仕組みの基本となるもので、機密データの暗号化および復号化のキーを生成するのに使用します。同じパスフレーズを持つデバイスは、そのパスフレーズから生成されたキーを使用してお互いの暗号化された機密データを復号化できます。

パスフレーズは次のルールに従う必要があります。

- [長さ]:8～16 文字。
- [文字クラス]:パスフレーズには、少なくとも 1 つの大文字、1 つの小文字、1 つの数字、1 つの特殊文字(例:#、$)が含まれなければなりません。

デフォルトおよびユーザ定義のパスフレーズ

すべてのデバイスには、デフォルトのすぐに使えるユーザにすぐ分かるパスフレーズが用意されています。デフォルトのパスフレーズは、コンフィギュレーション ファイルや CLI/GUI には一切表示されません。

セキュリティや保護をもっと改善したい場合、管理者はデバイスの SSD を設定して、デフォルトのパスフレーズではなくユーザ定義のパスフレーズを使用する必要があります。ユーザ定義のパスフレーズは十分に守られた秘密として取り扱われ、デバイスの機密データが侵害されないようにしなければなりません。

ユーザ定義のパスフレーズは、手動でプレーンテキストで設定することができます。またコンフィギュレーション ファイルから派生させることもできます。(「機密データ ゼロタッチ自動コンフィギュレーション」を参照してください)。デバイスは、常に暗号化されたユーザ定義のパスフレーズを表示します。

ローカル パスフレーズ

デバイスは、実行コンフィギュレーションのパスフレーズであるローカル パスフレーズを維持します。SSD は通常、ローカル パスフレーズから生成されるキーを使用して機密データの暗号化と復号化を実行します。

ローカル パスフレーズは、デフォルト パスフレーズとユーザ定義パスフレーズのどちらにでも設定できます。デフォルトでは、ローカル パスフレーズとデフォルト パスフレーズは同じになっています。コマンド ライン インターフェイス(利用できる場合)か Web ベースのインターフェイスのどちらかを使った管理者のアクションによって変更することができます。スタートアップ コンフィギュレーション ファイルがデバイスの実行コンフィギュレーションになると、パスフレーズはスタートアップ コンフィギュレーションファイルのものに自動的に変更されます。デバイスが工場出荷時設定にリセットされると、ローカル パスフレーズはデフォルト パスフレーズにリセットされます。

コンフィギュレーション ファイルのパスフレーズ制御

ファイルのパスフレーズ制御は、ユーザ定義のパスフレーズ、ユーザ定義のパスフレーズから生成されたキーによって暗号化される機密データに対する追加の保護を、テキストベースのコンフィギュレーション ファイルで提供します。

既存のパスフレーズ制御モードを次に示します。

- [制限なし](デフォルト):デバイスは、コンフィギュレーションファイルを生成する際にパスフレーズを含めます。これにより、コンフィギュレーション ファイルを受け取ったすべてのデバイスが、そのファイルからパスフレーズを知ることができるようになります。
- [制限あり]:デバイスは、パスフレーズをコンフィギュレーション ファイルにエクスポートされないようにします。[制限あり] モードは、コンフィギュレーション ファイルにある暗号化された機密データを、パスフレーズを持たないデバイスから保護します。このモードは、コンフィギュレーション ファイルにあるパスフレーズを見られたくない場合に使用します。

デバイスが工場出荷時設定にリセットされると、ローカル パスフレーズはデフォルト パスフレーズにリセットされます。その結果、デバイスは、管理セッション(GUI/CLI)から入力されたユーザ定義のパスフレーズに基づいて暗号化された任意の機密データ、または [制限あり] モードの任意のコンフィギュレーション ファイルにある機密データを復号化できなくなります。これには、デバイスが工場出荷時のデフォルトにリセットされる前にそのデバイス自体が作成したファイルを含みます。これはデバイスがユーザ定義のパスフレーズを使って手動で再設定されるまで維持されます。それ以外の場合、ユーザ定義のパスフレーズはコンフィギュレーション ファイルから取得されます。

コンフィギュレーションファイルの整合性の制御

ユーザは、[コンフィギュレーションファイルの整合性の制御] を使用してコンフィギュレーション ファイルを作成することにより、コンフィギュレーション ファイルを改ざんや変更から保護することができます。デバイスが、ユーザ定義のパスフレーズを [制限なしコンフィギュレーション ファイル パスフレーズ制御] で使用する場合は、[コンフィギュレーションファイルの整合性の制御] を有効にすることをお勧めします。

注意 整合性が保護されたコンフィギュレーション ファイルに何らかの変更が加えられた場合は、改ざんがあったと見なされます。

デバイスは、コンフィギュレーション ファイルの整合性が保護されているかどうかを、そのファイルの SSD 制御ブロックのファイル整合性制御コマンドを調べることによって判断します。ファイルの整合性が保護されていても、デバイスがそのファイルの整合性が完全ではないことを発見した場合には、デバイスはそのファイルを拒否します。それ以外の場合は、ファイルは受理されてその後の処理が行われます。

ファイルがスタートアップ コンフィギュレーション ファイルにダウンロードまたはコピーされた場合、デバイスはテキストベースのコンフィギュレーション ファイルの整合性を確認します。

読み取りモード

各セッションには読み取りモードがあります。読み取りモードは機密データがどのように表示されるかを決定します。読み取りモードは、機密データが通常のテキストとして表示される [プレーンテキスト] と、機密データが暗号化形式で表示される [暗号化] のどちらかです。

コンフィギュレーション ファイル

コンフィギュレーション ファイルにはデバイスのコンフィギュレーションがあります。デバイスには、実行コンフィギュレーション ファイル、スタートアップ コンフィギュレーション ファイル、ミラー コンフィギュレーション ファイル(オプション)、バックアップ コンフィギュレーション ファイルがあります。ユーザは、リモートのファイルサーバとの間でコンフィギュレーション ファイルを手動でアップロードおよびダウンロードすることができます。デバイスは、DHCP を使用した自動コンフィギュレーション ステージの間に、スタートアップ コンフィギュレーション ファイルをリモートのファイルサーバから自動的にダウンロードすることができます。リモートのファイルサーバに保存されているコンフィギュレーション ファイルは、リモート コンフィギュレーション ファイルと呼ばれます。

実行コンフィギュレーション ファイルは、現在デバイスが使用しているコンフィギュレーションを含みます。スタートアップ コンフィギュレーション ファイルにあるコンフィギュレーションは、リブート後に実行コンフィギュレーションになります。実行コンフィギュレーション ファイルおよびスタートアップ コンフィギュレーション ファイルは、内部形式でフォーマットされています。ミラー コンフィギュレーション ファイル、バックアップ コンフィギュレーション ファイル、リモート コンフィギュレーション ファイルは、テキストベースのファイルで、アーカイブ、記録、または復元用として維持されます。ソースのコンフィギュレーション ファイルをコピー、アップロード、およびダウンロードする際に 2 つのファイルのフォーマットが異なっている場合、デバイスは自動的にソースのコンテンツを宛先のフォーマットに変換します。

ファイル SSD インジケータ

実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルをテキストベースのコンフィギュレーション ファイルにコピーする場合、デバイスは、ファイル SSD インジケータを生成してテキストベースのコンフィギュレーション ファイルに配置し、ファイルが暗号化された機密データ、プレーンテキストの機密データ、または機密データが除外されているもののいずれであるかを示します。

- SSD インジケータが存在する場合には、コンフィギュレーション ヘッダー ファイルになければなりません。
- SSD インジケータを含まないテキストベースのコンフィギュレーションは、機密データを含まないと見なされます。

- SSD インジケータは、テキストベースのコンフィギュレーション ファイルの SSD 読み取り権限を強制するために使用されますが、コンフィギュレーション ファイルを実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーする際には無視されます。

ファイル中の SSD インジケータは、コピー中に、暗号化機密データ、プレーンテキスト機密データを含める、または機密データをファイルから除外するためにユーザの指示に従って設定されます。

SSD 制御ブロック

デバイスは、そのスタートアップ コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルからテキストベースのコンフィギュレーション ファイルを生成する際に、ユーザが機密データをファイルに含めるように要求した場合、SSD 制御ブロックをファイルに挿入します。この SSD 制御ブロックは、改ざんから保護されていて、ファイルを生成したデバイスの SSD ルールと SSD プロパティを含みます。SSD 制御ブロックは、それぞれ「ssd-control-start」で始まり、「ssd-control-end」で終わります。

スタートアップ コンフィギュレーション ファイル

デバイスは現在、実行コンフィギュレーション ファイル、バックアップ コンフィギュレーション ファイル、ミラー コンフィギュレーション ファイル、リモート コンフィギュレーション ファイルからスタートアップ コンフィギュレーション ファイルへのコピーをサポートしています。スタートアップ コンフィギュレーションにあるコンフィギュレーションは、リブート後に有効となり、実行コンフィギュレーション ファイルになります。ユーザは、SSD 読み取り権限および管理セッションの現在の SSD 読み取りモードに従って、スタートアップ コンフィギュレーション ファイルから暗号化またはプレーンテキストの機密データを取得することができます。

スタートアップ コンフィギュレーション ファイルの任意の形式の機密データへの読み取りアクセスは、スタートアップ コンフィギュレーション ファイルのパスフレーズとローカルのパスフレーズが異なる場合は除外されます。

SSD は、バックアップ コンフィギュレーション ファイル、ミラー コンフィギュレーション ファイル、リモート コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルへコピーする場合、次のルールを追加します。

- デバイスが工場出荷時のデフォルトにリセットされると、SSD ルールおよび SSD プロパティを含むすべてのコンフィギュレーションがデフォルトにリセットされます。
- ソースのコンフィギュレーション ファイルに暗号化された機密データが含まれるものの、SSD 制御ブロックがない場合、デバイスはソース ファイルを拒絶しコピーは失敗します。

- ソースのコンフィギュレーション ファイルに SSD 制御ブロックがない場合、スタートアップ コンフィギュレーション ファイルの SSD コンフィギュレーションはデフォルトにリセットされます。
- ソースのコンフィギュレーション ファイルの SSD 制御ブロックにパスフレーズがある場合、デバイスはソース ファイルを拒否し、ファイルに SSD 制御ブロックのパスフレーズから生成されたキーによって暗号化されたのではない暗号化された機密データがある場合、コピーは失敗します。
- ソースのコンフィギュレーション ファイルに SSD 制御ブロックがあり、そのファイルの SSD 整合性チェックまたはファイル整合性チェック、あるいはその両方が失敗した場合、デバイスはソース ファイルを拒否してコピーは失敗します。
- ソースのコンフィギュレーション ファイルの SSD 制御ブロックにパスフレーズがない場合、ファイル内のすべての暗号化された機密データは、ローカルのパスフレーズから生成されたキーまたはデフォルトのパスフレーズから生成されたキーのどちらかで暗号化される必要があります。ただし両方のキーを使うことはできません。それ以外の場合、ソース ファイルは拒否されてコピーは失敗します。
- デバイスは、ソースのコンフィギュレーション ファイルの SSD 制御ブロックのパスフレーズ、パスフレーズ制御、およびファイル整合性(ある場合)を、スタートアップ コンフィギュレーション ファイルへ設定します。スタートアップ コンフィギュレーション ファイルの設定は、ソースのコンフィギュレーション ファイルの機密データを暗号化するキーを生成するために使用するパスフレーズを用いて行われます。見あたらない SSD コンフィギュレーションは、デフォルトにリセットされます。
- ソースのコンフィギュレーション ファイルに SSD 制御ブロックがあり、そのファイルにプレーンテキスト、SSD 制御ブロックの SSD コンフィギュレーション以外の機密データがある場合、ファイルは受理されます。

実行コンフィギュレーション ファイル

実行コンフィギュレーション ファイルは、現在デバイスが使用しているコンフィギュレーションを含みます。ユーザは、SSD 読み取り権限および管理セッションの現在の SSD 読み取りモードに従って、実行コンフィギュレーション ファイルから暗号化またはプレーンテキストの機密データを取得することができます。ユーザは、バックアップ コンフィギュレーション ファイルまたはミラー コンフィギュレーション ファイルを、CLI、XML、SNMP などを介して他の管理アクション経由でコピーすることで実行コンフィギュレーション ファイルを変更することができます。

デバイスは、ユーザが実行コンフィギュレーションの SSD コンフィギュレーションを直接変更した場合、次のルールを適用します。

- 管理セッションを開いたユーザが、SSD 権限([両方] または [プレーンテキストのみ] 読み取り権限のいずれか)を持っていない場合、デバイスはすべての SSD コマンドを拒否します。
- ソース ファイルからコピーした場合、ファイル SSD インジケータ、SSD 制御ブロック整合性、および SSD ファイル整合性は検査も強制もされません。
- ソース ファイルからコピーした場合、ソース ファイルのパスフレーズがプレーンテキストだとコピーは失敗します。パスフレーズが暗号化されていると、無視されます。
- パスフレーズを実行コンフィギュレーションに直接(ファイル コピーでなく)設定する場合は、コマンドのパスフレーズはプレーンテキストで入力しなければなりません。それ以外では、コマンドは拒否されます。
- 暗号化された機密データを使ったコンフィギュレーション コマンドは、ローカルのパスフレーズから生成されたキーで暗号化され、実行コンフィギュレーションに設定されます。それ以外は、コンフィギュレーション コマンドはエラーとなり、実行コンフィギュレーション ファイルには組み込まれません。

バックアップ コンフィギュレーション ファイルとミラー コンフィギュレーション ファイル

自動ミラー コンフィギュレーション サービスが有効な場合、デバイスは、スタートアップ コンフィギュレーション ファイルからミラー コンフィギュレーション ファイルを定期的に生成します。デバイスは、必ず暗号化された機密データでミラー コンフィギュレーション ファイルを生成します。そのため、ミラー コンフィギュレーション ファイルのファイル SSD インジケータは、常に暗号化された機密データを含むファイルであることを示します。

デフォルトでは、自動ミラー コンフィギュレーション サービスが有効になります。自動ミラー コンフィギュレーションを有効化または無効化するように設定するには、[各種管理] > [ファイル管理] > [ファームウェア操作] をクリックします。

次のように、SSD 読み取り権限、現在のセッションの読み取りモード、およびソースファイルのファイル SSD インジケータに従って、ユーザは、ミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイル全体を表示、コピー、アップロードすることができます。

- ミラー コンフィギュレーション ファイルまたはバックアップ コンフィギュレーション ファイルにファイル SSD インジケータが存在しない場合、このファイルへのアクセスはすべてのユーザに許されます。

- [両方] の読み取り権限を持つユーザは、すべてのミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイルにアクセスすることができます。しかし、現在のセッションの読み取りモードがファイル SSD インジケータと異なる場合、ユーザには、そのアクションは許可されないことを示すプロンプトが提示されます。
- [プレーンテキストのみ] 権限を持つユーザは、そのファイル SSD インジケータが [除外] または [プレーンテキストのみ] 機密データを示している場合、ミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイルにアクセスすることができます。
- [暗号化のみ] 権限を持つユーザは、そのファイル SSD インジケータが [除外] または [暗号化] 機密データを示している場合、ミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイルにアクセスすることができます。
- [除外] 権限を持つユーザは、そのファイル SSD インジケータが [暗号化] または [プレーンテキスト] 機密データを示している場合、ミラー コンフィギュレーション ファイルおよびバックアップ コンフィギュレーション ファイルにアクセスできません。

ユーザは、ファイル内の機密データ(存在する場合)と競合するファイル SSD インジケータを手動で変更することはできません。それ以外の場合、プレーンテキストの機密データは想定外に漏洩する可能性があります。

機密データ ゼロタッチ自動コンフィギュレーション

SSD ゼロタッチ自動コンフィギュレーションは、暗号化された機密データを持つ対象デバイスの自動コンフィギュレーションです。そのとき機密データの暗号化にそのキーが使われるパスフレーズを使って手動で事前に対象デバイスを設定する必要はありません。

デバイスは、デフォルトで有効となる自動コンフィギュレーションを現在サポートしています。自動コンフィギュレーションが有効であり、ファイル サーバとブート ファイルを指定する DHCP オプションを利用しているデバイスは、ファイル サーバからブート ファイル(リモート コンフィギュレーション ファイル)をスタートアップ コンフィギュレーション ファイルにダウンロードしてからリブートします。

注 ファイル サーバは、DHCP オプション 150 およびデバイス上の静的設定に加え、bootp siaddr および sname フィールドにより指定されます。

ユーザは、暗号化された機密データによって対象デバイスを安全に自動設定することができます。まずコンフィギュレーションを持つデバイスからの自動コンフィギュレーションで使用されるコンフィギュレーション ファイルを作成します。デバイスには次の設定と指定が必要です。

- ファイルの機密データの暗号化
- ファイル コンテンツの整合性の強制
- デバイスおよび機密データへのセキュアなアクセスを適正に制御する、セキュアな認証コンフィギュレーション コマンドと SSD ルールを含める

コンフィギュレーション ファイルがユーザのパスフレーズで生成されていて、SSD ファイルのパスフレーズ制御が [制限あり] の場合、結果のコンフィギュレーション ファイルを目的の対象デバイスに自動設定することが可能です。しかし、自動コンフィギュレーションがユーザ定義のパスフレーズを継承する場合、対象デバイスは、ファイルを生成したゼロタッチではないデバイスと同一のパスフレーズにより手動であらかじめ設定されている必要があります。

コンフィギュレーション ファイルを生成するデバイスが、[制限なし] パスフレーズ制御モードにある場合、デバイスはパスフレーズをファイルに含めます。結果としてユーザは、対象デバイスをパスフレーズであらかじめ手動で設定しなくても、すぐに使えるデバイスや工場出荷時デフォルトのデバイスを含む対象デバイスを、コンフィギュレーション ファイルで自動設定することができます。対象デバイスがパスフレーズを直接コンフィギュレーション ファイルから取得するため、ゼロタッチと呼ばれます。

注 すぐに使える状態または工場出荷時デフォルト状態のデバイスは、デフォルトの匿名ユーザを使用して SCP サーバにアクセスします。

SSD 管理チャネル

デバイスは、telnet、SSH、Web などの管理チャネル経由で管理することができます。SSD はチャネルを、そのセキュリティやプロトコルに基づいて次のタイプに分類します。セキュア、セキュアでない、セキュア XML SNMP、およびセキュアでない XML SNMP です。

次に、SSD が各管理チャネルを「セキュア」または「セキュアでない」のどちらと見なしているかを示します。「セキュアでない」と見なした場合、表はパラレル セキュア チャネルを示します。

管理チャネル	SSD 管理チャネル タイプ	パラレル セキュア管理チャネル
コンソール	セキュア	
Telnet	セキュアでない	SSH
SSH	セキュア	
GUI/HTTP	セキュアでない	GUI/HTTPS
GUI/HTTPS	セキュア	
XML/HTTP	セキュアでない XML SNMP	XML/HTTPS
XML/HTTPS	セキュア XML SNMP	
SNMPv1/v2/v3（プライバシー機能なし）	セキュアでない XML SNMP	セキュア XML SNMP
SNMPv3（プライバシー機能あり）	セキュア XML SNMP（レベル 15 ユーザ）	
TFTP	セキュアでない	SCP
SCP（セキュア コピー）	セキュア	
HTTP ベースのファイル転送	セキュアでない	HTTPS ベースのファイル転送
HTTPS ベースのファイル転送	セキュア	

メニュー CLI とパスワード リカバリ

メニュー CLI インターフェイスは、読み取り権限が [両方] または [プレーンテキストのみ] のユーザだけに許可されます。その他のユーザは拒否されます。メニュー CLI 中の機密データは、常にプレーンテキストとして表示されます。

パスワード リカバリは現在、ブート メニューからアクティブ化され、ユーザは認証なしでターミナルにログオンできます。SSD がサポートされている場合、このオプションはローカルのパスフレーズがデフォルトのパスフレーズと同じ場合にのみ許可されます。デバイスがユーザ定義のパスフレーズで設定されている場合、ユーザはパスワードの復元をアクティブ化できません。

SSD の設定

SSD 機能は次のページで設定されます。

- SSD プロパティは、[SSD プロパティ] ページで設定します。
- SSD ルールは、[SSD ルール] ページで定義します。

SSD プロパティ

[プレーンテキストのみ] または [両方] の SSD 読み取り権限を持つユーザのみが SSD プロパティを設定できます。

グローバル SSD プロパティを設定するには次のようにします。

ステップ 1 [セキュリティ] > [セキュア機密データ管理]> [プロパティ].をクリックします。

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のタイプ]:デフォルトのパスフレーズまたはユーザ定義のパスフレーズのどちらが現在使用されているかを表示します。

ステップ 2 次の [永続的設定] フィールドを入力します。

- [コンフィギュレーション ファイルのパスフレーズの制御]:「コンフィギュレーション ファイルのパスフレーズ制御」で説明されたオプションを選択します。
- [コンフィギュレーションファイルの整合性の制御]: この機能を有効化するには、このフィールドを選択します。「コンフィギュレーションファイルの整合性の制御」を参照してください。

ステップ 3 現在のセッションの読み取りモードを選択します(SSD ルールの要素を参照)。

ステップ 4 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

ローカルのパスフレーズを変更するには次のようにします。

ステップ 1 [ローカル パスフレーズの変更] をクリックしてから新しい [ローカル パスフレーズ] を入力します。

- [デフォルト]: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)]:新しいパスフレーズを入力します。
- [パスフレーズの確認]:新しいパスフレーズを確認します。

ステップ 2 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

SSD ルール コンフィギュレーション

[プレーンテキストのみ] または [両方] の SSD 読み取り権限を持つユーザのみが SSD ルールを設定できます。

SSD ルールを設定するには次のようにします。

ステップ 1 [セキュリティ] > [セキュア機密データ管理] > [SSD ルール] をクリックします。

現在定義されているルールが表示されます。[ルールタイプ] フィールドは、ルールがユーザ定義かデフォルトかを示します。

ステップ 2 新しいルールを追加するには、[追加].をクリックします。次のフィールドを入力します。

- [ユーザ]:ルールを適用するユーザを定義します。次のいずれかのオプションを選択します。
  - [特定のユーザ]:ルールを適用する特定のユーザ名を選択して入力します(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)。
  - [デフォルトユーザ(cisco)]:ルールがデフォルト ユーザに適用されることを示します。
  - [レベル15]:ルールが特権レベル 15 を持つすべてのユーザに適用されます。
  - [すべて]:ルールがすべてのユーザに適用されることを示します。

- [チャネル]:ルール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。次のいずれかのオプションを選択します。
  - [セキュア]:ルールが、セキュアなチャネル(コンソール、SCP、SSH および HTTPS)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。
  - [セキュアでない]: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]:ルールが XML over HTTPS およびプライバシー機能のある SNMPv3 のみに適用されることを示します。
  - [セキュアでないXML SNMP]:ルールが XML over HTTP または SNMPv1/v2 およびプライバシー機能のない SNMPv3、あるいはその両方のみに適用されることを示します。
- [読み取り権限]:ルールと関連する読み取り権限。次のものがあります。
  - [除外]:最も低い読み取り権限。ユーザはいかなるフォームでも機密データを取得することが許可されません。
  - [プレーンテキストのみ]:上記よりも高い読み取り権限。ユーザはプレーンテキストのみで機密データを取得することが許可されます。
  - [暗号化のみ]:中間の読み取り権限。ユーザは暗号化のみで機密データを取得することが許可されます。
  - [両方(プレーンテキストおよび暗号化)]:最も高い読み取り権限。ユーザは、暗号化およびプレーンテキストの権限の両方を持ち、暗号化された機密データおよびプレーンテキストの機密データの取得が許可されます。
- [デフォルトの読み取りモード]:すべてのデフォルトの読み取りモードは、ルールの読み取り権限に従属します。次のオプションが存在しますが、ルールの読み込み権限によっては拒否されることがあります。
  - [除外]:機密データの読み取りを許可しません。
  - [暗号化]:機密データは暗号化形式で提示されます。
  - [プレーンテキスト]:機密データはプレーンテキストで提示されます。

ステップ 3 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

ステップ　4　次のアクションは選択したルールで実行されます。

- ルールの [追加]、[編集]、または [削除]、または [デフォルトへの復元]。
- [すべてのルールをデフォルトに戻す]:ユーザが変更したデフォルト ルールをデフォルト ルールに復元します。

23

セキュリティ:SSH サーバ

ここでは、デバイス上で SSH セッションを確立する方法について説明します。

具体的な内容は、次のとおりです。

概要

SSH サーバ機能を使用すれば、リモート ユーザは、デバイスに対して SSH セッションを確立することができます。これは、セッションが保護されることを除いて、Telnet セッションを確立する場合と同様です。

デバイスは、SSH サーバとして、パスワードと公開キーのどちらかでリモート ユーザを認証する SSH ユーザ認証をサポートします。一方、リモート ユーザは、SSH クライアントとして、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で SSH サーバ認証を実行することができます。

SSH サーバは次のモードで動作できます。

- **内部生成 RSA/DSA キー(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 アドレスを入力し、デバイス上でセッションを開こうとしたときに自動的に認証されます。
- **公開キー モード**:ユーザはデバイス上で定義されます。彼らの RSA/DSA キーは、PuTTY などの外部の SSH サーバ アプリケーションで生成されます。公開キーがデバイス上で入力されます。こうして、ユーザは、外部の SSH サーバ アプリケーションを介してデバイス上で SSH セッションを開くことができます。

一般的な作業

ここでは、SSH サーバ機能を使用して実行される一般的な作業について説明します。

ワークフロー 1:SSH ユーザ認証を使用せずに SSH セッションを構築するために、次の手順を実行します。

ステップ 1 [TCP/UDP サービス] ページで SSH サーバを有効にします。

ステップ 2 [SSH ユーザ認証] ページでパスワードと公開キーによる SSH ユーザ認証を無効にします。

ステップ 3 PUTTY などの SSH クライアント アプリケーションからデバイスに対して SSH セッションを確立します。

ワークフロー 2:パスワードによる SSH ユーザ認証を使用して SSH セッションを構築するために、次の手順を実行します。

ステップ 1 [TCP/UDP サービス] ページで SSH サーバを有効にします。

ステップ 2 [SSH ユーザ認証] ページでパスワードによる SSH ユーザ認証を有効にします。

ステップ 3 PUTTY などの SSH クライアント アプリケーションからデバイスに対して SSH セッションを確立します。

ワークフロー 3:公開キーによる SSH ユーザ認証を使用して SSH セッションを構築するには、次の手順を実行します。管理認証のバイパスをするかどうかは任意です。

ステップ 1 [TCP/UDP サービス] ページで SSH サーバを有効にします。

ステップ 2 [SSH ユーザ認証] ページで公開キーによる SSH ユーザ認証を有効にします。公開キーは、SSH クライアント上で事前に作成しておく必要があり、SSH クライアントがデバイス上で SSH サーバに対する SSH セッションを確立するときに使用されます。

ステップ 3 必要に応じて、[SSH ユーザ認証] ページで管理認証をパスすることによる自動ログインを有効にします。

ステップ 4 [SSH ユーザ認証] ページで SSH ユーザ認証テーブルにユーザとその公開キーを追加します。

ステップ 5 PUTTY などの SSH クライアント アプリケーションからデバイスに対して SSH セッションを確立します。

SSH ユーザ認証

[SSHユーザ認証] ページを使用して、公開キーまたはパスワードによる SSH ユーザ認証を有効にします。ユーザが公開キーを使用して SSH サーバを確立する場合は、ユーザ名と公開キーを SSH ユーザ認証テーブルに入力しておく必要があります。ユーザがパスワードを使用して SSH セッションを確立する場合は、ユーザ名とパスワードを管理アクセス権を持っているユーザのものにする必要があります。

ユーザを追加するためには、外部の SSH キー生成/クライアント アプリケーション(PuTTY など)でユーザの RSA または DSA キーを生成する必要があります。

自動ログイン

[SSHユーザ認証] ページを使用して、ローカル ユーザ データベース内ですでに設定済みのユーザの SSH ユーザ名を作成する場合。次のように、**自動ログイン**機能を設定することによって、追加の認証を避けることができます。

- [有効]:ユーザがローカル データベース内で定義されており、そのユーザが公開キーを使用した SSH 認証をパスした場合は、ローカル データベースのユーザ名とパスワードによる認証が省略されます。

  注 この特定の管理方式(コンソール、Telnet、SSH など)用に設定された認証方式は*ローカル*にする(つまり、*RADIUS* や *TACACS+* ではない)必要があります。詳細については、「管理アクセス方式」を参照してください。

- [無効]:SSH 公開キーによる認証が成功したら、ユーザ名がローカル ユーザ データベース内で設定されている場合でも、[管理アクセス認証] ページで設定された認証方式によってユーザが再度認証されます。

このページはオプションです。SSH でユーザ認証を操作する必要はありません。

認証を有効にしてユーザを追加するには、次のようにします。

ステップ 1 [セキュリティ] > [SSHサーバ] > [SSHユーザ認証] 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。

- [パスワードによる SSH ユーザ認証]: ローカル データベース内で設定されたユーザ名/パスワードを使用して SSH クライアント ユーザの認証を実行する場合に選択します(「ユーザ アカウント」を参照)。

- [公開キーによるSSHユーザ認証]:公開キーを使用して SSH クライアント ユーザの認証を実行する場合に選択します。
- [自動ログイン]:このフィールドは、[公開キーによるSSHユーザ認証] 機能が選択された場合に有効にすることができます。

ステップ 3 [適用] をクリックします。設定値が、実行コンフィギュレーション ファイルに保存されます。

設定されたユーザに関する次のフィールドが表示されます。

- [SSHユーザ名]:ユーザのユーザ名。
- [キータイプ]:RSA キーか DSA キーか。
- [フィンガープリント]:公開キーから生成されるフィンガープリント。

ステップ 4 [追加] をクリックして、新しいユーザを追加し、次のフィールドに値を入力します。

- [SSHユーザ名]:ユーザ名を入力します。
- [キータイプ]:[RSA] と [DSA] のどちらかを選択します。
- [公開キー]:このテキスト ボックスに、外部の SSH クライアント アプリケーション(PuTTY など)で生成された公開キーをコピーします。

ステップ 5 [適用] 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する次のフィールドが表示されます。

- [IPアドレス]:アクティブ ユーザの IP アドレス。
- [SSHユーザ名]:アクティブ ユーザのユーザ名。
- [SSHバージョン]:アクティブ ユーザによって使用される SSH のバージョン。
- [暗号]:アクティブ ユーザの暗号。
- [認証コード]: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ていることを保証します。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サーバ認証] 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。公開/秘密 RSA キーおよび DSA キーは、デバイスが工場出荷時設定からブートしたときに自動的に生成されます。各キーは、該当するユーザ設定キーがユーザによって削除されたときも自動的に作成されます。

RSA または DSA キーを再生成する、または、別のデバイス上で生成された RSA/DSA キーをコピーするには、次のようにします。

ステップ 1 [セキュリティ] > [SSHサーバ] > [SSHサーバ認証] の順にクリックします。

キーごとに次のフィールドが表示されます。

- [キータイプ]:RSA または DSA。
- [キーソース]:[自動生成] または [ユーザ定義]。
- [フィンガープリント]:キーから生成されるフィンガープリント。

ステップ 2 RSA キーと DSA キーのどちらかを選択します。

ステップ 3 次のアクションのいずれかを実行します。

- [生成]:選択されたタイプのキーを生成します。
- [編集]:別のデバイスからのキーをコピーできるようにします。次のフィールドを入力します。
  - [キータイプ]:上記参照。
  - [公開キー]:公開キーを入力します。
  - [秘密キー]:[暗号化済み] または [プレーンテキスト] のどちらかを選択して、秘密キーを入力します。

  [機密データを暗号化して表示] または [機密データを平文で表示] をクリックすると、機密データの表示方法が設定されます。
- [削除]:キーを削除できるようにします。

- [詳細]:生成されたキーを表示できるようにします。[詳細] ウィンドウでは、[機密データを平文で表示] をクリックすることもできます。これをクリックすると、キーが暗号化形式ではなく、平文で表示されます。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] 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。

24

セキュリティ:SSH クライアント

このセクションでは、SSH クライアントとして動作するデバイスについて説明します。

具体的な内容は、次のとおりです。

- 概要
- SSH ユーザ認証
- SSH サーバ認証
- SSH サーバのユーザ パスワードの変更

概要

セキュア コピー (SCP) と SSH

セキュア シェルまたは SSH は、SSH クライアント(この場合はデバイス)と SSH サーバとの間で、セキュリティの確保されたチャネル上でデータを交換することを可能にするネットワーク プロトコルです。

SSH クライアントによりユーザは、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コンフィギュレーション 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、ユーザ名/パスワードなどの機密データが盗まれないことが保証されます。

セキュア コピー (SCP) は、ファームウェア、ブート イメージ、コンフィギュレーション ファイル、言語ファイル、およびログ ファイルを、中央 SCP サーバからデバイスに安全に転送するために使用されます。

SSH において、デバイス上で実行される SCP は SSH クライアント アプリケーションであり、SCP サーバは SSH サーバ アプリケーションです。

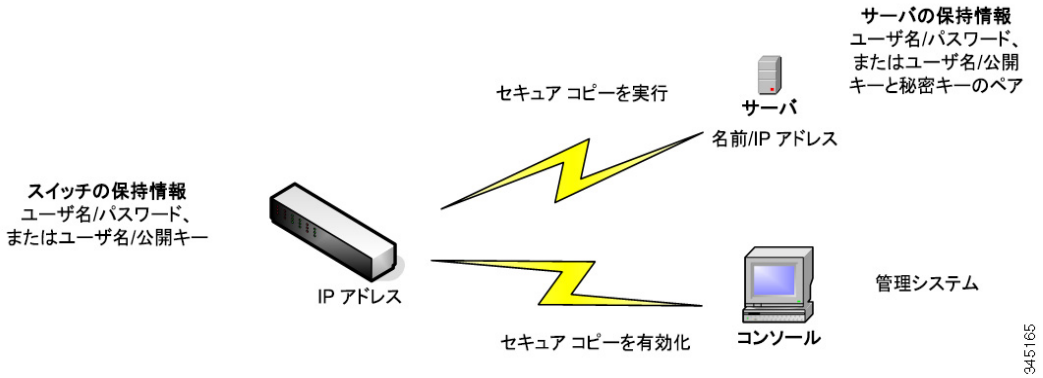
TFTP または HTTP を通じてファイルがダウンロードされる際、データ転送のセキュリティは確保されません。

SCP を通じてファイルがダウンロードされる場合、セキュリティが確保されたチャネルを通じて SCP サーバからデバイスに情報がダウンロードされます。そのセキュア チャネルの作成の前に、ユーザが操作を実行する許可を得るための認証が実行されます。

認証情報は、デバイス上でも SSH サーバ上でもユーザが入力する必要があります。ただし、このガイドではサーバの操作については説明しません。

SCP 機能を使用したネットワーク設定の典型的な処理について、以下の図に示します。

典型的なネットワーク設定処理



SSH サーバ認証

SSH クライアントとしてのデバイスは、信頼できる SSH サーバとのみ通信します。SSH サーバ認証が無効になっている場合(デフォルトの設定)、どの SSH サーバも信頼できるものと見なされます。SSH サーバ認証がオンの場合、ユーザは、信頼できるサーバのためのエントリを信頼 SSH サーバ テーブルに追加する必要があります。このテーブルには、SSH 信頼サーバごとに以下の情報が格納されます。最大 16 個のサーバについて、以下の情報が含まれます。

- サーバの IP アドレス/ホスト名
- サーバの公開キー フィンガープリント

SSH サーバ認証がオンの場合、デバイス上で実行されている SSH クライアントは、以下の認証プロセスを使用して SSH サーバの認証を実行します。

- 受信した SSH サーバ公開キーのフィンガープリントがデバイスにより計算されます。

- デバイスにより、SSH 信頼サーバ テーブルから SSH サーバの IP アドレス/ホスト名が検索されます。以下のいずれか 1 つが可能です。
  - 一致するものが検出された場合、サーバの IP アドレス/ホスト名とそのフィンガープリントの両方について、サーバが認証されます。
  - 一致する IP アドレス/ホスト名は検出されるものの、一致するフィンガープリントは見つからない場合、検索が続行されます。一致するフィンガープリントが見つからない場合、検索は完了し、認証は失敗します。
  - 一致する IP アドレス/ホスト名が見つからない場合、検索は完了し、認証は失敗します。
- 信頼サーバのリストの中に SSH サーバのエントリが見つからない場合、プロセスは失敗します。

即使用可能デバイス(出荷時設定のデバイス)の自動設定をサポートするため、デフォルトでは SSH サーバ認証が無効になっています。

SSH ユーザ認証

デバイス(SSH クライアント)が SSH サーバに対する SSH セッションを確立しようとしたときに、SSH サーバはさまざまな方法でクライアントを認証します。それらについて、以下に説明します。

パスワード

パスワード方式を使用するには、まず、ユーザ名/パスワードが SSH サーバ上で確立されていなければなりません。これは、デバイスの管理システムでは実行されません。ただし、サーバ上でユーザ名が確立された後に、デバイスの管理システムによりサーバパスワードを変更することは可能です。

その後、デバイス上でユーザ名/パスワードを作成する必要があります。デバイスが SSH サーバに対する SSH セッションを確立しようとしたときに、デバイスから提供されるユーザ名/パスワードがサーバ上のユーザ名/パスワードと一致する必要があります。

データは、セッション中にネゴシエートされるワンタイム対称キーを使用して暗号化できます。

管理対象の各デバイスには、それぞれ独自のユーザ名/パスワードが必要です。一方、スイッチについては、複数のスイッチで同じユーザ名/パスワードを使用できます。

パスワード方式は、デバイスでのデフォルトの方式です。

公開/秘密キー

SSH サーバによるクライアント認証に公開/秘密キー方式を使用するには、SSH クライアントであるデバイス上でユーザを作成して、公開/秘密キーのペアを生成/インポートします。その後で、SSH サーバ上で同じユーザを作成し、SSH クライアントで生成/入力された公開キー(またはフィンガープリント)を SSH サーバにコピーします。ユーザを作成して、公開キー(またはフィンガープリント)を SSH サーバにコピーする操作については、このガイドでは扱いません。

RSA と DSA のデフォルト キー ペアは、デバイス ブート時に生成されます。それらのキーのうちの 1 つが、SSH サーバからダウンロードするデータの暗号化のために使用されます。デフォルトでは RSA キーが使用されます。

ユーザがそれらのキーの一方または両方を削除した場合、それらは再生成されます。

公開/秘密キーは、暗号化されてデバイスのメモリに保管されます。キーはデバイスの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、暗号化された形またはプレーンテキストの形でユーザに対して表示可能です。

秘密キーを別のデバイスの秘密キーに直接コピーすることはできないため、秘密キーをデバイスからデバイスへコピーするインポート メソッドが存在します(「*キーのインポート*」を参照)。

キーのインポート

キー方式の場合、個々のデバイスに対して公開/秘密キーをそれぞれ別個に作成する必要があります。セキュリティ上の理由から、それらの秘密キーを、あるデバイスから別のデバイスに直接コピーすることはできません。

ネットワーク内に複数のスイッチがある場合、各公開/秘密キーを作成してからそれぞれ個別に SSH サーバにロードしなければならないため、全スイッチの公開/秘密キーを作成する処理には時間がかかります。

この処理を簡素化するため、暗号化された秘密キーをシステム内の全スイッチに安全な方法で転送することを可能にする付加的な機能があります。

デバイス上で秘密キーが作成される際は、それに関連する*パスフレーズ*を作成することも可能です。このパスフレーズは、秘密キーを暗号化して残りのスイッチにインポートするために使用されます。それにより、すべてのスイッチで同じ公開/秘密キーを使用することが可能になります。

デフォルト パスワード

デフォルトで、パスワードによる SSH ユーザ認証が有効になっており、ユーザ名/パスワードは「anonymous」です。

ユーザは、認証のための以下の情報を設定する必要があります。

- 使用する認証方式。
- ユーザ名/パスワードまたは公開/秘密キーのペア。

サポートされるアルゴリズム

デバイス(SSH クライアントとして動作)と SSH サーバの間の接続が確立済みの場合、クライアントと SSH サーバは、SSH トランスポート層で使用するアルゴリズムを決定するためにデータをやり取りします。

クライアント側では、以下のアルゴリズムがサポートされています。

- キー交換アルゴリズム-diffie-hellman
- 暗号化アルゴリズム
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - Chacha
  - Poly1305
- メッセージ認証コード アルゴリズム
  - hmac-sha1

注 圧縮アルゴリズムはサポートされていません。

作業を開始する前に

SCP 機能を使用するには、その前に、以下の操作を実行する必要があります。

- パスワード認証方式を使用する場合、SSH サーバ上でユーザ名/パスワードをセットアップする必要があります。
- 公開/秘密キー認証方式を使用する場合、SSH サーバ上で公開キーを保管する必要があります。

一般的な作業

ここでは、SSH クライアントとしてのデバイスで実行される共通タスクについて説明します。ここで参照されているページはすべて、メニュー ツリーのうち [SSHクライアント] の分岐の下にあるページです。

ワークフロー 1:SSH クライアントを設定し、リモート SSH サーバとの間でデータをやり取りするには、次の手順を実行します。

ステップ 1 パスワード方式と公開/秘密キー方式のどちらを使用するかを決定します。[SSH ユーザ認証] ページを使用します。

ステップ 2 パスワード方式が選択された場合、以下の手順を実行します。

a. 実際にセキュア データ転送をアクティブにする際、[SSH ユーザ認証] ページでグローバル パスワードを作成するか、[ファームウェア操作] または [ファイル操作] ページで一時パスワードを作成します。

b. SCP を使用し、[ファームウェア操作] ページの [SCP] オプションを選択することにより、ファームウェア、ブート イメージ、または言語ファイルをアップグレードします。このページでは、パスワードを直接入力するか、または [SSH ユーザ認証] ページで入力したパスワードを使用することができます。

c. SCP を使用し、[ファイル操作] ページの [SCP経由(SSHを使用)] オプションを選択することにより、コンフィギュレーション ファイルをダウンロード/バックアップします。このページでは、パスワードを直接入力するか、または [SSH ユーザ認証] ページで入力したパスワードを使用することができます。

