付録

この章では、Cisco Business スイッチの特定のモデルにのみ適用される一般的なトピックについて説明します。

スイッチのスタックの管理

スイッチは、単独で機能させることも、スイッチのスタックに接続することもできます。デフォルトで、デバイスはスタッカブルですが、スタック ポートを備えていません。デフォルトでは、スイッチ上のすべてのポートがネットワークポートになっています。スタックポートのないスイッチは、それ自体だけによるスタック内のアクティブユニットと見なすことができます。また、スタックポートのないスイッチをスタンドアロンスイッチと見なすこともできます。複数のスイッチをスタックするには、スイッチ上で必要なネットワークポートをスタックポートとして再設定し、そのスタックポートを備えたスイッチをリングまたはチェーントポロジに接続します。

スタック内のスイッチ（ユニット）は、スタックポートを介して接続されます。その後、これらのスイッチは、単一の論理スイッチとして一括して管理されます。スタック ポートを Link Aggregation Group（LAG）のメンバーにすることによって、スタック ポートの帯域幅を増やすこともできます。

スタックは、単一のアクティブ/スタンバイと複数のメンバーのモデルに基づいています。スタックには次のような利点があります。

- ネットワーク容量を動的に拡張または縮小することができます。管理者は、ユニットを追加することで、スタック内のポート数を動的に増やしながら、一元管理を維持することができます。同様に、ユニットを除去して、ネットワーク容量を減らすことができます。
- スタック構成のシステムは、次の方法で冗長性をサポートしています。
  - スタンバイユニットは、元のアクティブユニットに障害が発生すると、そのスタックのアクティブユニットになります。
  - スタック システムは、チェーンとリングの 2 タイプのトポロジをサポートしています。リングトポロジでは、スタックポートのいずれかで障害が生じると、スタックはチェーントポロジとなり継続して機能します。
  - リング スタック内のポートでは、スタック ポート リンクのいずれかで障害が生じた場合のデータ パケット損失期間を短縮するために、ファスト スタック リンク フェールオーバーと呼ばれるプロセスがサポートされています。スタックが新しいチェーントポロジに回復するまで、スタック ユニットは、障害の生じたスタック構成ポートを介して送信されると想定されるパケットをループ バックし、ループ バックされたパケットを残りのスタック構成ポートを介して宛先へ送信します。ファスト スタック リンク フェールオーバーの間は、アクティブ/スタンバイユニットがアクティブのまま正常に機能しつづけます。

スタック内のユニットのタイプ

スタックは最大8つのユニットで構成されます。スタック内のユニットは、次のタイプのいずれかです。

- **アクティブ**：アクティブユニットの ID は、1 または 2 のいずれかにする必要があります。スタックは、それ自体を管理するアクティブユニット、スタンバイユニット、およびメンバーユニットを介して管理されます。
- **スタンバイ**：アクティブユニットに障害が発生すると、スタンバイユニットがアクティブロールを引き継ぎます（スイッチオーバー）。スタンバイユニットの ID は、1 または 2 のいずれかにする必要があります。
- **メンバー**：これらのユニットは、アクティブユニットによって管理されます。

ユニットのグループをスタックとして機能させるためには、アクティブ対応ユニットが存在している必要があります。アクティブ対応ユニットに障害が発生した場合、スタンバイユニット（アクティブロールを引き継ぐメインユニット）がある限り、スタックは機能し続けます。アクティブユニットに加えて、スタンバイユニットに障害が発生した場合、機能する唯一のユ

ニットはメンバーユニットです。これらも 1 分後に機能を停止します。これは、たとえば、1 分後に、アクティブユニットを使用せずに動作していたメンバーユニットの 1 つにケーブルをつないでもリンクが確立されないことを意味します。

スタック内のユニット数の下位互換性

スタック可能スイッチは、4 ユニットから 8 ユニットまでサポートします。これは、スイッチのモデルによって異なります。以前のソフトウェアリリースからのアップグレードは、構成ファイルを変更せずに実行できます。ハイブリッドスタックモードをサポートしていないファームウェアバージョンがスタックにロードされ、スタックが再起動されると、スタックはネイティブスタックモードに戻ります。ハイブリッドスタックモードのデバイスに、ハイブリッドスタックモードをサポートしていないファームウェアバージョンが読み込まれると、そのシステムモードはデフォルトのシステムモードに戻ります。スタックのユニット ID が手動で構成された場合、ID が 4 より大きいユニットは自動番号付与に切り替えられます。

スタックトポロジ

スタック内のユニットは、次のタイプのトポロジのいずれかで接続できます。

- チェーン トポロジ：各ユニットがネイバー ユニットに接続されているが、最初と最後のユニットの間にケーブル接続はありません。
- リング トポロジ：各ユニットがネイバー ユニットに接続されています。最後のユニットは、最初のユニットに接続されます。以下は、8ユニット スタックのリング トポロジを示しています。