ステップ 3 リモート SSH サーバ上でユーザ名/パスワードをセットアップするか、パスワードを変更します。これはサーバに依存した作業であり、ここでは説明しません。

ステップ 4 公開/秘密キー方式を使用する場合は、以下の手順を実行します。

a. RSA と DSA のどちらのキーを使用するかを選択し、ユーザ名を作成した後、公開/秘密キーを生成します。

b. [詳細] ボタンをクリックすることにより、生成されたキーを表示し、ユーザ名と公開キーを SSH サーバに転送します。これはサーバに依存した作業であり、ここでは説明しません。

c. SCP を使用し、[ファームウェア操作] ページの [SCP] オプションを選択することにより、ファームウェアをアップグレード/バックアップします。

d. SCP を使用し、[ファイル操作] ページの [SCP] オプションを選択することにより、コンフィギュレーション ファイルをダウンロード/バックアップします。

ワークフロー 2:公開/秘密キーを 1 つのデバイスから別のデバイスにインポートするには、次の手順を実行します。

ステップ 1 [SSH ユーザ認証] ページで公開/秘密キーを生成します。

ステップ 2 [SSD プロパティ] ページで SSD のプロパティを設定し、新しいローカル パスフレーズを作成します。

ステップ 3 [詳細] をクリックして、生成された暗号化キーを表示し、それらを [詳細] ページから外部デバイスにコピーします(Begin および End フッタを含む)。公開キーと秘密キーを別個にコピーします。

ステップ 4 もう一方のデバイスにログオンし、[SSH ユーザ認証] ページを開きます。必要なキーのタイプを選択して [編集] をクリックします。公開/秘密キーを貼り付けます。

ステップ 5 [適用] をクリックして、公開/秘密キーを第 2 のデバイスにコピーします。

ワークフロー 3:SSH サーバ上でパスワードを変更するには、次の手順を実行します。

ステップ 1 [SSH サーバのユーザ パスワードの変更] ページでサーバを特定します。

ステップ 2 新しいパスワードを入力します。

ステップ 3 [適用] をクリックします。

ワークフロー 4:信頼サーバを定義するには、次の手順を実行します。

ステップ 1 [SSH サーバ認証] ページで SSH サーバ認証を有効にします。

ステップ 2 [追加] をクリックして、新しいサーバを追加し、その識別情報を入力します。

ステップ 3 [適用] をクリックして、サーバを信頼 SSH サーバ テーブルに追加します。

SSH ユーザ認証

このページは、パスワード方式が選択されている場合は SSH ユーザ認証方式を選択したり、デバイス上のユーザ名とパスワードを設定したりするため、また、公開/秘密キー方式が選択されている場合は RSA または DSA キーを生成するために使用されます。

認証方式を選択し、ユーザ名/パスワード/キーを設定するには、次の手順を実行します。

ステップ 1 [セキュリティ] > [SSHクライアント] > [SSHユーザ認証] をクリックします。

ステップ 2 [SSHユーザ認証方式] を選択します。これは、セキュア コピー用に定義されているグローバルな方式です (SCP)。次のいずれかのオプションを選択します。

- [パスワード]: 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、デフォルトのパスワードをそのまま受け入れます。
- [RSA公開キーによる]: これが選択されている場合、[SSHユーザキーテーブル] のブロックで RSA の公開キーと秘密キーを作成します。
- [DSA公開キーによる]: これが選択されている場合、[SSHユーザキーテーブル] のブロックで DSA の公開/秘密キーを作成します。

ステップ 3 (どの方式が選択されている場合でも) [ユーザ名] を入力するか、またはデフォルトのユーザ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なければなりません。

ステップ 4 [パスワード] 方式が選択されている場合は、パスワード ([暗号化] または [プレーンテキスト]) を入力するか、またはデフォルトの暗号化パスワードをそのまま受け入れます。

ステップ 5 次のいずれかの操作を実行します。

- [適用]: 選択した認証方式が、そのアクセス方式に割り当てられます。
- [デフォルトのクレデンシャルの復元]: デフォルトのユーザ名とパスワード (anonymous) が復元されます。
- [機密データを平文で表示]: 現在のページの秘密データがプレーンテキストとして表示されます。

[SSHユーザキーテーブル]: 各キーについて、以下のフィールドが含まれています。

- [キータイプ]: RSA または DSA。
- [キーソース]: [自動生成] または [ユーザ定義]。
- [フィンガープリント]: キーから生成されるフィンガープリント。

ステップ 6 RSA キーまたは DSA キーを処理するには、[RSA] か [DSA] を選択してから、以下の操作のいずれかを実行します。

- [生成]:新しいキーを生成します。
- [編集]:別のデバイスにコピー/ペーストするキーを表示します。
- [削除]:キーを削除します。
- [詳細]:キーを表示します。

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。

ステップ 1 [セキュリティ] > [SSHクライアント] > [SSHサーバ認証] をクリックします。

ステップ 2 [有効] を選択して、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 SSH サーバとの通信に使用されるメッセージ用ソース IPv4 アドレスとして IPv4 アドレスを使用するソース 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 SSH サーバとの通信に使用されるメッセージ用ソース IPv6 アドレスとして IPv6 アドレスを使用するソース インターフェイスを選択します。

  注 [自動] オプションが選択されている場合、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。

ステップ 3 [適用] をクリックします。

ステップ 4 [追加] をクリックし、SSH 信頼サーバについての以下のフィールドを入力します。

- [サーバ指定方法]:SSH サーバを特定するための方法を 1 つ選択します。
  - [IPアドレス]:これが選択されている場合、以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]:これが選択されている場合、[サーバの IP アドレス/名前] 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 アドレスで SSH サーバを指定することを選択した場合、その IP アドレスが IPv4 アドレスなのか、それとも IPv6 アドレスなのかを選択します。
- [IPv6アドレスタイプ]:SSH サーバ IP アドレスが IPv6 アドレスの場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能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]: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。
- [ログサーバのIPアドレス/名前]:[サーバ指定方法] での選択内容に応じて、SSH サーバの IP アドレスか、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]:SSH サーバのフィンガープリントを入力します(そのサーバからコピーしたもの)。

ステップ 5 [適用] をクリックします。信頼できるサーバの定義が、実行コンフィギュレーション ファイルに保存されます。

SSH サーバのユーザ パスワードの変更

SSH サーバ上でパスワードを変更するには、次のようにします。

ステップ 1 [セキュリティ] > [SSHクライアント] > [SSHサーバのユーザパスワードの変更] をクリックします。

ステップ 2 次のフィールドを入力します。

- [サーバ指定方法]:[IPアドレス] か [名前] のいずれかを選択することにより、SSH サーバを定義します。[ログサーバのIPアドレス/名前] フィールドに、サーバの名前またはサーバの IP アドレスを入力します。

- [IPバージョン]:IP アドレスで SSH サーバを指定することを選択した場合、その IP アドレスが IPv4 アドレスなのか、それとも IPv6 アドレスなのかを選択します。
- [IPv6アドレスタイプ]:SSH サーバ IP アドレスが IPv6 アドレスの場合、IPv6 アドレス タイプを選択します。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能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]: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。
- [ログサーバのIPアドレス/名前]:[サーバ指定方法] での選択内容に応じて、SSH サーバの IP アドレスか、またはその名前のいずれかを入力します。
- [ユーザ名]:これは、サーバで定義されているユーザ名と一致していなければなりません。
- [古いパスワード]:これは、サーバで定義されているパスワードと一致していなければなりません。
- [新しいパスワード]:新しいパスワードを入力し、[パスワードの確認] フィールドでその確認入力をします。

ステップ 3 [適用] をクリックします。SSH サーバ上のパスワードが変更されます。

25

セキュリティ:IPv6 ファースト ホップ セキュリティ

ここでは、IPv6 ファースト ホップ セキュリティ(FHS)の動作と GUI での設定方法を説明します。

具体的な内容は、次のとおりです。

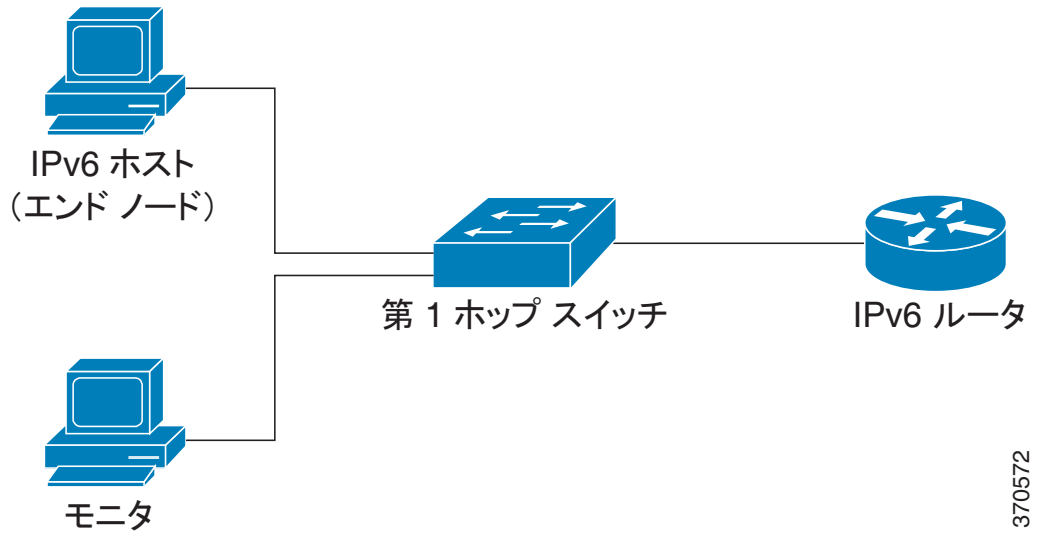
- IPv6 ファースト ホップ セキュリティの概要
- ルータ アドバタイズメント ガード
- ネイバー探索インスペクション
- DHCPv6 ガード
- ネイバー バインディング完全性
- IPv6 ソース ガード
- 攻撃に対する保護
- ポリシー、グローバル パラメータ、およびシステム デフォルト
- 一般的な作業
- デフォルト設定とコンフィギュレーション
- Web GUI を介した IPv6 ファースト ホップ セキュリティの設定

IPv6 ファースト ホップ セキュリティの概要

IPv6 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(図 1 を参照)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。

図 1 IPv6 ファースト ホップ セキュリティの設定



IPv6 ファースト ホップ セキュリティの別個の独立したインスタンスが、この機能が有効になっている各 VLAN 上で動作します。

略称

名前	説明
CPA メッセージ	認証パス アドバタイズメント メッセージ
CPS メッセージ	認証パス請求メッセージ
DAD-NS メッセージ	重複アドレス検出ネイバー送信要求メッセージ
FCFS-SAVI	先着順 - 送信元アドレス検証改善

名前	説明
NA メッセージ	ネイバー アドバタイズメント メッセージ
NDP	ネイバー探索プロトコル
NS メッセージ	ネイバー送信要求メッセージ
RA メッセージ	ルータ アドバタイズメント メッセージ
RS メッセージ	ルータ送信要求メッセージ
SAVI	送信元アドレス検証改善

IPv6 ファースト ホップ セキュリティのコンポーネント

IPv6 ファースト ホップ セキュリティには次の機能が含まれます。

- IPv6 ファースト ホップ セキュリティの共通機能
- RAガード
- ND インスペクション
- ネイバー バインディング完全性
- DHCPv6 ガード
- IPv6 ソース ガード

これらのコンポーネントは VLAN 上で有効または無効にできます。

各機能には、vlan_default および port_default という 2 つの空の定義済みポリシーが用意されています。前者はユーザ定義ポリシーにアタッチされていない各 VLAN にアタッチされ、後者はユーザ定義ポリシーにアタッチされていない各インターフェイスおよび VLAN に接続されます。これらのポリシーをユーザが明示的にアタッチすることはできません。「ポリシー、グローバル パラメータ、およびシステム デフォルト」を参照してください。

IPv6 ファースト ホップ セキュリティのパイプ

VLAN 上で IPv6 ファースト ホップ セキュリティが有効な場合、スイッチは次のメッセージをトラップします。

- ルータ アドバタイズメント(RA)メッセージ
- ルータ送信要求(RS)メッセージ

- ネイバー アドバタイズメント(NA)メッセージ
- ネイバー送信要求(NS)メッセージ
- ICMPv6 リダイレクト メッセージ
- 認証パス アドバタイズメント(CPA)メッセージ
- 認証パス請求(CPS)メッセージ
- DHCPv6 メッセージ

トラップされた RA、CPA、および ICMPv6 リダイレクト メッセージは、RA ガード機能に渡されます。RA ガードはこれらのメッセージを検証し、不正なメッセージをドロップして、有効なメッセージを ND インスペクション機能に渡します。

ND インスペクションはこれらのメッセージを検証し、不正なメッセージをドロップして、有効なメッセージを IPv6 ソース ガード機能に渡します。

トラップされた DHCPv6 メッセージは、DHCPv6 ガード機能に渡されます。DHCPv6 ガードはこれらのメッセージを検証し、不正なメッセージをドロップして、有効なメッセージを IPv6 ソース ガード機能に渡します。

トラップされたデータ メッセージは、IPv6 ソース ガード機能に渡されます。IPv6 ソース ガードは受信したメッセージ(トラップしたデータ メッセージ、ND インスペクションから受信した NDP メッセージ、および DHCPv6 ガードから受信した DHCPv6 メッセージ)をネイバー バインディング テーブルを使用して検証し、不正なメッセージをドロップして、有効なメッセージをフォワーディングに渡します。

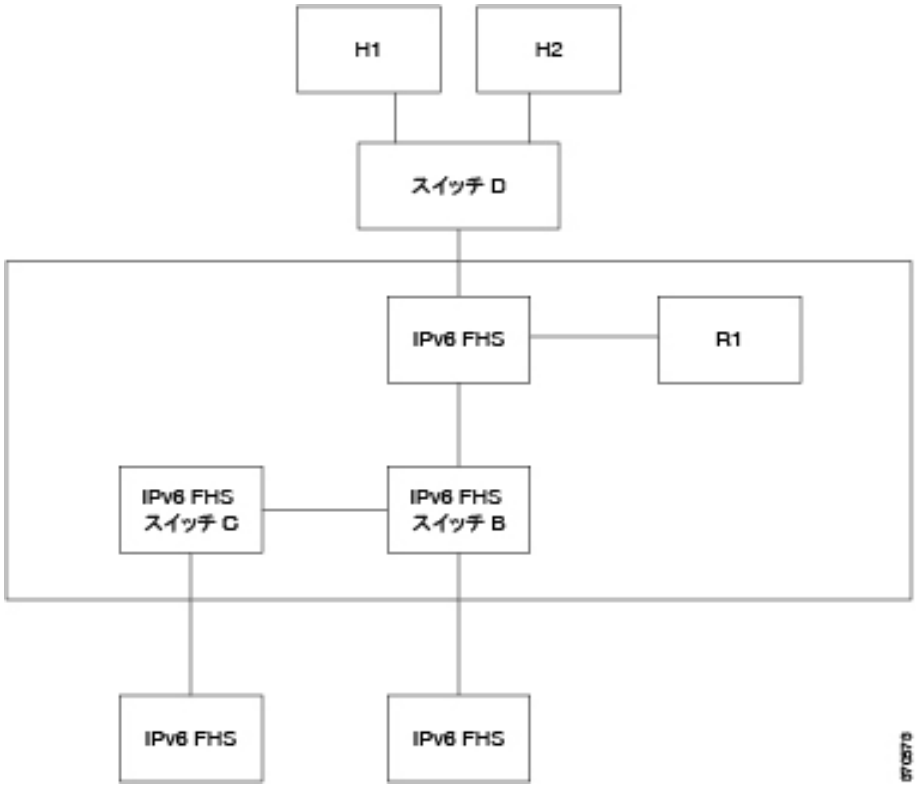
ネイバー バインディング完全性は、受信したメッセージ(NDP メッセージと DHCPv6 メッセージ)からネイバーを学習し、それらをネイバー バインディング テーブルに保存します。さらに、スタティック エントリを手動で追加することもできます。アドレスを学習した後、NBI 機能はフレームをフォワーディングに渡します。

トラップされた RS、CPS NS および NA メッセージも ND インスペクション機能に渡されます。ND インスペクションはこれらのメッセージを検証し、不正なメッセージをドロップして、有効なメッセージを IPv6 ソース ガード機能に渡します。

IPv6 ファースト ホップ セキュリティの境界

IPv6 ファースト ホップ セキュリティのスイッチにより、信頼できるエリアと信頼されていないエリアを分ける境界を形成できます。境界内に含まれるすべてのスイッチは、IPv6 ファースト ホップ セキュリティをサポートし、この境界内のホストやルータは信頼されているデバイスと見なされます。たとえば、図 2 では、スイッチ B とスイッチ C は保護エリア内にある内部リンクです。

図 2　IPv6 ファースト ホップ セキュリティの境界



ネイバー バインディング ポリシー設定画面の **device-role** コマンドで、境界を指定します。

IPv6 ファースト ホップ セキュリティの各スイッチが、エッジでパーティションに分割されているネイバーのバインディングを確立します。このようにして、バインディング エントリが IPv6 ファースト ホップ セキュリティのデバイスに広まって、境界が形成されます。IPv6 ファースト ホップ セキュリティのデバイスはこのようにして境界内にバインディング完全性を提供でき、各デバイスですべてのアドレスのバインディングを設定する必要はありません。

ルータ アドバタイズメント ガード

ルータ アドバタイズメント(RA)ガードは、トラップされた RA メッセージを処理する最初の FHS 機能です。RA ガードは次の機能をサポートしています。

- 受信した RA、CPA、および ICMPv6 リダイレクト メッセージのフィルタリング。
- 受信した RA メッセージの検証。

受信した RA、CPA、および IPCMv6 リダイレクト メッセージのフィルタリング

RA ガードは、ロールがルータではないインターフェイスで受信された RA メッセージと CPA メッセージを廃棄します。インターフェイスのロールは、[RA ガード設定] ページから設定します。

RA メッセージの検証

RA ガードは、インターフェイスにアタッチされている RA ガード ポリシーに基づくフィルタリングを使用して、RA メッセージを検証します。これらのポリシーは、[RA ガード設定] ページから設定できます。

検証に合格しなかったメッセージはドロップされます。FHS 共通コンポーネント上でロギング パケット ドロップ設定が有効になっている場合、レート制限付きの SYSLOG メッセージが送信されます。

ネイバー探索インスペクション

ネイバー探索(ND)インスペクションは次の機能をサポートしています。

- 受信したネイバー探索プロトコル メッセージの検証。
- 出力フィルタリング

メッセージの検証

ND インスペクションは、インターフェイスにアタッチされている ND インスペクション ポリシーに基づいて、ネイバー探索プロトコル メッセージを検証します。このポリシーは、[ND インスペクション設定] ページから定義できます。

ポリシーで定義されている検証に合格しなかったメッセージはドロップされ、レート制限付きの SYSLOG メッセージが送信されます。

出力フィルタリング

ND インスペクションは、ホスト インターフェイスとして設定されているインターフェイスでの RS メッセージと CPS メッセージのフォワーディングをブロックします。

DHCPv6 ガード

DHCPv6 ガードは、トラップされた DHCPv6 メッセージを処理します。DHCPv6 ガードは次の機能をサポートしています。

- 受信した DHCPv6 メッセージのフィルタリング。

  DHCP ガードは、ロールがクライアントであるインターフェイスで受信された DHCPv6 応答メッセージを廃棄します。インターフェイスのロールは、[DHCPv6 ガード設定] ページから設定します。

- 受信した DHCPv6 メッセージの検証。

  DHCPv6 ガードは、インターフェイスにアタッチされている DHCPv6 ガード ポリシーに基づくフィルタリングと一致する DHCPv6 メッセージを検証します。

検証に合格しなかったメッセージはドロップされます。FHS 共通コンポーネント上でロギング パケット ドロップ設定が有効になっている場合、レート制限付きの SYSLOG メッセージが送信されます。

ネイバー バインディング完全性

ネイバー バインディング（NB）完全性は、ネイバーのバインディングを確立します。

NB 完全性の別個の独立したインスタンスが、この機能が有効になっている各 VLAN 上で動作します。

アドバタイズされた IPv6 プレフィックスの学習

NB 完全性は、RA メッセージでアドバタイズされた IPv6 プレフィックスを学習し、これをネイバー プレフィックス テーブル内に保存します。このプレフィックスは、割り当てられたグローバル IPv6 アドレスの検証に使用されます。

デフォルトで、この検証は無効になっています。有効にすると、[ネイバー バインディング設定] ページにあるプレフィックスに照らしてアドレスが検証されます。

アドレスの検証に使用するスタティックなプレフィックスは、[ネイバー プレフィックス テーブル] ページから追加できます。

グローバル IPv6 アドレスの検証

NB 完全性は次の検証を実行します。

- NS メッセージまたは NA メッセージに含まれるターゲット アドレスがグローバル IPv6 アドレスの場合、このアドレスは RA プレフィックス テーブルで定義済みのいずれかのプレフィックスに属している必要があります。
- DHCPv6 サーバによって提供されるグローバル IPv6 アドレスは、IPv6 プレフィックス リスト（[IPv6 プレフィックス] ページ内）で定義済みのいずれかのプレフィックスに属している必要があります。

この検証に合格しなかったメッセージはドロップされ、レート制限付きの SYSLOG メッセージが送信されます。

ネイバー バインディング テーブルのオーバーフロー

新規のエントリを作成するのに必要な空き領域が存在しない場合、エントリは作成されず、SYSLOG メッセージが送信されます。

ネイバーのバインディング確立

IPv6 ファースト ホップ セキュリティのスイッチは、次の方式を使用してバインディング情報を検出し、記録できます。

- **NBI-NDP 方式**: スヌープされたネイバー探索プロトコル メッセージから IPv6 アドレスを学習します
- **NBI-DHCP 方式**: スヌープされた DHCPv6 メッセージから IPv6 アドレスを学習します
- **NBI 手動方式:** 手動設定による方式です

IPv6 アドレスは、ホストのネットワーク アタッチメントのリンク層プロパティにバインドされます。このプロパティは「バインディング アンカー」と呼ばれ、ホストへの接続で経由されるインターフェイスの ID(ifIndex)と、ホストの MAC アドレスで構成されます。

IPv6 ファースト ホップ セキュリティのスイッチは、境界インターフェイスでのみバインディングを確立します(「IPv6 ファースト ホップ セキュリティの境界」参照)。

バインディング情報はネイバー バインディング テーブルに保存されます。

NBI-NDP メソッド

使用される NBI-NDP メソッドは、RFC6620 で指定されている FCFS- SAVI メソッドに基づくものですが、両者には次の相違点があります。

- リンク ローカル IPv6 アドレス間のバインディングのみをサポートする FCFS-SAVI とは異なり、NBI-NDP ではグローバル IPv6 アドレスのバインディングもサポートしています。
- NBI-NDP がサポートする IPv6 アドレス バインディングは、NDP メッセージから学習した IPv6 アドレスに限られます。データ メッセージの送信元アドレス検証は、IPv6 送信元アドレスガードにより提供されます。
- NBI-NDP では、アドレス所有権の検査は、原則先着順に行われます。特定の送信元アドレスの所有権を最初に主張したホストが、その後別の通知があるまでそのアドレスの所有者となります。ホストの変更は認められないため、新しいプロトコルを必要としない何らかの方法で、アドレス所有権を確証する必要があります。このために、スイッチは、NDP メッセージから新たな IPv6 アドレスを学習すると、そのアドレスをインターフェイスにバインドします。この IPv6 アドレスを含むそれ以後の NDP メッセージは、同じバインディング アンカーに照らして検査され、発信元がその送信元 IP アドレスを所有しているかどうかが確認されます。

  このルールの例外が生じるのは、IPv6 ホストが L2 ドメイン内でローミングする場合や、ホストの MAC アドレスが変更された場合です。この場合、ホストは依然としてその IP アドレスの所有者ですが、関連付けられているバインディング アンカーが変更されている可能性があります。このような状況に対処するため、定義済みの NBI-NDP の動作は、前のバインディング インターフェイスに DAD-NS メッセージを送信することにより、ホストが今でも到達可能かどうかを検証するものになっています。前に登録されたバインディング アンカーではホストに到達できなくなっている場合、NBI-NDP は新しいほうのアンカーが有効であると見なして、バインディング アンカーを変更します。前に登録されたバインディング アンカーを使用してホストに到達可能な場合は、バインディング インターフェイスは変更されません。

ネイバー バインディング テーブルのサイズを小さくするために、NBI-NDP は境界インターフェイスでのみバインディングを確立し(「IPv6 ファースト ホップ セキュリティの境界」参照)、NS メッセージと NA メッセージを使用してバインディング情報を内部インターフェイス全体に配信します。NBI-NDP ローカル バインディングを作成する前に、デバイスは DAD-NS メッセージを送信して、関係するアドレスを照会します。ホストがこのメッセージに対して NA メッセージで応答してきた場合、DAD-NS メッセージを送信したデバイスは、そのアドレスのバインディングが別のデバイス内に存在していると推察し、そのアドレスのローカル バインディングを作成しません。DAD-NS メッセージへの応答として NA メッセージを受信しなければ、ローカル デバイスはそのアドレスのバインディングが他のデバイス内には存在しないものと推察し、そのアドレスのローカル バインディングを作成します。

NBI-NDP はライフタイム タイマーをサポートしています。タイマーの値は、[ネイバー バインディング設定] ページから設定できます。タイマーは、バインドされた IPv6 アドレスが確認されるたびに再起動されます。タイマーの設定時間が経過すると、デバイスは最大 2 つの DAD-NS メッセージを短い間隔をあけて送信し、ネイバーを検証します。

NBI-DHCP 方式

NBI-NDP 方式は、DHCP 用 SAVI ソリューションの draft-ietf-savi-dhcp-15(2012 年 9 月 11 日版)で指定されている SAVI-DHCP 方式に基づいています。

NBI-NDP と同様、NBI-DHCP は拡張性のために境界バインディングを提供します。NBI-DHCP 方式と NBI-FCFS 方式には、次の相違点があります。NBI-DHCP は DHCPv6 メッセージ内で宣言されている状態を把握するため、NS メッセージや NA メッセージで状態を配信する必要はありません。

NB 完全性のポリシー

IPv6 ファースト ホップ セキュリティの他の機能の動作と同様に、インターフェイスでの NB 完全性の動作は、インターフェイスにアタッチされている NB 完全性のポリシーによって指定されます。これらのポリシーは、[ネイバー バインディング設定] ページで設定されます。

IPv6 ソース ガード

ネイバー バインディング完全性(NB 完全性)が有効な場合、IPv6 ソース ガードが有効かどうかに関係なく、IPv6 ソース ガードは NDP メッセージおよび DHCPv6 メッセージの送信元 IPv6 アドレスを検証します。IPv6 ソース ガードと NB 完全性がどちらも有効な場合、IPv6 ソース ガードは、TCAM を設定して、転送、ドロップ、および CPU へのトラップの対象にする IPv6 データ フレームを指定し、トラップされた IPv6 データ メッセージの送信元 IPv6 アドレスを検証します。NB 完全性が有効になっていない場合、IPv6 ソース ガードが有効かどうかに関係なく、IPv6 ソース ガードはアクティブ化されません。

新しいルールの追加に必要な空き容量が TCAM にない場合、TCAM オーバーフロー カウンタが増加し、インターフェイス ID、ホストの MAC アドレス、およびホストの IPv6 アドレスが含まれたレート制限付きの SYSLOG メッセージが送信されます。

IPv6 ソース ガードは、受信したすべての IPv6 メッセージの送信元アドレスを、ネイバー バインディング テーブルを使用して検証します。しかし例外として次のメッセージは検証せずに通過させます。

- RS メッセージ:送信元 IPv6 アドレスが未指定の IPv6 アドレスに等しい場合。
- NS メッセージ:送信元 IPv6 アドレスが未指定の IPv6 アドレスに等しい場合。
- NA メッセージ:送信元 IPv6 アドレスがターゲット アドレスに等しい場合。

IPv6 ソース ガードは、送信元 IPv6 アドレスが未指定の IPv6 アドレスに等しい他のすべての IPv6 メッセージをドロップします。

IPv6 ソース ガードは、境界に属している信頼されていないインターフェイスでのみ動作します。

IPv6 ソース ガードは、次の場合、入力 IPv6 メッセージをドロップします。

- ネイバー バインディング テーブルにその IPv6 アドレスが含まれていない場合。
- ネイバー バインディング テーブルにその IPv6 アドレスが含まれているものの、別のインターフェイスにバインドされている場合。

IPv6 ソース ガードは、不明な送信元 IPv6 アドレスに対する DAD_NS メッセージを送信してネイバー リカバリ プロセスを開始します。

攻撃に対する保護

ここでは、IPv6 ファースト ホップ セキュリティにより提供される、攻撃に対する保護機能を説明します。

IPv6 ルータ スプーフィングに対する保護

IPv6 ホストでは、受信した RA メッセージを次の用途に使用する場合があります。

- IPv6 ルータ ディスカバリ
- ステートレス アドレス コンフィギュレーション

悪意のあるホストが、そのホスト自身を IPv6 ルータとしてアドバタイズし、ステートレス アドレス コンフィギュレーションに偽のプレフィックスを提供する RA メッセージを送信してくる場合があります。

RA ガードは、IPv6 ルータが接続できないすべてのインターフェイスのインターフェイス ロールをホスト インターフェイスとして設定することにより、このような攻撃に対する保護を提供します。

IPv6 アドレス解決スプーフィングに対する保護

悪意のあるホストが、NA メッセージを送信して、そのホスト自身を特定の IPv6 アドレスを持つ IPv6 ホストとしてアドバタイズしてくる場合があります。

NB 完全性は、次のようにして、このような攻撃に対する保護を提供します。

- 指定された IPv6 アドレスが不明な場合、ネイバー送信要求(NS)メッセージは内部インターフェイスでのみ転送されます。
- 指定された IPv6 アドレスが既知のものである場合、NS メッセージはその IPv6 アドレスがバインドされているインターフェイスでのみ転送されます。
- ターゲット IPv6 アドレスが別のインターフェイスにバインドされている場合、ネイバー アドバタイズメント(NA)メッセージはドロップされます。

IPv6 重複アドレス検出スプーフィングに対する保護

IPv6 ホストは、割り当て済みのそれぞれの IPv6 アドレスについて、特別な NS メッセージ(重複アドレス検出ネイバー送信要求(DAD_NS)メッセージ)を送信することにより、重複アドレス検出を実行する必要があります。

悪意のあるホストが、DAD_NS メッセージに応答して、特定の IPv6 アドレスを持つ IPv6 ホストとしてそのホスト自身をアドバタイズする応答を送信してくる場合があります。

NB 完全性は、次のようにして、このような攻撃に対する保護を提供します。

- 指定された IPv6 アドレスが不明な場合、DAD_NS メッセージは内部インターフェイスでのみ転送されます。
- 指定された IPv6 アドレスが既知のものである場合、DAD_NS メッセージはその IPv6 アドレスがバインドされているインターフェイスでのみ転送されます。
- ターゲット IPv6 アドレスが別のインターフェイスにバインドされている場合、NA メッセージはドロップされます。

DHCPv6 サーバ スプーフィングに対する保護

IPv6 ホストでは、DHCPv6 プロトコルを次の用途に使用する場合があります。

- ステートレス情報コンフィギュレーション
- ステートフル アドレス コンフィギュレーション

悪意のあるホストが、そのホスト自身を DHCPv6 サーバとしてアドバタイズし、偽のステートレス情報や IPv6 アドレスを提供する DHCPv6 応答メッセージを送信してくる場合があります。DHCPv6 ガードは、DHCPv6 サーバが接続できないすべてのポートのインターフェイス ロールをクライアント ポートとして設定することにより、このような攻撃に対する保護を提供します。

NBD キャッシュ スプーフィングに対する保護

IPv6 ルータは、ネイバー探索プロトコル(NDP)キャッシュをサポートしています。このキャッシュは、ラスト ホップ ルーティングのために IPv6 アドレスを MAC アドレスにマップするものです。

悪意のあるホストが、ラスト ホップ フォワーディングの宛先 IPv6 アドレスとして異なるアドレスが指定された複数の IPv6 メッセージを送信し、NBD キャッシュをオーバーフローさせる場合があります。

NDP 実装に埋め込まれたメカニズムにより、ネイバー探索キャッシュ内で許可される未完了状態のエントリ数が制限されています。これにより、テーブルがハッカーによってフラッディングされないように保護できます。

ポリシー、グローバル パラメータ、およびシステム デフォルト

FHS の各機能の有効または無効は、個別に設定できます。デフォルトでは、どの機能も有効になっていません。

各機能を使用するには、まず特定の VLAN 上で有効にする必要があります。機能を有効する際に、その機能の検証ルールに対するグローバル コンフィギュレーション値を定義することもできます。これらの検証ルールに対するさまざまな値を含むポリシーを定義しない場合は、グローバル値を使用してパケットにこの機能が適用されます。

ポリシー

ポリシーには入力パケットに対して実行される検証ルールが含まれます。ポリシーは、VLAN の他に、ポートや LAG にもアタッチできます。この機能が VLAN 上で有効にされていない場合、ポリシーの影響はありません。

ポリシーには、ユーザ定義ポリシーとデフォルト ポリシーがあります(次を参照)。

デフォルト ポリシー

各 FHS 機能には空のデフォルト ポリシーが存在し、これらがデフォルトですべての VLAN およびインターフェイスにアタッチされています。これらのデフォルトのポリシーの名前は「vlan_default」および「port_default」です(各機能に存在します)。

- これらのデフォルト ポリシーにルールを追加できます。デフォルト ポリシーをインターフェイスに手動でアタッチすることはできません。これらはデフォルトでアタッチ済みです。
- デフォルト ポリシーは削除できません。ユーザが追加したコンフィギュレーションのみ削除できます。

ユーザ定義ポリシー

デフォルト ポリシーの他に、ユーザがポリシーを定義することもできます。

ユーザ定義ポリシーがインターフェイスにアタッチされると、そのインターフェイスのデフォルト ポリシーはデタッチされます。ユーザ定義ポリシーがインターフェイスからデタッチされると、デフォルト ポリシーが再アタッチされます。

次の要件が満たされると、ポリシーは有効になります。

- ポリシー内の機能が、そのインターフェイスが含まれる VLAN 上で有効になっている
- ポリシーがそのインターフェイス(VLAN、ポート、または LAG)にアタッチされている。

ポリシーをアタッチすると、そのインターフェイスに対するデフォルト ポリシーはデタッチされます。ポリシーをインターフェイスから削除すると、デフォルト ポリシーが再アタッチされます。

1 つの VLAN には、(1 つの特定の機能の)ポリシーを 1 つのみアタッチできます。

各インターフェイスには、(1 つの特定の機能の)ポリシーを複数アタッチできます。ただし、それぞれのポリシーで別々の VLAN を指定している必要があります。

検証ルールのレベル

インターフェイス上の入力パケットに適用される最後のルール セットは、次のようにして構築されます。

- パケットを受け取るインターフェイス(ポート、または LAG)にアタッチされているポリシーで設定されたルールが、セットに追加されます。
- VLAN にアタッチされているポリシーで設定されたルールは、ポートのレベルでそのルールがすでに追加されていなければ、セットに追加されます。
- グローバル ルールは、VLAN またはポートのレベルでそのルールがすでに追加されていなければ、セットに追加されます。

ポートのレベルで定義されたルールは、VLAN のレベルで設定されたルールをオーバーライドします。VLAN のレベルで設定されたルールは、グローバルに設定されたルールをオーバーライドします。グローバルに設定されたルールは、システムのデフォルト設定をオーバーライドします。

一般的な作業

IPv6 ファースト ホップ セキュリティの共通機能のワークフロー

ステップ 1 [FHS 設定] ページで、この機能が有効になっている VLAN のリストを入力します。

ステップ 2 同じページで、グローバル パケット ドロップ ロギング機能を設定します。

ステップ 3 必要に応じ、この機能に対してユーザ定義ポリシーを設定するか、この機能のデフォルト ポリシーにルールを追加します。

ステップ 4 [ポリシー適用(VLAN)] ページか [ポリシー適用(ポート)] ページから、ポリシーを VLAN、ポート、または LAG にアタッチします。

ルータ アドバタイズメント ガードのワークフロー

ステップ 1 [RA ガード設定] ページで、この機能が有効になっている VLAN のリストを入力します。

ステップ 2 同じページで、ポリシーで値が設定されていない場合に使用されるグローバル コンフィギュレーション値を設定します。

ステップ 3 必要に応じ、この機能に対してユーザ定義ポリシーを設定するか、この機能のデフォルト ポリシーにルールを追加します。

ステップ 4 [ポリシー適用(VLAN)] ページか [ポリシー適用(ポート)] ページから、ポリシーを VLAN、ポート、または LAG にアタッチします。

DHCPv6 ガードのワークフロー

ステップ 1 [DHCPv6 ガード設定] ページで、この機能が有効になっている VLAN のリストを入力します。

ステップ 2 同じページで、ポリシーで値が設定されていない場合に使用されるグローバル コンフィギュレーション値を設定します。

ステップ 3 必要に応じ、この機能に対してユーザ定義ポリシーを設定するか、この機能のデフォルト ポリシーにルールを追加します。

ステップ 4 [ポリシー適用(VLAN)] ページか [ポリシー適用(ポート)] ページから、ポリシーを VLAN、ポート、または LAG にアタッチします。

ネイバー探索インスペクションのワークフロー

ステップ 1 [ND インスペクション設定] ページで、この機能が有効になっている VLAN のリストを入力します。

ステップ 2 同じページで、ポリシーで値が設定されていない場合に使用されるグローバル コンフィギュレーション値を設定します。

ステップ 3 必要に応じ、この機能に対してユーザ定義ポリシーを設定するか、この機能のデフォルト ポリシーにルールを追加します。

ステップ 4 [ポリシー適用(VLAN)] ページか [ポリシー適用(ポート)] ページから、ポリシーを VLAN、ポート、または LAG にアタッチします。

ネイバー バインディングのワークフロー

ステップ 1 [ネイバー バインディング設定] ページで、この機能が有効になっている VLAN のリストを入力します。

ステップ 2 同じページで、ポリシーで値が設定されていない場合に使用されるグローバル コンフィギュレーション値を設定します。

ステップ 3 必要に応じ、この機能に対してユーザ定義ポリシーを設定するか、この機能のデフォルト ポリシーにルールを追加します。

ステップ 4 必要に応じて [ネイバー バインディング テーブル] ページから手動でエントリを追加します。

ステップ 5 [ポリシー適用(VLAN)] ページか [ポリシー適用(ポート)] ページから、ポリシーを VLAN、ポート、または LAG にアタッチします。

IPv6 ソース ガードのワークフロー

ステップ 1 [IPv6 ソース ガード設定] ページで、この機能が有効になっている VLAN のリストを入力します。

ステップ 2 必要に応じ、この機能に対してユーザ定義ポリシーを設定するか、この機能のデフォルト ポリシーにルールを追加します。

ステップ 3 [ポリシー適用(VLAN)] ページか [ポリシー適用(ポート)] ページから、ポリシーを VLAN、ポート、または LAG にアタッチします。

デフォルト設定とコンフィギュレーション

VLAN 上で IPv6 ファースト ホップ セキュリティが有効にされている場合、スイッチはデフォルトで次のメッセージをトラップします。

- ルータ アドバタイズメント(RA)メッセージ
- ルータ送信要求(RS)メッセージ
- ネイバー アドバタイズメント(NA)メッセージ
- ネイバー送信要求(NS)メッセージ
- ICMPv6 リダイレクト メッセージ
- 認証パス アドバタイズメント(CPA)メッセージ
- 認証パス請求(CPS)メッセージ
- DHCPv6 メッセージ

FHS 機能はデフォルトで無効になっています。

Web GUI を介した IPv6 ファースト ホップ セキュリティの設定

FHS 設定

[FHS設定] ページを使用して、指定した VLAN グループで FHS の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に対するグローバル コンフィギュレーション値を設定します。必要に応じ、ポリシーやパケット ドロップ ロギングを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のパラメータを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [FHS設定] の順にクリックします。

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 [ポリシータイプ] 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]:IPv6 ファースト ホップ セキュリティが有効になっている VLAN を 1 つ以上入力します。
- [パケット ドロップ ロギング]:選択すると、ファースト ホップ セキュリティのポリシーによってパケットが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 [適用] をクリックし、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 必要に応じ、[追加] をクリックして FHS ポリシーを作成します。

次のフィールドを入力します。

- [ポリシー名]:ユーザ定義のポリシー名を入力します。
- [パケット ドロップ ロギング]:選択すると、このポリシー内のファースト ホップ セキュリティ機能によってパケットがドロップされたときに SYSLOG が作成されます。
  - [継承]:VLAN またはグローバル コンフィギュレーションの値を使用します。
  - [有効]: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たときに SYSLOG が作成されます。
  - [無効]: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 [適用] をクリックし、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 6 このポリシーをインターフェイスにアタッチするには、次のようにします。

- [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)] 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)] ページにジャンプし、このポリシーをポートにアタッチできます。

RA ガード設定

[RAガード設定] 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、この機能に対するグローバル コンフィギュレーション値を設定できます。必要に応じ、このページでポリシーを追加したり、システム定義のデフォルト RA ガード ポリシーを設定したりできます。

RA ガードを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [RAガード設定] の順にクリックします。