リング トポロジの方が、チェーン トポロジより信頼性が高いです。リング内の 1 つのリンクの障害はスタックの機能に影響しませんが、一方、チェーン接続の 1 つのリンクの障害はスタックの分割を引き起こすことがあります。

トポロジディスカバリ

スタックは、トポロジディスカバリと呼ばれるプロセスによって確立されます。このプロセスは、スタック ポートのアップ/ダウン状態の変更によってトリガーされます。このプロセスをトリガーするイベントの例を次に示します。

- リングからチェーンへのスタック トポロジが変化する
- 2 つのスタックが 1 つのスタックにマージされる
- スタックが分割される
- 他のメンバーユニットがスタックに挿入される（たとえば、ユニットが障害のために、それ以前にスタックから切断されたため）。これは、チェーン トポロジで、スタックの中間のユニットで障害が生じた場合に発生することがあります。

トポロジディスカバリ中には、スタック内の各ユニットが、トポロジ情報を含むパケットを交換します。トポロジ ディスカバリ プロセスが完了すると、各ユニットには、スタック内のすべてのユニットのスタック マッピング情報が含まれます。

ユニット ID の割り当て

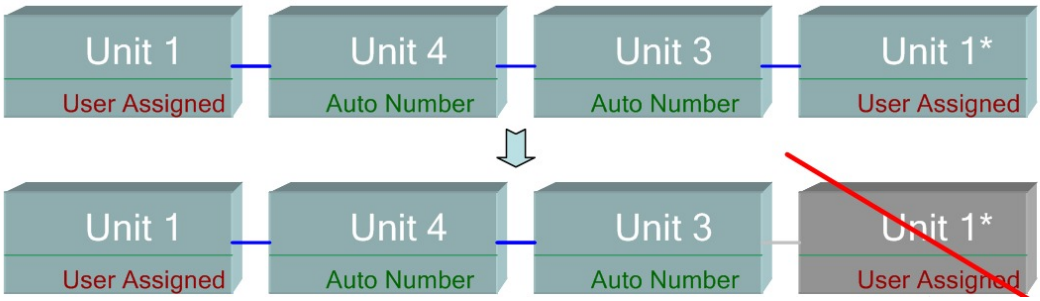
トポロジディスカバリが完了すると、スタック内の各ユニットに一意のユニット ID が指定されます。ユニット ID は、[System Mode and Stack Management] ページで、次の方法のいずれかで設定されます。

- **自動（Auto）**：ユニット ID は、トポロジディスカバリ プロセスによって指定されます。これがデフォルト設定です。
- **手動**：ユニット ID は、1 ～ 8 の整数に手動で設定されます。

重複ユニット ID

同じユニット ID を 2 つの個別のユニットに指定すると、それらの一方だけがそのユニット ID を使用してスタックに参加できます。自動番号付けを選択している場合、重複ユニットには、新しいユニット番号が指定されます。自動番号付けが選択されていない場合、重複ユニットはシャットダウンされます。2 つのユニットに手動で同じユニット ID が割り当てられたケースを以下に示します。ユニット 1 はスタックに参加せず、シャットダウンされます。アクティブ対応ユニット（1 または 2）の間のアクティブ選択プロセスで勝ち残れませんでした。

重複ユニットのシャットダウン



アクティブ選択プロセス

アクティブユニットは、アクティブ対応ユニット（1 または 2）から選択されます。アクティブユニットを選択する要因は、次の優先順位で考慮されます。

- [Force Active]：[Force Active] がユニットでアクティブになっている場合、そのユニットが選択されます。
- [System Up Time]：アクティブ対応ユニットは、10 分間のセグメント単位で測定される稼働時間を交換します。セグメント数が多いユニットが選択されます。両方のユニットが同じ時間セグメント数で、一方のユニットのユニット ID が手動で設定されていて、他方のユニットのユニット ID が自動的に設定されている場合は、手動定義のユニット ID を持つユニットが選択されます。それ以外の場合は、より小さいユニット ID を持つユニットが選択されます。両方のユニット ID が同じ場合は、最小の MAC アドレスを持つユニットが選択されます。

（注） スイッチ フェールオーバー プロセスでスタンバイユニットがアクティブとして選択されると、その稼働時間が保持されます。

- **ユニット ID**：両方のユニットの時間セグメント数が同じ場合、最小のユニット ID を持つユニットが選択されます。
- **MAC アドレス**：両方のユニット ID が同じ場合、最小の MAC アドレスを持つユニットが選択されます。