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 [ポリシータイプ] が表示されます。

ステップ 2 次の [グローバルコンフィギュレーション] フィールドに入力します。

- [RAガードVLANリスト]:RA ガードが有効になっている VLAN を 1 つ以上入力します。

後述するその他のコンフィギュレーション フィールドを入力します。

ステップ 3 ポリシーを追加するには、[追加] 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]:ユーザ定義のポリシー名を入力します。
- [デバイス ロール]:次のオプションのいずれかを表示して、RA ガード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]: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。
  - [ホスト]:デバイス ロールはホストです。
  - [ルータ]:デバイス ロールはルータです。
- [マネージド コンフィギュレーション フラグ]: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マネージド アドレス 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。
  - [継承]:機能は 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。
  - [検証なし]:アドバタイズされたマネージド アドレス コンフィギュレーション フラグの検証を無効にします。
  - [オン]:アドバタイズされたマネージド アドレス コンフィギュレーション フラグの検証を有効にします。
  - [オフ]:フラグの値は 0 である必要があります。

- [他のコンフィギュレーション フラグ]: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。
  - [継承]:機能は 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。
  - [検証なし]:アドバタイズされた他のコンフィギュレーション フラグの検証を無効にします。
  - [オン]:アドバタイズされた他のコンフィギュレーション フラグの検証を有効にします。
  - [オフ]: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]:フィルタリングするアドレスのリストを指定します。
  - [継承]:値は VLAN またはシステム デフォルト(検証なし)から継承されます。
  - [検証なし]:アドバタイズされたアドレスは検証されません。
  - [一致リスト]:照合される IPv6 アドレス リスト。
- [RA プレフィックス リスト]:フィルタリングするアドレスのリストを指定します。
  - [継承]:値は VLAN またはシステム デフォルト(検証なし)から継承されます。
  - [検証なし]:アドバタイズされたプレフィックスは検証されません。
  - [一致リスト]:照合されるプレフィックス リスト。
- [最小ホップ限度]: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確認するかどうかを示します。
  - [継承]:機能は 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。
  - [限度なし]:ホップ カウント限度の下限の検証を無効にします。
  - [ユーザ定義]:ホップ カウント限度がこの値以上であるか検証します。
- [最大ホップ限度]: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。
  - [継承]:機能は 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。
  - [限度なし]:ホップ カウント限度の上限の検証を無効にします。

- [ユーザ定義]:ホップ カウント限度がこの値以下であるか検証します。上限の値は、下限の値以上に設定する必要があります。

- [最小ルータプリファレンス]: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]:機能は 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。
  - [検証なし]: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の検証を無効にします。
  - [低]:アドバタイズされたデフォルト ルータ プリファレンスの許容最小値を指定します。次の値を指定できます。低、中、高(RFC4191 参照)。
  - [中]:アドバタイズされたデフォルト ルータ プリファレンスの許容最小値を指定します。次の値を指定できます。低、中、高(RFC4191 参照)。
  - [高]:アドバタイズされたデフォルト ルータ プリファレンスの許容最小値を指定します。次の値を指定できます。低、中、高(RFC4191 参照)。
- [最大ルータプリファレンス]: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]:機能は 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。
  - [検証なし]: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の検証を無効にします。
  - [低]:アドバタイズされたデフォルト ルータ プリファレンスの許容最大値を指定します。次の値を指定できます。低、中、高(RFC4191 参照)。
  - [中]:アドバタイズされたデフォルト ルータ プリファレンスの許容最大値を指定します。次の値を指定できます。低、中、高(RFC4191 参照)。
  - [高]:アドバタイズされたデフォルト ルータ プリファレンスの許容最大値を指定します。次の値を指定できます。低、中、高(RFC4191 参照)。

ステップ 4 [適用] をクリックし、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 5 システム定義のデフォルト ポリシーまたは既存のユーザ定義ポリシーを設定するには、[ポリシーテーブル] でポリシーを選択し、[編集] をクリックします。

ステップ 6 このポリシーをインターフェイスにアタッチするには、次のようにします。

- [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)] 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)] 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ガード設定] 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、この機能に対するグローバル コンフィギュレーション値を設定できます。必要に応じ、このページでポリシーを追加したり、システム定義のデフォルト DHCPv6 ガード ポリシーを設定したりできます。

DHCPv6 ガードを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [DHCPv6ガード設定] の順にクリックします。

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 [ポリシータイプ] 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ガードVLANリスト]:DHCPv6 ガードが有効になっている VLAN を 1 つ以上入力します。
- [デバイスロール]: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。
- [最小プリファレンス]:このフィールドは、受信したパケット内のアドバタイズされたプリファレンスの最小値を、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]: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の検証を無効にします。
  - [ユーザ定義]:アドバタイズされたプリファレンス値がこの値以上であるか検証します。この値は、最大プリファレンス値未満に設定する必要があります。

- [最大プリファレンス]:このフィールドは、受信したパケット内のアドバタイズされたプリファレンスの最大値を、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、[最小プリファレンス] 値より大きな値に設定する必要があります。
  - [検証なし]:ホップ カウント限度の下限の検証を無効にします。
  - [ユーザ定義]:アドバタイズされたプリファレンス値がこの値以下であるか検証します。

ステップ 3 [適用] をクリックし、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。

既存のポリシーが表示されます。その下に [ポリシータイプ] フィールド以外のフィールドが表示されます。[ポリシー タイプ] フィールドには、ポリシーがユーザ定義なのか、デフォルトなのかが表示されます。

ステップ 4 必要に応じて、[追加] をクリックし、DHCPv6 ポリシーを作成します。

ステップ 5 次のフィールドを入力します。

- [ポリシー名]:ユーザ定義のポリシー名を入力します。
- [デバイスロール]:[サーバ] または [クライアント] のいずれかを選択して、DHCPv6 ガード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]:デバイスのロールは 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。
  - [クライアント]:デバイスのロールはクライアントです。
  - [サーバ]:デバイスのロールはサーバです。
- [一致応答プレフィックス]:選択すると、DHCPv6 ガード ポリシー内で、受信した DHCP 応答メッセージに含まれるアドバタイズされたプレフィックスの検証が有効になります。
  - [継承]:値は VLAN またはシステム デフォルト(検証なし)から継承されます。
  - [検証なし]:アドバタイズされたプレフィックスは検証されません。
  - [一致リスト]:照合される IPv6 プレフィックス リスト。
- [一致サーバアドレス]:選択すると、DHCPv6 ガード ポリシー内で、受信した DHCP 応答メッセージに含まれる 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]:値は VLAN またはシステム デフォルト(検証なし)から継承されます。

- [検証なし]:DHCP サーバの IPv6 アドレスとリレーの IPv6 アドレスの検証を無効にします。
- [一致リスト]:照合される IPv6 プレフィックス リスト。

- [最小プリファレンス]:このフィールドは、受信したパケット内のアドバタイズされたプリファレンスの最小値を、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]:最小プリファレンスは 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。
  - [検証なし]: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の検証を無効にします。
  - [ユーザ定義]:アドバタイズされたプリファレンス値がこの値以上であるか検証します。この値は、最大プリファレンス値未満に設定する必要があります。
- [最大プリファレンス]:このフィールドは、受信したパケット内のアドバタイズされたプリファレンスの最大値を、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、[最小プリファレンス] 値より大きな値に設定する必要があります。
  - [継承]:最小プリファレンスは 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。
  - [検証なし]:ホップ カウント限度の下限の検証を無効にします。
  - [ユーザ定義]:アドバタイズされたプリファレンス値がこの値以下であるか検証します。

ステップ 6 [適用] をクリックし、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 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、次のようにします。

- [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)] 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)] 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

[ネイバー探索(ND)インスペクション] 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、この機能に対するグローバル コンフィギュレーション値を設定できます。必要に応じ、このページでポリシーを追加したり、システム定義のデフォルト ND インスペクション ポリシーを設定したりできます。

ND インスペクションを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [NDインスペクション設定] の順にクリックします。

既存のポリシーが表示されます。その下に [ポリシータイプ] フィールド以外のフィールドが表示されます。[ポリシー タイプ] フィールドには、ポリシーがユーザ定義なのか、デフォルトなのかが表示されます。

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。

- [NDインスペクションVLANリスト]:ND インスペクションが有効になっている VLAN を 1 つ以上入力します。
- [デバイス ロール]:次に説明するデバイス ロールを表示します。
- [ドロップ アンセキュア]:選択すると、IPv6 ND インスペクション ポリシー内で、CGA 署名オプションまたは RSA 署名オプションが設定されていないメッセージのドロップが有効になります。
- [最低セキュリティ レベル]:アン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]:セキュリティ レベルの検証を無効にします。
  - [ユーザ定義]:転送されるメッセージのセキュリティ レベルを指定します。
- [ソース MAC の検証]:選択すると、リンク層アドレスに対する送信元 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 [適用] をクリックし、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 必要に応じて、[追加] をクリックし、ND インスペクション ポリシーを作成します。

ステップ 5 次のフィールドを入力します。

- [ポリシー名]:ユーザ定義のポリシー名を入力します。
- [デバイスロール]:次のいずれかを選択して、ND インスペクション用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]:デバイスのロールは 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。
- [ホスト]:デバイスのロールはホストです。
- [ルータ]:デバイスのロールはルータです。

• [ドロップアンセキュア]:次のいずれかのオプションを選択します。
- [継承]:VLAN またはシステム デフォルト(無効)から値を継承します。
- [有効]:IPv6 ND インスペクション ポリシー内で、CGA 署名オプションまたは RSA 署名オプションが設定されていないメッセージのドロップが有効になります。
- [無効]:IPv6 ND インスペクション ポリシー内で、CGA 署名オプションまたは RSA 署名オプションが設定されていないメッセージのドロップが無効になります。

• [最低セキュリティ レベル]:アン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(そのレベルを下回るとメッセージが転送されないことを意味する)を選択します。
- [継承]:VLAN またはシステム デフォルト(無効)から値を継承します。
- [検証なし]:セキュリティ レベルの検証を無効にします。
- [ユーザ定義]:転送されるメッセージのセキュリティ レベルを指定します。

• [ソースMACの検証]:リンク層アドレスに対する送信元 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]:VLAN またはシステム デフォルト(無効)から値を継承します。
- [有効]:リンク層アドレスに対する送信元 MAC アドレスのチェックを有効にします。
- [無効]:リンク層アドレスに対する送信元 MAC アドレスのチェックを無効にします。

ステップ 6 [適用] をクリックし、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 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、次のようにします。

• [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)] 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)] 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。

ネイバー バインディング設定

ネイバー バインディング テーブルは、デバイスに接続された IPv6 ネイバーのデータベース テーブルで、ネイバー探索プロトコル(NDP)スヌーピングなどの情報源を基に作成されます。このデータベース(バインディング)テーブルは、さまざまな IPv6 ガード機能でスプーフィングやリダイレクト攻撃を防止するために使用されます。

[ネイバーバインディング設定] ページを使用して、指定した VLAN グループでネイバー バインディング機能を有効にし、この機能に対するグローバル コンフィギュレーション値を設定できます。必要に応じ、このページでポリシーを追加したり、システム定義のデフォルト ネイバー バインディング ポリシーを設定したりできます。

ネイバー バインディングを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [ネイバーバインディング設定] の順にクリックします。

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 つ以上入力します。
- [デバイスロール]: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 コンフィギュレーションを 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。
  - [任意]: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]: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、ステートレス自動コンフィギュレーションのみ許可します。
  - [無効]:NDP メッセージからのバインディングを無効にします。

- [DHCPv6 メッセージからのバインディング]:DHCPv6 からのバインディングを許可します。

[ネイバー バインディング エントリ限度]:インターフェイスまたはアドレスのタイプごとの、ネイバー バインディング エントリ数の上限を指定します。

- [VLAN ごとのエントリ数]:VLAN ごとのネイバー バインディングの限度を指定します。[限度なし] を選択するか、[ユーザ定義] 値を入力します。
- [インターフェイスごとのエントリ数]:インターフェイスごとのネイバー バインディングの限度を指定します。[限度なし] を選択するか、[ユーザ定義] 値を入力します。
- [MAC アドレスごとのエントリ数]:MAC アドレスごとのネイバー バインディングの限度を指定します。[限度なし] を選択するか、[ユーザ定義] 値を入力します。

ステップ 3 [適用] をクリックし、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 必要に応じて、[追加] をクリックし、ネイバー バインディング ポリシーを作成します。

ステップ 5 次のフィールドを入力します。

- [ポリシー名]:ユーザ定義のポリシー名を入力します。
- [デバイスロール]: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]:デバイスのロールは 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。
  - [境界]:ポートは、IPv6 ファースト ホップの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]:ポートは、IPv6 ファースト ホップの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]:ロギング オプションはグローバル値と同じに設定されます。
  - [有効]:バインディング テーブルのメイン イベントのロギングを有効にします。
  - [無効]:バインディング テーブルのメイン 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]:検証オプションはグローバル値と同じに設定されます。
  - [有効]:アドレスの検証を有効にします。
  - [無効]: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]:有効にすると、グローバル アドレス バインディング設定が使用されます。
- [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 コンフィギュレーションを 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。
  - [任意]: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]: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、ステートレス自動コンフィギュレーションのみ許可します。
  - [無効]:NDP メッセージからのバインディングを無効にします。
- [DHCPv6メッセージからのバインディング]:選択すると、DHCPv6 からのバインディングが有効になります。

[ネイバーバインディングエントリ限度]:**上記参照。**

- [VLAN ごとのエントリ数]:グローバル値を使用する場合は [継承]、エントリ数の限度を設定しない場合は [限度なし]、このポリシーに特別な値を設定する場合は [ユーザ定義] を選択します。
- [インターフェイスごとのエントリ数]:グローバル値を使用する場合は [継承]、エントリ数の限度を設定しない場合は [限度なし]、このポリシーに特別な値を設定する場合は [ユーザ定義] を選択します。
- [MACアドレスごとのエントリ数]:グローバル値を使用する場合は [継承]、エントリ数の限度を設定しない場合は [限度なし]、このポリシーに特別な値を設定する場合は [ユーザ定義] を選択します。

ステップ 6 [適用] をクリックし、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 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、次のようにします。

- [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)] 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)] 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ソースガード設定] 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。必要に応じ、このページでポリシーを追加したり、システム定義のデフォルト IPv6 ソース ガード ポリシーを設定したりできます。

IPv6 ソース ガードを設定するには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [IPv6ソースガード設定] の順にクリックします。

既存のポリシーが表示されます。その下に [ポリシータイプ] フィールド以外のフィールドが表示されます。[ポリシー タイプ] フィールドには、ポリシーがユーザ定義なのか、デフォルトなのかが表示されます。

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。

- [IPv6ソースガードVLANリスト]:IPv6 ソース ガードが有効になっている VLAN を 1 つ以上入力します。
- [ポート信頼]:デフォルトではポリシーの対象が信頼できないポートであることが表示されます。この設定はポリシーごとに変更できます。

ステップ 3 必要に応じて、[追加] をクリックし、ファースト ホップ セキュリティのポリシーを作成します。

ステップ 4 次のフィールドを入力します。

- [ポリシー名]:ユーザ定義のポリシー名を入力します。
- [ポート信頼]:ポリシーのポート信頼ステータスを選択します。
  - [継承]: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。
  - [信頼済み]:ポリシーをポートにアタッチした時点で、信頼済みです。

ステップ 5 [適用] をクリックし、ポリシーをアタッチします。

ステップ 6 このポリシーをインターフェイスにアタッチするには、[ポリシーをインターフェイスにアタッチ] をクリックします。すると、[ポリシー適用(ポート)] ページに移動するので、そのページからこのポリシーをポートにアタッチできます。

ポリシー適用(VLAN)

ポリシーを 1 つ以上の VLAN にアタッチするには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [ポリシー適用(VLAN)] の順にクリックします。

すでにアタッチされているポリシーとそれらの [ポリシー タイプ]、[ポリシー名]、および [VLAN リスト] が一覧で表示されます。

ステップ 2 VLAN にポリシーをアタッチするには、[追加] 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]: インターフェイスにアタッチするポリシー タイプを選択します。
- [ポリシー名]: 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リスト]:ポリシーがアタッチされる VLAN を選択します。

ステップ 3 [適用] をクリックし、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。

ポリシー適用(ポート)

ポリシーを 1 つ以上のポートまたは LAG にアタッチするには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [ポリシー適用(ポート)] の順にクリックします。

すでにアタッチされているポリシーのリストが、[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] と一緒に表示されます。

ステップ 2 ポートまたは LAG にポリシーをアタッチするには、[追加] をクリックして、次のフィールドに入力します。

- [インターフェイス]: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]: インターフェイスにアタッチするポリシー タイプを選択します。IPv6 ファースト ホップ セキュリティの概要。
- [ポリシー名]: 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リスト]:ポリシーがアタッチされる VLAN を選択します。

ステップ 3 [適用] をクリックし、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。

ネイバー バインディング テーブル

ネイバー バインディング テーブルのエントリを表示するには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [ネイバーバインディングテーブル] の順にクリックします。

ステップ 2 次の [テーブルのクリア] オプションのいずれかを選択します。

- [スタティックのみ]:テーブルに含まれるスタティックなエントリすべてをクリアします。
- [ダイナミックのみ]:テーブルに含まれるダイナミックなエントリすべてをクリアします。
- [すべてのダイナミックおよびスタティック]: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。

各ポリシーに対して、次のフィールドが表示されます([追加] ページにないフィールドのみ表示されます)。

- [オリジン]:IPv6 アドレスを追加したプロトコル(ダイナミックなエントリでのみ使用可能)。
  - [スタティック]:手動で追加したもの。
  - [NDP]:ネイバー探索プロトコル メッセージから学習したもの。
  - [DHCP]:DHCPv6 プロトコル メッセージから学習したもの。
- [状態]:エントリの状態。
  - [暫定]:新しいホストの IPv6 アドレスを検証中。ライフタイムが 1 秒未満であるため、期限切れ時間は表示されません。
  - [有効]:ホストの IPv6 アドレスはバインド済み。
- [期限切れ時間(秒)]:エントリが確認されない場合、削除されるまでの残り時間(秒単位)。
- [TCAM オーバーフロー]:[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、[追加] をクリックして、以下のフィールドに入力します。

- [VLAN ID]:エントリの VLAN ID。
- [IPv6 アドレス]:エントリの送信元 IPv6 アドレス。
- [インターフェイス]:パケットが受信されるポート。

- [MAC アドレス]:パケットのネイバー MAC アドレス。

ステップ 4 [適用] をクリックし、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。

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なプレフィックスを追加できます。ダイナミックなエントリは、「アドバタイズされた IPv6 プレフィックスの学習」で説明されている方法で学習されます。

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、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [ネイバープレフィックステーブル] の順にクリックします。

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、[テーブルのクリア] フィールドで、次のオプションのいずれかを選択します。

- [スタティックのみ]:スタティックなエントリのみクリアします。
- [ダイナミックのみ]:ダイナミックなエントリのみクリアします。
- [すべてのダイナミックおよびスタティック]:スタティックなエントリとダイナミックなエントリをクリアします。

ステップ 3 消去されるエントリに関して、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 プレフィックス]:IPv6 プレフィックス。
- [プレフィックス長]:IPv6 プレフィックス長。
- [オリジン]:エントリがダイナミック(学習による)かスタティック(手動設定による)か。
- [オートコンフィグ]:ステートレス コンフィギュレーションにプレフィックスを使用できます。
- [期限切れ時間(秒)]:エントリが削除されるまでの残り時間の長さ。

ステップ 4 [追加] をクリックしてテーブルに新規のエントリを追加し、その新規エントリに対して上記のフィールドを入力します。

FHS ステータス

FHS 機能のグローバル コンフィギュレーションを表示するには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [FHSステータス] の順にクリックします。

ステップ 2 FHS 状態のレポートを表示するポート、LAG、または VLAN を選択します。

ステップ 3 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。

- [FHSステータス]
  - [現在のVLAN上のFHS状態]:現在の VLAN 上で FHS が有効かどうか。
  - [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(すなわち、グローバル コンフィギュレーションのレベルか、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 ステータス]
  - [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。
  - [デバイス ロール]:RA デバイス ロール。
  - [マネージド コンフィギュレーション フラグ]:マネージド コンフィギュレーション 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]:他のコンフィギュレーション 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 ステータス]
  - [現在の 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。
  - [デバイス ロール]:DHCPv6 デバイス ロール。
  - [一致応答プレフィックス]: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 アドレス]:DHCP サーバ アドレスの検証が有効かどうか。
  - [最小プリファレンス]:最小プリファレンスの検証が有効かどうか。
  - [最大プリファレンス]:最大プリファレンスの検証が有効かどうか。
- [NDインスペクション ステータス]
  - [現在の VLAN 上の ND インスペクション状態]:現在の VLAN で ND インスペクションが有効になっているかどうか。
  - [デバイス ロール]:ND インスペクション デバイス ロール。
  - [ドロップ アンセキュア]:アン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]:アン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。
- [ネイバーバインディング ステータス]
  - [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。
  - [デバイス ロール]:ネイバー バインディング デバイス 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]:検証の対象となるメッセージ。
  - [VLAN ごとの最大エントリ]: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。

- [インターフェイスごとの最大エントリ数]: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アドレスごとの最大エントリ数]: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。
- [ポート信頼]: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 統計情報を表示するには、次のようにします。

ステップ 1 [セキュリティ] > [IPv6ファーストホップのセキュリティ] > [FHS統計情報] の順にクリックします。

ステップ 2 統計情報がリフレッシュされるまでの時間を示す [リフレッシュレート] を選択します。

ステップ 3 次のグローバル オーバーフロー カウンタが表示されます。

- [ネイバーバインディングテーブル]:テーブルのサイズが最大値に達したためにテーブルに追加できなかったエントリ数。
- [ネイバープレフィックステーブル]:テーブルのサイズが最大値に達したためにテーブルに追加できなかったエントリ数。
- [TCAM]:TCAM オーバーフローが原因で追加できなかったエントリ数。

ステップ 4 インターフェイスを選択すると、次のフィールドが表示されます。

- [NDP(ネイバー探索プロトコル)メッセージ]:次のタイプのメッセージについて、[受信済み] メッセージ数と [ドロップ済み] メッセージ数が表示されます。
  - [RA]:ルータ アドバタイズメント メッセージ
  - [REDIR]:リダイレクト メッセージ
  - [NS]:ネイバー送信要求メッセージ
  - [NA]:ネイバー アドバタイズメント メッセージ
  - [RS]:ルータ送信要求メッセージ

- [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 クエリー応答メッセージ
  - [RLS]:リリース済みメッセージ
  - [DEC]:拒否済みメッセージ

[FHSドロップ済みメッセージテーブル] に次のフィールドが表示されます

- [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)。
- [カウント]:ドロップされたメッセージ数。
- [理由]:メッセージがドロップされた理由。

ステップ 5 グローバル オーバーフロー カウンタをクリアするには、[グローバルカウンタのクリア] をクリックします。

26

アクセス制御

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 定義は、特定のサービス品質（QoS）が付与されるトラフィック フローの定義に使用するメカニズムの 1 つです。詳細については、「サービス品質」を参照してください。

ネットワーク マネージャは、ACL を使用して入力トラフィックのパターン（フィルタとアクション）を定義できます。ACL がアクティブなポートまたは LAG 上のデバイスに届いたパケットは、エントリを許可または拒否されます。

ここで説明する内容は次のとおりです。

- 概要
- MAC ベース ACL の作成
- IPv4 ベース ACL の作成
- IPv6 ベース ACL の作成
- ACL バインディング

概要

アクセス コントロール リスト（ACL）は、分類フィルタとアクションの番号付きリストです。それぞれの分類規則とそのアクションを、アクセス コントロール要素（ACE）と呼びます。

各 ACE は、トラフィック グループを区別するフィルタと、それらのフィルタに関連付けられたアクションで構成されています。1 つの ACL には 1 つ以上の ACE が含まれることがあります。ACE は、入力フレームのコンテンツと照合されます。コンテンツがフィルタに一致するフレームには、DENY アクションか PERMIT アクションが適用されます。

さまざまなデバイスが次の数の ACL および ACE をサポートします。

デバイス	最大 ACL 数	最大 ACE 数
SG550XG	2K	2K
Sx550X	3K	3K
SG350XG	2K	2K
SG350 および Sx350	1K	1K
Sx250	512	512

単一ポートまたは単一 ACL で最大 256 の ACE を設定できます。

パケットが ACE フィルタに一致した場合、その ACE アクションが実行され、ACL 処理は中止されます。パケットが ACE フィルタに一致しない場合は、次の ACE アクションが処理されます。1 つの ACL に含まれるどの ACE とも一致しない場合、他にも ACL があれば、その ACL が同様に処理されます。

注 関連するすべての ACL に含まれるどの ACE とも一致しない場合、そのパケットは破棄されます(デフォルトのアクション)。このような場合、デフォルトでパケットが破棄されるため、ACE を ACL に明示的に追加し、必要なトラフィックが許可されるように設定する必要があります。必要なトラフィックには、デバイス自体に送信される、Telnet、HTTP、SNMP などの管理トラフィックが含まれます。たとえば、ACL の条件と一致しないパケットをすべて廃棄しないようにするには、最もプライオリティの低い ACE を ACL に明示的に追加して、すべてのトラフィックを許可する必要があります。

ACL がバインドされているポートで IGMP/MLD スヌーピングが有効になっている場合は、ACE フィルタをその ACL に追加して、IGMP/MLD パケットがデバイスに転送されるようにします。追加しない場合、IGMP/MLD スヌーピングはそのポートで失敗します。

最初に一致した ACE が適用されるため、ACL 内における ACE の順序は重要です。ACE は、先頭のものから順次処理されます。

ACL は、特定のトラフィック フローを許可または拒否するなどの方法により、セキュリティ目的で使用する場合があります。また、QoS 拡張モードにおけるトラフィックの分類や優先順位付けにも使用されます。

注 ポートには、ACL を使用したセキュリティか QoS 拡張ポリシーを設定できますが、両方を同時に設定することはできません。

1 つのポートに関連付けられる ACL は、原則として 1 つのみです。ただし例外として、IP ベース ACL と IPv6 ベース ACL は、両方とも 1 つのポートに関連付けることができます。

1 つのポートに複数の ACL を関連付けるには、1 つ以上のクラス マップを含むポリシーを使用する必要があります。

定義できる ACL のタイプは、フレーム ヘッダーのどの部分を検査対象とするかにより異なっており、次のとおりです。

- MAC ACL：レイヤ 2 フィールドのみを検査します。「Defining MAC-based ACLs」を参照してください。
- IP ACL：IP フレームのレイヤ 3 レイヤを検査します。「IPv4 ベース ACL」を参照してください。
- IPv6 ACL：IPv4 フレームのレイヤ 3 レイヤを検査します。「Defining IPv6-Based ACL」を参照してください。

ACL 内のフィルタと一致したフレームは、その ACL の名前と同じ名前を持つフローとして定義されます。拡張 QoS の場合、このフロー名を使用してこれらのフレームを参照でき、QoS をこれらのフレームに適用できます。

ACL ロギング

この機能により、ACE にロギング オプションを追加できます。この機能が有効になっている場合、ACE が許可または拒否したパケットはすべて、これに関連する情報 SYSLOG メッセージを生成します。

ACL ロギングが有効な場合、ACL をインターフェイスにバインドすることにより、ACL ロギングをインターフェイスごとに指定できます。この場合、このインターフェイスに関連付けられている許可 ACE または拒否 ACE と一致するパケットに対して、SYSLOG が生成されます。

フローは、同一の特徴を持つパケットのストリームとして、次のように定義されます。

- 「レイヤ 2 パケット」：同じ送信元と宛先の MAC アドレス
- 「レイヤ 3 パケット」：同じ送信元と宛先の IP アドレス
- 「レイヤ 4 パケット」：同じ送信元と宛先の IP および L4 ポート

新しいフローの場合は常に、特定のインターフェイスからトラップされた先頭のパケットにより情報 SYSLOG メッセージが生成されます。同じフローの追加パケットは CPU にトラップされますが、このフローに対する SYSLOG メッセージは、5 分につき 1 メッセージのみ生成されます。この SYSLOG により、過去 5 分以内に少なくとも 1 パケットはトラップされたことがわかります。

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

サポートされるフロー数は次のとおりです。

- SG350xx ファミリ：ユニットごとに 150 個
- SG550XG ファミリ：スタック内のユニットごとに 150 個

SYSLOG

SYSLOG メッセージには情報の重大度が示され、パケットが拒否ルールか許可ルールと一致したかどうかが記述されます。

- レイヤ 2 パケットの場合、SYSLOG には次の情報が含まれます（該当する場合）：送信元 MAC、宛先 MAC、イーサタイプ、VLAN ID、および CoS キュー。
- レイヤ 3 パケットの場合、SYSLOG には次の情報が含まれます（該当する場合）：ソース IP、宛先 IP アドレス、プロトコル、DSCP 値、ICMP タイプ、ICMP コード、および IGMP タイプ。
- レイヤ 4 パケットの場合、SYSLOG には次の情報が含まれます（該当する場合）：送信元ポート、宛先ポート、および TCP フラグ。

次に SYSLOG の例を示します。

- 非 IP パケットの場合：
  - 06-Jun-2013 09:49:56 %3SWCOS-I-LOGDENYMAC: gi0/1: deny ACE 00:00:00:00:00:01 -> ff:ff:ff:ff:ff:ff, Ethertype-2054, VLAN-20, CoS-4, trapped
- IP パケット（v4 および v6）の場合：
  - 06-Jun-2013 12:38:53 %3SWCOS-I-LOGDENYINET: gi0/1: deny ACE IPv4(255) 1.1.1.1 -> 1.1.1.10, protocol-1, DSCP-54, ICMP Type-Echo Reply, ICMP code-5 , trapped
- L4 パケットの場合：
  - 06-Jun-2013 09:53:46 %3SWCOS-I-LOGDENYINETPORTS: gi0/1: deny ACE IPv4(TCP) 1.1.1.1(55) -> 1.1.1.10(66), trapped

ACL の設定

ここでは、ACL の作成方法と、ルールの（ACE）の追加方法について説明します。

ACL の作成ワークフロー

ACL を作成してインターフェイスと関連付けるには、次の操作を実行します。

1. 次のタイプの ACL を 1 つ以上作成します。
   a. MAC ベース ACL：[MAC ベース ACL] ページと [MAC ベース ACE] ページを使用して作成
   b. IP ベース ACL：[IPv4 ベース ACL] ページと [IPv4 ベース ACE] ページを使用して作成
   c. IPv6 ベース ACL：[IPv6 ベース ACL] ページと [IPv6 ベース ACE] ページを使用して作成
2. [ACL バインディング(VLAN)] ページと [ACL バインディング(ポート)] ページを使用して、ACL をインターフェイスに関連付けます。

ACL の変更ワークフロー

使用していない ACL のみ、変更できます。ACL を変更するために、ACL をアンバインドする手順を次に示します。

1. ACL が QoS 拡張モード クラス マップには属しておらず、インターフェイスに関連付けられている場合、[ACL バインディング(VLAN)] *または* [ACL バインディング(ポート)] ページを使用してインターフェイスからアンバインドします。
2. ACL がクラス マップの一部になっていて、インターフェイスにバインドされていない場合、その ACL は変更できます。
3. ACL が、インターフェイスにバインドされているポリシーに含まれるクラス マップの一部になっている場合、アンバインドするには次に示す一連の手順を実行する必要があります。
   - [ポリシーバインディング] を使用して、クラス マップを含むポリシーをインターフェイスからアンバインドします。
   - [ポリシーの設定]（**編集**）を使用して、ACL を含むクラス マップをポリシーから削除します。
   - [クラスマッピングの定義] を使用して、ACL を含むクラス マップを削除します。

このようにして初めて、この項で説明しているとおり、ACL を変更できます。

MAC ベース ACL の作成

MAC ベース ACL は、レイヤ 2 フィールドに基づいてトラフィックをフィルタ処理するために使用します。MAC ベース ACL は、一致するかどうかすべてのフレームを検査します。

MAC ベース ACL は [MAC ベース ACL] ページで定義します。ルールは [MAC ベース ACE] ページで定義します。

MAC ベース ACL

MAC ベース ACL を定義するには、次のようにします。

ステップ 1 [アクセスコントロール] > [MACベースACL] の順にクリックします。

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 [追加] 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 [適用] をクリックします。MAC ベース ACL が実行コンフィギュレーション ファイルに保存されます。

MAC ベース ACE

注 MAC ベースのルールは、それぞれ 1 つの TCAM ルールを使用します。TCAM 割り当てはペアで実行されることにご注意ください。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、次のようにします。

ステップ 1 [アクセスコントロール] > [MACベースACE] の順にクリックします。

ステップ 2 ACL を選択し、[実行] をクリックします。ACL に含まれる ACE が一覧表示されます。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

- [ACL名]:ACE を追加する ACL の名前が表示されます。
- [プライオリティ]:ACE のプライオリティを入力します。プライオリティが高い ACE が最初に処理されます。プライオリティは 1 が最高です。
- [アクション]:一致した場合に実行するアクションを選択します。次のオプションがあります。
  - [許可]:ACE 条件に一致するパケットを転送します。
  - [拒否]: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。このポートは、[エラー回復設定] ページから再アクティブ化できます。
- [ロギング]:選択すると、ACL ルールと一致する ACL フローのロギングが有効になります。
- [時間範囲]:選択すると、ACL の使用時間が指定した時間範囲に制限されます。
- [時間範囲名]:[時間範囲] 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。
- [宛先 MAC アドレス]:すべての宛先アドレスを許可する場合は [任意] を選択します。宛先アドレスを入力するか宛先アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先 MAC アドレス値]:宛先 MAC アドレスの照合に使用する MAC アドレスを入力します。必要に応じて、マスクも入力します。
- [宛先 MAC ワイルドカード マスク]:MAC アドレスの範囲を定義するためのマスクを入力します。このマスクは、サブネット マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、**1** に設定したビットの値はマスクせず、**0** に指定したビットの値はマスクします。

  注 0000 0000 0000 0000 0000 0000 1111 1111 というマスクを例に説明します。0 になっているビットの一致は照合され、1 になっているビットの一致は照合されません。1 を 10 進数の整数に変換し、4 つずつの 0 をまとめて 0 として記述する必要があります。この例では、1111 1111 = 255 で、マスクは 0.0.0.255 と記述されます。
- [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 [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。

- [送信元MACアドレス値]:送信元 MAC アドレスの照合に使用する MAC アドレスを入力します。必要に応じて、マスクも入力します。
- [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] を選択します。
- [802.1p値]: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 [適用] をクリックします。MAC ベース ACE 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 ベース ACL の作成

IPv4 ベース ACL は、IPv4 パケットを検査する際に使用します。ARP などその他の種類のフレームは検査されません。

照合できるフィールドは次のとおりです。

- IPプロトコル(既知のプロトコルの場合は名前で照合可。または値で直接照合)
- TCP/UDP トラフィックの送信元ポート/宛先ポート
- TCP フレームのフラグの値
- ICMP および IGMP のタイプとコード
- 送信元 IP アドレスおよび宛先 IP アドレス(ワイルドカードを含む)
- DSCP/IP 優先度値

注 ACL は、フローごとに QoS 処理を実行する際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] ページから、システムに ACL を追加できます。ルールは [IPv4 ベース ACE] ページで定義します。

IPv6 ACL は [IPv6ベースACL] ページで定義します。

IPv4 ベース ACL

IPv4 ベース ACL を定義するには、次のようにします。

ステップ 1 [アクセス コントロール] > [IPv4 ベース ACL] の順にクリックします。

このページには、現在定義されている IPv4 ベース ACL がすべて表示されます。

ステップ 2 [追加] 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 [適用] をクリックします。IPv4 ベース ACL 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 ベース ACE

注 IPv4 ベースのルールは、それぞれ 1 つの TCAM ルールを使用します。TCAM 割り当てはペアで実行されることにご注意ください。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 IPv4 ベース ACL に追加するには、次のようにします。

ステップ 1 [アクセスコントロール] > [IPv4ベースACE] の順にクリックします。

ステップ 2 ACL を選択し、[実行] をクリックします。選択した ACL に対して現在定義されている IP ACE が表示されます。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

- [ACL名]：ACL の名前が表示されます。
- [プライオリティ]：プライオリティを入力します。プライオリティが高い ACE が最初に処理されます。
- [アクション]：ACE と一致するパケットに割り当てるアクションを選択します。選択項目は次のとおりです。
  - [許可]：ACE 条件に一致するパケットを転送します。
  - [拒否]：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、パケットの宛先ポートを無効にします。ポートは [エラー回復設定] ページで再アクティブ化できます。

- [ロギング]:選択すると、ACL ルールと一致する ACL フローのロギングが有効になります。
- [時間範囲]:選択すると、ACL の使用時間が指定した時間範囲に制限されます。
- [時間範囲名]:[時間範囲] 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。
- [プロトコル]:選択すると、特定のプロトコルまたはプロトコル ID に基づく ACE が作成されます。すべての IP プロトコルを受け入れるには、[任意(IPv4)] を選択します。それ以外の場合は、次のプロトコルのうちの 1 つを、[リストから選択] ドロップダウンリストから選択します。
  - [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]:伝送制御プロトコル
  - [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
- [照合するプロトコルID]：名前を選択するのではなく、プロトコル ID を入力します。

- [送信元 IP アドレス]：すべての送信元アドレスを許可する場合は [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [送信元IPアドレス値]：送信元 IP アドレスの照合に使用する IP アドレスを入力します。
- [送信元 IP ワイルドカード マスク]：IP アドレスの範囲を定義するためのマスクを入力します。このマスクは、サブネット マスクなどの他のマスクとは異なる点にご注意ください。このマスクでは、1 に設定したビットの値はマスクせず、0 に指定したビットの値はマスクします。

  注 0000 0000 0000 0000 0000 0000 1111 1111 というマスクを例に説明します。0 になっているビットの一致は照合され、1 になっているビットの一致は照合されません。1 を 10 進数の整数に変換し、4 つずつの 0 をまとめて 0 として記述する必要があります。この例では、1111 1111 = 255 で、マスクは 0.0.0.255 と記述されます。
- [宛先IPアドレス]：すべての宛先アドレスを許可する場合は [任意] を選択します。宛先アドレスを入力するか宛先アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先IPアドレス値]：宛先 IP アドレスの照合に使用する IP アドレスを入力します。
- [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。

- [送信元ポート]:次のいずれかを選択します。
  - [任意]: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]: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、[リストから選択] ドロップダウン メニューで [800/6-TCP] または [800/17-UDP] が選択されている場合にのみアクティブになります。
  - [番号で1つ]: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、[リストから選択] ドロップダウン メニューで [800/6-TCP] または [800/17-UDP] が選択されている場合にのみアクティブになります。
  - [範囲]:パケットを照合する TCP/UDP 送信元ポートの範囲を選択します。設定可能なポート範囲は 8 種類あり、送信元ポートと宛先ポートで共有されています。TCP プロトコルと UDP プロトコルには、それぞれ 8 種類のポート範囲が設定されています。
- [宛先ポート]:使用可能な値のいずれかを選択します。値は、上述の [送信元ポート] フィールドと同じです。

  注 ACE の IP プロトコルを指定してからでなければ、送信元ポートや宛先ポートを入力できません。
- [TCPフラグ]: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。フィルタ処理されたパケットは、転送されるかドロップされます。TCP フラグを使用してパケットをフィルタ処理すると、パケットをきめ細かく制御できるので、ネットワーク セキュリティが向上します。
- [タイプ オブ サービス]:IP パケットのサービス タイプ。
  - [任意]:任意のサービス タイプ。
  - [照合するDSCP]: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 で説明されているとおり、IP ヘッダー内のサービス タイプ バイトで最も上位の 3 ビットを使用します。
- [ICMP]:ACL の IP プロトコルが ICMP である場合、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 タイプ名を選択するか、メッセージ タイプ番号を入力します。
  - [任意]:すべてのメッセージ タイプを受け入れます。
  - [リストから選択]:メッセージ タイプ名を選択します。
  - [照合するICMPタイプ]:フィルタリングに使用するメッセージ タイプ番号。

- [ICMPコード]: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。次のいずれかのオプションを選択して、このコードに基づいてフィルタリングするかどうかを設定します。
  - [任意]:すべてのコードを受け入れます。
  - [ユーザ定義]:フィルタリングに使用する 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 タイプ名を選択するか、メッセージ タイプ番号を入力します。
  - [任意]:すべてのメッセージ タイプを受け入れます。
  - [リストから選択]: メッセージ タイプ名を選択します。
  - [照合するIGMPタイプ]:フィルタリングに使用するメッセージ タイプ番号。

ステップ 5 [適用] をクリックします。IPv4 ベース ACE 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 ベース ACL の作成

[IPv6 ベース ACL] ページでは、純粋な IPv6 ベース トラフィックを検査する IPv6 ACL を表示および作成できます。IPv6 ACL では、IPv6 over IPv4 パケットや ARP パケットは検査しません。

注 ACL は、フローごとに QoS 処理を実行する際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

IPv6 ベース ACL を定義するには、次のようにします。

ステップ 1 [アクセス コントロール] > [IPv6 ベース ACL] の順にクリックします。

このウィンドウには、定義されている ACL とそのコンテンツのリストが表示されます。

ステップ 2 [追加] 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 [適用] をクリックします。IPv6 ベース ACL 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 ベース ACE

注 IPv6 ベースのルールは、それぞれ 2 つの TCAM ルールを使用します。

ステップ 1 [アクセスコントロール] > [IPv6ベースACE] の順にクリックします。

このウィンドウには、指定した ACL（ルールのグループ）に対する ACE（ルール）が表示されます。

ステップ 2 ACL を選択し、[実行] をクリックします。選択した ACL に対して現在定義されている IP ACE が表示されます。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

- [ACL名]：ACE を追加する ACL の名前が表示されます。
- [プライオリティ]：プライオリティを入力します。プライオリティが高い ACE が最初に処理されます。
- [アクション]：ACE と一致するパケットに割り当てるアクションを選択します。選択項目は次のとおりです。
  - [許可]：ACE 条件に一致するパケットを転送します。
  - [拒否]：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、パケットの宛先ポートを無効にします。ポートは [エラー回復設定] ページで再アクティブ化できます。
- [ロギング]：選択すると、ACL ルールと一致する ACL フローのロギングが有効になります。
- [時間範囲]：選択すると、ACL の使用時間が指定した時間範囲に制限されます。
- [時間範囲名]：[時間範囲] を選択した場合、使用する時間範囲を選択します。時間範囲については、「システムの時刻」の項で説明します。

- [プロトコル]:選択すると、特定のプロトコルに基づく ACE が作成されます。すべての IP プロトコルを受け入れるには、[任意(IPv6)] を選択します。

  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。

  - [TCP]:伝送制御プロトコル。2 台のホスト間で通信とデータ ストリームの交換を行うことができます。TCP を使用すると、確実にパケットが送達されるだけでなく、送信された順序どおりにパケットが伝送および受信されます。
  - [UDP]:ユーザ データグラム プロトコル。パケットを送信しますが、送達は保証されません。
  - [ICMP]:パケットをインターネット制御メッセージ プロトコル(ICMP)と照合します。

  または

  - [照合するプロトコル ID]:照合するプロトコルの ID を入力します。
- [送信元 IP アドレス]:すべての送信元アドレスを許可する場合は [任意] を選択します。送信元アドレスを入力するか送信元アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [送信元IPアドレス値]: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。必要に応じて、マスクも入力します。
- [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。
- [宛先IPアドレス]:すべての宛先アドレスを許可する場合は [任意] を選択します。宛先アドレスを入力するか宛先アドレスの範囲を指定する場合は [ユーザ定義] を選択します。
- [宛先IPアドレス値]:宛先 IP アドレスの照合に使用する IP アドレスを入力します。必要に応じて、マスクも入力します。
- [宛先 IP プレフィックス長]:IP アドレスのプレフィックス長を入力します。
- [送信元ポート]:次のいずれかを選択します。
  - [任意]: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]: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、[IPプロトコル] ドロップダウン メニューで [800/6-TCP] または [800/17-UDP] が選択されている場合にのみアクティブになります。

- [番号で1つ]: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、[IPプロトコル] ドロップダウン メニューで [800/6-TCP] または [800/17-UDP] が選択されている場合にのみアクティブになります。
- [範囲]:パケットを照合する TCP/UDP 送信元ポートの範囲を選択します。

- [宛先ポート]:使用可能な値のいずれかを選択します。値は、上述の [送信元ポート] フィールドと同じです。

  注 ACL の IPv6 プロトコルを指定してからでなければ、送信元ポートや宛先ポートを設定できません。

- [フロー ラベル]:IPv6 フロー ラベル フィールドに基づいて IPv6 トラフィックを分類します。これは IPv6 パケット ヘッダーに含まれる 20 ビットのフィールドです。送信元ステーションでは IPv6 フロー ラベルを使用して、同じフローに属する複数のパケットにラベルを付けることができます。すべてのフロー ラベルを受け入れ可能な場合は [任意] を選択します。または [ユーザ定義] を選択して、ACL で受け入れる特定のフロー ラベルを入力します。
- [TCPフラグ]: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。フィルタ処理されたパケットは、転送されるかドロップされます。TCP フラグを使用してパケットをフィルタ処理すると、パケットをきめ細かく制御できるので、ネットワーク セキュリティが向上します。フラグのタイプごとに、次のオプションのいずれかを選択します。
  - [設定]:フラグが SET の場合に照合します。
  - [設定解除]:フラグが Not SET の場合に照合します。
  - [設定しない]:TCP フラグを無視します。
- [タイプ オブ サービス]:IP パケットのサービス タイプ。
  - [任意]:任意のサービス タイプ。
  - [照合するDSCP]: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 で説明されているとおり、IP ヘッダー内のサービス タイプ バイトで最も上位の 3 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 タイプ名を選択するか、メッセージ タイプ番号を入力します。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]:すべてのメッセージ タイプを受け入れます。
- [リストから選択]:ドロップダウン リストからメッセージ タイプ名を選択します。
- [照合するICMPタイプ]:フィルタリングに使用するメッセージ タイプ番号。

• [ICMPコード]: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。次のいずれかのオプションを選択して、このコードに基づいてフィルタリングするかどうかを設定します。

- [任意]:すべてのコードを受け入れます。
- [ユーザ定義]:フィルタリングに使用する ICMP コードを入力します。

ステップ 5 [適用] をクリックします。

ACL バインディング

ACL をインターフェイス(ポート、LAG、または VLAN)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デフォルトのルールと照合され、このルールにも一致しないパケットはドロップされます。

1 つのインターフェイスにバインドできる ACL は 1 つのみですが、インターフェイスをポリシー マップにまとめ、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。

インターフェイスにバインドした ACL は、バインド先または使用中のポートすべてから削除しない限り、編集、変更、削除できません。

注 インターフェイス(ポート、LAG、または VLAN)は、ポリシーや ACL にバインドできますが、ポリシーと ACL の両方に同時にバインドすることはできません。

注 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。

ACL バインディング(VLAN)

ACL を VLAN にバインドするには、次のようにします。

ステップ 1 [アクセスコントロール] > [ACLバインディング(VLAN)] の順にクリックします。

ステップ 2 VLAN を選択して、[編集] をクリックします。

必要な VLAN が表示されない場合は、新規に追加します。

ステップ 3 次のいずれかを選択します。

- [MACベースACL]: インターフェイスにバインドする MAC ベース ACL を選択します。
- [IPv4 ベース ACL]: インターフェイスにバインドする IPv4 ベース ACL を選択します。
- [IPv6ベースACL]: インターフェイスにバインドする IPv6 ベース ACL を選択します。
- [デフォルト アクション]: 次のいずれかのオプションを選択します。
  - [いずれも拒否]: ACL に一致しないパケットは拒否(ドロップ)されます。
  - [いずれも許可]: ACL に一致しないパケットは許可(転送)されます。

  注 [デフォルトアクション] 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 [適用] をクリックします。ACL バインディングが変更され、実行コンフィギュレーション ファイルが更新されます。

注 ACL が選択されていない場合は、VLAN にバインド済みの ACL がバインド解除されます。

ACL バインディング(ポート)

ACL をポートまたは LAG にバインドするには、次のようにします。

ステップ 1 [アクセスコントロール] > [ACLバインディング(ポート)] の順にクリックします。

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] を選択します。

ステップ 3 [実行] をクリックします。選択したインターフェイスの各タイプについて、そのタイプのインターフェイスすべてと、それらの現在の ACL のリスト（**入力 ACL** と**出力 ACL**）が表示されます。

- [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）。
- [デフォルトアクション]：ACL のルールのアクション（[いずれもドロップ] または [いずれも許可]）。

  注 1 つのインターフェイスからすべての ACL をアンバインドするには、そのインターフェイスを選択し、[クリア] 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、[編集] 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。

入力ACL

- [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。
- [デフォルト アクション]：次のいずれかのオプションを選択します。
  - [いずれも拒否]：ACL に一致しないパケットは拒否（ドロップ）されます。
  - [いずれも許可]：ACL に一致しないパケットは許可（転送）されます。

  注 [デフォルトアクション] 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。

出力ACL

- [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。
- [デフォルト アクション]: 次のいずれかのオプションを選択します。
  - [いずれも拒否]: ACL に一致しないパケットは拒否(ドロップ)されます。
  - [いずれも許可]: ACL に一致しないパケットは許可(転送)されます。

  注 [デフォルトアクション] 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 [適用] をクリックします。ACL バインディングが変更され、実行コンフィギュレーション ファイルが更新されます。

注 ACL が選択されていない場合は、インターフェイスにバインド済みの ACL がバインド解除されます。

27

サービス品質

サービス品質(QoS)機能をネットワーク全体に適用した場合、基準に従ってネットワーク トラフィックにプライオリティが設定され、重要なトラフィックが優先的に処理されます。

ここで説明する内容は次のとおりです。

QoS の機能とコンポーネント

QoS 機能は、ネットワークのパフォーマンスを最適化する目的で使用されます。

QoS を使用すると、次のことが可能です。

- 次の属性に基づいて着信パケットをトラフィック クラスに分類する。
  - デバイス コンフィギュレーション
  - 入力インターフェイス
  - パケット内容
  - これらの属性の組み合わせ

QoS には、以下のことが含まれます。

- **トラフィック分類**:着信パケットのそれぞれを、パケットの内容やポートに基づいて、特定のトラフィック フローに属するものとして分類します。分類は ACL(アクセス コントロール リスト)によって行われ、ACL の条件を満たすトラフィックだけが CoS または QoS 分類の対象になります。
- **ソフトウェア キューへの割り当て**:着信パケットが転送キューに割り当てられます。パケットは特定のキューに送信され、そのパケットが所属するトラフィック クラスの機能として処理されます。「キュー」を参照してください。
- **その他のトラフィック クラス処理属性**:QoS 機構が各種のクラス(帯域幅管理など)に適用されます。

QoS 動作

信頼されるヘッダー フィールドのタイプは [グローバル設定] ページで入力します。また、[CoS/802.1p 値のキューへのマッピング] ページ(信頼モードが CoS/802.1p の場合)または [DSCP 値のキューへのマッピング] ページ(信頼モードが DSCP の場合)で、そのフィールドの値ごとに、フレームが送信される出力キューが割り当てられます。

QoS モード

選択されている QoS モードは、システム内のすべてのインターフェイスに適用されます。

- **基本モード**:サービス クラス(CoS)。

  同じクラスのトラフィックはすべて、同じように処理されます。具体的には、着信フレーム内で示されている QoS 値に基づいて、出力ポート上の出力キューを決定するという 1 つの QoS アクションが実行されます。この QoS 値は、レイヤ 2 においては VLAN Priority Tag(VPT)802.1p 値、レイヤ 3 においては、IPv4 の場合は Differentiated Service Code Point(DSCP)値、IPv6 の場合はトラフィック クラス(TC)値です。デバイスが基本モードで動作している場合、外部デバイス上で割り当てられたこの QoS 値が信頼されます。この QoS 値によって、このパケットのトラフィック クラスと QoS が決定されます。

  信頼されるヘッダー フィールドは、[グローバル設定] ページで入力します。また、[CoS/802.1p 値のキューへのマッピング] ページ(信頼モードが CoS/802.1p の場合)または [DSCP 値のキューへのマッピング] ページ(信頼モードが DSCP の場合)で、そのフィールドの値ごとに、フレームが送信される出力キューが割り当てられます。

- **拡張モード**：フローごとのサービス品質（QoS）。

  拡張モードの場合、フローごとの QoS は、クラス マップやポリサーで構成されます。

  - クラス マップは、フローのトラフィックの種類を定義し、1 つ以上の ACL が含まれています。ACL に合致するパケットは、フローに属します。
  - ポリサーは、設定されている QoS をフローに適用します。フローの QoS 設定に含められるのは、出力キュー、DSCP または CoS/802.1p 値、およびプロファイル外の（超過）トラフィックに対するアクションです。

- **無効モード**：このモードでは、すべてのトラフィックが単一のベスト エフォート キューにマッピングされまるため、特に優先されるトラフィックのタイプはありません。

アクティブになるのは、一度に 1 つのモードのみです。システムが QoS 拡張モードで動作するように設定されているときには、QoS 基本モードの設定値はアクティブになりません。その逆も同じです。

モードが変更されると、以下のことが発生します。

- QoS 拡張モードからその他のモードに変更される場合、ポリシー プロファイル定義とクラス マップが削除されます。インターフェイスに直接適用されている ACL は、適用された状態のままになります。
- QoS 基本モードから拡張モードに変更される場合、基本モードでの QoS 信頼モードの設定は保持されません。
- QoS が無効にされた場合、シェーパーとキューの設定（WRR/SP 帯域幅の設定）はデフォルト値にリセットされます。

その他のすべてのユーザ設定は、そのまま維持されます。

QoS を設定する手順

QoS の一般パラメータを設定するには、次のようにします。

ステップ 1 [QoS プロパティ] ページで、システムの QoS モード（基本、拡張、または無効。詳しくは、QoS モードを参照）を選択します。以下の手順では、QoS を有効にしてあることを前提としています。

ステップ 2 [QoS プロパティ] ページで、各インターフェイスにデフォルトの CoS プライオリティを割り当てます。

ステップ 3 [キュー] ページで、各出力キューに対してスケジュール方式（完全優先または WRR）と WRR 帯域割り当て率を設定します。

ステップ 4 [DSCP 値のキューへのマッピング] ページで、各 IP DSCP/TC 値に出力キューを割り当てます。デバイスが DSCP 信頼モードで動作している場合、着信パケットはその DSCP/TC 値に基づいて出力キューに格納されます。

ステップ 5 各 CoS/802.1p プライオリティに出力キューを割り当てます。デバイスが CoS/802.1 信頼モードで動作している場合、すべての着信パケットは、その CoS/802.1p プライオリティに基づいて出力キューに格納されます。この作業は [CoS/802.1p 値のキューへのマッピング] ページで行います。

ステップ 6 レイヤ 3 トラフィックで必要とされる場合のみ、[DSCP 値のキューへのマッピング] ページで、各 DSCP/TC 値にキューを割り当てます。

ステップ 7 以下のページで、帯域幅とレート制限を設定します。

a. [キューあたりの出力シェーピング] ページで、各キューに対する出力シェーピングを設定します。

b. [帯域幅] ページで、各ポートに対する入力レート制限と出力シェーピング レートを設定します。

ステップ 8 以下のうちのいずれか 1 つを実行することにより、選択したモードを設定します。

a. *基本 QoS モードの設定手順*に記載されているように基本モードを設定します。

b. *拡張 QoS モードの設定手順*に記載されているように拡張モードを設定します。

QoS を設定する手順

QoS の一般パラメータを設定するには、次のようにします。

ステップ 1 [QoS プロパティ] ページで信頼モードを選択し、QoS を有効にします。次に、[インターフェイス設定] ページで、ポートに対する QoS を有効にします。

ステップ 2 [QoS プロパティ] ページで、各インターフェイスにデフォルトの CoS または DSCP プライオリティを割り当てます。

ステップ 3 [キュー] ページで、各出力キューに対してスケジュール方式（完全優先または WRR）と WRR 帯域割り当て率を設定します。

ステップ 4 [DSCP 値のキューへのマッピング] ページで、各 IP DSCP/TC 値に出力キューを割り当てます。デバイスが DSCP 信頼モードで動作している場合、着信パケットはその DSCP/TC 値に基づいて出力キューに格納されます。

ステップ 5 各 CoS/802.1p プライオリティに出力キューを割り当てます。デバイスが CoS/802.1 信頼モードで動作している場合、すべての着信パケットは、その CoS/802.1p プライオリティに基づいて出力キューに格納されます。この作業は [CoS/802.1p 値のキューへのマッピング] ページで行います。

ステップ 6 以下のページで、帯域幅とレート制限を設定します。

a. [キューあたりの出力シェーピング] ページで、各キューに対する出力シェーピングを設定します。

b. [帯域幅] ページで、各ポートに対する入力レート制限と出力シェーピング レートを設定します。

全般

ここで説明する内容は次のとおりです。

- QoS プロパティ
- キュー
- CoS/802.1p 値のキューへのマッピング
- DSCP 値のキューへのマッピング
- 帯域幅
- キューあたりの出力シェーピング
- VLAN 入力レート制限
- iSCSI
- TCP 輻輳回避

QoS プロパティ

[QoS プロパティ] ページには、システムの QoS モード（基本、拡張、または無効：詳しくは、QoS モードの項を参照）を設定するためのいくつかのフィールドが含まれています。

QoS を有効にして、QoS モードを選択するには、次のようにします。

ステップ 1 [Quality of Service] > [全般] > [QoSプロパティ] をクリックします。

ステップ 2 QoS モードを設定します。次のオプションが選択できます。

- [無効]：デバイス上で QoS は無効になります。
- [基本]：デバイス上で QoS は基本モードで有効になります。
- [拡張]：デバイス上で QoS は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とその CoS 情報を表示または修正するには、[ポート] を選択します。すべての LAG とその CoS 情報を表示または修正するには、[LAG] を選択します。その後、[実行] をクリックします。

すべてのポートまたは LAG に対して次のフィールドが表示されます。

- [インターフェイス]：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 のデフォルト値は 0 です。デフォルトが関係するのは、タグなしフレームの場合のみ、かつ、システムが基本モードであり [グローバル設定] ページで [CoSを信頼] が選択されている場合のみです。

ステップ 4 [適用] 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、[編集] をクリックします。

ステップ 1 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（サービス クラス）値を選択します。

ステップ 2 [適用] をクリックします。この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、[CoS デフォルトの復元] 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、SP と WRR の 2 とおりがあります。

- [完全優先]:プライオリティが最も高いキュー内の出力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が空になった後に送出されます。つまり、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。
- [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。つまり、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ります。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 モードを選択するには、[キュー] ページを使用します。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 WRR の場合は、まず、キューからパケットが送出されます。そのキューに割り当てられた帯域幅がすべて使用されると、続いて、別のキュー内のパケットの送出が開始します。

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します。WRR モードの各キューに対する相対的なパケット送出割合は、各キューに割り当てられているウェイトによって決まります。

優先順位方式を選択し、WRR データを入力するには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [キュー] 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。
- [スケジューリング方式]:次のオプションのいずれかを選択します。
  - [完全優先]: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 [適用] 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値のキューへのマッピング] ページでは、802.1p 値(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] では、着信パケットの格納先となる出力キューが、そのパケットの VLAN タグ内の 802.1p 値に基づいて決定されます。タグが設定されていない着信パケットの場合、802.1p プライオリティが、入力ポートに割り当てられているデフォルトの CoS/802.1p プライオリティとなります。

キューが 8 個の場合のデフォルトのマッピングを、以下の表に示します。

802.1p Values (0 ～ 7。プライオリティは 7 が最高)	キュー (キューが 8 個 (1 ～ 8) の場合。プライオリティは 8 が最高)	7 個のキュー (8 が、スタック コントロール トラフィックで使用される最高のプライオリティ) スタック	備考
0	1	1	バックグラウンド
1	2	1	ベスト エフォート
2	3	2	エクセレント エフォート
3	6	5	基幹アプリケーション: LVS 電話の SIP
4	5	4	ビデオ
5	8	7	音声:Cisco 製 IP 電話のデフォルト値
6	8	7	インターワーク制御 LVS 電話の RTP
7	7	6	ネットワーク コントロール

CoS/802.1p 値とキューのマッピング ([CoS/802.1p 値のキューへのマッピング])、キューのスケジュール方式と帯域割り当て ([キュー] ページ) を調整することにより、ネットワークでのサービス品質目標を達成できます。

CoS/802.1p 値からキューへのマッピングは、以下のいずれかが存在する場合にのみ適用されます。

- デバイスが QoS 基本モードかつ CoS/802.1p 信頼モードである場合。
- デバイスが QoS 拡張モードであり、CoS/802.1p が信頼されているフローにパケットが属する場合

キュー 1 には最低のプライオリティが、350 および 550 ファミリのキュー 8 には最高のプライオリティが割り当てられます。

CoS 値を出力キューにマッピングするには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [CoS/802.1p 値のキューへのマッピング] 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]: 出力キューに割り当てる 802.1p プライオリティ タグ値が表示されます。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 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。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 がプライオリティの最も高い出力キューで、キュー 1 のプライオリティが最低です。

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 [適用]、[キャンセル]、または [デフォルトの復元] をクリックします。801.1p 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値のキューへのマッピング] ページでは、DSCP 値を出力キューにマッピングできます。[DSCP 値のキューへのマッピング テーブル] は、着信パケットの格納先となる出力キューが、そのパケットの DSCP 値に基づいて決定されます。着信パケットの VPT 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 値とキューのマッピングを 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。または、
- 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 をキューにマップするには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [DSCP 値のキューへのマッピング] 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、および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 [適用] 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。

帯域幅

[帯域幅] ページには、各インターフェイスに対する帯域幅情報が表示されます。

帯域幅情報を表示するには、次のようにします。

ステップ 1 [Quality of Service] > [全般] > [帯域幅] をクリックします。

このページ内のフィールドは [編集] ページで説明されます。ただし、次のフィールドを除きます。

- **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。
  - [レート制限(キロビット/秒)]: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 (バイト)]: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。
- **出力シェーピング レート:**
  - [ステータス]:出力シェーピング レートが有効になっているかどうかが表示されます。
  - [CIR (キロビット/秒)]:出力インターフェイスの最大帯域幅が表示されます。
  - [CBS (バイト)]: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、[編集] 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指定します。

- [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)。
- [入力レート制限(キロビット/秒)]: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)。
- [認定バーストサイズ(CBS)]:この入力インターフェイスに対する最大バースト データ サイズをバイトで入力します。この値は、使用帯域幅が一時的に許容制限を超えるとしても送信できるデータ量を意味します。このフィールドは、インターフェイスがポートの場合のみ利用可能です。(LAG とは無関係です)。

- [出力シェーピングレート]: このインターフェイスで出力シェーピングを有効にする場合、このフィールドを選択します。
- [認定情報レート(CIR)]: この出力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。
- [出力認定バーストサイズ(CBS)]: この出力インターフェイスに対する最大バースト データ サイズをバイトで入力します。この値は、使用帯域幅が一時的に許容制限を超えるとしても送信できるデータ量を意味します。

ステップ 5 [適用] をクリックします。帯域幅設定値が、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。

キューあたりの出力シェーピング

このデバイスでは、[帯域幅] ページで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の出力レートを制限できます。レートが制限されていないパケットは、レート計算において無視されます。つまり、それらのパケットのサイズは合計レート制限に含まれません。

キュー単位出力レート シェーピングは、無効にすることもできます。

キュー単位出力シェーピングを定義するには、次のようにします。

ステップ 1 [サービス品質] > [全般] > [キューあたりの出力シェーピング] をクリックします。

[キューあたりの出力シェーピング] ページには、各キューに対するレート制限とバースト サイズが表示されます。

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、[実行] をクリックします。

ステップ 3 ポートまたは LAG を選択し、[編集] 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 [インターフェイス] を選択します。

ステップ 5 必要な各キューに対して、次のフィールドの値を入力します。

- [有効]: このキューに対して出力シェーピングを有効にする場合に選択します。
- [認定情報レート(CIR)]: 最大レート値(CIR)を入力します(単位: Kbps)。CIR は、送信できる平均データ量です。
- [認定バーストサイズ(CBS)]: 最大バースト サイズ(CBS)をバイトで入力します。CBS は、CIR を一時的に超えて送信できるデータ量を意味します。

ステップ 6 [適用] をクリックします。帯域幅設定値が、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。

VLAN 入力レート制限

[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、以下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、パケット プロセッサのそれぞれに独立して適用されます。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、48 ポート以上のデバイスではパケット 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、そしてスタック中のユニット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、次のようにします。

ステップ 1 [サービス品質] > [全般] > [VLAN入力レート制限] をクリックします。

このページには、VLAN 入力レート制限の一覧表が表示されます。

ステップ 2 [追加] 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。
- [認定情報レート(CIR)]:VLAN への入力として受け入れ可能な最大平均データ量を、Kbps 単位で入力します。
- [認定バーストサイズ(CBS)]:この出力インターフェイスに対する最大バースト データ サイズをバイトで入力します。この値は、使用帯域幅が一時的に許容制限を超えるとしても送信できるデータ量を意味します。LAG の場合は入力できません。

ステップ 4 [適用] をクリックします。VLAN レート制限が追加され、実行コンフィギュレーション ファイルが更新されます。

iSCSI

このページでは、iSCSI 最適化をアクティブにすることができます。これは、iSCSI トラフィックを他のタイプのトラフィックより優先するメカニズムのセットアップを意味します。この機能がデバイス上で有効になっている場合は、すべてのインターフェイス上の iSCSI トラフィックに定義済みの優先順位が割り当てられ、iSCSI トラフィックはインターフェイス上で設定された ACL またはポリシー ルールの影響を受けなくなります。

iSCSI トラフィックは、iSCSI ターゲットが要求をリッスンする TCP ポート、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、次のようにします。

ステップ 1 [サービス品質] > [全般] > [iSCSI] をクリックします。

ステップ 2 次のフィールドを入力します。

- [iSCSI ステータス]:デバイス上の iSCSI トラフィックの処理を有効にする場合に選択します。
- [VPT 割り当て]:[未変更] を選択してパケット内のオリジナルの VLAN Priority Tag(VPT)値をそのまま使用するか、[再割り当て] フィールドに新しい値を入力します。

- [DSCP 割り当て]:[未変更] を選択してパケット内のオリジナルの DSCP 値をそのまま使用するか、[再割り当て] 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 3 [適用] をクリックし、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 と 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 [フロー タイプ] は [デフォルト] です。新しいフローを追加すると、その [フロー タイプ] が [スタティック] になります。

新しいフローを追加するには、次のようにします。

ステップ 4 [追加] をクリックして、以下のフィールドに入力します。

- [TCP ポート]:これは、iSCSI ターゲットが要求をリッスンする TCP ポート番号です。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。
- [ターゲット IP アドレス]:iSCSI ターゲットの IP アドレス(データが保存される)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] 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、[ユーザ定義] 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 5 [適用] をクリックし、設定を保存します。

デフォルト フローを復元する場合は、[デフォルト フローの復元] をクリックします。

TCP 輻輳回避

[TCP 輻輳回避] 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、次のようにします。

ステップ 1 [サービス品質] > [全般] > [TCP輻輳回避] をクリックします。

ステップ 2 [有効] をクリックして TCP 輻輳回避を有効にし、[適用] をクリックします。

QoS 基本モード

ここで説明する内容は次のとおりです。

概要

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。

基本 QoS モードの設定手順

基本 QoS モードを設定するには、次のようにします。

1. [QoS プロパティ] ページで、システムの基本モードを選択します。
2. [グローバル設定] ページで、信頼の動作を選択します。デバイスでは、CoS/802.1p 信頼モードおよび DSCP 信頼モードがサポートされています。CoS/802.1p 信頼モードでは、VLAN タグの 802.1p プライオリティが使用されます。DSCP 信頼モードでは、IP ヘッダーの DSCP 値が使用されます。

あるポートでは、例外として、着信 CoS マークを信頼しないことにする場合は、[インターフェイス設定] ページで、そのポートでの QoS 状態を無効にします。

グローバルに選択されている信頼モードを、ポートで有効または無効する場合は、[インターフェイス設定] ページを使用します。信頼モードなしでポートが無効にされている場合、その入力パケットはすべてベスト エフォートで転送されます。着信パケットの CoS/802.1p 値や DSCP 値が信頼できないポートでは、信頼モードを無効にするようお勧めします。そうしない場合、ネットワークのパフォーマンスが低下する可能性があります。

グローバル設定

[グローバル設定] ページには、デバイス上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 [信頼モード] 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 ドメインに入ってくるパケットは、その QoS ドメインの境界で分類されます。

信頼設定を定義するには、次のようにします。

ステップ 1 [サービス品質] > [QoS基本モード] > [グローバル設定] をクリックします。

ステップ 2 デバイスが基本モードになっているときに [信頼モード] を選択します。パケット CoS レベルおよび DSCP タグがそれぞれ別個のキューにマッピングされる場合、そのパケットの割り当て先キューは信頼モードによって決まります。

- [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、[CoS/802.1p 値のキューへのマッピング] 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 とキューの実際のマッピングは、[DSCP 値のキューへのマッピング] ページで設定できます。トラフィックが IP トラフィックではない場合、ベスト エフォート キューにマッピングされます。
- [CoS/802.1p、DSCP]：CoS/802.1p と DSCP のうち、いずれか設定されているほう。

ステップ 3 着信パケット中の元の DSCP 値を、DSCP オーバーライド テーブルに入力された新しい値でオーバーライドする場合は、[入力DSCPのオーバーライド] を選択します。[入力DSCPのオーバーライド] 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 [入力DSCPのオーバーライド] を有効にした場合は、[DSCPオーバーライドテーブル] をクリックして DSCP を設定し直します。（**DSCP オーバーライド テーブル**を参照）。

ステップ 5 [DSCP 入力] 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出力] の値を選択して、マッピングする発信値を指定します。

ステップ 6 [適用] 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。

インターフェイス設定

[インターフェイス設定] ページでは、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、次のようにします。

ステップ 1 [サービス品質] > [QoS基本モード] > [インターフェイス設定] をクリックします。

ステップ 2 [ポート] または [LAG] を選択して、ポートまたは LAG のリストを表示します。

[QoS 状態] に、各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、[編集] 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 このインターフェイスの QoS 状態(有効か無効か)をクリックして設定します。

ステップ 6 [適用] 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

ここで説明する内容は次のとおりです。

- ポリシー クラス マップ
- ポリシー バインディング

概要

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。これらのフローには、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り使用されます。ポリシーとそのコンポーネントには、以下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)アクションを伴う ACL ルール(ACE)のみに合致するパケットは、同じフローに属するものと見なされ、同じサービス品質が適用されます。そのようにして、1 つのポリシーに 1 つ以上のフローが含まれ、そのそれぞれにユーザ定義 QoS があります。
- クラス マップ(フロー)の QoS は関連するポリサーにより適用されます。ポリサーには、シングル ポリサーと集約ポリサーの 2 種類があります。それぞれのポリサーは、QoS 仕様により設定されます。シングル ポリサーは、そのポリサーの QoS 仕様に基づいて QoS を単一のクラス マップに、したがって単一のフローに適用します。集約ポリサーは、1 つ以上のクラス マップに、したがって 1 つ以上のフローに QoS を適用します。集約ポリサーは、異なる複数のポリシーからのクラス マップをサポート可能です。

  2 レート 3 カラー(2R3C)機能がデバイス上でサポートされます。この機能では、すべてのポリサーに 2 つのしきい値が割り当てられます。1 つ目のしきい値に到達すると、ユーザ設定の超過アクションが実行されます。2 つ目のしきい値に到達すると、ユーザ設定の違反アクションが実行されます(集約ポリサーを参照)。
- フローごとの QoS は、ポリシーを目的のポートにバインドすることによりフローに適用されます。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できません。

備考:

- シングル ポリサーと集約ポリサーは、デバイスがレイヤ 2 モードの場合に利用可能です。
- ACL については、ポリシーに関係なく、1 つの ACL を 1 つ以上のクラス マップに対して設定可能です。
- クラス マップは 1 つのポリシーにのみ属することができます。
- シングル ポリサーを使用するクラス マップが複数ポートにバインドされている場合、各ポートがそれぞれシングル ポリサーの独自のインスタンスを持ち、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。
- 集約ポリサーは、ポリシーおよびポートには関係なく、集約中のすべてのフローに QoS を適用します。

拡張 QoS 設定値は、3 つの部分で構成されます。

- マッチング ルールの定義。単一のルール グループに合致するすべてのフレームは、1 つの *フロー*と見なされます。
- ルールに合致する各フロー内のフレームに適用されるアクションの定義。
- ルールとアクションの組み合わせの、1 つ以上のインターフェイスへのバインド。

拡張 QoS モードの設定手順

拡張 QoS モードを設定するには、次のようにします。

1. [QoSプロパティ] ページで、システムの拡張モードを選択します。[グローバル設定] ページで、信頼モードを選択します。パケット CoS レベルおよび DSCP タグがそれぞれ別個のキューにマッピングされる場合、そのパケットの割り当て先キューは信頼モードによって決まります。
   - 内部 DSCP 値が着信パケットで使用されているものとは異なる場合、[アウトオブプロファイル DSCP リマーク] ページで、外部値を内部値にマッピングします。それにより、[DSCPリマーク テーブル] ページが表示されます。
2. 「ACL ワークフローの作成」の説明に従って、ACL を作成します。
3. ACL が定義されている場合は、[クラスマッピング] ページでクラス マップを作成して、ACL をクラス マップに関連付けます。

4. [ポリシーテーブル] ページでポリシーを作成し、[ポリシークラスマップ] ページでそのポリシーを 1 つ以上のクラス マップに関連付けます。また、必要なら、クラス マップをポリシーに関連付ける際にポリサーをそのクラス マップに割り当てることによって、QoS を指定することもできます。

   - **シングルポリサー**:[ポリシーテーブル] ページと[クラス マッピング] ページを使用して、クラス マップをシングル ポリサーに関連付けるポリシーを作成します。ポリシー内で、シングル ポリサーを定義します。
   - **集約ポリサー**:[集約ポリサー] ページで、フローごとに、合致するフレームすべてを同じポリサー(集約ポリサー)に送る QoS アクションを作成します。[ポリシーテーブル] ページで、クラス マップを集約ポリサーに関連付けるポリシーを作成します。

5. [ポリシーバインディング] ページで、ポリシーをインターフェイスにバインドします。

グローバル設定

[グローバル設定] ページには、デバイス上で信頼を有効にするための情報が含まれています。QoS ドメインに入ってくるパケットは、その QoS ドメインの境界で分類されます。

信頼設定を定義するには、次のようにします。

ステップ 1 [サービス品質] > [QoS拡張モード] > [グローバル設定] 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 [信頼モード] を選択します。パケット CoS レベルおよび DSCP タグがそれぞれ別個のキューにマッピングされる場合、そのパケットの割り当て先キューは信頼モードによって決まります。

- [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、[CoS/802.1p 値のキューへのマッピング] 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 とキューの実際のマッピングは、[DSCP 値のキューへのマッピング] 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]:非 IP トラフィックに信頼 CoS モード、および IP トラフィックに信頼 DSCP を使用する場合に選択します。

ステップ 3 [デフォルト モードのステータス] 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 でデフォルトで（ポリシーを作成することなく）CoS/DSCP を信頼できるようになります。

[QoS 拡張モード] で、[デフォルト モードのステータス] が [信頼できない] 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はキュー 1 に送られます。詳しくは、[サービス品質] > [QoS 拡張モード] > [グローバル設定] ページを参照してください。

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り、合致しないトラフィックはドロップされます。

ステップ 4 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。[入力DSCPのオーバーライド] 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 5 [入力DSCPのオーバーライド] を有効にした場合は、[DSCPオーバーライドテーブル] をクリックして DSCP を設定し直します。

DSCP オーバーライド テーブル

ステップ 1 次のフィールドを入力します。

- [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。

ステップ 2 [適用] をクリックします。

アウトオブプロファイル DSCP リマーク

クラス マップ(フロー)にポリサーが割り当てられている場合、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 マッピング 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、新しい DSCP 値によって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。出荷時設定では、パケットはこのテーブルの 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。

例: サービスのレベルとして、シルバー、ゴールド、プラチナの 3 種類があり、それらのレベルを示すマークとして使用する DSCP 着信値がそれぞれ 10、20、30 だとします。このトラフィックが、別のサービス プロバイダー(同じ 3 種類のレベルのサービスがあるが、DSCP 値として 16、24、48 が使用されている)に転送されると、**アウト オブ プロファイル DSCP リマーク**により、着信値から発信値へのマッピングに従って、着信値が変更されます。

DSCP 値をマップするには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [アウト オブ プロファイル DSCP リマーク] 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 入力] 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。

[アクションタイプ] に基づいてフィルタすることによって、すべての**超過**または**違反**を表示することができます。これにより、トラフィックがポリサーの超過しきい値または違反しきい値を超えたときのリマーキングを設定できます。

ステップ 2 着信値のマッピング結果となる [DSCP 出力] 値を選択します。

ステップ 3 [適用] 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 テーブルにより更新されます。

ステップ 4 このインターフェイスの CoS 情報を工場出荷時設定に戻すには、[デフォルトの復元] を選択します。

クラス マッピング

クラス マップは、その上で定義された ACL(アクセス コントロール リスト)を使用してトラフィック フローを定義します。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 マップに関連するアクションが、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 マップを定義しても、QoS には影響しません。そのクラス マップが使用されるようになるには、しなければならないことが他にもあります。

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(ポリシー テーブルを参照)。

注 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。

[クラスマッピング] ページには、定義されているクラス マップと、そ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 マップを追加したり削除したりできます。

クラス マップを定義するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [クラス マッピング] をクリックします。

クラス マップごとに、その上で定義された ACL がそれらの関係と一緒に表示されます。最大 3 つの ACL を [一致] と一緒に表示できます。[一致] 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 [追加] 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 個の場合、フレームがそれら ACL の両方に合致しなければならないのか、それとも選択された ACL のうち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。

- [クラスマップ名]:新しいクラス マップの名前を入力します。
- [一致ACLタイプ]: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および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または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 ACL を選択します。
- [優先ACL]:パケットを IP ベース ACL と MAC ベース ACL のどちらと最初に照合するのかを選択します。

ステップ　4　[適用] 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

事前定義ルール セットに合致するトラフィックのレートを測定し、ポートで許可されるファイル転送トラフィックのレートの制限などの制限を適用することができます。

これは、クラス マップの ACL を使用して目的のトラフィックを照合したり、ポリサーを使用して合致トラフィックに QoS を適用したりすることによって行えます。

ポリサーは、QoS 仕様により設定されます。ポリサーには、以下の 2 種類あります。

- **シングル(標準)ポリサー**:シングル ポリサーは、ポリサー QoS 仕様に基づいて QoS を単一のクラス マップに、つまりは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 マップが複数ポートにバインドされている場合、各ポートがそれぞれシングル ポリサーの独自のインスタンスを持ち、本来は互いに独立しているポートでクラス マップ(フロー)に QoS を適用します。シングル ポリサーは、[ポリシーテーブル] 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、つまりは 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、ポリシーおよびポートには関係なく、集約中のすべてのフローに QoS を適用します。集約ポリサーは、[集約ポリサー] 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、以下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。

- [ピーク強制]:ピーク バースト サイズを超えたらアクションを有効にするには、これを選択します。
- [最大情報レート(PIR)]:ピーク トラフィック レート(PIR)をキロビット/秒(kbps)単位で入力します。
- [ピークバーストサイズ(PBS)]:ピーク バースト サイズ(PBS)をキロビット/秒(kbps)単位で入力します。
- [違反アクション]:ピーク サイズを超えた場合のアクションを次の中から 1 つ選択します。
  - [ドロップ]:ピーク サイズが違反しているフレームをドロップします。
  - [アウトオブプロファイルDSCP]:事前に設定した DSCP 値でピーク サイズが違反し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)(単位:Kbps)。
- トラフィック量(入力認定バースト サイズ、CBS)(単位:バイト)。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)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て、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。
- 指定されたレートとオプション アクションに基づいてトラフィック ポリシングを設定します。CIR と、これらのオプション値と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、[集約ポリサー] ページで、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、次のようにします。

ステップ 1 [サービス品質] > [QoS拡張モード] > [集約ポリサー] 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 [追加] 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。
- [入力認定情報レート(CIR)]:最大帯域幅(単位:bps)。[帯域幅] ページにある説明を参照してください。
- [入力認定バーストサイズ(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(単位:バイト)を入力します。[帯域幅] ページにある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。選択項目は次のとおりです。
  - [ドロップ]:定義されている CIR 値を超えるパケットはドロップされます。
  - [アウト オブ プロファイル 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プされます。
- [ピーク強制]:ピーク バースト サイズを超えたらアクションを有効にするには、これを選択します。
- [最大情報レート(PIR)]:ピーク トラフィック レート(PIR)をキロビット/秒(kbps)単位で入力します。
- [ピークバーストサイズ(PBS)]:ピーク バースト サイズ(PBS)をキロビット/秒(kbps)単位で入力します。
- [違反アクション]:ピーク サイズを超えた場合のアクションを次の中から 1 つ選択します。
  - [ドロップ]:ピーク サイズが違反しているフレームをドロップします。
  - [アウトオブプロファイルDSCP]:事前に設定した DSCP 値でピーク サイズが違反しているフレームをマークします。

ステップ 4 [適用] 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

[ポリシー テーブル マップ] 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、ポリシーを作成したり削除したりすることもできます。インターフェイスにバインドされているポリシーだけがアクティブになります([ポリシーバインディング] ページを参照)。

各ポリシーは、以下のもので構成されます。

- ポリシーの中のトラフィック フローを定義する ACL の 1 つ以上のクラス マップ。
- ポリシーの中のトラフィック 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、[ポリシーテーブル] ページで、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、次のようにします。

ステップ 1 [サービス品質] > [QoS拡張モード] > [ポリシーテーブル] 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 [ポリシークラスマップテーブル] をクリックして、[ポリシークラスマップ] ページを表示します。
または
[追加] をクリックして、[ポリシーテーブルの追加] ページを表示します。

ステップ 3 [新規ポリシー名] フィールドに、新しいポリシーの名前を入力します。

ステップ 4 [適用] 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 マップを追加することができます。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。

ポリシーにクラス マップを追加するには、次のようにします。

ステップ 1 [サービス品質] > [QoS 拡張モード] > [ポリシー クラス マップ] をクリックします。

ステップ 2 フィルタでポリシーを選択して、[実行] をクリックします。そのポリシーの中のすべてのクラス 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、[追加] をクリックします。

ステップ 4 パラメータを入力します。

- [ポリシー名]: クラス マップの追加先ポリシーが表示されます。
- [クラス マップ名]: ポリシーに関連付ける既存のクラス マップを選択します。クラス マップは、[クラスマッピング] ページで作成されます。
- [アクションタイプ]: 合致するすべてのパケットの入力 CoS/802.1p や DSCP の値に関連するアクションを選択します。
  - [デフォルト信頼モードを使用する]: このオプションが選択されている場合は、デフォルト モード ステータスをグローバル信頼モードで使用します。デフォルト モード ステータスが「信頼できない」の場合は、入力 CoS/802.1p と DSCP の値を無視します。一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。
  - [常に信頼]: 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 ([グローバル設定] 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 ([グローバル設定] 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、そのプライオリティ値と [CoS/802.1p値のキューへのマッピングテーブル] 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、新しい DSCP と [DSCP値のキューへのマッピングテーブル] 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。

    そうでない場合、新しい値 (1..8) を、すべての合致パケットの出力キュー番号として使用します。
- [トラフィック リダイレクト]: 一致したトラフィックをリダイレクトするかどうかを選択します。リダイレクトする場合は、トラフィックをリダイレクトするユニット/ポートを選択します。
- [リダイレクト先]: トラフィックをリダイレクトするユニット/ポートを選択します。