（注） スタックを動作させるためには、アクティブユニットが必要です。アクティブユニットは、アクティブの役割を引き受けるメインユニットとして定義されます。スタックには、アクティブ選択プロセスの後に、ユニット 1 およびユニット 2、またはどちらか一方が含まれている必要があります。そうしなかった場合は、スタックとそのすべてのユニットが、完全な電源オフとしてではなく、部分的にシャットダウンされますが、トラフィック通過機能は停止されます

スタックの変更

このセクションでは、スタックに変更を引き起こすことのあるさまざまなイベントについて説明します。次のいずれかの状況が発生すると、スタック トポロジが変更されます

- スタックとの間で1つまたは複数のユニットが接続されるか、切断される、またはその両方が発生する。
- スタック ポートのいずれかでリンクがアップまたはダウンする。
- スタックが、リング形態とチェーン形態の間で変化する。

スタックとの間でユニットが追加または削除されるか、その両方が発生した場合、トポロジの変更、マスター選択プロセス、および/またはユニット ID の割り当てがトリガーされます。

新しいユニットの接続

ユニットがスタックに挿入されると、スタック トポロジの変更がトリガーされます。ユニット ID が指定され（自動番号付けの場合）、ユニットはアクティブユニットによって設定されます。

既存のスタックに新しいユニットを接続すると、次のいずれかが発生することがあります。

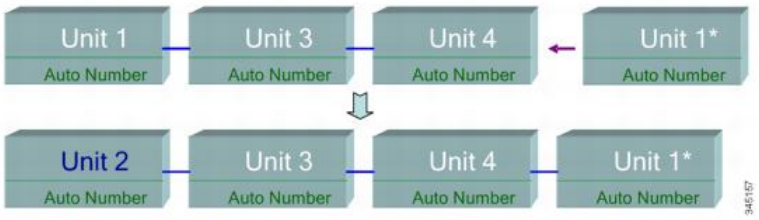
- 重複ユニット ID は存在しません。
  - ユーザ定義 ID を持つユニットが、自身のユニット ID を保持する。
  - 自動的に指定された ID を持つユニットが、自身のユニット ID を保持する。

- ファクトリー デフォルトのユニットは、使用可能な中で最小の ID で始まるユニット ID を自動的に受信する。

- 1 つ以上の重複ユニット ID が存在します。自動番号付けが、競合を解決し、ユニット ID を指定します。手動での番号付けの場合、1 つのユニットのみがそのユニット ID を保持し、その他はシャットダウンされます。
- スタック内のユニット数が、許可されるユニットの最大数を超えます。スタックに参加する新しいユニットはシャットダウンされ、SYSLOG メッセージが生成されて、マスターユニット上に表示されます

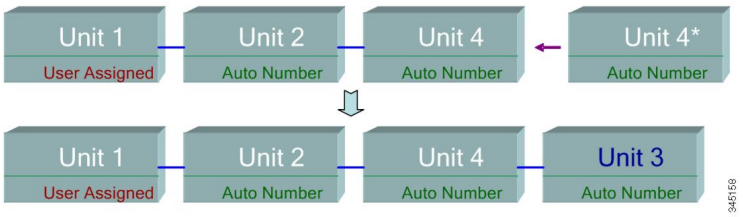
アクティブ対応ユニットがスタックに参加したときの自動番号付けの例を、以下に示します。ユニット ID が 1 の 2 つのユニットがあります。アクティブ選択プロセスでは、アクティブユニットとして最適なユニットが選択されます。最適なユニットは、10 分間のセグメントでより長い稼働時間を持つユニットです。その他のユニットは、バックアップとなります

自動番号付けされたアクティブ対応ユニット



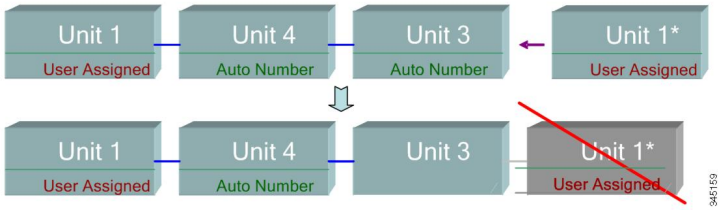
新しいユニットがスタックに参加したときの自動番号付与の例を以下に示します。既存のユニットはその ID を保持します。新しいユニットが使用可能な最小の ID を受け取ります。

自動番号ユニット



すでにユーザー指定されたユニット ID 1 のアクティブユニットが存在するスタックに、ユーザー指定のユニット ID 1 のアクティブ対応ユニットが参加したときに何が起きるかを、以下に示します。より新しいユニット 1 は、スタックに参加せず、シャットダウンされます。