- [トラフィックミラー]:トラフィック フローをアナライザのイーサネット ポートにミラーするように設定します。このオプションが選択されている場合は、トラフィックが SPAN セッション ID 1 で指定された宛先ポートにミラーされます。SPAN セッション ID 1 でターゲット ポートが指定されていない場合は、ミラー アクションが実行されません。トラフィック ミラー アクションを伴うポリシー クラス マップがインターフェイスに適用され、その同じインターフェイスが SPAN セッション 1 の送信元ポートとして定義されている場合は、特定のフローだけでなく、すべてのトラフィックがミラーされます。

  トラフィック ミラー アクションが設定されている場合でも、インターフェイスに適用されたポリシー(および ACL)の追加のルールとアクションが適用されます。例:

  - ミラー対象フローの ACL アクションが許可されている場合は、ミラーリングに加えて、フロー トラフィックも転送されます。フロー ACL のアクションが拒否になっている場合は、フロー トラフィックはミラーされますが、出力ネットワーク インターフェイスに転送されません(ドロップ動作)。
  - ポリシーが適用されるインターフェイス上のトラフィック フローがミラー対象のクラス マップ分類と一致しない場合は、デフォルト ポリシーのデフォルト アクションに従います。
- [ポリシングタイプ]:ポリシーのポリサー タイプを選択します。次のオプションがあります。
  - [なし]:ポリシーは使用されません。
  - [シングル]:ポリシーのポリサーはシングル ポリサーです。
  - [集約]:ポリシーのポリサーは集約ポリサーです。

ステップ 5 [ポリシングタイプ] が [集約] の場合は、[集約ポリサー] を選択します。

ステップ 6 [ポリシングタイプ] が [シングル] である場合、以下の QoS パラメータを入力します。

- [入力認定情報レート(CIR)]:CIR を Kbps 単位で入力します。[帯域幅] ページにある説明を参照してください。
- [入力認定バーストサイズ(CBS)]:CBS をバイト単位で入力します。[帯域幅] ページにある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]:定義されている CIR 値を超えるパケットはドロップされます。
  - [アウト オブ プロファイル DSCP]:定義されている CIR 値を超える IP パケットは、アウト オブ プロファイル DSCP リマーク テーブルに由来する新しい DSCP を使用して転送されます。

- [ピーク強制]:ピーク バースト サイズを超えたらアクションを有効にするには、これを選択します。
- [最大情報レート(PIR)]:ピーク トラフィック レート(PIR)をキロビット/秒(kbps)単位で入力します。
- [ピークバーストサイズ(PBS)]:ピーク バースト サイズ(PBS)をキロビット/秒(kbps)単位で入力します。
- [違反アクション]:ピーク サイズを超えた場合のアクションを次の中から 1 つ選択します。
  - [ドロップ]:ピーク サイズが違反しているフレームをドロップします。
  - [アウトオブプロファイルDSCP]:事前に設定した DSCP 値でピーク サイズが違反しているフレームをマークします。

ステップ 7 [適用] をクリックします。

ポリシー バインディング

[ポリシー バインディング] 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 プロファイルが特定のポートにバインドされている場合、それはそのポートでアクティブです。1 つのポートと 1 つの方向に設定できるポリシー プロファイルは 1 つのみですが、1 つのポリシーを複数のポートにバインドすることはできます。

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する(アンバインド)必要があります。

注 ポートは、ポリシーか ACL のいずれかにバインドできますが、その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、次のようにします。

ステップ 1 [サービス品質] > [QoS拡張モード] > [ポリシーバインディング] をクリックします。

ステップ 2 必要に応じて、[インターフェイスタイプ] を選択します。

ステップ 3 [実行] 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 [編集] をクリックします。

ステップ 5 入力ポリシー/インターフェイスに対して以下を選択します。

- [入力ポリシーバインディング]: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。
- [デフォルト アクション]:パケットがポリシーと一致した場合のアクションを選択します。
  - [いずれも拒否]: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一致したら転送する場合に選択します。
  - [いずれも許可]:インターフェイス上のパケットがどのポリシーにも合致しないならそれらを転送する場合に選択します。

  注 [いずれも許可] 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にのみです。

ステップ 6 出力ポリシー/インターフェイスに対して以下を選択します。

- [出力ポリシーバインディング]:出力ポリシーをインターフェイスにバインドする場合に選択します。
- [ポリシー名]:バインドする出力ポリシーを選択します。
- [デフォルト アクション]:パケットがポリシーと一致した場合のアクションを選択します。
  - [いずれも拒否]: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一致したら転送する場合に選択します。
  - [いずれも許可]:インターフェイス上のパケットがどのポリシーにも合致しないならそれらを転送する場合に選択します。

  注 [いずれも許可] 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にのみです。

ステップ 7 [適用] 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

これらのページでは、シングル ポリサーおよび集約ポリサーを管理したり、キュー統計情報を表示したりすることができます。

ポリサー統計

シングル ポリサーは、1 つのポリシー内の 1 つのクラス マップに割り当てられます。集約ポリサーは、1 つ以上のポリシー内の 1 つ以上のクラス マップに割り当てられます。

シングル ポリサー統計情報の表示

[シングルポリサー統計] ページでは、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、次のようにします。

ステップ 1 [サービス品質] > [QoS統計情報] > [シングルポリサー統計] 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。

- [インターフェイス]: 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。
- [クラスマップ]: 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。
- [アウトオブプロファイルバイト]: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 [追加] 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。
- [ポリシー名]:ポリシー名を選択します。
- [クラスマップ名]: クラス名を選択します。

ステップ 4 [適用] をクリックします。統計情報を求める付加的な要求が作成され、実行コンフィギュレーション ファイルが更新されます。

集約ポリサー統計情報の表示

集約ポリサー統計情報を表示するには、次のようにします。

ステップ 1 [サービス品質] > [QoS統計情報] > [集約ポリサー統計] 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。
- [プロファイル内バイト]:受信されたプロファイル内パケットの数。
- [アウトオブプロファイルバイト]: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 [追加] をクリックします。

ステップ 3 統計情報表示の対象となる [集約ポリサー名]、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 [適用] をクリックします。統計情報を求める付加的な要求が作成され、実行コンフィギュレーション ファイルが更新されます。

キュー統計情報

[キュー統計情報] ページには、転送されたパケットや破棄されたパケットなどのキュー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て、表示する統計情報（カウンタ セット）を定義するには、次のようにします。

ステップ 1 [Quality of Service] > [QoS統計情報] > [キュー統計情報] 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。

- [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。オプションは次のとおりです。
  - [リフレッシュなし]: 統計情報はリフレッシュされません。
  - [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 秒ごとにリフレッシュされます。
  - [60 秒]: 統計情報は 60 秒ごとにリフレッシュされます。

特定のユニットと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、[実行] 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。

- [キュー]: パケットが転送またはテール ドロップされたキュー。
- [送信パケット数]: 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割合。
- [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割合。

28

SNMP

このセクションでは、ネットワーク デバイスを管理する Simple Network Management Protocol（SNMP）機能について説明します。

具体的な内容は、次のとおりです。

- 概要
- エンジン ID
- ビュー
- グループ
- ユーザ
- コミュニティ
- トラップ設定
- 通知受信者
- 通知フィルタ

概要

SNMP バージョンとワークフロー

デバイスは SNMP エージェントとして機能し、SNMPv1、v2、および v3 をサポートします。さらに、サポートされる MIB（Management Information Base）で定義されたトラップを使用して、システム イベントをトラップ レシーバに報告します。

SNMPv1 および v2

このシステムへのアクセスを制御するには、コミュニティ エントリのリストを定義します。各コミュニティ エントリは、*コミュニティ ストリング*とそのアクセス権限で構成されています。システムは、適切な権限と適切な動作が設定されたコミュニティを指定する SNMP メッセージにのみ応答します。

SNMP エージェントは、デバイスの管理に使用される変数のリストを維持します。これらの変数は、*Management Information Base*（MIB; 管理情報ベース）内で定義されています。

注 SNMPv3 の使用が推奨されています。他のバージョンにはセキュリティの脆弱性があるためです。

SNMPv3

SNMPv3 では、SNMPv1 および SNMPv2 の機能に加え、SNMPv1 および SNMPv2 の PDU にアクセス制御機構と新しいトラップ機構が適用されてます。また、SNMPv3 では次のような User Security Model（USM）も規定されています。

- **認証**：データの整合性が確保されます。また、データ送信元を認証できます。
- **プライバシー**：メッセージの内容が開示されないように保護することができます。*暗号ブロック連鎖*（CBC-DES）が暗号化に使用されます。SNMP メッセージでは、認証のみを有効にすることも、認証とプライバシーの両方を有効にすることもできます。認証を有効にせずにプライバシーのみを有効にすることはできません。
- **適時性**：メッセージ遅延攻撃やメッセージ再生攻撃を防ぐことができます。SNMP エージェントでは、受信メッセージのタイム スタンプとメッセージ着信時刻が比較されます。
- **キー管理**：キーの生成、更新、および使用について定義できます。このデバイスでは、*Object ID*（OID）に基づく SNMP 通知フィルタを使用できます。OID は、デバイスの機能を管理する目的でシステムによって使用されます。

SNMP ワークフロー

注 セキュリティ上の理由から、SNMP はデフォルトで無効になっています。SNMP 経由でデバイスを管理する前に、[TCP/UDP サービス] ページで SNMP を有効にしておく必要があります。

SNMP を設定する際の推奨手順を次に示します。

SNMPv1 または SNMPv2 を使用する場合:

ステップ 1 [コミュニティ] ページに移動して、[追加] をクリックします。コミュニティは、基本モードの場合はアクセス権限とビューに関連付けることができます。拡張モードの場合はグループに関連付けることができます。コミュニティのアクセス権限は次の 2 つの方法で定義できます。

- **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、読み取りと書き込み、SNMP Admin のいずれかに設定できます。また、[ビュー] ページで定義されたビューを選択することによって、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、[グループ] ページで定義されたグループによって定義されます。グループには、特定のセキュリティ モデルを設定できます。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。

ステップ 2 SNMP 管理ステーションを 1 つのアドレスに制限するのか、それともすべてのアドレスから SNMP 管理を許可するのかを選択します。SNMP 管理を 1 つのアドレスに制限する場合は、[IPアドレス] フィールドに SNMP 管理 PC のアドレスを入力します。

ステップ 3 [コミュニティストリング] フィールドに一意のコミュニティ ストリングを入力します。

ステップ 4 オプションで、[トラップ設定] ページを使用してトラップを有効にします。

ステップ 5 オプションで、[通知フィルタ] ページを使用して通知フィルタを定義します。

ステップ 6 [SNMPv1.2 通知受信者] ページで通知受信者を設定します。

SNMPv3 を使用する場合:

ステップ 1 [エンジン ID] ページで SNMP エンジンを定義します。一意のエンジン ID を作成するか、またはデフォルトのエンジン ID を使用します。エンジン ID 設定を適用すると、SNMP データベースがクリアされます。

ステップ 2 オプションで、[ビュー] ページで SNMP ビューを定義します。これを指定すると、コミュニティまたはグループで利用できる OID の範囲が制限されます。

ステップ 3 [グループ] ページを使用してグループを定義します。

ステップ 4 [ユーザ] ページを使用してユーザを定義します。ここで、ユーザをグループに関連付けることができます。SNMP エンジン ID が設定されていない場合、ユーザが作成されない可能性があります。

ステップ 5 オプションで、[トラップ設定] ページを使用してトラップを有効または無効にします。

ステップ　6　オプションで、[通知フィルタ] ページを使用して通知フィルタを定義します。

ステップ　7　オプションで、[SNMPv3 通知受信者] ページを使用して通知受信者を定義します。

サポートされる MIB

サポートされる MIB のリストについては、以下の URL にアクセスし、**Cisco MIBS** としてリストされているダウンロード エリアに移動してください。

www.cisco.com/cisco/software/navigator.html

モデル OID

550 / 350 ファミリの OID は次のとおりです。

SKU 名	ファミリ名	OID
SG350-8PD	8 ポート PoE マネージド スイッチと 2 X 2.5G および 6 X Gig	9.6.1.95.8.11
SG350X-8PMD	8 ポート 2.5G PoE スタッカブル マネージド スイッチ	9.6.1.95.8.11
SG350X-24PD	24 ポート PoE スタッカブル マネージド スイッチと 4 X 2.5G および 20 X Gig	9.6.1.94.23.11
SF350-48	SF350-48 48 ポート 10/100 マネージド スイッチ	9.6.1.96.48.1
SF350-48P	SF350-48P 48 ポート 10/100 PoE マネージド スイッチ	9.6.1.96.48.5
SF350-48MP	SF350-48MP 48 ポート 10/100 PoE マネージド スイッチ	9.6.1.96.48.6
SG350XG-24F	SG350XG-24F 24 ポート 10 G SFP+ スタッカブル マネージド スイッチ	9.6.1.91.24.8
SG350XG-24T	SG350XG-24T 24 ポート 10 G Base-T スタッカブル マネージド スイッチ	9.6.1.91.24.9
SG350XG-48T	SG350XG-48T 48 ポート 10GBase-T スタッカブル マネージド スイッチ	9.6.1.91.48.9

SKU 名	ファミリ名	OID
SG350XG-2F10	SG350XG-2F10 12 ポート 10G スタッカブル マネージド スイッチ	9.6.1.91.12.9
SG350-8PD		9.6.1.95.8.11
SG350X-8PMD		9.6.1.94.8.12
SG350X-24PD		9.6.1.94.24.11
SG350-10	SG350-10 10 ポート ギガビット マネージド スイッチ	9.6.1.95.10.3
SG350-10P	SG350-10P 10 ポート ギガビット PoE マネージド スイッチ	9.6.1.95.10.5
SG355-10P	SG355-10P 10 ポート ギガビット PoE マネージド スイッチ	9.6.1.95.10.10
SG350-10MP	SG350-10MP 10 ポート ギガビット PoE マネージド スイッチ	9.6.1.95.10.6
SG350-28	SG350-28 28 ポート ギガビット マネージド スイッチ	9.6.1.95.28.1
SG350-28P	SG350-28P 28 ポート ギガビット PoE マネージド スイッチ	9.6.1.95.28.5
SG350-28MP	SG350-28MP 28 ポート ギガビット PoE マネージド スイッチ	9.6.1.95.28.6
SG350X-24	24 ポート ギガビット スタッカブル マネージド スイッチ	9.6.1.94.24.1
SG350X-24P	24 ポート ギガビット PoE スタッカブル マネージド スイッチ	9.6.1.94.24.5
SG350X-24MP	24 ポート ギガビット PoE スタッカブル マネージド スイッチ	9.6.1.94.24.6
SG350X-48	48 ポート ギガビット スタッカブル マネージド スイッチ	9.6.1.94.48.1
SG350X-48P	48 ポート ギガビット PoE スタッカブル マネージド スイッチ	9.6.1.94.48.5

SKU 名	ファミリ名	OID
SG350X-48MP	48 ポート ギガビット PoE スタッカブル マネージド スイッチ	9.6.1.94.48.6
SF550X-24	24 ポート 10/100 スタッカブル マネージド スイッチ	9.6.1.92.24.1
SF550X-24P	24 ポート 10/100 PoE スタッカブル マネージド スイッチ	9.6.1.92.24.5
SF550X-24MP	24 ポート 10/100 PoE スタッカブル マネージド スイッチ	9.6.1.92.24.6
SF550X-48	48 ポート 10/100 スタッカブル マネージド スイッチ	9.6.1.92.48.1
SF550X-48P	48 ポート 10/100 PoE スタッカブル マネージド スイッチ	9.6.1.92.48.5
SF550X-48MP	48 ポート 10/100 PoE スタッカブル マネージド スイッチ	9.6.1.92.48.6
SG550XG-8F8T	SG550XG-8F8T 16 ポート 10G スタッカブル マネージド スイッチ	9.6.1.90.16.9
SG550XG-24T	SG550XG-24T 24 ポート 10 G Base-T スタッカブル マネージド スイッチ	9.6.1.90.24.9
SG550XG-24F	24 ポート SFP+ 10 ギガビット スタッカブル スイッチ(2 コンボ、RPS サポート付き)	9.6.1.90.24.8
SG550XG-48T	SG550XG-48T 48 ポート 10GBase-T スタッカブル マネージド スイッチ	9.6.1.90.48.9

プライベート オブジェクト ID は、enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101) の下に配置されています。

エンジン ID

エンジン ID は、エンティティを一意に識別するために SNMPv3 エンティティで使用されます。SNMP エージェントは、正規の SNMP エンジンであると見なされます。つまり、エージェントは着信メッセージ（Get、GetNext、GetBulk、Set）に応答し、また、トラップ メッセージをマネージャに送信します。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 のメッセージ交換で使用されるローカル情報を維持します。デフォルトの SNMP エンジン ID は、企業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、管理ドメイン内で一意である必要があります。つまり、1 つのネットワーク上には、同じエンジン ID を持つデバイスは複数台存在しません。

ローカル情報は、読み取り専用の 4 個の MIB 変数（snmpEngineId、snmpEngineBoots、snmpEngineTime、および snmpEngineMaxMessageSize）に格納されます。

注意　エンジン ID を変更すると、設定されていたユーザとグループはすべて消去されます。

SNMP エンジン ID を定義するには、次のようにします。

ステップ 1　[SNMP] > [エンジンID] の順にクリックします。

ステップ 2　[ローカルエンジンID] に使用するエンジン ID を選択します。

- [デフォルトを使用]: デバイスによって生成されたエンジン ID を使用する場合に選択します。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ます。これは、規格ごとに次のように定義されています。
  - *第 1 ～ 4 オクテット*: 第 1 ビットは「1」、第 2 ～ 4 ビットは IANA 企業番号です。
  - *第 5 オクテット*: 3 に設定されます。これは、続くオクテットが MAC アドレスであることを意味します。
  - *第 6 ～ 11 オクテット*: デバイスの MAC アドレスです。
- [なし]: エンジン ID を使用しません。
- [ユーザ定義]: 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 進数文字列で入力します（**範囲: 10 ～ 64**）。16 進数文字列の各バイトは 2 桁の 16 進数で表されます。

すべてのリモート エンジン ID とその IP アドレスは、リモート エンジン ID テーブルに表示されます。

ステップ　3　[適用] 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 テーブルには、エンジンとエンジン ID の IP アドレスの間のマッピングが表示されます。

エンジン ID の IP アドレスを追加するには、次のようにします。

ステップ　4　[追加] をクリックします。次のフィールドを入力します。

- [サーバ指定方法]:エンジン ID サーバを IP アドレスで指定するか、名前で指定するかを選択します。
- [IP バージョン]:サポートする IP 形式を選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:リストからリンク ローカル インターフェイスを選択します(IPv6 アドレス タイプとしてリンク ローカルが選択されている場合)。
- [サーバのIPアドレス/名前]:ログ サーバの IP アドレスまたはドメイン名を入力します。
- [エンジンID]:エンジン ID を入力します。

ステップ　5　[適用] 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。

ビュー

ビューとは、MIB サブツリーの集合を表すユーザ定義ラベルのことです。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）が使用されます。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（「モデル OID」を参照）を入力します。

各サブツリーを定義中のビューに含めるか除外します。

[ビュー] ページでは、SNMP ビューを作成および編集できます。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。

ビューをグループにアタッチするには、[グループ] ページを使用します。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には、[コミュニティ] ページを使用します。

SNMP ビューを定義するには、次のようにします。

ステップ 1 [SNMP] > [ビュー] の順にクリックします。

ビューごとに次のフィールドが表示されます。

- [オブジェクトIDサブツリー]: ビューに含めるかまたは含めない MIB ツリー内のノード。
- [オブジェクトIDサブツリービュー]: ノードを含めるか含めないか。

ステップ 2 [追加] 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。

- [ビュー名]: 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]: 選択した SNMP ビューに含めるかまたは除外する MIB ツリー内のノードを選択します。オブジェクトの選択方法には次のものがあります。
  - [リストから選択]: MIB ツリー内を探索できます。選択されているノードの親または兄弟のレベルに移動するには、上矢印ボタンを押します。選択されているノードの子のレベルに移動するには、下矢印ボタンを押します。ノードからその兄弟ノードに移動するには、ビューでそのノードをクリックします。兄弟ノードがビューに表示されていない場合は、スクロールバーを使用します。
  - [ユーザ定義]: [リストから選択] オプションにない OID を入力します。

ステップ 4 [ビューに含める] を選択または選択解除します。これを選択した場合、選択された MIB がビューに組み込まれます。選択しなかった場合は、除外されます。

ステップ 5 [適用] をクリックします。

ステップ 6 ビューの設定を確認するために、[フィルタ] の[ビュー名] リストでユーザ定義ビューを選択します。デフォルトで存在するビューは次のとおりです。

- [デフォルト]:読み取りビューおよび読み取り/書き込みビュー用のデフォルトの SNMP ビュー。
- [DefaultSuper]:管理ビュー用のデフォルトの SNMP ビュー。

グループ

SNMPv1 および SNMPv2 では、SNMP フレームとともにコミュニティ ストリングが送信されます。コミュニティ ストリングは、SNMP エージェントへのアクセス権限を取得するためのパスワードの役割を果たします。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。そのため、SNMPv1 および SNMPv2 は安全ではありません。

SNMPv3 では、次のセキュリティ機構を設定できます。

- **認証**:デバイスで、SNMP ユーザが正規のシステム管理者であるかどうかを検査します。この検査は、フレームごとに実行されます。
- **プライバシー**:SNMP フレームで暗号化データを送信することができます。

それで、SNMPv3 では、次の 3 段階のセキュリティ レベルがあります。

- セキュリティなし(認証なし、プライバシーなし)
- 認証(認証あり、プライバシーなし)
- 認証およびプライバシー

SNMPv3 では、各ユーザが読み取りまたは書き込みをできる内容およびユーザが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/書き込み権限およびセキュリティ レベルを定義します。グループが機能するのは、そのグループに SNMP ユーザまたはコミュニティが関連付けられている場合です。

注 グループにデフォルトでないビューを関連付けるには、まず [ビュー] ページでビューを作成します。

SNMP グループを作成するには、次のようにします。

ステップ 1 [SNMP] > [グループ] の順にクリックします。

このページには、既存の SNMP グループとそのセキュリティ レベルが含まれています。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [グループ名]: 新しいグループ名を入力します。
- [セキュリティモデル]: このグループに関連付ける SNMP バージョン（SNMPv1、SNMPv2、または SNMPv3）を選択します。

さまざまなセキュリティ レベルと組み合わせて 3 種類のビューを定義できます。各セキュリティ 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]: セキュリティ レベルを有効にする場合にこのフィールドを選択します。
- [セキュリティレベル]: グループに関連付けるセキュリティ レベルを定義します。SNMPv1 と SNMPv2 は、認証とプライバシーのどちらもサポートしません。SNMPv3 を選択した場合は、次のいずれかを選択します。
  - [認証なし、プライバシーなし]: [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ません。
  - [認証、プライバシーなし]: SNMP メッセージを認証し、SNMP メッセージの送信元を認証しますが、それらを暗号化しません。
  - [認証、プライバシー]: SNMP メッセージを認証し、それらを暗号化します。
- [ビュー]: ビューにグループの読み取り、書き込み、通知のアクセス権限を関連付けることにより、グループが読み取り、書き込み、および通知アクセス権限を持つ MIB ツリーの範囲が制限されます。
  - [読み取り]: 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。それ以外の場合、このグループに関連付けられたユーザまたはコミュニティは、SNMP 自体を制御する MIB を除くすべての MIB を読み取ることができます。
  - [書き込み]: 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。それ以外の場合、このグループに関連付けられたユーザまたはコミュニティは、SNMP 自体を制御する MIB を除くすべての MIB に書き込むことができます。

- [通知]:利用可能なトラップの内容を、選択したビューに含まれるものだけに制限します。それ以外の場合、トラップに含まれる内容に制限はありません。このフィールドは、SNMPv3 の場合のみ選択できます。

ステップ 4 [適用] 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。

ユーザ

SNMP ユーザを定義するには、ログイン資格情報(ユーザ名、パスワード、および認証方式)、および、コンテキストとスコープを設定します。このコンテキストとスコープの中で、ユーザはグループおよびエンジン ID と関連付けられます。

設定されたユーザには、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。

グループを使用した場合、ネットワーク管理者は、アクセス権限を 1 人のユーザではなくユーザのグループに割り当てることができます。

各ユーザは、1 つのグループにしか所属できません。

SNMPv3 ユーザを作成するには、次の条件が満たされている必要があります。

- このデバイス上でエンジン ID が設定されていること。この作業は [エンジン ID] ページで行います。
- SNMPv3 グループを使用できること。SNMPv3 グループを定義するには、[グループ] ページを使用します。

SNMP ユーザを表示したり、新規に定義したりするには、次のようにします。

ステップ 1 [SNMP] > [ユーザ] の順にクリックします。

このページには、既存のユーザが表示されます。このページ内のフィールドは [追加] ページで説明されます。ただし、次のフィールドを除きます。

- [IPアドレス]:エンジンの IP アドレスが表示されます。

ステップ 2 [追加] をクリックします。

このページでは、SNMP アクセス制御権限を SNMP ユーザに割り当てるための情報が提供されます。

ステップ 3 パラメータを入力します。

- [ユーザ名]:ユーザの名前を入力します。
- [エンジンID]:このユーザが接続する SNMP エンティティが、ローカルとリモートのどちらであるかを選択します。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。インフォーム要求メッセージを受信したり情報を要求したりするには、ローカル ユーザとリモート ユーザの両方を作成する必要があります。
  - [ローカル]:ユーザはローカル デバイスに接続されます。
  - [リモートIPアドレス]:ユーザはローカル デバイスに加えて別の 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要求メッセージを受信しますが、情報を要求することはできません。

    リモート エンジン ID を入力します。
- [グループ名]:この SNMP ユーザを所属させる SNMP グループを選択します。SNMP グループは、[グループの追加] ページで定義します。

  注 削除されたグループに所属するユーザはそのまま残りますが、非アクティブになります。
- [認証方式]:認証方式を選択します。割り当てられたグループ名に応じて、認証方式が変わります。グループが認証を要求しない場合、そのユーザは、いずれの認証も設定することはできません。次のオプションがあります。
  - [なし]:ユーザ認証を行いません。
  - [MD5]:MD5 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。
  - [SHA]:SHA(Secure Hash Algorithm)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。
- [認証パスワード]:MD5 パスワードまたは SHA パスワードを使用して認証を行う場合は、ローカル ユーザ パスワードを [暗号化] または [プレーンテキスト] のいずれかに入力します。ローカル ユーザ パスワードは、ローカル データベースと照合されます。ASCII 文字 32 字以内で入力します。
- [プライバシー方式]:次のいずれかのオプションを選択します。
  - [なし]:プライバシー パスワードは暗号化されません。
  - [DES]:プライバシー パスワードは、DES(Data Encryption Standard)に従って暗号化されます。

- [プライバシーパスワード]:DES プライバシー方式が選択されている場合、16 バイトが必要です(DES 暗号化キー)。このフィールドは、ちょうど 32 文字の 16 進数でなければなりません。[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 [適用] をクリックし、設定を保存します。

コミュニティ

SNMPv1 および SNMPv2 におけるアクセス権限を管理するには、[コミュニティ] ページでコミュニティを定義します。コミュニティ名は、SNMP 管理ステーションとデバイスの間で共有されるパスワードのようなものです。これは、SNMP 管理ステーションを認証する目的で使用されます。

コミュニティを定義するのは、SNMPv1 と SNMPv2 の場合のみです。SNMPv3 では、コミュニティの代わりにユーザを使用します。ユーザはグループに所属し、そのグループにアクセス権限が割り当てられます。

[コミュニティ] ページでは、直接(基本モード)またはグループを介して(拡張モード)、コミュニティにアクセス権限が関連付けられます。

- **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、読み取りと書き込み、SNMP Admin のいずれかに設定できます。また、[ビュー] ページで定義されたビューを選択することによって、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、[グループ] ページで定義されたグループによって定義されます。グループには、特定のセキュリティ モデルを設定できます。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、次のようにします。

ステップ 1 [SNMP] > [コミュニティ] の順にクリックします。

このページには、設定された SNMP コミュニティとそのプロパティに関する表が表示されます。このページ内のフィールドは [追加] ページで説明されます。ただし、次のフィールドを除きます。

- [コミュニティタイプ]:コミュニティのモードが表示されます([基本] または [拡張])。

ステップ 2 [追加] をクリックします。

このページで、ネットワーク管理者は新しい SNMP コミュニティを定義および設定することができます。

ステップ 3 [SNMP 管理ステーション]: 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 アドレスを入力するには、[ユーザ定義] をクリックします。どの IP デバイスもこの SNMP コミュニティにアクセスできるようにするには、[すべて] をクリックします。

- [IPバージョン]: IPv4 または IPv6 を選択します。
- [IPv6アドレスタイプ]: サポートされる IPv6 アドレス タイプを選択します（IPv6 が使用される場合）。次のオプションがあります。
  - [リンク ローカル]: IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]: IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]: IPv6 アドレス タイプがリンク ローカルの場合、VLAN と ISATAP のどちらから IPv6 アドレスを受け取るかを選択します。
- [IPアドレス]: SNMP 管理ステーションの IP アドレスを入力します。
- [コミュニティストリング]: 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。
- [(コミュニティタイプ)基本]: このコミュニティ タイプでは、どのグループへも接続されません。選択できるのは、コミュニティ アクセス レベル（読み取り、読み取りと書き込み、または SNMP Admin）のみで、さらに任意で特定のビュー用に修飾することができます。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、次の各フィールドを入力します。
  - [アクセスモード]: このコミュニティのアクセス権限を選択します。次のオプションがあります。

    [読み取り専用]: 管理アクセス権限は読み取り専用に制限されます。コミュニティに変更を加えることはできません。

    [読み取りと書き込み]: 管理アクセス権限は読み取りと書き込みです。デバイス コンフィギュレーションに変更を加えることはできますが、コミュニティに変更を加えることはできません。

[SNMP Admin]：ユーザは、すべてのデバイス コンフィギュレーション オプションにアクセスできます。また、コミュニティを修正するアクセス許可が与えられます。SNMP Admin は、SNMP MIB を除くすべての MIB の読み取りと書き込みと同等です。SNMP Admin は、SNMP MIB にアクセスする際に必要です。

- [ビュー名]：SNMP ビュー（アクセスが付与されている MIB サブツリーの集合）を選択します。

- [(コミュニティタイプ)拡張]：選択されたコミュニティに対してこのタイプを選択します。
  - [グループ名]：SNMP グループを選択します。このグループによってアクセス権限が決まります。

ステップ 4 [適用] 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。

トラップ設定

[トラップ設定] 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、いつ通知を送信するかを設定できます。SNMP 通知の受信者を設定するには、[SNMPv1.2 通知受信者] ページまたは [SNMPv3 通知受信者] ページを使用します。

トラップ設定を定義するには、次のようにします。

ステップ 1 [SNMP] > [トラップ設定] の順にクリックします。

ステップ 2 このデバイスから SNMP 通知を送信できるように指定するには、[SNMP通知] で [有効] 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、[認証通知] で [有効] を選択します。

ステップ 4 [適用] をクリックします。SNTP トラップ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。

通知受信者

RFC 1215 で規定されているように、トラップ メッセージは、システム イベントを報告するために生成されます。このシステムでは、サポート対象の MIB で定義されるトラップを生成できます。

トラップ受信者（通知受信者）は、デバイスからトラップ メッセージが送信されるネットワーク ノードです。通知受信者のリストを定義できます。

トラップ受信者エントリは、ノードの IP アドレス、および、トラップ メッセージに格納されるバージョンに対応する SNMP 資格情報で構成されています。トラップ メッセージの送信が必要なイベントが発生した場合、通知受信者テーブル内のすべてのノードに送信されます。

[SNMPv1.2 通知受信者] ページおよび [SNMPv3 通知受信者] ページでは、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。[追加] ポップアップ ウィンドウおよび [編集] ポップアップ ウィンドウでは、通知の属性を設定できます。

SNMP 通知は、デバイスから SNMP 管理ステーションに送信されるメッセージであり、リンク アップ、リンク ダウンなど、何らかのイベントが発生したことを意味します。

特定の通知をフィルタリングすることもできます。これを行うには、[通知フィルタ] ページでフィルタを作成し、それを SNMP 通知受信者にアタッチします。通知フィルタを使用することにより、送信する通知の OID に基づいて、管理ステーションに送信する SNMP 通知の種類をフィルタリングできます。

SNMPv1.2 通知受信者

SNMPv1、v2 の受信者を定義するには、次のようにします。

ステップ 1 [SNMP] > [通知受信者SNMPv1、2] の順にクリックします。

このページには、SNMPv1、v2 の受信者が表示されます。

ステップ 2 次のフィールドを入力します。

- [IPv4送信元インターフェイスを通知する]：IPv4 SNMP サーバとの通信に使用するインフォーム要求メッセージ内で、IPv4 アドレスをソース 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。
- [IPv6 送信元インターフェイスをトラップする]：IPv4 SNMP サーバとの通信に使用するトラップ メッセージ内で、IPv6 アドレスをソース IPv6 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。

- [IPv6送信元インターフェイスを通知する]:IPv4 SNMP サーバとの通信に使用するインフォーム要求メッセージ内で、IPv4 アドレスをソース 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。
- [IPv6 送信元インターフェイスをトラップする]:IPv6 SNMP サーバとの通信に使用するトラップ メッセージ内で、IPv6 アドレスをソース IPv6 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。

  注 [自動] オプションが選択されている場合、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。

ステップ 3 [追加] をクリックします。

ステップ 4 パラメータを入力します。

- [サーバ指定方法]: リモート ログ サーバを 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]:IPv4 または IPv6 を選択します。
- [IPv6アドレスタイプ]:[リンクローカル] または [グローバル] を選択します。
  - [リンク ローカル]: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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能かつアクセス可能なグローバル ユニキャスト IPV6 タイプになります。
- [リンクローカルインターフェイス]:IPv6 アドレス タイプがリンク ローカルの場合、VLAN と ISATAP のどちらから IPv6 アドレスを受け取るかを選択します。
- [受信者のIPアドレス/名前]: トラップの送信先の IP アドレスまたはサーバ名を入力します。
- [UDPポート]: 受信デバイス側で通知に使用される UDP ポートを入力します。
- [通知タイプ]: トラップとインフォーム要求のどちらを送信するかを選択します。両方とも送信する必要がある場合は、受信者を 2 つ作成する必要があります。
- [タイムアウト]: 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。
- [リトライ回数]: デバイスがインフォーム要求を再送信する回数を入力します。

- [コミュニティ ストリング]:プルダウンからトラップ マネージャのコミュニティ ストリングを選択します。コミュニティ ストリング名は、[コミュニティ]ページにリストされた名前から生成されます。
- [通知バージョン]:トラップの SNMP バージョンを選択します。SNMPv1 と 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。一度に有効にできるのは 1 つのバージョンのみです。
- [通知フィルタ]:管理ステーションに送信する SNMP 通知の種類をフィルタリングする場合に選択します。フィルタは、[通知フィルタ] ページで作成します。
- [フィルタ名]: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] ページで定義)を選択します。

ステップ 5 [適用] をクリックします。SNTP 通知受信者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。

SNMPv3 通知受信者

SNMPv3 の受信者を定義するには、次のようにします。

ステップ 1 [SNMP] > [通知受信者SNMPv3] の順にクリックします。

このページには、SNMPv3 の受信者が表示されます。

- [IPv4送信元インターフェイスを通知する]:IPv4 SNMP サーバとの通信に使用するインフォーム要求メッセージ内で、IPv4 アドレスをソース 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。
- [IPv6 送信元インターフェイスをトラップする]:IPv4 SNMP サーバとの通信に使用するトラップ メッセージ内で、IPv6 アドレスをソース IPv6 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。
- [IPv6送信元インターフェイスを通知する]:IPv4 SNMP サーバとの通信に使用するインフォーム要求メッセージ内で、IPv4 アドレスをソース 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。
- [IPv6 送信元インターフェイスをトラップする]:IPv6 SNMP サーバとの通信に使用するトラップ メッセージ内で、IPv6 アドレスをソース IPv6 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 2 [追加] をクリックします。

ステップ　3　パラメータを入力します。

- [サーバ指定方法]:リモート ログ サーバを 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]:IPv4 または IPv6 を選択します。
- [IPv6 アドレス タイプ]:IPv6 アドレス タイプを選択します(IPv6 が使用される場合)。次のオプションがあります。
  - [リンク ローカル]:IPv6 アドレスによって、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。リンク ローカル アドレスは 1 つだけサポートされます。リンク ローカル アドレスがインターフェイス上に存在している場合、この入力値が、コンフィギュレーション内のアドレスと置き換わります。
  - [グローバル]:IPv6 アドレスは、他のネットワークから認識可能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]: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 タイプとしてリンク ローカルが選択されている場合)。
- [受信者のIPアドレス/名前]:トラップの送信先の IP アドレスまたはサーバ名を入力します。
- [UDPポート]:受信デバイス側で通知に使用される UDP ポートを入力します。
- [通知タイプ]:トラップとインフォーム要求のどちらを送信するかを選択します。両方とも送信する必要がある場合は、受信者を 2 つ作成する必要があります。
- [タイムアウト]:デバイスがインフォーム要求またはトラップを再送信するまでの待機時間を秒数で入力します。タイムアウト:範囲:1 ～ 300、デフォルト:15
- [リトライ回数]: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。リトライ回数:範囲:1 ～ 255、デフォルト:3
- [ユーザ名]:ドロップダウン リストから SNMP 通知送信先ユーザを選択します。通知を受け取るには、このユーザが [ユーザ] ページで定義されていて、そのエンジン ID がリモートである必要があります。
- [セキュリティ レベル]: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、選択したユーザ名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] の選択肢は [認証なし] のみです。ただし、[ユーザ] ページでこのユーザ名に認証およびプライバシーが割り当てられた場合、この画面のセキュリティ レベルの選択肢は、認証なし、認証のみ、または認証とプライバシーのいずれかになります。

次のオプションがあります。

- [認証なし]:パケットに対して認証処理も暗号化処理も実行されません。
- [認証]:パケットに対して認証処理は実行されますが、暗号化処理は実行されません。
- [プライバシー]:パケットに対して認証処理と暗号化処理の両方が実行されます。

- [通知フィルタ]:管理ステーションに送信する SNMP 通知の種類をフィルタリングする場合に選択します。フィルタは、[通知フィルタ] ページで作成します。
- [フィルタ名]: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] ページで定義)を選択します。

ステップ 4 [適用] をクリックします。SNTP 通知受信者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。

通知フィルタ

[通知フィルタ] ページでは、SNMP 通知フィルタ、および、検査される OID を設定できます。通知フィルタを作成したら、[SNMPv1.2 通知受信者] ページおよび [SNMPv3 通知受信者] ページで、通知受信者にアタッチすることができます。

通知フィルタを使用することにより、送信する通知の OID に基づいて、管理ステーションに送信する SNMP 通知の種類をフィルタリングできます。

通知フィルタを定義するには、次のようにします。

ステップ 1 [SNMP] > [通知フィルタ] の順にクリックします。

[通知フィルタ] ページでは、フィルタごとに通知情報が表示されます。[フィルタ名] を使用して、このテーブル内の通知エントリをフィルタリングすることができます。

ステップ 2 [追加] をクリックします。

ステップ 3 パラメータを入力します。

- [フィルタ名]: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]:選択した SNMP フィルタに含めるかまたは除外する MIB ツリー内のノードを選択します。オブジェクトの選択方法には次のものがあります。
  - [リストから選択]:MIB ツリー内を探索できます。選択されているノードの親または兄弟のレベルに移動するには、上矢印ボタンを押します。選択されているノードの子のレベルに移動するには、下矢印ボタンを押します。ノードからその兄弟ノードに移動するには、ビューでそのノードをクリックします。兄弟ノードがビューに表示されていない場合は、スクロールバーを使用します。
  - [オブジェクトID] を使用する場合、[フィルタに含める] オプションが選択されていると 、**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 [フィルタに含める] を選択または選択解除します。これを選択した場合、選択された MIB がフィルタに組み込まれます。選択しなかった場合は、除外されます。

ステップ 5 [適用] 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。

29

スマート ネットワーク アプリケーション(SNA)

ここでは、スマート ネットワーク アプリケーション(SNA)システムについて説明します。このシステムは、デバイスとトラフィックの詳細なモニタリング情報を含む、ネットワーク トポロジの概要を表示します。このシステムでは、ネットワーク内でサポートされているすべてのデバイスの構成をグローバルに表示して変更することができます。

この章では以下のトピックを取り上げます。

- SNA セッション
- SNA グラフィックス
- トポロジ表示
- 右側の情報パネル
- 操作
- オーバーレイ
- タグ
- 検索
- 通知
- デバイス認可制御(DAC)
- サービス
- SNA 設定の保存
- 技術的詳細

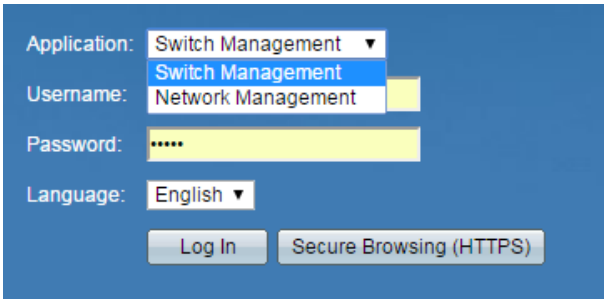
SNA セッション

SNA を起動するには、以下のようにします。

ステップ 1 Web ブラウザを開きます。

ステップ 2 ブラウザのアドレス バーに、構成しているデバイスの IP アドレスを入力し、Enter キーを押します。

ステップ 3 ログイン ウィンドウが表示されたら、ユーザ名とパスワードを入力して、[ネットワーク管理] を選択します。



[スイッチ管理] を選択すると、下の図のように、トップ バナーから [SNA] を選択できます。

初めて SNA に入ると、トポロジ マップが空の状態で表示され、モーダルの後ろでブロックされます。クレデンシャル(最大 20 文字のユーザ名と最大 64 文字のパスワード)を入力するように要求されます。クレデンシャルが拒否された場合は、拒否とその理由が通知されます。

SNA が読み込まれると、SNA へのログインに使用されたものと同じクレデンシャルを使用して、WebSocket 経由でネットワーク内の他のすべての SNA 対応デバイスとの管理セッションが作成されます。その結果、同じクレデンシャルを使用している SNA 対応デバイスのみがデータと管理機能を提供します。他のデバイスは、SNA 機能を備えていても SNA デバイスとして表示されません。

SNA セッションには次のアクセス権限レベルがあります。

- **フル**:セッションはフル アクセス モードで開始します。すべての SNA 操作が可能です。
- **読み取り専用**:アイドル状態が 15 分以上続くと、セッションは読み取り専用になります。このモードでは、デバイスに書き込んだり、デバイスを構成したりするアクションがすべてブロックされるため、呼び出すにはセッションをフル セッションにアップグレードするしかありません。アップグレードは、クレデンシャルを再入力することでいつでも実行できます。

デバイスの設定を変更しない操作であれば、セッションのアクセス モードに関係なく実行できます。

SNA は、Web スイッチ管理アプリケーションと同じクレデンシャルを使用して、それが機能する HTTP 管理セッションを作成します。SNA セッションは、アクティブな通常の Web 管理セッションとともに、同時に起動できる SNA マネージャの Web 管理セッションの数をカウントします。

セッション設定は保存することができます。「SNA 設定の保存」を参照してください。

SNA グラフィックス

SNA の特色は、ユーザ ネットワークのグラフィカル表現です。SNA のメイン ページを開くと、画面が次の部分に分割されて表示されます。

- トポロジ表示
- 右側の情報パネル
- トポロジ オーバーレイ
- オーバーレイ

SNA で使用されるアイコンは以下の通りです。

表 1　アイコンの説明

アイコン	説明
	クラウド
	バックボーン デバイス。オレンジ色の数字は、そのデバイスの既存の通知の数を表しています。
	オフライン デバイス(灰色表示)
	アクセス ポイント
	クライアント PC
	クライアント電話機
	クライアント不明デバイス

表 1　アイコンの説明

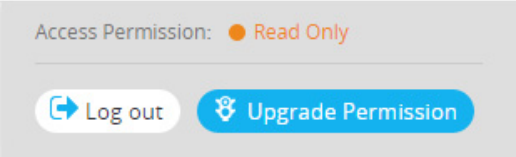
アイコン	説明
	側面パネル接続
	側面パネル複数選択
	側面パネル ポート

右上のメニュー

右上のメニューでは、さまざまな操作を実行できます。このメニューは次のように表示されます。

アイコンをクリックすることによって次のアクションを実行します。

- **A**:構成の変更をスタートアップ コンフィギュレーション ファイルに保存します。
- **B**:DAC リスト管理システムを開きます。「デバイス認可制御(DAC)」を参照してください。
- **C**:グローバル通知ページを開きます。「通知」を参照してください。
- **D**:次のウィンドウを開きます。



このウィンドウは、以下を表示または有効にします。

- アクセス権限を表示します。
- [ログアウト] をクリックすることによってシステムからログアウトします。
- [許可のアップグレード] をクリックすることによって許可をアップグレードします。

• E:選択したデバイスを削除する場合にクリックします。

トポロジ表示

トポロジ表示は SNA のメイン ビューです。

図 1 は、個別のデバイスとそれらをつないでいる接続情報を含む、ネットワークをグラフィカルに表したものです。

図 1　トポロジ表示:

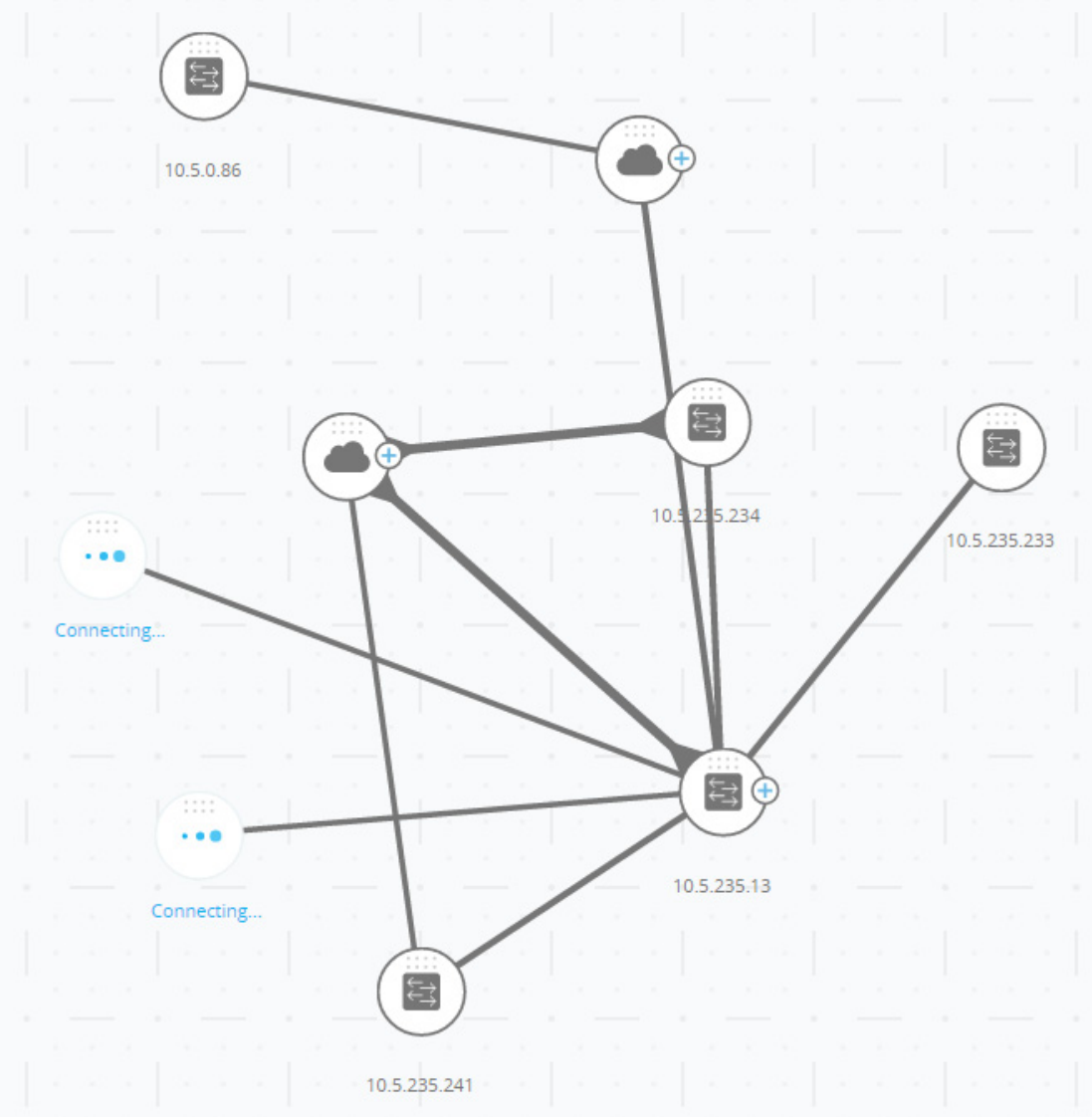


図　1 に示されているネットワーク ノードの説明については、「アイコンの説明」を参照してください。

要素のグラフィック表現に影響するさまざまなオーバーレイをトポロジ表示に対して選択できます。「トポロジ オーバーレイ」を参照してください。

トポロジ ディスカバリ メカニズムは、LLDP と CDP TLV から収集された情報を使用して、ネットワーク内のデバイスを識別します。

トポロジ内で提供される情報を最大化するには、これらのプロトコルをサポートしているネットワーク内のすべてのデバイスでプロトコルを有効にする必要があります。

トポロジは参加している SNA デバイスとの管理セッションを作成することによって生成されます。そのため、HTTPS プロトコルを使用して SNA を起動している場合は、ネットワーク内のすべての SNA スイッチが、SNA に使用される Web クライアント(ブラウザ)で認可されるか、証明書例外リストに追加されていなければなりません。

トポロジ オーバーレイ

トポロジ表示の要素のグラフィック表現のコンテンツを決定するさまざまなオーバーレイがサポートされています。サポートされているオーバーレイには、次のものがあります:VLAN メンバーシップ、スパニング ツリー、PoE、リンク使用率。たとえば、VLAN メンバーシップのオーバーレイを選択した場合は、VLAN 情報がトポロジ表示に追加されます。詳しい説明については、「オーバーレイ」を参照してください。

トポロジ要素

トポロジ表示には、次のタイプのエンティティが表示されます。

- デバイス
- ポート
- デバイス間の接続
- クラウド

デバイス

図 1 に示されているように、検出されたデバイスはトポロジ表示でノードとして表現されます。

デバイスをクリックすると、右側の情報パネルに次の情報が表示されます(情報がある場合)。

- [デバイスタイプ]:アイコンの形状がデバイス タイプを表します。デバイス タイプには、スイッチ、アクセス ポイント、PC、または IP 電話などがあります。デバイス タイプが事前に定義されていない場合または何らかの理由でタイプが正しく検出されない場合は、デバイス タイプが**不明**として表示されます。

  ネットワーク上で検出されたスイッチには、次のタイプのいずれかのラベルが付けられます。

  - **SNA スイッチ**:フル SNA 機能セットを有するスイッチ(バージョン 2.2.5 以降を実行)。

- **部分 SNA スイッチ**:SNA スイッチ経由で管理セッションを開始することにより、リモートでアクセス可能なスイッチ。この場合、ディスカバリ、サービス エクスプローラ、フル SNA 機能セットはありません。
- **管理対象外スイッチ**:SNA 経由でアクセスできないスイッチ。

- [デバイス名]
- [IP アドレス](複数発見された場合は一覧表示)
- [MAC アドレス](複数発見された場合は一覧表示)
- [通知数]:通知数は、デバイス アイコンのオレンジ色の数字で示されます。実際の通知は、右側の情報パネルに表示されます。
- [SNA サポート]
- [メーカー]

一部のデバイス(特に SNA 対応デバイス)には、個別のポート情報など、さらに多くの情報があります。このような情報は、デバイスのアイコンをクリックしてデバイス エクスプローラ画面を表示することによって見ることができます。

ネットワーク内のデバイスは、次のカテゴリに分類されます。

- **バックボーン デバイス**:ネットワークの基本骨格。ネットワーク上で検出されたすべてのスイッチ、ルータ、アクセス ポイントは、デフォルトで自動的にバックボーン デバイスに指定されます。

  バックボーン デバイスが検出されたら、手動で削除されるまでトポロジ マップに残ります。デバイスがネットワークから切り離された場合は、オフライン デバイスとしてトポロジ マップ上に表示されます。

  SNA 対応デバイスまたは管理対象デバイスは、以前使用していたものと同じ IP アドレスでネットワークに接続されている限り、検出された状態を保ちます。

- **オフライン デバイス**:以前トポロジに追加されていた(トポロジ検出メカニズムか手動のどちらかによって)バックボーン デバイス。このようなデバイスは、SNA によって検出されなくなっています。

  オフライン デバイスには次のような特長があります。

  - トポロジ マップのオンライン デバイスとは異なる外観(「トポロジ表示:」を参照)。
  - トポロジ上で移動したり、その位置を保存したりできる。デバイスにタグを追加することもできる(タグを参照)。

- 選択したり、検索機能を使って検出したりできる。オフライン デバイスを選択すると、情報パネルにそのデバイスの基本識別情報とタグが表示されますが、基本 ID 以外の、サービス、通知、一般情報は表示されません。
- オフライン デバイスのデバイス エクスプローラやデバイス管理 GUI は起動できない。
- 手動で削除できる。デバイスを削除すると、検出されるか手動で追加されるまでトポロジ マップに表示されなくなります。このデバイスに関連付けられたすべてのタグは失われ、その後デバイスが再度検出されても復元されません。

SNA は、定期的に、オフライン デバイスに接続を試みて、管理対象スイッチや SNA スイッチがオンラインに復帰したかどうかを確認します。このような試みの最中は、デバイスにインジケータが表示されます。

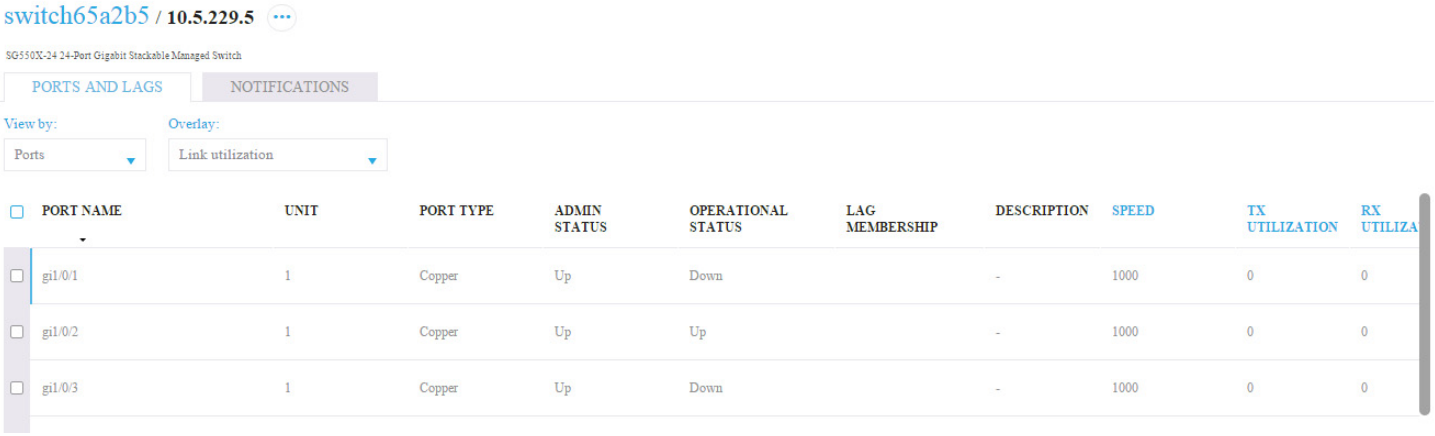
- **クライアント デバイス**:通常バックボーン デバイスに接続されているネットワークのエンドポイント クライアント(PC や IP 電話など)。トポロジ マップでは、これらのデバイスが、同じバックボーン デバイスに接続されている同じタイプの他のデバイスと一緒にまとめて表示されます。このようなデバイスのグループは*クライアント グループ*と呼ばれており、クライアント グループを構成する個々のクライアントはクリックしてそのエクスプローラに入ることによって見ることができます(エクスプローラを参照)。

  デバイスに 1 つ以上のクライアント デバイスが接続されている場合は、その上に + が表示されます。

  + をクリックすると、クライアントが表示されます。下のサンプルは、1 つのクラウド デバイスに 2 つのクライアント(クライアント PC デバイスと不明なタイプのデバイス)が接続されている様子を示しています。

ポート

デバイスのポートを表示するには、そのデバイスを選択してから、ダブルクリックします。こうすると、デバイスのすべてのポートを表示するパネルが開きます。デバイスがスタック モードの場合はすべてのユニットが含まれます。

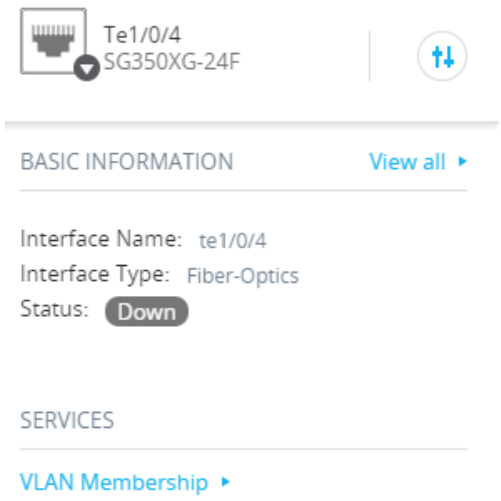


次の属性が表示されます。

- ポート名
- ユニット
- 管理ステータス

- 動作ステータス(ポートがソフトウェアによってオフになっている場合は、無効の理由を含む)
- LAG メンバーシップ
- 説明(説明が定義されていた場合)
- 速度
- スイッチポート モード
- ポート使用率(受信と送信)

このパネルでポートを選択すると、下の図のように、側面パネルに詳しい情報が表示されます。



インターフェイスの命名

SNA デバイスまたは部分 SNA デバイスのインターフェイスの名前は、次の部分で構成されます。

- ポート タイプに基づくプレフィックス:高速ポートの場合は FE、ギガ ポートの場合は GE、10 ギガバイト ポートの場合は XG。
- インターフェイス ID:非スタッキング デバイスの場合はインターフェイス番号、スタッキング デバイスの場合はスラッシュで区切られたユニット ID とインターフェイス ID。

ポートのスロットは SNA では表示されません。たとえば、ギガバイト ポート **gi1/0/12** は SNA では **GE1/12** と表示されます。

SNA 機能がないデバイスで検出されたポートの名前は、操作なしでアドバタイズされた場合のように表示されます。

デバイス間の接続

デバイス間の接続は、現在のオーバーレイに応じて色分けされます(オーバーレイを参照)。

接続は、デバイス間の単一のリンクを表す場合と、2 つのデバイス間のリンクの集合を表す場合があります。

トポロジ マップ上のスイッチ間の接続の幅は、接続で使用可能な帯域幅を集約したものを表します。これは、接続のリンクの動作速度によって決定されます。

次の接続幅があります(最も狭いものから最も広いものの順)。

- レベル 1 - 1 GB 未満
- レベル 2 - 1 GB 以上 10 GB 未満
- レベル 3 - 10 GB 以上

容量が計算できないリンク、または、バックボーン デバイスとそのクライアント間のリンクは、レベル 1 リンクとして表示されます。

SNA 対応デバイス間の接続は両側で検出されます。両側で計算された接続容量が異なる場合は、低い方の値に基づいて幅が描画されます。

特定のリンクをクリックすると、そのリンクの接続エクスプローラに入ることができます。次の情報が表示されます。

- リンクの両側のポート名(わかっている場合)
- 該当する場合の LAG ID
- 接続されたデバイスに関する基本情報:デバイス タイプ/デバイス名/IP
- 接続を構成する各リンクのリンク帯域幅

クラウド

クラウドは、SNA が詳細にマップできないネットワークのセクションです。これらは次のアイコンで示されます。

SNA は、複数のデバイスが特定のポートを経由してネットワークに接続されていることは判断できますが、それらのデバイス間の関係をマップすることはできません。これは、それらの間に SNA 対応デバイスが存在しないためです。SNA は、トポロジマップ上にクラウドを描画し、そのクラウド内で検出されたデバイスを接続されたクライアントとして表示します。

ほとんどの SNA 操作はクラウドに適用されません。

右側の情報パネル

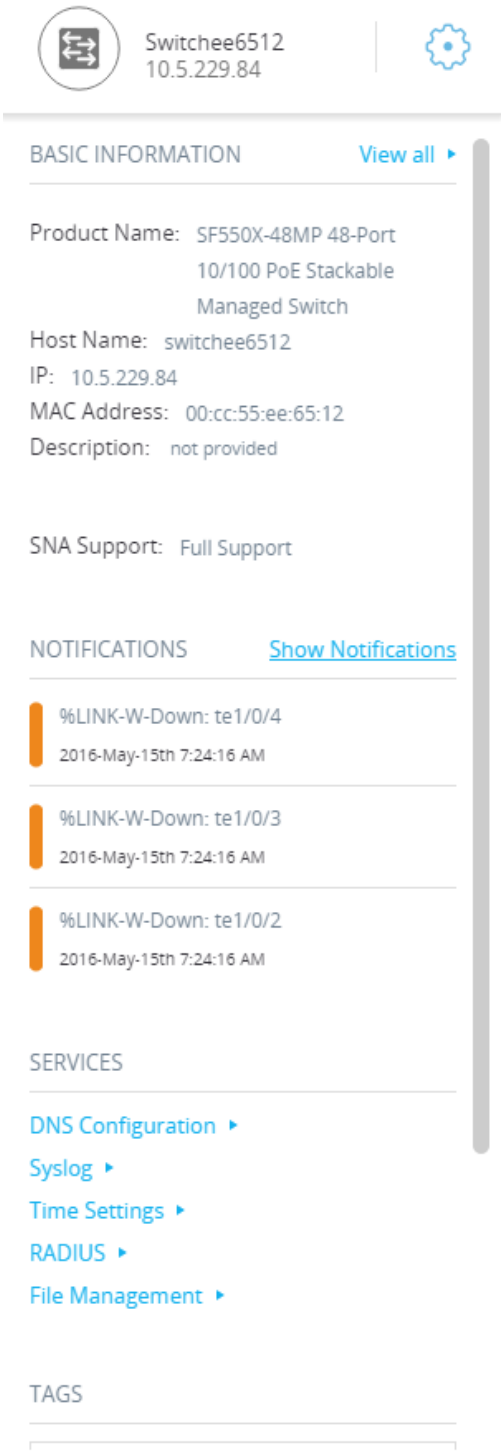
トポロジ表示の右側の領域には、選択された要素の属性を表示し、それらに対してアクションを実行できる情報パネルが表示されます。

右側の情報パネルには、次のブロックが含まれています。

- ヘッダー ブロック
- 右側の情報パネルの歯車
- 基本情報ブロック
- 通知ブロック
- サービス ブロック
- タグ
- 統計情報

図　2 に、右側の情報パネルの例を示します。

図 2　右側の情報パネル

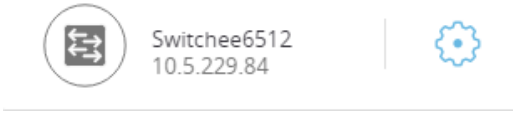


ヘッダー ブロック

ヘッダーには、選択された要素のアイコンが表示されます。要素が 1 つしか選択されていない場合は、下の図のように、ヘッダーに識別情報が表示されます。

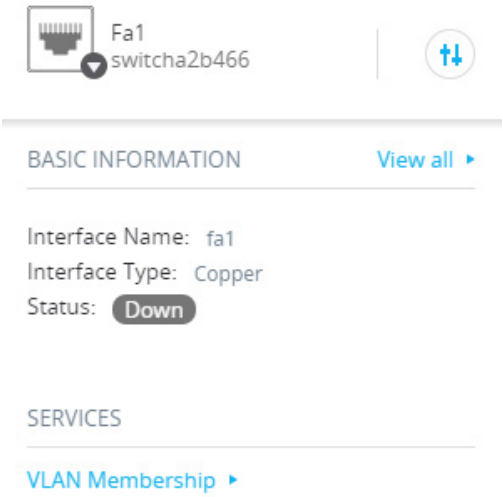
選択されたエンティティのタイプに応じて、次の情報がヘッダーに表示されます。

- [デバイス]:デバイスのタイプと、デバイスが認識された ID の中でより強力な 2 つのフォーム。識別方法の階層は次のようになっています:ホスト名 → IP アドレス → MAC アドレス。例:

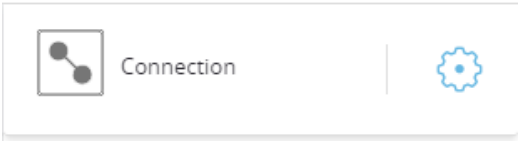


たとえば、デバイスのホスト名、IP アドレス、MAC アドレスがわかっている場合は、ホスト名と IP アドレスが表示されます。ホスト名または IP アドレスがわからない場合は、その不明な属性の代わりに MAC アドレスが表示されます。

- [インターフェイス]:識別情報は、インターフェイスの名前と、それが属しているデバイスの ID の中で最も強力なフォーム(ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスが両方とも不明の場合は MAC アドレス)です。



- [接続]:識別情報は、接続の両側のデバイスの ID の中でより強力な 2 つのフォーム(ホスト名 → IP アドレス → MAC アドレス)になります。接続には 1 つ以上のリンクがあります。



下の図のように、複数の要素を選択すると、ヘッダーに選択された要素の数が表示され、選択された要素がすべて同じタイプの場合は、ヘッダーにそれらのタイプも表示されます(下の図ではタイプが一貫していないため表示されていない)。

クライアント グループを選択すると、そのグループ内のすべてのメンバーを選択することができます。ヘッダーに、グループ内のデバイスの数とタイプが表示されます。

クライアント グループと一緒に他のデバイスを選択すると、クライアント グループに含まれているデバイスの数としてカウントされます。たとえば、1 つのバックボーン デバイスと、5 つのクライアントを含む 1 つのクライアント グループを選択した場合は、6 つのデバイスが選択されているとヘッダーに表示されます。

デバイスに関する通知がある場合は、通知の数が表示されます。

右側の情報パネルの歯車

選択したデバイスまたは接続に対して次のアクションを実行できます。これらのアクションを実行するには、右側の情報パネル内の歯車アイコン( )をクリックします。

- [デバイスの管理]:このオプションは、SNA スイッチと部分 SNA スイッチでしか使用できず、単一のデバイスが選択されている場合にのみ表示されます。このアクションを選択すると、スイッチ管理アプリケーションを使用して、選択されたスイッチの Web 管理セッションが起動します。このセッションを起動するためにクレデンシャルを入力する必要はありません。
- [デバイスの探索]:このオプションは、SNA スイッチでしか使用できず、単一のデバイスが選択されている場合にのみ表示されます。このアクションを選択すると、選択されたスイッチのデバイス エクスプローラが開きます。

- [デバイスの特定]: このオプションは、SNA スイッチにのみ使用できます。このアクションを選択すると、デバイスの物理 LED が 5 分間の点滅を開始します。点滅が起こると、特定機能が動作中であることを伝えるダイアログが表示され、この操作をキャンセルすることができます。
- [接続の探索]: このオプションは、単一の接続が選択されたときに表示されます。このアクションを選択すると、選択された接続の接続エクスプローラが開きます。
- [クライアントグループの探索]: このオプションは、クライアント グループが選択されているときに表示されます。このアクションを選択すると、クライアント グループ内のデバイスのタイプ別にフィルタされたクライアント エクスプローラが開きます。
- [削除]: このオプションは、選択されたすべてのデバイスがオフライン デバイスである場合にのみ表示されます。このアクションを選択すると、選択されたすべてのデバイスがトポロジ マップから削除されます。

基本情報ブロック

[基本情報] ブロックには、選択された 1 つの要素の属性が表示されます(詳しい説明は下の表を参照)。複数のエンティティが選択されているときは、このブロックは表示されません。

常に表示される情報もあれば、[すべて表示] ボタンがクリックされた場合にのみ表示される情報もあります。

特定のパラメータに関する情報が受け取れない場合は、そのパラメータは [基本情報] セクションに表示されません。

バックボーン デバイスに関する次の情報が表示されます。

パラメータ名	備考	例
製品名	デバイス記述 MIB から。 このフィールドは、デバイスが一部の SNA 機能またはフル SNA 機能を備えたスイッチである場合にのみ表示されます。	SG500-52P:52 ポート ギガビット PoE スタッカブル マネージド スイッチ
ホスト名	最大 58 文字の文字列	RND_1

パラメータ名	備考	例
IP アドレス	SNA がデバイスに接続するために使用する IP アドレスが表示されます。その他のアドバタイズされた既存のアドレス(IPv4 と IPv6)は、ラベルの横にあるアイコンを押すことによって表示できます。	192.168.1.55 923:a8bc::234
MAC アドレス	デバイスの基本 MAC アドレス	00:00:b0:83:1f:ac
説明	最大 80 文字の編集可能なフィールド。 SNA ストレージに保存されている。	
SNA サポート	可能な値: • SNA デバイスにはフル サポート • 管理対象デバイスには部分サポート • 管理対象外デバイスには SNA サポートなし このパラメータは、スイッチの場合にのみ表示されます。	
以下のパラメータは、[すべて表示] がクリックされた場合にのみ表示されます。このオプションは、デバイスが部分 SNA 機能またはフル SNA 機能を備えたスイッチである場合にのみ使用できます。		
既存の VLAN	デバイス上で作成された VLAN のリスト。連続する VLAN を表現する場合は破線を使用します。	1、6、13-19、1054、2012-2100、4094
アクティブなファームウェア バージョン	アクティブなファームウェアのバージョン番号	2.2.0.53
システム稼働時間	デバイスが起動して以降の日単位、時間単位、分単位、および秒単位の時間。	
システム ローカル時間	アクティブな言語ファイルの形式で示される、デバイス上のローカル時間。	英語ファイルの例: 2015-Nov-04 17:17:53
ユニットの数	スタッカブル デバイスでのみ表示されます。	2

パラメータ名	備考	例
ユニット番号に基づく PoE 電力/使用可能な PoE 電力	PoE 対応デバイスにのみ表示されます。 最大電力のうち使用可能な電力が表示されます。 デバイスがスタック型デバイスの場合は、スタック内の PoE 対応ユニットごとにフィールドがユニット ID とともに表示されます。デバイスがスタンドアローンまたは単一ユニットの場合は、フィールドのラベルにユニット ID が含まれません。 これは、最大で 8 つのフィールドがここに表示される可能性があるを意味します。	15.22W/18.0W

最後の既知の情報には、オフライン バックボーン デバイスに関する次の情報が表示されます。

パラメータ名	備考	例
製品名	デバイス記述 MIB から取得されます。 このフィールドは、デバイスが一部の SNA 機能またはフル SNA 機能を備えたスイッチである場合にのみ表示されます。	SG500-52P:52 ポート ギガビット PoE スタッカブル マネージド スイッチ
ホスト名	最大 58 文字の文字列	RND_1
IP アドレス	前回確認したときに、デバイスへの接続に使用された IP アドレスが表示されます。	192.168.1.55
MAC アドレス	デバイスの基本 MAC アドレス	00:00:b0:83:1f:ac
説明	最大 80 文字の編集可能なフィールド。	
前回の検出	デバイスが SNA によって前回確認された日付と時刻(アクティブな言語ファイルの形式)。	英語ファイルの例: 2015-Nov-04 17:17:53

クライアント(PC などのエンド ポイント デバイス)に関する次の情報が表示されます。

パラメータ名	備考	例
ホスト名	最大 58 文字の文字列	RND_1
IP アドレス	SNA がデバイスに接続するために使用する IP アドレスが表示されます。その他のアドバタイズされたアドレス(IPv4 と IPv6)は、ラベルの横にあるアイコンをクリックすることによって表示できます。	192.168.1.55 923:a8bc::234
MAC アドレス	デバイスの基本 MAC アドレス	00:00:b0:83:1f:ac
デバイス タイプ	クライアント デバイスのタイプ	電話 ホスト 不明
接続されたインターフェイス	デバイスが最も近いスイッチで到達されたインターフェイス。	GE1/14
次のパラメータは、[すべて表示] がクリックされた場合にのみ表示されます。		
接続速度		100 M 10 G
VLAN メンバーシップ	接続されたインターフェイスがメンバーとして所属しているアクティブな VLAN が表示されます。連続する VLAN を結合する場合は破線を使用します。	1、6、13-19、1054、2012-2100、4094
ポート使用率(送信/受信)	接続されたポートからの情報に基づきます。	80/42
PSE 電力消費	クライアントが PoE ポートに接続されている場合にのみ表示されます。	8900 mW

クライアント グループに関する次の情報が表示されます。

パラメータ名	備考	例
ホスト名	これは、クライアント グループの親デバイスのホスト名です。 このパラメータと親デバイスに関する他のすべての情報は、[接続先] ヘッダーに表示されます。 最大 58 文字の文字列	RND_1
親デバイスの IP アドレス	SNA が親デバイスに接続するために使用する IP アドレスが表示されます。その他のアドバタイズされたアドレス(IPv4 と IPv6)は、ラベルの横にあるアイコンを押すことによって表示できます。	192.168.1.55 923:a8bc::234
親デバイスの MAC アドレス	親デバイスの基本 MAC アドレス。	00:00:b0:83:1f:ac
クラウド経由で接続	このラベルは、クライアント グループがクラウド経由でネットワークに接続されている場合に表示されます。このラベルが、ホスト名、IP アドレス、MAC アドレスの代わりに使用されます。	

インターフェイスに関する次の情報が表示されます。

パラメータ名	備考	例
インターフェイス名		GE1/14 LAG12
インターフェイスのタイプ	ポートの場合にのみ表示される	カッパー 1 G
ステータス	インターフェイスの動作ステータス。	アップ ダウン ダウン(ACL)
以下のパラメータは、[すべて表示] がクリックされた場合にのみ表示されます。		
インターフェイスの説明	インターフェイスの ifAlias MIB の値を使用。 最大 64 文字の文字列。	"WS 28"

パラメータ名	備考	例
動作速度		100 M 10 G
LAG メンバーシップ	ポートの場合にのみ表示される [なし] または LAG 名になる場合あり。	LAG15
メンバーポート	LAG の場合にのみ表示され、LAG 内でアクティブなメンバーであるインターフェイスが一覧表示されます。インターフェイスの連続範囲はダッシュで結合します。	GE1/4、GE1/6、XG2/4-8
VLAN メンバーシップ	インターフェイスがメンバーとして所属しているアクティブ VLAN が表示されます。連続する VLAN を結合する場合は破線を使用します。	1、6、13-19、1054、2012-2100、4094
ポート使用率(送信/受信)	ポートの場合にのみ表示されます。	80/42
LAG タイプ	LAG の場合にのみ表示。可能な値は、[標準] または [LACP]。	
スイッチボードモード	可能な値: • アクセス • トランク • 全般 • カスタマー • プライベート - ホスト • プライベート - プロミスキャス	
PSE 電力消費	PoE 対応ポートの場合にのみ表示。	8900 MW
スパニング ツリー状態	インターフェイスの STP 状態を表示。	ブロッキング 転送 無効

注 クライアントまたはレイヤ 2 クラウドを選択した場合は、[基本情報] セクションが表示されません。

通知ブロック

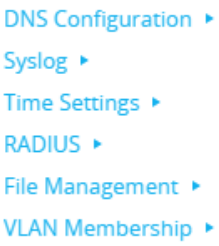
通知ブロックには、選択されたデバイスで記録された最新の通知(SYSLOG)が表示されます。

通知セクションは、1 つの SNA デバイスを選択したときにのみ表示されます。

その他の詳細については、「通知」を参照してください。

サービス ブロック

情報パネルのこのセクションには、現在選択されている要素に対して使用可能なサービスが表示されます。選択されたすべての要素に関連しているサービスのみが表示されます。サービスをサポートしていない要素が選択に含まれている場合やデバイスとインターフェイスが一緒に選択されている場合は、このセクションが表示されません。



追加情報については、「サービス」を参照してください。

タグ

タグは、属性によってトポロジ内の要素を識別するために使用します(タグを参照)。右側の情報パネルの [タグ] ブロックには、自動的にまたはユーザによって要素に割り当てられたすべてのタグが表示されます。パネルのこの部分から選択された要素のタグを管理することもできます。追加情報については、「タグ」を参照してください。

統計情報

SNA 対応デバイスまたは SNA 対応デバイスのインターフェイスを表示しているときに、そのインターフェイスやデバイスの統計情報の履歴を表示させることができます。

統計情報ビューは、右側の情報パネルからアクセスします。

インターフェイスまたはデバイスの統計情報の履歴を表示するには、組み込みカウンタ履歴機能でサポートされているパラメータに従って、使用可能なパラメータのリストから表示する特定のパラメータを選択します。それから、前年の選択されたインターフェイスに関するそのパラメータのステータスを表示できます。

次のグラフを表示できます。

- ポート使用率グラフ
- PoE 消費グラフ(ポート)
- PoE 消費グラフ(デバイス)
- トラフィック グラフ(バイト)
- トラフィック グラフ(パケット)

ポート使用率グラフ

このグラフは、一定期間のポート使用率を示すポート レベルのグラフです。SNA を完全にサポートするデバイスのすべてのポートに使用できます。

対照比較を実行するポートの数を選択できます。

データは、表示された時間スケールに基づくサンプルの数と頻度を用いて、パーセンテージ(0 ～ 100)で表示されます。

- この 5 分間 - 20 サンプル(15 秒に 1 つ)
- この 1 時間 - 60 サンプル(1 分に 1 つ)
- この 1 日 - 24 サンプル(1 時間に 1 つ)
- この 1 週間 - 7 サンプル(1 日に 1 つ)
- この 3 ヵ月 - 12 サンプル(1 週間に 1 つ)

PoE 消費グラフ(ポート)

このグラフは、一定期間のポートの PoE 使用率を示すポート レベルのグラフです。SNA を完全にサポートするデバイスのすべての PoE ポートに使用できます。

対照比較を実行するポートの数を選択できます。

データは、表示された時間スケールに基づくサンプルの数と頻度を用いて、ワット数(0 ～ 30/60(ポートが PoE+ 機能を備えているかどうかによって異なる))で表示されます。

- この 1 時間 - 60 サンプル(1 分に 1 つ)
- この 1 日 - 24 サンプル(1 時間に 1 つ)
- この 1 週間 - 7 サンプル(1 日に 1 つ)
- この 1 年 - 52 サンプル(1 週間に 1 つ)

PoE 消費グラフ(デバイス)

このグラフは、一定期間のデバイスの PoE 使用率を示すデバイス レベルのグラフです。SNA を完全にサポートするすべての PoE デバイスに使用できます。

このグラフは、ユニットごとに表示され、同時に表示させるユニットの数を(単一のスタックまたは複数のスタックから)選択できます。

データは、表示された時間スケールに基づくサンプルの数と頻度を用いて、ワット数(0 ～容量が最も高い選択されたユニットの PoE 容量)で表示されます。

- この 1 時間 - 60 サンプル(1 分に 1 つ)
- この 1 日 - 24 サンプル(1 時間に 1 つ)
- この 1 週間 - 7 サンプル(1 日に 1 つ)
- この 1 年 - 52 サンプル(1 週間に 1 つ)

トラフィック グラフ(バイト)

このグラフは、一定期間のインターフェイス上の合計トラフィックをバイト単位で示すインターフェイス レベルのグラフです。SNA を完全にサポートし、送信トラフィックと受信トラフィックで別々の回線を利用しているデバイスのすべてのインターフェイスに使用できます。

対照比較を実行するポートの数とトラフィックのタイプを選択できます。

データは、表示された時間スケールに基づくサンプルの数と頻度を用いて、オクテット数(0 ～選択されたインターフェイス/期間内で最も高いサンプル)で表示されます。

- この 5 分間 - 20 サンプル(15 秒に 1 つ)
- この 1 時間 - 60 サンプル(1 分に 1 つ)
- この 1 日 - 24 サンプル(1 時間に 1 つ)
- この 1 週間 - 7 サンプル(1 日に 1 つ)
- この 3 ヵ月 - 12 サンプル(1 週間に 1 つ)

トラフィック グラフ(パケット)

このグラフは、一定期間のインターフェイス上の合計トラフィックをパケット単位で示すインターフェイス レベルのグラフです。SNA を完全にサポートするデバイスのすべてのインターフェイス(ポートまたは LAG)に使用できます。

どちらのバージョンのデータも、表示された時間スケールに基づくサンプルの数と頻度を用いて、パケット数(0 がサンプリング範囲で最も高い値)で表示されます。

- この 5 分間 - 20 サンプル(15 秒に 1 つ)
- この 1 時間 - 60 サンプル(1 分に 1 つ)
- この 1 日 - 24 サンプル(1 時間に 1 つ)
- この 1 週間 - 7 サンプル(1 日に 1 つ)
- この 3 ヵ月 - 12 サンプル(1 週間に 1 つ)

操作

トポロジ表示には、ネットワーク内の要素とその接続が表示されます。操作はトポロジ表示に表示されている要素に対して実行できます。

トポロジ内の要素を選択して、次のアクションを実行できます。

- 要素に関する情報を表示する - エクスプローラを参照
- 要素を構成する - サービスを参照
- トポロジ表示にデバイスまたはスイッチを追加する - デバイスまたはスイッチをトポロジ表示に手動で追加するを参照

注 複数の要素を選択した場合は、そのすべての要素に対して適用可能なアクションしか使用できません。

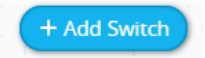
SNA 対応デバイスには、トポロジ内の他のデバイスよりも多くの操作を実行できます。

SNA 対応デバイスに対して次のアクションが実行できます。

- インターフェイスの詳細ビューにズームインする。
- 管理対象デバイス/SNA デバイスが SNA へのログインと同じクレデンシャルを使用した管理セッションを許可している場合に、SNA 経由で(ログイン画面をバイパスして)他の SNA 対応デバイスと管理対象デバイスで Web 管理セッションを起動する。

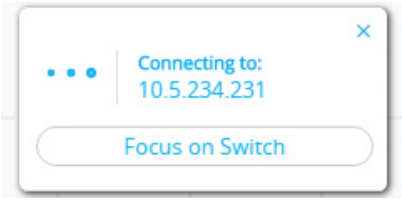
デバイスまたはスイッチをトポロジ表示に手動で追加する

要素を手動でトポロジ表示に追加することができます。ネットワーク内に存在するSNA 対応デバイスまたは管理対象スイッチが自動的に検出されず、トポロジに表示されない場合は、次の操作を実行して手動で追加することができます。

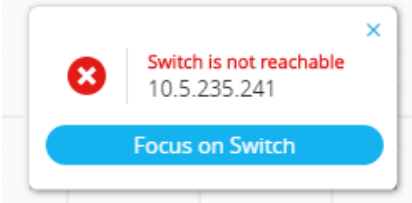
ステップ 1 トポロジ表示の右上にある 

をクリックします。[IP アドレスの入力] テキスト ボックスが表示されます。

ステップ 2 追加するスイッチの IP アドレスを入力します。次のメッセージが表示されます。



デバイスが検出されなかった場合はフィードバックが表示され、そのデバイスはオフラインの管理対象外スイッチとしてトポロジ表示に追加されます。



この方法によって追加されたデバイスは、手動で削除されるまでトポロジ マップ内に残ります。このようなデバイスが接続されていない場合または SNA で検出されない場合は、オフライン デバイスとして表示されます。

エクスプローラ

エクスプローラを使用すれば、SNA 対応スイッチ、接続、およびクライアント グループに関してさらに詳しい情報を見ることができます。

注 エクスプローラに入るには、デバイスを表すノードまたは接続をクリックします。エクスプローラによって表示される情報は、選択されたオーバーレイによって異なる可能性があります(オーバーレイを参照)。

次のエクスプローラがあります。

- デバイス エクスプローラ
- 接続エクスプローラ
- クライアント エクスプローラ

デバイス エクスプローラ

このエクスプローラは、フル SNA デバイスとそのインターフェイスに関する追加情報を提供します。

スイッチのポートと既存の LAG を示す表が表示されます。表の各エントリには、基本的な列が数列と、関連するオーバーレイがアクティブになっているときにだけ表示される追加の列がいくつかあります。

ここから、デバイスのホスト名を編集して保存することもできます。

デバイス エクスプローラの表には次の列が表示されます。

- [ポート/LAG 名]: インターフェイスのフルネーム。
- [ユニット ID]: スタック型スイッチのポート表にのみ表示されます。
- [ポートタイプ]: ポート表にのみ表示されます。ポートの物理タイプ。
- [管理ステータス]: インターフェイスの管理ステータス。
- [動作ステータス]: インターフェイスの動作ステータス。インターフェイスが一時停止の場合は、その理由が括弧内に表示されます。
- [LAG メンバーシップ]: ポート表にのみ表示されます。ポートが LAG のメンバーの場合は、この列に LAG ID が表示されます。
- [ポート メンバー]: LAG 表にのみ表示されます。この LAG のメンバーになっているポートが一覧表示されます。ポートのリストが長くなる場合があります。リストが表に収まり切らない場合は、右側の情報パネルに表示されます。
- [説明]: インターフェイスの説明。MIB ifAlias を使用します。
- [リンク使用率]オーバーレイが選択されている場合は、次の列が表示されます。
  - [現在の速度]: インターフェイスの現在の速度(10 M、100 M、1 G など)。
  - [送信使用率]: 現在の速度のうちのパーセンテージで表される、インターフェイスの送信使用率。LAG の場合は、この列が表示されません。
  - [受信使用率]: 現在の速度のうちのパーセンテージで表される、インターフェイスの受信使用率。LAG の場合は、この列が表示されません。
- [PoE] **オーバーレイ**が選択されている場合は、次の列が表示されます。
  - [最大電力割り当て]: ポート表にのみ表示されます。最大電力割り当てが MW 単位で表示されます。ポートが PoE をサポートしていない場合は、[N/A] が表示されます。

- [消費電力]:ポート表にのみ表示されます。実際の消費電力が MW 単位で表示されます。ポートが PoE をサポートしていない場合は、[N/A] が表示されます。

- [VLAN] **オーバーレイ**が選択されている場合は、次の列が表示されます。
  - [スイッチポートモード]:インターフェイスのアクティブな VLAN モード。
  - [VLAN メンバーシップ]:インターフェイスがメンバーになっている VLAN のリスト。トランク モードでは、タグなし VLAN の横に [U] が表示されます。VLAN のリストが長くなる場合があります。リストがテーブルに収まり切らない場合は、右側の情報パネルにすべてが表示されます。
- [スパニングツリー]オーバーレイが選択されている場合は、次の列が表示されます。
  - [STP モード]:インターフェイスのアクティブな STP モード。
  - [ポート ロール]:インターフェイスの STP ロール。
  - [スパニング ツリー状態]:インターフェイスの STP 状態。

接続エクスプローラ

このエクスプローラには、バックボーン デバイス間または SNA 対応デバイスとクラウド間の単一の接続に収集された個別のリンクに関する追加の詳細が表示されます。

特定の接続のエクスプローラに入ると、探索された接続内のリンクごとの表現が表示されます。

エクスプローラには、接続の両側にあるデバイスに関する基本情報が表示されます。この情報は、右側の情報パネルでも参照できる基本情報と同じです。エクスプローラには、両側で接続をアンカーしているインターフェイスが表示されます。インターフェイスが SNA 対応デバイスに属している場合にしか表示されない情報もあります。

この情報を表示するには、ダブルクリックして接続が太くし、2 回目のクリックで、次の情報が表示されます。

接続内のリンクごとに、次の基本情報が表示されます。

- リンクの両側のインターフェイスの名前
- リンクの両側の LAG の名前(存在する場合)
- リンクの速度

インターフェイス名と LAG メンバーシップに関する情報は、SNA 対応デバイスに属している接続側でしか参照できません。接続のどちらかの側がスイッチでない場合、そのポートは表示されません。

エクスプローラ内の特定のリンクは、アクティブなオーバーレイの影響も受けるため、選択されたオーバーレイに関連したステータスに応じてリンクの外観が変化します。「オーバーレイ」を参照してください。

接続エクスプローラのリンクを選択すると、両側でそのリンクをアンカーしているインターフェイスが選択されます。

クライアント エクスプローラ

このエクスプローラでは、IP 電話のグループなど、クライアント グループ内で選択されたクライアントに関する情報を表示できます。

このエクスプローラは、クライアント グループ内の各デバイスに 1 行ずつの表で構成されます。この表の一部の列は、特定のオーバーレイがアクティブになっている場合にのみ表示されます。

クライアント エクスプローラは、クラウド経由でネットワークに接続されているクライアント グループに関してはサポートされません。

クライアント エクスプローラの表には次の情報が表示されます。

- **デバイス ID**:デバイスに関する既知の情報(デバイスのホスト名、デバイスが親スイッチに接続するための IP アドレス、およびデバイスの MAC アドレス)。ここには、入手可能な情報だけが表示されます。入手できない情報のプレースホルダーは存在しません。
- **デバイス タイプ**:クライアント デバイスのタイプ。
- **接続先ポート**:このクライアントの接続先となっている親スイッチのポート。
- **リンク使用率オーバーレイ列**
  - **接続速度**:親スイッチへの接続の速度(10 M、100 M、1 G)が表示されます。
  - **送信使用率**:現在の速度のうちのパーセンテージとして表される、デバイスの送信(接続先のポートの受信)使用率。

- **受信使用率**:現在の速度のうちのパーセンテージとして表される、デバイスの受信(接続先のポートの送信)使用率。

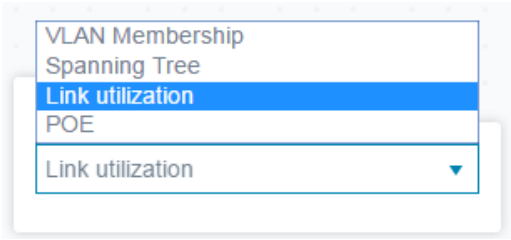
- **PoE オーバーレイ列**
  - **消費電力**:デバイスで消費される電力が MW 単位で表示されます。接続先のポートが PoE をサポートしていない場合は、[N/A] が表示されます。
- **VLAN オーバーレイ列** - 接続先の VLAN。接続先のポートがメンバーになっている VLAN が表示されます。VLAN のリストが長くなる場合があります。リストがテーブルに収まり切らない場合は、クライアントを選択したときに右側の情報パネルに表示されます。

クライアント エクスプローラは、クラウド経由でネットワークに接続されているクライアント グループに関してはサポートされません。

オーバーレイ

オーバーレイは、トポロジ表示でアクティブにすることができる情報のレイヤです。さらに情報を追加したり、トポロジの表示方法を変化させたりすることができます。これは、さまざまな基準に基づいてトポロジ要素を色分けしたり、選択したオーバーレイに関連した詳細なデータを表示するためにトポロジ要素上に表示されるアイコンを変更したりすることにより、実現することができます。

使用可能なオーバーレイのリストから使用するオーバーレイを選択します。



オーバーレイによっては、VLAN オーバーレイのように、パラメータが関連付けられている場合があります。たとえば、VLAN オーバーレイを選択した場合は、特定の VLAN も選択する必要があります。

一度にアクティブにできるオーバーレイは 1 つだけのため、新しくオーバーレイを選択すると現在アクティブなオーバーレイが非アクティブになります。

次のオーバーレイがサポートされています。

- リンク使用率
- PoE 情報
- VLAN メンバーシップ
- STP 情報

リンク使用率

このオーバーレイは、ネットワーク内の接続の現在の使用率レベル(この 15 秒間)に関する情報を、トポロジ マップとエクスプローラ画面に追加します。

接続とリンクは、それらを両方向に流れるトラフィック量に応じて色分けされます。

デフォルトのしきい値とその色を以下に示します。

- 0 ～ 69% - 標準
- 70 ～ 89% - 黄色
- 90 ～ 100% - 赤色

トポロジ表示のデバイス間の接続は、接続内で使用率が最も高いリンクに基づいて色分けされます。接続エクスプローラを表示すると、各リンクに両方向の使用率が表示されます。

リンクの各方向の使用率は、両側の情報をチェックし、リンクが SNA 対応デバイス間の場合は、高い方の値を使用率値として使用して計算されます。

たとえば、デバイス A のポート 1 とデバイス B のポート 2 の間のリンクである場合、ポート 1 の送信値とポート 2 の受信値を比較して一方向の使用率が計算されます。高い方の値がそのリンクの使用率になります。

リンクの片側だけが SNA 対応デバイスの場合は、そのリンクの使用率は SNA 対応デバイスの情報によってのみ判断されます。

トポロジ マップの集合表示で最も使用率の高いリンクを判断する際は、リンクの各方向が別々のリンクと見なされます。例: リンクのどちらかの方向の使用率が 5% で、その逆方向の使用率が 92% の場合は、接続内で最も高い使用率が 92% になるため、トポロジ マップ内の集合接続が赤色になります。

PoE 情報

PoE オーバーレイには、ネットワーク内の要素の電力供給と電力消費のステータスが表示されます。

このオーバーレイのリンクの色分けは、残存電力と、電力供給装置につながっているリンクにより供給されている電力の量に従って行われます。また、要求した電力を受け取っていない電力要求デバイスを強調表示します。ユーザは、これらの色が変化する各データ タイプのしきい値と、各しきい値に達したときに使用される特定の色を選択できます。

1 つのアイコンが電力供給スイッチに追加され、スイッチの電力バジェット消費に基づいて色分けされます。

- 電力バジェットの 0 ～ 80% を供給しているデバイス - 標準
- 電力バジェットの 81 ～ 95% を供給しているデバイス - 黄色
- 電力バジェットの 96 ～ 100% を供給しているデバイス - 赤色

イーサネット経由で電力を受け取っているデバイスは、丸で囲まれます。

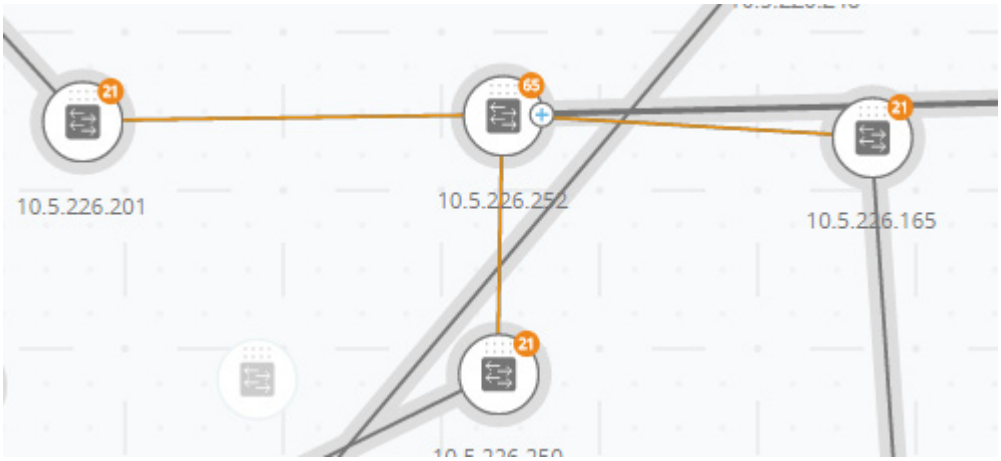
電力が供給されている少なくとも 1 つのリンクを含む接続がトポロジ マップ内で強調表示されます。

接続エクスプローラでは、電力を伝送している各リンクに、電力供給のインジケータと、電力フローの方向が表示されます。このインジケータは、リンクが LAG 内に存在する場合でも、ポート単位で表示されます。LAG 内の一部のリンクだけが電力を供給する場合もあります。

VLAN メンバーシップ

このオーバーレイによって、ネットワーク内のさまざまなポートとデバイスの VLAN メンバーシップを見ることができます。

たとえば、下の図の黄色の線は非対称接続を表しています。つまり、リンクの一方の端は選択された VLAN のメンバーですが、もう一方の端はそうではない場合です。



このオーバーレイをアクティブにすると、ネットワーク内の既存の VLAN のリストが表示されます(VLAN ID 順)。VLAN ノードを選択すると、その VLAN のメンバーが強調表示されます。

デバイス間のリンクは次の状態のいずれかで表示されます。

- SNA デバイス間のリンクで、どちらのデバイスの接続インターフェイスも VLAN のメンバーではない場合、そのリンクはマークされません。
- SNA デバイスと非 SNA デバイス間のリンクで、SNA デバイスのインターフェイスが VLAN 内に存在しない場合、そのリンクはマークされません。
- SNA デバイス間のリンクで、両方のデバイスの接続インターフェイスが VLAN のメンバーである場合、そのリンクは VLAN のメンバーとして強調表示されます。
- SNA デバイスと非 SNA デバイス間のリンクで、SNA デバイスのインターフェイスが VLAN のメンバーである場合、そのリンクは強調表示されます。
- SNA デバイス間の非対称リンク(接続インターフェイスの一方が VLAN のメンバーで、もう一方がそうではない)は、黄色でマークされます。

トポロジ マップ内のデバイス間のリンク(LAG)の集合間の接続は、次のルールに従ってマークされます。

- 少なくとも 1 つのリンクが強調表示されている場合は、接続が強調表示されます。
- 少なくとも 1 つのリンクに非対称接続が含まれている場合は、接続が黄色になります。

接続エクスプローラでは、すべてのリンクを個別に表示できます。リンクに非対称構成が含まれている場合は、黄色の色分けに加えて、接続エクスプローラにどちらの側が VLAN のメンバーではないのかが表示されます。

STP 情報

このオーバーレイには、ネットワークのアクティブ トポロジが表示されます。このオーバーレイがアクティブになっていると、インジケータがスパニング ツリー ルート デバイスとすべての接続に追加されます。このインジケータは、共通のスパニング ツリーによってブロックされているリンクを強調表示します。

接続エクスプローラが表示されている場合は、すべてのブロックされているリンクが強調表示されます。

リンクがブロックされている場合は、接続エクスプローラが、リンクのどちら側が実際にブロックされているインターフェイスであるかを指摘します。

タグ

タグは、トポロジ表示内のデバイスを属性またはユーザ定義の名前で識別するために使用します。また、特定のタグを検索することによって、複数の要素をすばやく選択するためにも使用します。たとえば、「IP 電話」というタグが付けられたすべてのネットワーク ノードを検索することができます。

タグには、組み込みのものと、ユーザ定義のものがあります。

- **組み込みタグ**:検出プロトコルによって収集された情報に基づいて自動的にノードに適用されます。「組み込みタグ」を参照してください。
- **ユーザ定義タグ**:手動で追加され、トポロジ マップ内のノードに割り当てられます。「ユーザ定義タグ」を参照してください。

組み込みタグとユーザ義タグは、視覚的に区別できます。

組み込みタグ

このタグは、ノードがトポロジに追加されたときに自動的に適用されます。永続にすることも、状態ベースにすることもできます。タグがデバイスに適用されている限り、そのデバイスから削除できません。組み込みタグのリストを以下に示します。

タグ	タグの割り当て方法
SNA	SNA 内部データに基づく
部分 SNA	SNA 内部データに基づく
オフライン	SNA 内部データに基づく

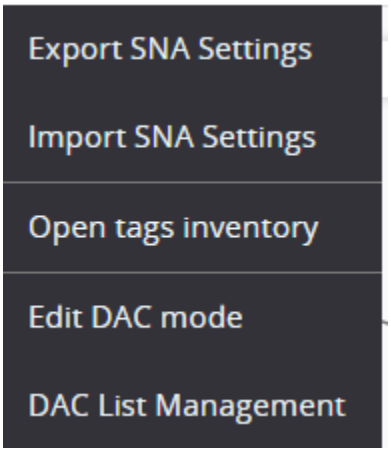
タグ	タグの割り当て方法
スイッチ	検出プロトコルでアドバタイズされたデータに基づく
ルータ	検出プロトコルでアドバタイズされたデータに基づく
アクセス ポイント	検出プロトコルでアドバタイズされたデータに基づく
IP 電話	検出プロトコルでアドバタイズされたデータに基づく
PC	検出プロトコルでアドバタイズされたデータに基づく(ホスト)
通知	SNA 内部データに基づく状態ベース、デバイスに未読通知がある場合に表示されます。
PoE PSE	SNA 内部データに基づく - デバイスが PoE 経由で電力を供給可能な場合に表示されます(実際は電力を供給していない場合でも)。
PoE PD	SNA 内部データに基づくこれは、デバイスが PoE 経由で電力を受け取り可能な場合に表示されます(実際は電力を受け取っていない場合でも)。

タグの表示

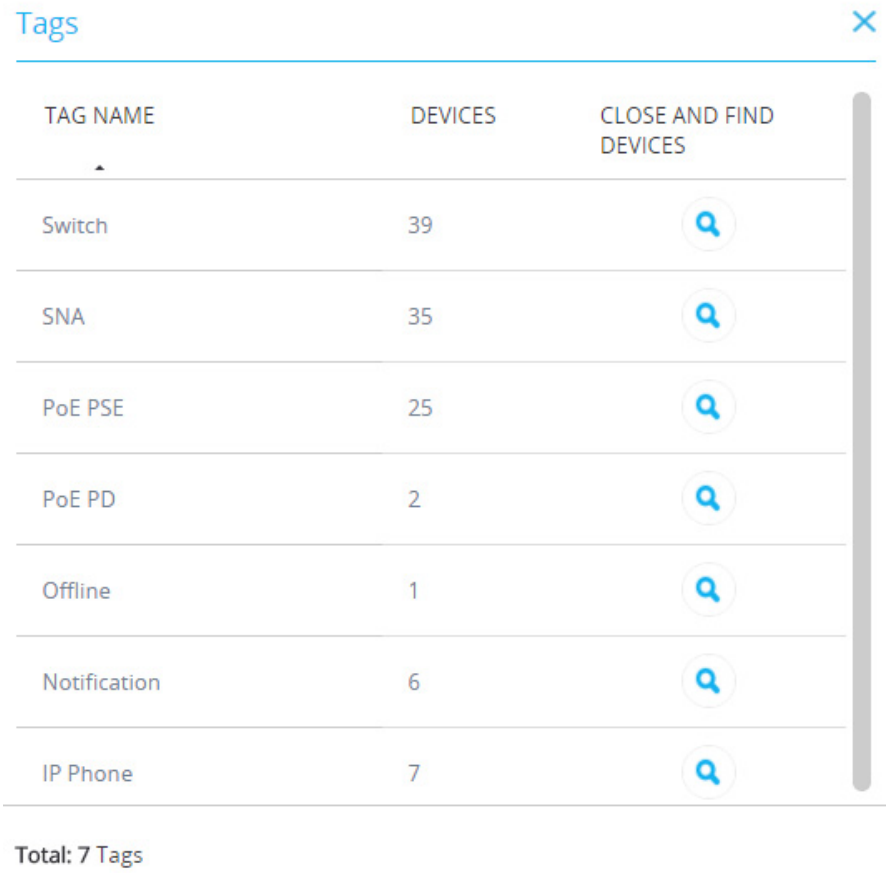
タグの全一覧を表示するには、次の手順を実行します。

ステップ 1 トポロジ表示の左側にあるハンバーガー メニューをクリックします。☰

次のメニューが表示されます。



ステップ 2 [タグ インベントリを開く] を選択します。下の図のように、タグのリストが表示されます。



ステップ 3 [閉じてデバイスを検索] 列内の特定のタグの検索アイコンをクリックして、選択されたタグが付いているデバイスのリストを表示します。

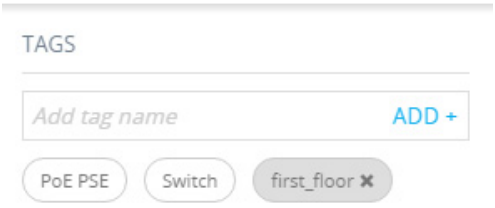
ユーザ定義タグ

右側の情報パネルの [タグ] セクションで、新しいタグを作成し、それらをトポロジ内で選択した要素に手動で追加することができます。

新しいタグを作成するには、次の手順を実行します。

ステップ 1 [タグ] セクションで、[タグ名の追加] テキスト ボックスをクリックして、タグ名を入力します。

ステップ 2 [追加 +] をクリックします。タグ名が表示されます。下の図は、**first_floor** というタグが作成されたところを示しています。



組み込みタグと同じ名前のタグを追加することもできます。これらのタグは、ユーザ定義タグと同様に表示され、いつでも削除できます。これらのタグは組み込みタグと区別されるため、一方がユーザ定義でもう一方が組み込みである限り、同じ名前の 2 つのタグを 1 つの要素の上に表示することができます。

タグをデバイスに追加するには、次の手順を実行します。

ステップ 1 デバイスを選択します。

ステップ 2 [タグ] セクションで、[タグ名の追加] テキスト ボックスをクリックします。タグのリストが表示されます。

ステップ 3 デバイスに適用するタグを選択します。

検索

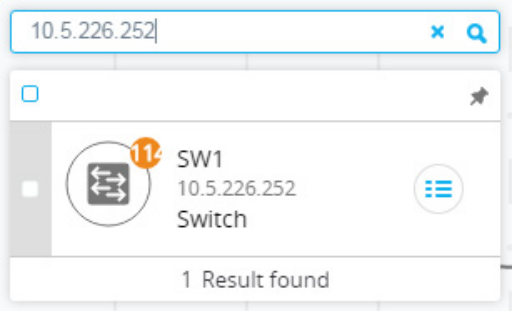
トポロジ表示内の特定のデバイスを探すには、検索機能を使用します。

入力された検索語が SNA に認識されている情報内で検索されます。

次の項目を検索できます。

- IP アドレス
- MAC アドレス
- ホスト名
- 製品名
- 説明
- タグ

検索結果は、クリック可能な ID カードのリストとして表示されます。ID カードをクリックすると、トポロジ マップが真ん中に表示され、そのトポロジ要素が拡大表示されます。

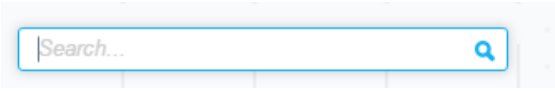


検索するフィールドを限定するキーワードを追加することにより、検索を絞り込むことができます。キーワードの後ろにコロンと検索語を入力すると、指定されたフィールドでのみ検索語が検索されます。サポートされているキーワードは、以下の通りです:**IP**、**MAC**、および**タグ**。

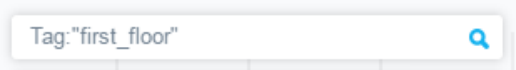
検索語が引用符で囲まれている場合は、完全一致のみが検索されます。

タグによる検索の例を以下に示します。

ステップ 1 検索ボックスをクリックします。



ステップ 2 下の図のように、キーワードの「タグ」とタグの名前を入力します。



ステップ 3 をクリックします。結果が表示されます。

ダッシュボード

ネットワーク ダッシュボードは、ネットワークのステータスに関する一般情報を表示する、トポロジとは別の画面です。

ダッシュボードは次のセクションで構成されます。

ネットワークの概要

このセクションには、ネットワークに関する一般情報が表示されます。ここに表示されるすべての情報は、ネットワーク上の SNA デバイスと部分 SNA デバイスによって提供されます。

次の情報が表示されます。

- ネットワーク上の PoE デバイスによって供給される PoE 電力 - これはワット単位で表示されます。
- Green Ethernet によって節約された現在の電力 - パーセンテージとワット値で表示されます(例:20%、5 ワット)。
- Green Ethernet によって節約された累積電力 - ワット * 時間で表示されます。
- Green Ethernet による予想年間電力節約 - ワット * 時間で表示されます。
- 電力管理ポリシーによって節約された現在の電力 - ワットで表示されます。
- 電力管理ポリシーによって節約された累積電力 - ワット * 時間で表示されます。
- 電力管理ポリシーによる予想年間電力節約 - ワット * 時間で表示されます。

アラート

このセクションには、ネットワークの最新のアラートが 10 件表示されます。アラートは、セキュリティ ランク 1 の通知です(通知ブロックを参照)。

このアラートは、次の列を含む表内に表示されます。

- 発信側デバイス

  これは、集合通知表示内にのみ表示されます。発信側デバイスは、次の優先順位に基づき、入手可能なものの中から一番強力なフォームの ID で識別されます。ホスト名 > IP アドレス > MAC アドレス

- タイムスタンプ
- 重大度
- Syslog テキスト

リストは、デバイス、時刻、または重大度順に並べ替えることができ、デバイスまたは重大度でフィルタをかけることができます。

デフォルトで、リストはタイムスタンプ順に表示されます。最新の通知が一番上に表示されます。

ネットワークの健全性

ネットワーク内の SNA デバイス上でヘルス問題が検出された場合に、このセクションにアラートが表示されます。

アラートは、発生元のデバイスまたは接続を示し、該当するデバイスまたは接続のエクスプローラにつながるリンクと問題の特性を提供します。

次のイベントに関して表示されます。

- ファンが故障した。
- 温度センサーが異常に高い温度を検知した。
- PoE が過負荷状態になった(予算を超えたために、PoE に対する要求が発行できない)。
- 接続のトラフィック使用率が 70%/90% を超えた。
- デバイスの CPU 使用率が 96% を超えた。

このセクションは、ネットワーク内でヘルス問題が発生しなければ表示されません。

一時停止されたインターフェイス

このセクションには、ネットワーク内のすべての一時停止されたポートに関する情報が表示されます。

一時停止された各インターフェイスの次の情報が表示されます。

- デバイス ID
- インターフェイス名
- 一時停止の理由(最大 20 文字の文字列)
- 自動回復ステータス(有効/無効)
- インターフェイスを再アクティブ化するためのボタン(このボタンを使うには、SNA をフル権限モードにする必要があります)。

このセクションは、ネットワーク内に一時停止されたインターフェイスが存在しなければ表示されません。

通知

通知は、システム管理者の注意を必要とする、ネットワーク上で発生したイベントです。通知メカニズムは、ネットワーク内の SNA スイッチの SYSLOG 機能を使用して、トポロジ マップに通知を表示します。

通知の表示

SNA デバイスによって SYSLOG メッセージが生成されると、トポロジ表示にそのデバイスに関するインジケータが表示されます。

通知は、SNA スイッチの RAM ログから抽出されるため、RAM ログに対して設定された重大度しきい値を渡す SYSLOG だけが SNA によって検出されます。

SNA の通知は、SYSLOG 重大度レベルに基づくカテゴリ別に分類されます。次のように、通知の色はその重大度を示しています。

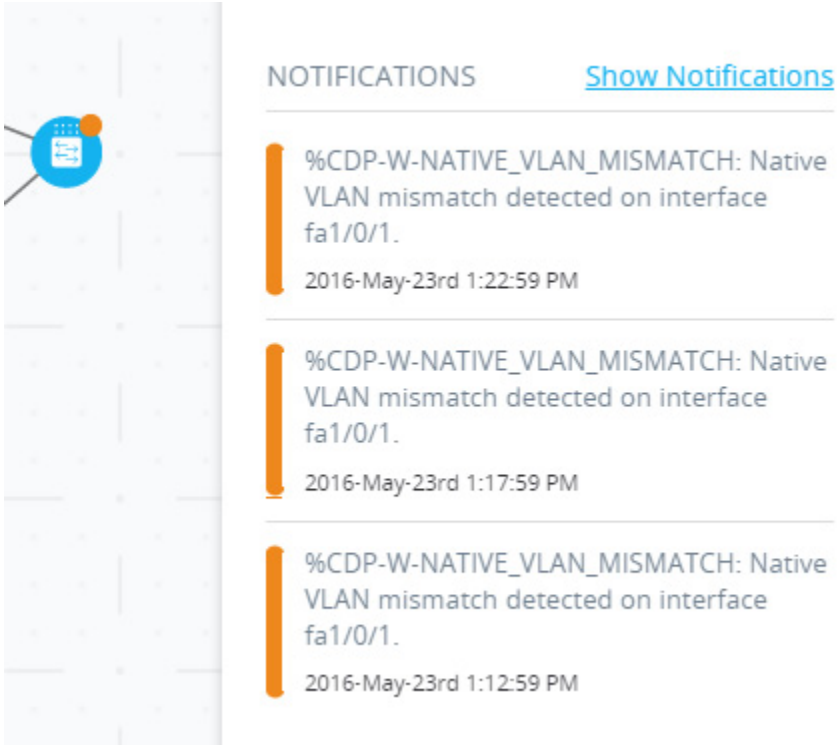
- ランク 1(赤色):重大、アラート、または緊急
- ランク 2(オレンジ色):警告またはエラー
- ランク 3(青色):情報または注意

通知を生成するイベントが発生すると、関連する SNA デバイス上にインジケータが表示され、そのデバイス上の新しい通知の数と最も深刻な通知の重大度が示されます。たとえば、 69 は、最も深刻な通知が警告であることを示します。

加えて、通知が存在する場合は、アプリケーション マストヘッドに一般通知アイコンが表示されます。このインジケータは、ログアウト時に消去されますが、SNA の動作中にイベントが発生すると再び更新されます。

通知は次の方法で表示することができます。

- 管理対象スイッチまたは SNA スイッチを 1 つ選択します。重大度と時間順に並べられた上位 3 つの通知が右側の情報パネルの [通知] セクションに表示されます。



- [通知を表示] をクリックすると、右側の情報パネルのリストが展開され、デバイス上で記録された最新の 100 件の SYSLOG を含む表が表示されます。このオプションは、すべての SNA スイッチで使用することができ、SNA セッションがアクティブと非アクティブのどちらのときに発生したかに関係なく、最新の 100 件の SYSLOG を表示します。
-  をクリックすると、ネットワーク全体の通知の集合リストを含む表が表示されます。この表には、SNA デバイスまたは部分 SNA デバイスによって記録されたネットワーク内の最新の 300 件のイベントが表示されます。

特定の通知を表示すると、トポロジ表示から新しい通知の注釈は削除されますが、すべての通知は通知ログに残っているため、最新の通知を側面パネルで見ることができます。

通知を表示すると、次の属性が表示されます。

- [発信側デバイス]:集合通知の表示にのみ表示されます。発信側デバイスは、次の優先順位に基づき、入手可能なものの中から一番強力なフォームの ID で識別されます。ホスト名 → IP アドレス → MAC アドレス
- [タイムスタンプ]
- [重大度]
- [SYSLOGテキスト]

デバイス認可制御(DAC)

デバイス認可制御(DAC)機能を使用して、ネットワーク内の認可されたクライアントデバイスのリストを作成します。DAC はネットワーク内の SNA デバイスの 802.1x 機能を有効化します。そうすると、いずれかの SNA デバイスに組み込み RADIUS サーバ(RADIUS ホスト サーバ)を設定することができます。デバイスの認可は MAC 認証により行われます。

DAC ワークフロー

DAC ワークフローは次のステップで構成されます。

ステップ 1 DAC をアクティブにします。「DAC へのアクセス」を参照してください。

ステップ 2 RADIUS サーバ デバイスとクライアント デバイスを構成します。「RADIUS サーバとクライアントの指定」を参照してください。

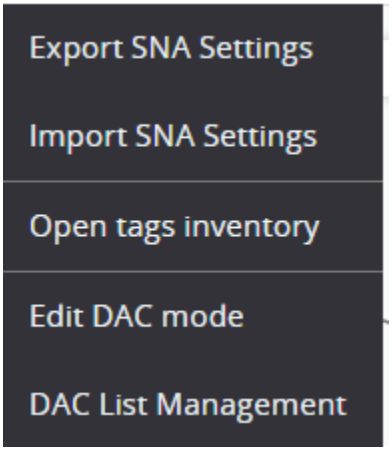
ステップ 3 ホワイト リストにクライアント デバイスを追加します。「DAC リスト管理」を参照してください。

DAC へのアクセス

DAC にアクセスするには、次の手順を実行します。

ステップ 1 マストヘッドの左側にあるオプション メニューをクリックします。

次のメニューが表示されます。

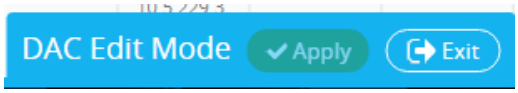


ステップ 2 [DAC モードの編集] を選択します。

RADIUS サーバとクライアントの指定

ステップ 1 オプション メニューの [DAC モードの編集] をクリックします。

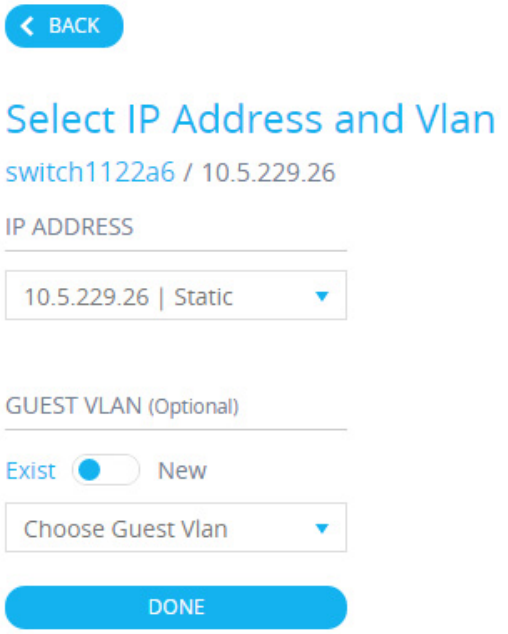
ステップ 2 アプリケーションが DAC 編集モードに入ります(これは、トポロジ マップと画面下部のコントロール パネルを囲む青色のフレームで示されます)。



ステップ 3 SNA デバイスの 1 つを選択し、その メニューをクリックします。

ステップ 4 [+ DAC サーバとして設定] をクリックすることにより、そのデバイスをネットワークの RADIUS サーバに指名します。

次のメニューが表示されます。



ステップ 5 デバイスに複数の IP アドレスが設定されている場合は、その中の 1 つを DAC によって使用されるアドレスとして選択します。アドレスのリストには、IP インターフェイスが静的か動的かが示されます。アドレスが安定しないおそれがある動的インターフェイスを選択した場合は、警告が表示されます。既存の DAC サーバを編集するときは、現在そのクライアントによって使用されているアドレスが事前に選択されています。

ステップ 6 DAC RADIUS サーバとネットワーク上のそのすべてのクライアントによって使用されるキー文字列を入力します。

ステップ 7 [完了] をクリックします。

DAC RADIUS サーバがトポロジ表示内で強調表示されます。

ステップ 8 サーバを選択してから、クライアントとして追加するデバイスの ☰ メニューをクリックします。[+ クライアントとして設定] をクリックします。

- スイッチがすでに DAC RADIUS サーバのクライアントになっている(その IP アドレスが RADIUS サーバの NAS テーブル内に入っており、RADIUS サーバがその RADIUS サーバ テーブル内でプライオリティ 0 の [802.1x] または [すべて] の使用タイプに設定されている)場合は、スイッチが事前に選択されています。

- 選択したクライアントに 802.1x 用に構成されている RADIUS サーバ(以前に選択されているサーバ以外)がすでにある場合、先に進むと既存の RADIUS サーバの操作が中断されることが通知されます。
- 選択したクライアントにプライオリティ 0 の 802.1x 用に構成されている RADIUS サーバ(以前に選択されているサーバ以外)がある場合、エラーメッセージが表示され、DAC はそのクライアントに設定されません。
- DAC RADIUS サーバに対して少なくとも 1 つのクライアントを選択します。クライアントが選択されていないと、設定を適用できなくなります。

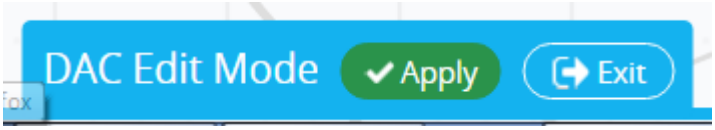
ステップ 9 スイッチがクライアントとして選択されている場合は、そのポートを含むウィンドウが表示されます。クライアント スイッチから 802.1 x 認証を適用するポートを選択します。

SNA では、すべてのエッジ ポート(他のスイッチまたはクラウドに接続されていることが判明していないすべてのポート)の一覧が推奨されています。次をクリックすることにより、これらの推奨ポートを選択できます。

このセレクションに対してポートを追加または削除することができます。この段階では、フル DAC 構成(表 を参照)になっているすべてのポートが事前選択されて表示されます。

ステップ 10 [完了] をクリックします。

ステップ 11 次の [適用] をクリックします。



DAC が構成されると、ブラック リストに掲載されていない新しいデバイスが DAC 対応 RADIUS サーバを通してネットワークで拒否されるたびにアラートが表示されます。二度とアラートが表示されないように、このデバイスを認可デバイスのホワイト リストに追加するのか、ブラック リストに送信するのかが尋ねられます。

新しいデバイスに関してユーザに通知するときに、SNA は、そのデバイスの MAC アドレスと、デバイスがネットワークへのアクセスを試みた時に経由したデバイスとポートを示します。

拒否イベントが DAC RADIUS サーバではないデバイスから届いた場合は、そのメッセージは無視され、その後の 20 分間は、そのデバイスからのすべてのメッセージが無視されます。20 分が経過すると、SNA が、再度、そのデバイスが DAC RADIUS サーバかどうかをチェックします。ユーザがホワイト リストに追加されると、そのデバイスがすべての DAC サーバの DAC グループに追加されます。この設定を保存するときに、すぐにサーバのスタートアップ構成に保存(このオプションはデフォルトで選択されています)するかどうかを決定できます。

デバイスは、ホワイト リストに追加されるまで、ネットワークへのアクセスが拒否されます。

DAC RADIUS サーバが定義され、到達可能である限り、いつでもホワイト リストとブラック リストを表示して変更することができます。

DAC 設定を適用するときに、参加デバイスに適用されるアクションを一覧表示したレポートが表示されます。変更を承認したら、その設定を対象のデバイスのスタートアップ コンフィギュレーション ファイルに追加でコピーするかどうかを決定できます(このオプションはデフォルトで選択されています)。最後に、構成を適用します。

DAC 構成プロセスの一部の手順が不足している場合の警告と、デバイスによって処理されたアクションのステータスがレポートに表示されます。

次のフィールドがレポートに表示されます。

フィールド	値	コメント
デバイス	デバイス識別子(ホスト名、IP アドレス)	
アクション	DAC サーバに可能なアクション: • RADIUS サーバの有効化 • RADIUS サーバの無効化 • クライアント リストの更新 • RADIUS サーバ グループの作成 • RADIUS サーバ グループの削除 DAC クライアントに可能なアクション: • RADIUS サーバ接続の追加 • RADIUS サーバ接続の更新 • RADIUS サーバ接続の削除 • 802.1x 設定の更新 • インターフェイス認証設定の更新 • インターフェイス ホストおよびセッション設定の更新	各デバイスに対して複数のアクションが表示される場合があります(その確率のほうが高い)。 アクションごとに独自のステータスがあります。
警告	DAC サーバに関して発生しうる警告: • 選択された IP インターフェイスが動的です。 DAC クライアントに関して発生しうる警告: • デバイスはすでに別の RADIUS サーバのクライアントになっています。 • ポートが選択されていません。	警告には、問題に対処できる DAC のセクションへのリンクも含まれています。 警告が表示されたら、変更を適用できます。
ステータス	• 保留中 • 成功 • エラー	ステータスが障害の場合は、アクションに関するエラー メッセージが表示されます。

DAC リスト管理

クライアント デバイスを追加して、認証するポートを選択したら、それらのポート上で検出されたすべての非認証デバイスが非認証デバイスのリストに追加されます。

DAC は、デバイスの次のリストをサポートします。

- **ホワイト リスト**:認証してもよいすべてのサーバのリスト
- **ブラック リスト**:認証してはいけないサーバのリスト

認証したいデバイスとそのポートは、ホワイト リストに追加する必要があります。それらを認証しない場合は、必要なアクションはありません。それらはデフォルトでブラック リストに追加されます。

このようなデバイスをホワイト リストに追加するまたはブラック リストから削除するには、次のようにします。

ステップ 1 非認証デバイス アイコン をクリックします。

[DAC リスト管理] ページが開いて、非認証デバイスのリストが表示されます。

ステップ 2 ホワイト リストに追加するデバイスを選択して、[ホワイト リストに追加] をクリックします。

ステップ 3 ブラック リストに追加するデバイスを選択して、[ブラック リストに追加] をクリックします。

ステップ 4 [適用] をクリックします。デバイスのポートから入ってくるパケットは、RADIUS サーバ上で認証されます。

ホワイト リストまたはブラック リストを管理するには、それぞれ、[ホワイト リスト] タブまたは [ブラック リスト] タブをクリックします。

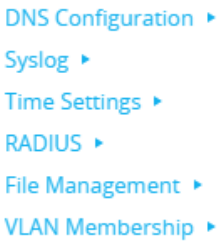
これらページでは次のタスクを実行できます。

- **リストから削除**:選択したデバイスをリストから削除します。
- **ブラック リストに移動/ホワイト リストに移動**:選択したデバイスを指定したリストに移動します。
- **デバイスの追加**:MAC アドレスを入力して、[追加 +] を押すことにより、デバイスをブラック リストとホワイト リストのどちらかに追加します。
- **MAC アドレスでデバイスを検索**:MAC アドレスを入力して [検索] をクリックします。システムは、このデバイスからのトラフィックが発生した日付と時刻(前回の検出)と、システムがネットワークへのアクセスを試みたポート/デバイス(検出場所)を返します。

サービス

サービスとは、複数の SNA 対応デバイスやインターフェイスで同時にアクティベートできる構成のことです。SNA を完全にサポートするデバイスまたはそのようなデバイスのインターフェイスでのみ使用できます。

サービスは右側の情報パネルから選択します。



サービスを適用するには、トポロジ表示から 1 つ以上のデバイスまたはインターフェイスを選択します。これは、マップから手動で、あるいは検索結果から選択することで行えます。選択したすべての要素に適用可能なサービスをアクティベートすることができます。

サービスを選択すると、そのサービス専用の GUI が表示されます。選択したすべての要素の関連機能の現在の設定が表示されます。サービスごとに表示される特定のパラメータについては後述します。選択したデバイスまたはインターフェイスの設定を更新したり、あるデバイスから選択したエントリを別のデバイスにコピーしたりできます。

また、あるデバイスまたはインターフェイスの設定を、選択した他のすべてのデバイスまたはインターフェイスの設定として使用することもできます。

ほとんどのサービスでは、GUI ページが表示されます。そこで、そのサービスに固有のパラメータを定義することができます。GUI ページでパラメータを入力し、それらに対して可能なすべてのクライアント側検証を実行したら、その設定が選択したデバイスまたはインターフェイスに送信されます。それが受け取られると、サービスの結果を示すレポートが表示されます。サービスの受信側のそれぞれのステータス(送信中、成功、失敗)が表示され、エラーが受信された場合は、エラー メッセージの詳細が受信側に表示されます。

SNA と構成先デバイス間の通信エラーが原因で構成が失敗した場合は、その構成を再試行できるオプションが表示されます。

デフォルトでは、すべてのサービスが、構成が終わったら自動的に実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルにコピーします。このオプションは無効にすることができます。

デバイス レベル サービス

以下のサービスは、スイッチに使用可能です。

- RADIUS クライアント構成
- DNS クライアント構成
- SYSLOG サーバ構成
- 時刻設定の構成
- ファイル管理
- 電力管理ポリシー(デバイス レベル)
- VLAN メンバーシップ(デバイス レベル)

これらのデバイス レベル サービスごとに、選択したデバイスの現在の構成を示すチケットに、次の識別情報とサービス固有のパラメータが表示されます。

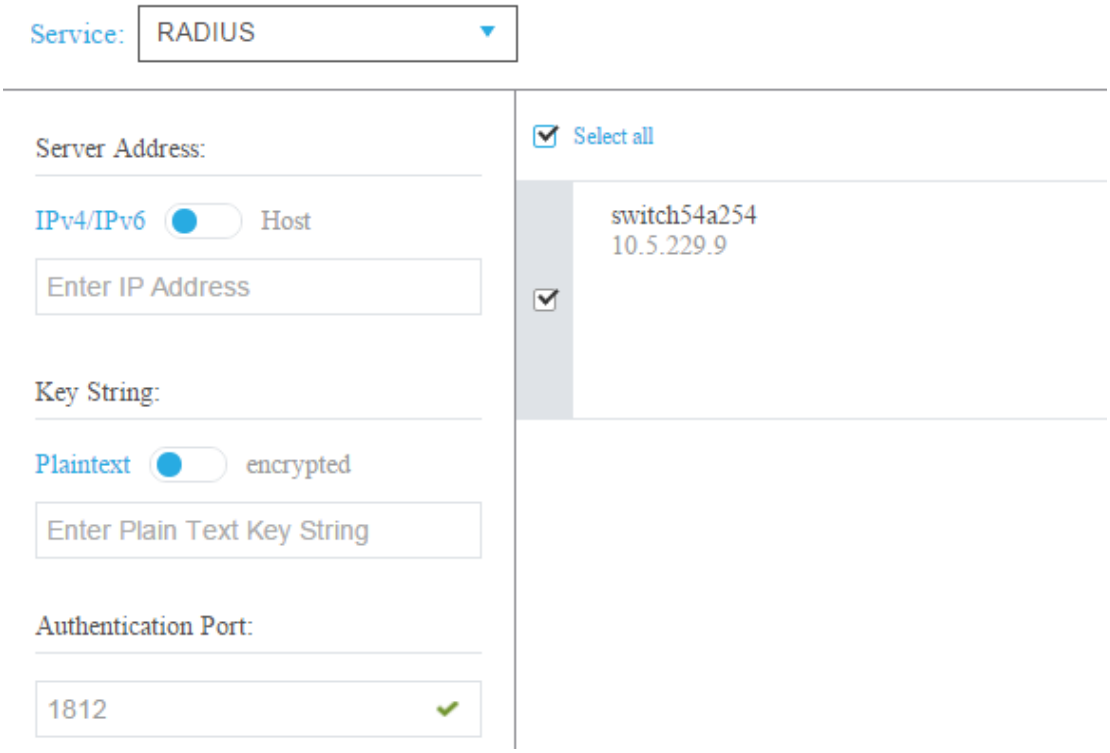
- デバイス ホスト名
- IP アドレス:デバイスの IP アドレスが複数存在する場合は、SNA がそのデバイスにアクセスするために使用するアドレスが表示されます。
- デバイス モデル:デバイス モデルを表す英数字文字列。例:SG350XG-2F10。

RADIUS クライアント構成

このサービスを使用すれば、ログインに使用する RADIUS サーバを定義することにより、1 つ以上のデバイスを RADIUS クライアントとして構成することができます。

現在の構成

選択した各デバイスの現在の構成が右側の情報パネルに表示されます。最低のプライオリティの RADIUS サーバで、使用タイプが [ログイン] または [すべて] という構成になっています。



最低のプライオリティの RADIUS サーバが複数存在する場合は、次の順に 1 つのサーバが表示されます。

- ホスト名で定義された最初の RADIUS サーバ(アルファベット順)
- 一番低い IPv4 アドレスを持つ RADIUS サーバ
- 一番低い IPv6 アドレスを持つ RADIUS サーバ

サービスによって作成されたエントリは、0 のプライオリティで、使用タイプが [ログイン] になっています。

IP アドレスまたはホスト名が新しいエントリと同じで、プライオリティが 0、使用タイプが [802.1x] のエントリがすでに存在する場合は、既存のエントリが使用タイプ [すべて] に更新されます。

IP アドレスまたはホスト名が異なるエントリがすでに存在する場合は、そのエントリが表示され、その使用タイプが [ログイン] であれば、新しいエントリに置換されます。その使用タイプが [すべて] だった場合は、[802.1x] に変更されます。

IP アドレスまたはホスト名が同じで、プライオリティが 0 より低いエントリがすでに存在する場合は、そのエントリのプライオリティが 0 に変更され、必要に応じて、[ログイン] の使用タイプが追加されます。

表示される/編集可能なパラメータ

選択したデバイスを現在構成している RADIUS サーバとは別の RADIUS サーバのクライアントとして構成するには、次のフィールドに値を入力します。

- [サーバアドレス]:RADIUS サーバの IPv4 アドレスまたは IPv6 アドレス。
- [キー文字列]:RADIUS サーバに使用されるキー文字列(最大 128 文字)。

このパラメータは暗号化形式で表示されます。キー文字列を暗号化形式で入力するか、プレーンテキスト形式で入力するかを選択できます。

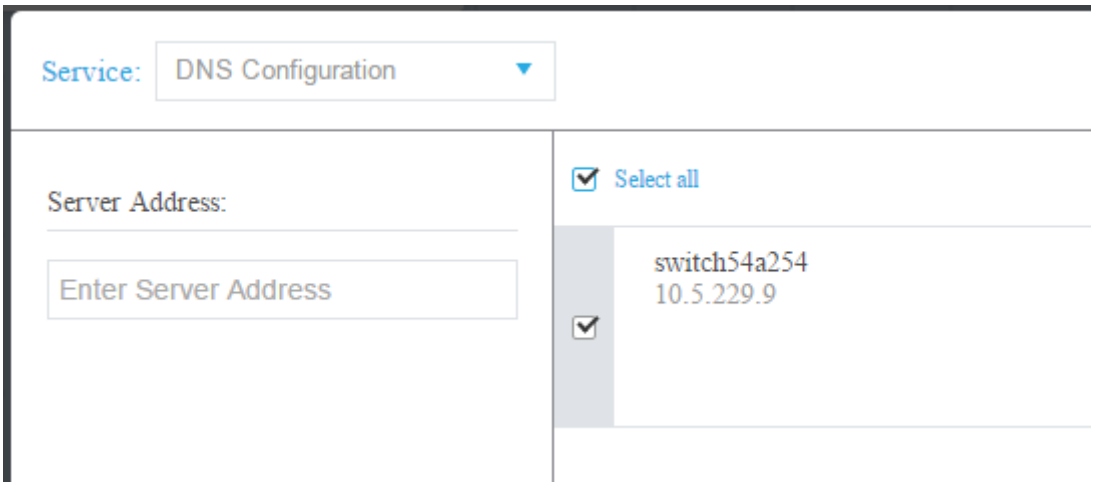
- [認証ポート]:認証ポートの番号。
- [認証方式]:SNA で現在使用されているチャネル(HTTP または HTTPS)により各デバイスに使用される認証方式のリスト。このパラメータの一般的な値は、[ローカル] または [RADIUS、ローカル] です。デバイスの現在値が他の値の場合は、そのデバイスに対してコピー オプションが使用できません。設定をコピーすると、[RADIUS、ローカル] の値が [RADIUS プライマリ認証方式] ラジオ ボタンにマップされます。
- [プライマリ認証方式]:構成セクションに表示される書き込み専用パラメータ。次の 2 つの選択肢があります:[ローカル データベース]、[RADIUS]。[RADIUS] を選択した場合、すべてのチャネルに対して構成される実際の値は [RADIUS、ローカル] になります。

DNS クライアント構成

DNS クライアント構成サービスを使用すれば、選択したデバイスが使用する DNS サーバを定義することができます。

現在の構成

選択した各デバイスの現在の構成が右側に表示されます、現在の DNS サーバはプリファレンス 1 を使用しています。複数の DNS サーバが存在する場合は、静的に定義されたサーバが表示されます。



表示されたサーバが動的エントリの場合は、そのことが通知され、そのサーバが削除されないようになっています。

サービスによって作成されたエントリは、プリファレンス 1 になります。プリファレンス 1 の静的エントリがすでに存在し、それが表示されていた場合は、静的サーバが新しいエントリに置き換えられます。

表示される/編集可能なパラメータ

新しい DNS サーバを定義するには、その IPv4 または IPv6 アドレスを入力します。

SYSLOG サーバ構成

このサービスを使用すれば、選択したデバイスによって使用される SYSLOG サーバを定義することができます。

現在の構成

選択したデバイスごとに、SYSLOG テーブルで最も低いインデックスの SYSLOG サーバが表示されます。

静的エントリがすでに存在し、それが表示されていた場合は、サービスによって作成された新しいエントリに置き換えられます。

表示される/編集可能なパラメータ

新しい SYSLOG サーバを定義するには、そのサーバの IPv4 または IPv6 アドレスを入力します。

ホスト名は保存されないため、サーバ アドレスの設置プロセスの一環として IP 解決が SNA によって実行されます。その結果、チケット上のサーバ アドレスは常に IP アドレスとして表示されます。

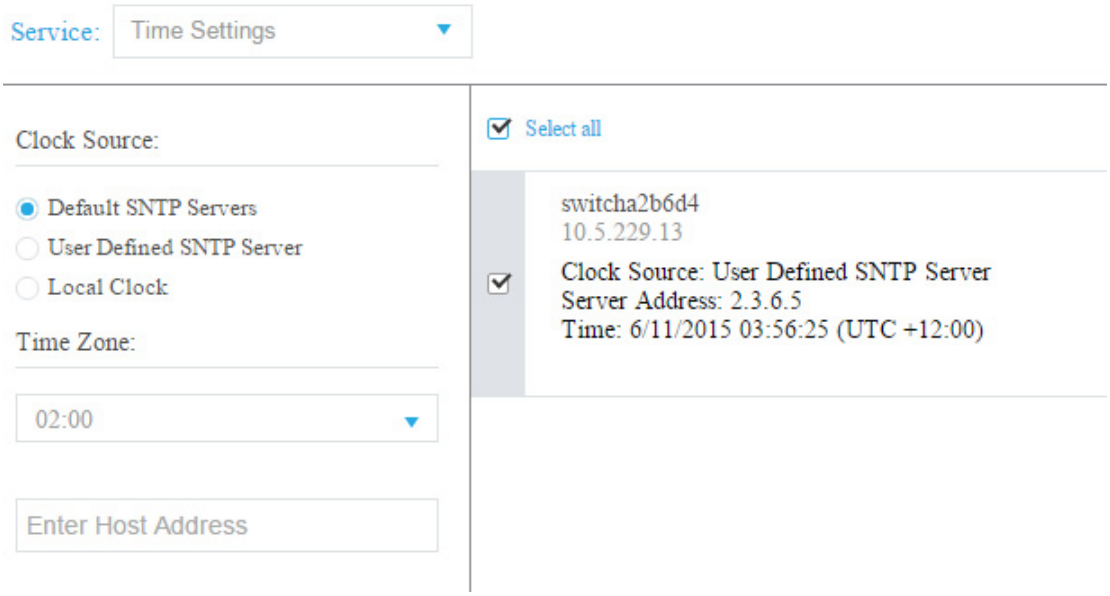
時刻設定の構成

このサービスを使用すれば、選択したデバイスの時刻源とシステム時刻を定義することができます。

注 ネットワーク内のすべてのデバイス間の時刻設定を同期するために、このサービスを実行することを強くお勧めします。特に、複数のデバイスで履歴統計情報を見る際にお勧めします。

現在の構成

選択した各デバイスの現在の設定が表示されます。



以下のオプションとともに、現在のクロック ソースが表示されます。

- [デフォルトSNTPサーバ]:クロック ソースが SNTP の場合に表示されるデフォルト サーバ。
- [ユーザ定義のデフォルトSNTPサーバ]:クロック ソースが SNTP で、現在の構成に 1 つ以上の非デフォルト SNTP サーバが含まれている場合に表示されます。この場合は、次の優先順位に従って上位の SNTP サーバが表示されます。
  - ホスト名で定義された最初の SNTP サーバ(アルファベット順)
  - IPv4 で定義された最下位の SNTP サーバ
  - IPv6 で定義された最下位の SNTP サーバ
- [ローカルクロック]:クロック ソースがローカルの場合に表示されます。
- [現在の時刻]:現在の時刻とタイム ゾーン オフセットの表示。

編集可能なパラメータ

クロック ソースを変更するには、次のオプションのいずれかを選択します。

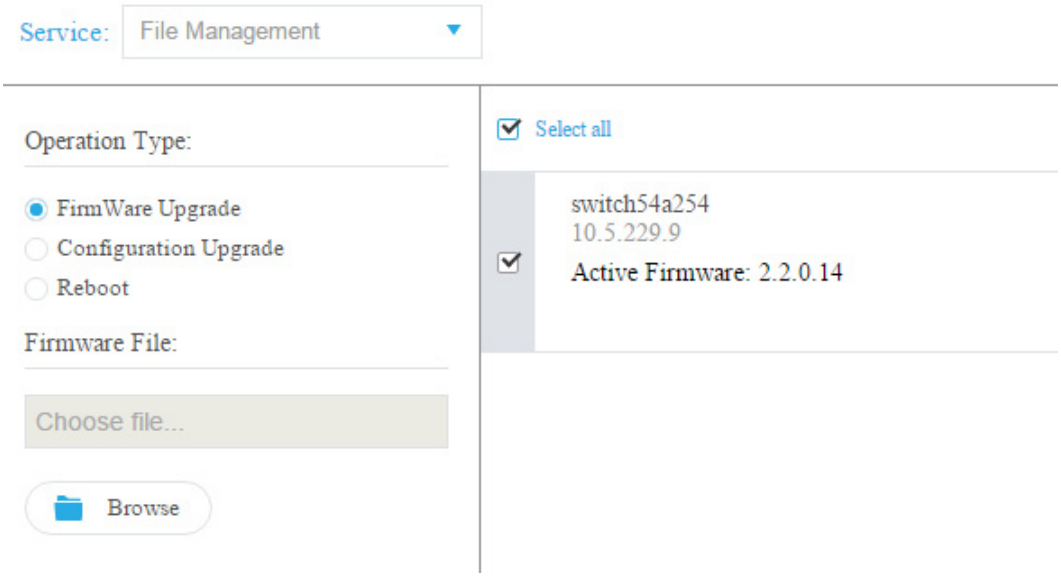
- [デフォルトSNTPサーバ]:構成したすべての SNTP サーバを削除し、3 つのデフォルト サーバを作り直します。
- [ユーザ定義のデフォルトSNTPサーバ]:ホスト名、IPv4、または IPv6 のいずれかを入力することにより、SNTP サーバのアドレスを追加します。サーバを適用すると、現在構成されているすべてのサーバが削除され、サーバ 1 が追加されます。このオプションと一緒に [タイム ゾーン] を構成する必要があります。
- [ローカルクロック]:デバイスのクロック ソースをローカル クロックに変更します。日付、時刻、およびタイム ゾーンを構成する必要があります。
- [日時の設定]:ローカル クロックが構成された場合の日付と時刻。
- [タイムゾーン]:ユーザ定義の SNTP サーバまたはローカル時刻が設定された場合のタイム ゾーン オフセット。

ファイル管理

これまで説明してきたサービスとは違って、ファイル管理サービスは、選択されたデバイスの構成を直接変えるものではありません。代わりに、選択されたすべてのデバイスに対して操作を実行します。このサービスは、新しいファームウェア バージョンまたはコンフィギュレーション ファイルを、選択したデバイスにダウンロードしたり、それらをデバイスをリブートしたりするために使用します。

現在の構成

次にように、現在の構成には、アクティブ ファームウェア バージョンが表示されます。



操作

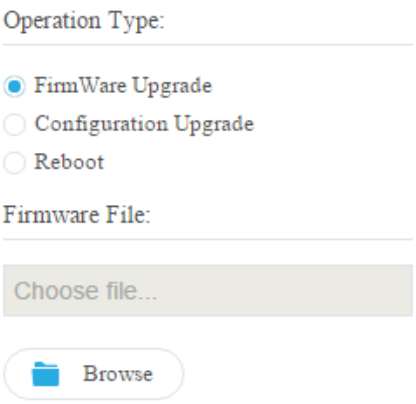
サービスから次の操作を使用できます。

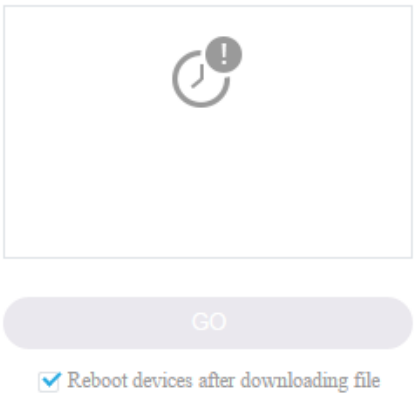
- HTTP 経由のファームウェアのダウンロード

  新しいファームウェア ファイルをダウンロードするために使用します。ローカル ファイル システムで、新しいファームウェア ファイルをブラウズして選択します。このファイルがサービスに参加しているすべてのデバイスにダウンロードされます。

  新しいファームウェアのダウンロード後に、デバイスはそれを自動的にアクティブ ファームウェア バージョンにします。

この操作を選択するときに、ダウンロードを完了したすべてのデバイスが自動的にリブートして、アップグレード処理を完了するように要求することもできます(このオプションはデフォルトで選択されています)。

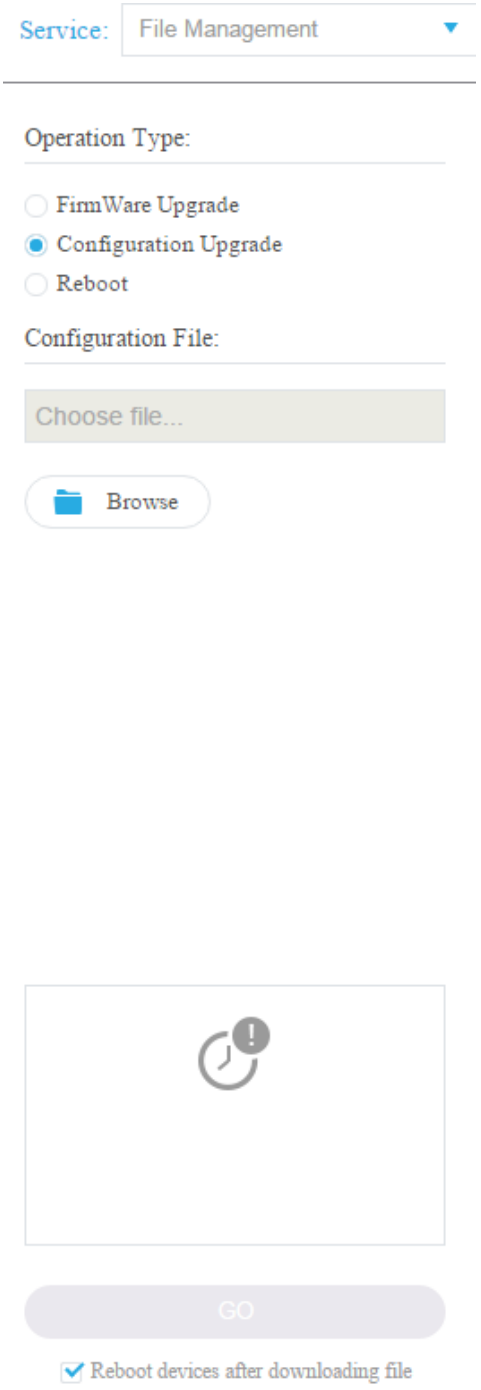




- HTTP 経由の構成のダウンロード

  新しいコンフィギュレーション ファイルをダウンロードするために使用します。ローカル ファイル システムで、新しいコンフィギュレーション ファイルをブラウズして選択します。このファイルがサービスに参加しているすべてのデバイスのスタートアップ構成にダウンロードされます。

ダウンロードをアクティブにするときに、コンフィギュレーション ファイルのダウンロード後にすべてのデバイスがリブートして、新しい構成を有効にするように要求することができます。



- リブート:

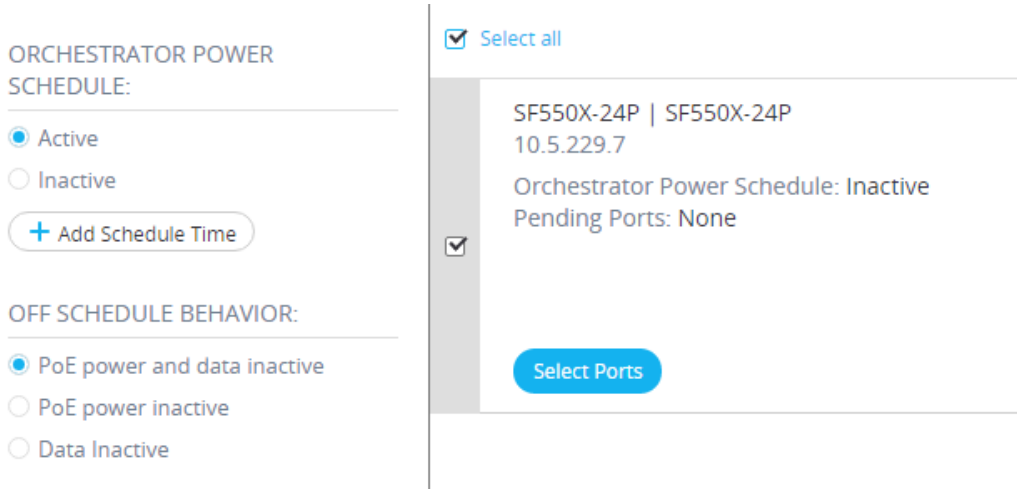
  [実行] をクリックすれば、他のアクションを実行しなくてもデバイスをリブートすることができます。

電力管理ポリシー(デバイス レベル)

このサービスを使用すれば、選択したデバイスの電力ポリシーを設定することができます。

現在の構成

下の図のように、選択した各デバイスの、現在の電力スケジュール パラメータが表示されます。



次のパラメータが表示されます。

- SNA 電力スケジュール(アクティブ/非アクティブ)
- アクティブな場合の電力スケジュールの詳細
- 時間電力を毎日(月曜日から日曜日まで)アクティブにするかどうか
- オフスケジュール時間帯のポートの動作次のようなオプションがあります。
  - PSE 電力非アクティブ
  - データ非アクティブ
  - PoE 電力非アクティブとデータ非アクティブ

- カスタム:SNA 作成スケジュールがすべてのアクセス ポートに均一に適用されていない場合に表示されます。アクセス ポートは、VLAN モードが「アクセス」になっているポートです。
- 構成済みポート:SNA 作成スケジュールにバインドされたすべてのポートのリスト。

編集可能なパラメータ

電力スケジュールを作成して(電力管理ポリシーのセットアップを参照)、それをデバイスに適用することができます。このアクションを実行するには、日単位のアクティビティの開始時刻と終了時刻を選択してから、オフタイムの動作を以下の中から選択します。

- PSE 電力非アクティブ
- データ非アクティブ
- PoE 電力非アクティブとデータ非アクティブ(デフォルト)

デバイスのスケジュールを適切にアクティブにするには、デバイスごとに少なくとも 1 つのポートが選択されている必要があります。

少なくとも 1 つの PoE デバイスが選択されていれば、1 つの動作だけ選択することができます。そうでない場合は、スケジュールを作成または削除することしかできません。

このサービスによって作成されたスケジュールでは、予約済みの名前(orch_power_sched)が使用されます。他の名前の時間範囲は SNA で無視されます。

設定を適用すると、適用された動作が選択されたすべてのポートにバインドされます。選択されなかったすべてのポートは、これまでバインドされていたスケジュールからバインド解除されます。

非 PoE ポートは、データを停止する動作のいずれかが選択されている場合にのみ、影響を受けます。選択されたポートが選択された動作の影響を受けない場合は、注意書きが成功メッセージに追加されます。この注意書きは、選択された動作が一部のポートに適用されなかったために、それらのポートがバインドされなかったことをユーザに伝達します。

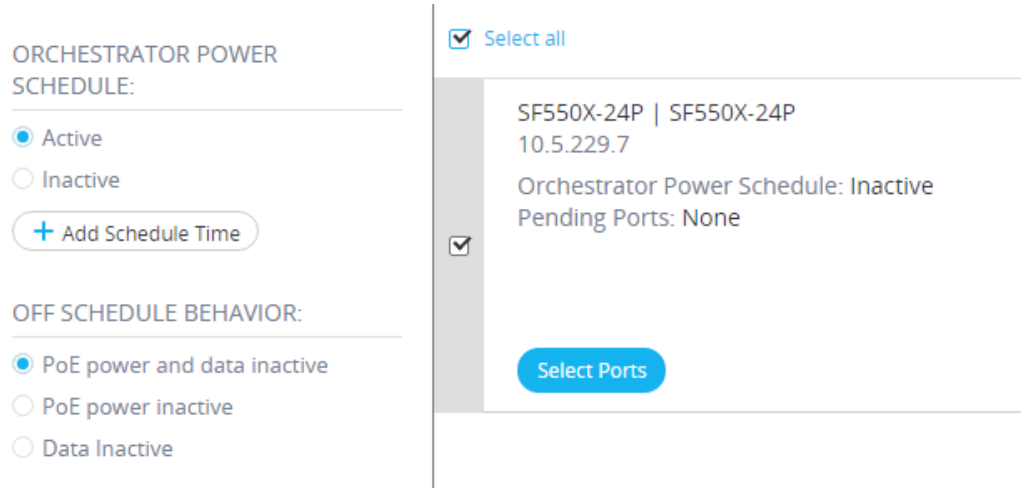
電力管理ポリシーのセットアップ

電力管理ポリシーをセットアップするには、次のようにします。

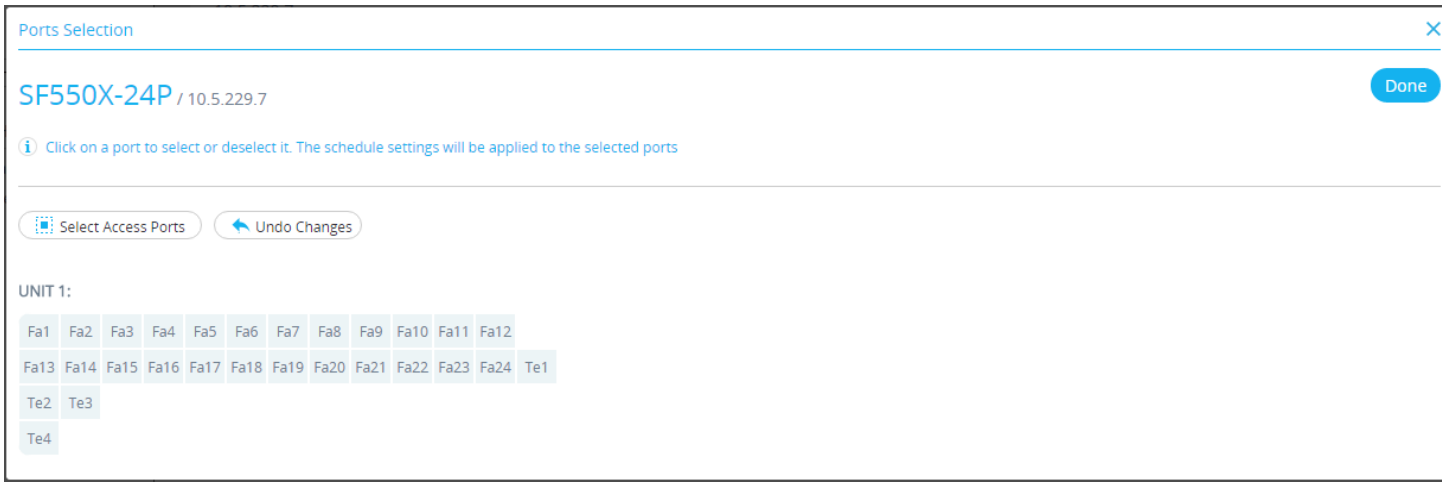
ステップ 1 トポロジ表示でデバイスを選択します。

ステップ 2 右側の情報パネルで [電力管理] サービスを選択します。

以下が表示されます。

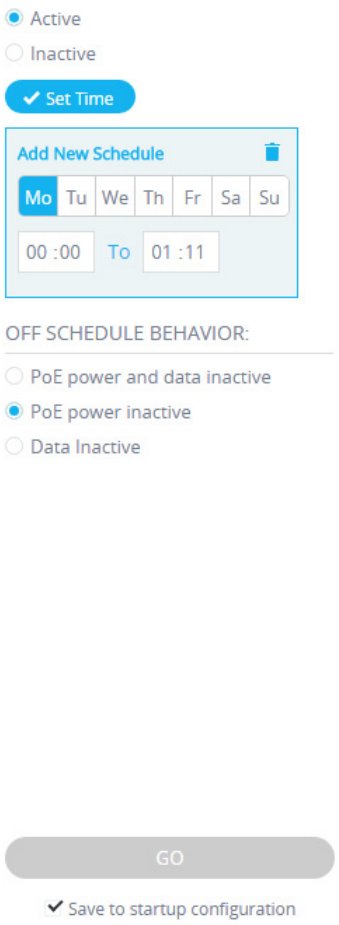


ステップ 3 [ポートの選択] をクリックします。



ステップ 4 1 つ以上のポートを選択して、[完了] をクリックします。

ステップ　5　[+ スケジュール時間の追加] をクリックします。



ステップ　6　フィールドに値を入力(上記参照)し、[実行] をクリックします。

電力管理ポリシーが定義されました。

VLAN メンバーシップ(デバイス レベル)

このサービスは、複数のデバイスのインターフェイスの VLAN メンバーシップを設定します。

現在の構成

デバイスごとに、次のパラメータが表示されます。

- アクセス ポート:アクセス VLAN モードになっているポートのリスト。このリストは、ポートが属しているアクセス VLAN 別にグループ分けされます。ポートの連続範囲はダッシュを使用して結合します。
- トランク ポート:トランク VLAN モードになっているポートのリスト。このリストは、ポートが属しているネイティブ VLAN 別にグループ分けされます。ポートの連続範囲はダッシュを使用して結合します。

編集可能なパラメータ

VLAN メンバーシップを編集する場合は、操作する VLAN をまず選択します。この VLAN 選択では、ネットワーク内の既存のすべての VLAN から選ぶオプションと、新しい VLAN を作成するオプションが用意されています。

VLAN を選択したら、各デバイスのカードに接続されているポート選択パネルを開きます。

このパネルでは、選択した VLAN のメンバーになっているすべてのポートがメンバーシップ タイプに応じて次のようにマークされます。

- A:VLAN 内のタグなしメンバーになっているアクセス ポート。
- U:VLAN 内のタグなし(ネイティブ)メンバーでになっているトランク ポート。
- "*":上記以外の状態。当該 VLAN のメンバーではないか、別の VLAN モードのメンバーになっている。

ポートをクリックすると、A の状態と U の状態(および "*" の状態、ポートが元々その状態だった場合)が切り替わります。

LAG メンバーになっているポートには、その LAG に基づくマーキングが表示されます。このようなポートをクリックすると、同じ LAG のすべてのメンバーで切り替わります。

メンバーシップを編集して適用したら、ポートの所属先となるすべてのデバイスで VLAN が作成されます(VLAN が事前に存在していなかった場合)。

インターフェイス レベル サービス

一部のサービスは、デバイスよりもインターフェイスに関係しています。このようなサービスをアクティベートする場合は、1 つ以上のインターフェイスを選択してから、使用可能なサービスのリストからサービスを選択します。

インターフェイスに使用可能なサービスは次のとおりです。

- **電力管理設定(ポート)**:PoE プライオリティとスケジュール動作の適用。「電力管理設定(インターフェイス レベル)」を参照してください。
- **VLAN メンバーシップ(ポート/LAG)**:スイッチポート タイプ(アクセスとトランク)、アクセスとトランクのメンバーシップ。「VLAN メンバーシップ(インターフェイス レベル)」を参照してください。

各サービスで、選択されたインターフェイスの現在の構成を示すチケットに、次の識別情報とサービス固有のパラメータが表示されます。

- インターフェイス名
- デバイス ホスト名(インターフェイスの親デバイスの)
- IP アドレス(インターフェイスの親デバイスの):デバイスの IP アドレスが複数存在する場合は、SNA がデバイスにアクセスするために使用する IP アドレスが表示されます。
- デバイス モデル(インターフェイスの親デバイスの):デバイス モデルを表す英数字文字列。例:SG350XG-2F10。

電力管理設定(インターフェイス レベル)

このサービスは、特定のポートの電力設定を構成します。このサービスは、選択されたすべてのポートが同じデバイス(またはスタック)に属している場合にのみ実行できます。

表示されるパラメータ

- PoE 管理ステータス(有効/無効):このパラメータは PoE ポートの場合にのみ表示されます。
- ポート電力プライオリティ(低/高/重大):このパラメータは PoE ポートの場合にのみ表示されます。
- SNA 電力スケジュール(適用済み/未適用):このパラメータは、デバイスに SNA によって作成された電力スケジュールがある場合にのみ表示されます。

- スケジュール動作:この情報は、ポートに SNA 定義の電力スケジュールが適用されている場合にのみ表示されます。表示される値は次のとおりです。
  - PSE 電力非アクティブ
  - データ非アクティブ
  - PoE 電力非アクティブとデータ非アクティブ

編集可能なパラメータ

- PoE 管理ステータス(有効/無効):このコントロールは、少なくとも 1 つの PoE ポートがサービスに対して選択されている場合にのみ表示され、PoE ポートにのみ適用されます。
- ポート電力プライオリティ(低/高/重大):このコントロールは、少なくとも 1 つの PoE ポートがサービスに対して選択されている場合にのみ表示され、PoE ポートにのみ適用されます。
- SNA 電力スケジュール(適用済み/未適用):このコントロールは、デバイスに SNA によって作成された電力スケジュールがある場合にのみ表示されます。
- スケジュール動作:このコントロールは、ユーザがスケジュールの適用を選択した場合にのみ表示されます。可能な値を以下に示します。
  - PSE 電力非アクティブ
  - データ非アクティブ
  - PoE 電力非アクティブとデータ非アクティブ

PoE ポートが選択されていない場合は、スケジュールをポートに適用するか、ポートから削除することしかできず、どの動作も選択できません。スケジュールをポートに適用すると、[データ非アクティブ] オプションを選択した場合と同じ動作をします。

PoE ポートと非 PoE ポートの組み合わせが選択されている状態で設定を PoE ポートに適用すると、[PoE 電力非アクティブとデータ非アクティブ] オプションは [データ非アクティブ] であるかのように処理され、[PoE 電力非アクティブ] オプションはスケジュールが非 PoE ポート上でアクティブになっていないかのように処理されます。

VLAN メンバーシップ(インターフェイス レベル)

このサービスは、選択されたインターフェイスの VLAN メンバーシップを構成します。

表示される/編集可能なパラメータ

- インターフェイス名(読み取り専用)
- スイッチポート モード:表示時は、[アクセス]、[トランク]、[全般]、[カスタマー]、[プライベート - ホスト]、または [プライベート - プロミスキャス] から選択できます。ユーザは、構成時に [アクセス] か [トランク] を選択できます。
- アクセス VLAN:アクセス モード時のみ表示されます。表示時はアクセス VLAN ID が表示され、構成時はアクセス VLAN を選択できます。
- ネイティブ VLAN(SNA バージョン 2.3):トランク モード時のみ表示されます。表示時はネイティブ VLAN ID が表示され、構成時はネイティブ VLAN を選択できます。

VLAN は、ネットワーク上に存在する選択可能なすべての VLAN のリストから選択します。選択したインターフェイスが属しているデバイスに VLAN がない場合は、その VLAN がサービス操作の一部として作成されます。

ユーザは、VLAN(1 ～ 4094)を追加するオプションを選択することもできます。この VLAN は、サービスに選択されたインターフェイスを持つすべてのスイッチに追加されます。

インターフェイス設定

このサービスは、ポートまたは LAG の基本的なインターフェイス設定を構成します。

表示パラメータ

- 管理ステータス:アップ/ダウン。
- 現在のステータス:アップ/ダウン/一時停止。ポートが一時停止されている場合は、その理由が括弧内に表示されます。例:"一時停止(ACL)"。
- 自動ネゴシエーション:有効/無効。
- 管理速度:このパラメータは、自動ネゴシエーションが無効になっている場合にのみ表示されます。

  値は、10 M、100 M、1000 M、2500 M、5 G、または 10 G になります。
- 現在の速度:10 M、100 M、1000 M、2500 M、5 G、または 10 G。

- 管理デュプレックス モード:このパラメータは、自動ネゴシエーションが無効になっている場合にのみ表示されます。

  値は、[半二重] または [全二重] にすることができます。

- 現在のデュプレックス モード:[半二重] または [全二重]。

編集可能なパラメータ

- 管理ステータス:アップ/ダウン。
- 自動ネゴシエーション:有効/無効。
- 速度:このパラメータは、自動ネゴシエーションが無効になっている場合にのみ編集に使用できます。速度の可能な値は次のとおりです。10 M、100 M、1000 M、2500 M、5 G、または 10 G。ポートのタイプが異なるとこれらの値のサブセットも異なる可能性があり、サービスで表示されるオプションは現在選択されているポートのタイプによって異なります。
- デュプレックス モード:このパラメータは、自動ネゴシエーションが無効になっており、かつ選択された速度が 10 M または 100 M の場合にのみ使用できます。

SNA 設定の保存

SNA システム自体で(サービスを使用せずに)行われた変更はすべて保存できます。これらの設定は、ネットワークで起動した次の SNA セッションに使用できます。この保存された情報は、同じユーザ名を使用している限り、次に、同じネットワークに接続された SNA デバイスやブラウザからネットワークにアクセスするときにも使用できます。

設定の保存中に、SNA は、オンラインで検出されたすべての SNA デバイス(フラッシュの特別な **SNA** フォルダ)に変更を保存しようとします。設定のコピーを保存できない場合は、失敗が通知されます。

特定のデバイスまたはすべてのデバイスで保存操作が失敗した場合は、設定が保存されなかったデバイスを示すレポートを要求できます。レポートの各デバイスに、その ID とそこで記録されたエラーが表示されます。

SNA の実行中に、ネットワーク内の特定のデバイスでより新しいバージョンの SNA 設定が検出された場合は、より新しいバージョンが検出されたこと(その作成時刻とそれを検出したデバイスを含む)が通知され、SNA が使用するべき設定のバージョンを選択するプロンプトが出されます。

保存可能な設定は次のとおりです。

- ネットワーク内のすべてのバックボーン デバイスの位置。
- バックボーン デバイスとして指名されたクライアント デバイスがこのステータスを保持しています。
- ネットワーク内の要素に手動で追加されたタグ。
- ネットワークに手動で追加されたデバイス。
- バックボーン デバイスの説明文。
- DAC によって使用されるブラック リスト。

SNA 設定をネットワークに保存することに加えて、さらにバックアップを取るため、設定を外部ファイルにエクスポートしたり、そこからインポートしたりすることもできます。

ファイルをインポートしたり、ネットワーク上で検出されたより新しいファイルを受け入れたりすると、現在の SNA 設定が新しいファイルの設定で上書きされます。ファイルがインポートされ、トポロジが新しいパラメータに更新されたら、変更を維持するか、以前の設定に戻すことができるプロンプトが出されます。

変更を維持することにした場合は、新しい設定がネットワーク内のすべてのデバイスに保存されます。以前の設定に戻すことにした場合は、トポロジが以前の設定に戻されます。

新しいファイルのインポート後に設定を手動で保存すると、元に戻すオプションは使用できなくなります。

技術的詳細

SNA 機能の技術的詳細を以下に示します。

- サポートされるブラウザ:IE10 以降、Chrome、FireFox。
- MAC OS の Safari:6.1.2 ～ 7.0.2
- サポートされる OS:Win 7、Win 8、Win 8.1、Linux 2.6 ～ 3.11、MAC OSX バージョン 10.7 以降