ユーザー指定のアクティブ対応ユニット



スタック内のユニットの障害

アクティブユニットに障害が発生すると、スタンバイユニットがプライマリの役割を引き継ぎ、スタックは正常に動作しつづけます。

スタンバイスイッチがアクティブスイッチの代わりになることができるように、両方のユニットは常に予約された状態が維持されます。予約モードでは、アクティブスイッチとそのスタンバイスイッチがスタティック設定（スタートアップ コンフィギュレーション ファイルと実行コンフィギュレーション ファイルの両方に含まれる）と同期されます。スタンバイ スイッチ コンフィギュレーション ファイルは、前のアクティブスイッチに残ります。

STP 状態テーブル、動的に学習された MAC アドレス、動的に学習された SmartPort タイプ、MAC マルチキャスト テーブル、LACP、GVRP などのダイナミック プロセス状態情報は、同期されません。アクティブスイッチの設定中は、スタンバイユニットとすぐに同期されます。同期は、コマンドが実行されるとすぐに、実行されます。これは透過的です。

アクティブスイッチの設定中は、バックアップとすぐに同期されます。同期は、コマンドが実行されるとすぐに、実行されます。これは透過的です。

ユニットが動作中のスタックに挿入され、スタンバイユニットとして選択されると、アクティブスイッチはスタンバイユニットが最新の設定を保持できるようにそれと同期し、その後、SYNC COMPLETE SYSLOG メッセージを生成します。これは、スタンバイユニットとアクティブユニットが同一化したときにのみ表示される一意の SYSLOG メッセージで、次のように表示されます：%DSYNCH-I-SYNCH_SUCCEEDED: Synchronization with unit 2 is finished successfully.

アクティブ/スタンバイのスイッチオーバー

スタックのアクティブスイッチで障害が発生すると、スイッチオーバーが発生します。スタンバイユニットがアクティブとなり、そのプロセスとプロトコルスタックがすべて初期化され、スタック全体の責任を担います。その結果、このユニット内のトラフィック転送が一時的に中断されますが、メンバーユニットはアクティブのままです。

（注） STP が使用され、ポートのリンクがアップしている場合、STP ポートの状態は一時的に「ブロッキング」になり、トラフィックを転送したり、MAC アドレスを学習したりすることはできません。これによって、アクティブなユニット間のスパニング ツリー ループを防いでいます。

メンバーユニットの取り扱い

スタンバイユニットがアクティブスイッチになっている間、メンバーユニットはアクティブなままで、元のアクティブスイッチからの設定に基づいてパケットの転送を継続します。これにより、ユニット内でのデータ トラフィックの中断は最小限に抑えられます。スタンバイユニットがアクティブ状態への移行を完了したら、次の操作を実行することによって、メンバーユニットを一度に 1 つずつ初期化します。

- メンバーユニットの設定をクリアしてデフォルトにリセットします（新しいアクティブユニットからの間違った設定を回避するため）。その結果、メンバーユニットでのトラフィック転送が中断されます。
- 関連するユーザー設定をメンバーユニットに適用します。
- ポートの STP 状態、動的 MAC アドレス、アクティブユニットとメンバーユニットの間のリンク稼働/ダウンステータスといった動的情報を交換します。アクティブスイッチが STP に基づいてポートの状態を「転送中」に設定すると、メンバーユニットでのパケット転送が再開されます。

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

フェールオーバー後の元のアクティブユニットの再接続

フェールオーバー後に、元のアクティブスイッチが再接続されると、アクティブ選択プロセスが実行されます。元のアクティブスイッチ（ユニット 1）がアクティブユニットとして再選択されると、現在のアクティブスイッチ（元のバックアップユニットだったユニット 2）はリブートし、再度バックアップになります。

（注） アクティブユニットのフェールオーバー中も、スタンバイユニットの稼働時間は保持されます。

スタック内でのソフトウェアの自動同期

スタック内のすべてのユニットが同じソフトウェアバージョン（ファームウェアとブートコード）を実行する必要があります。スタック内の各ユニットは、実行しているファームウェアまたはブートコードが、アクティブユニットが実行しているものと異なっていた場合、自動的にアクティブユニットからファームウェアとブートコードをダウンロードします。ユニットは自動的に自身をリブートし、新しいバージョンを実行します。

スタック ポート

デフォルトでは、デバイス上のすべてのポートは、ネットワーク（アップリンク）ポートです。ユニットを接続するには、デバイスを接続するために使用するポートのタイプをスタックポートとして変更する必要があります。これらのポートは、ユニットの間でデータおよびプロトコル パケットを転送するために使用されます。

スタック ポート リンク アグリゲーション

隣接する2台のユニットが接続されている場合は、それらを接続しているスタック ポートが自動的にスタックLAGに割り当てられます。この機能によって、単一ポートの帯域幅を超えて、スタック ポートのスタック帯域幅を増やすことができます。ユニットあたり最大2つのスタック LAG を指定できます。

スタック LAG は、2 ～最大数（ユニット タイプに応じる）のスタック ポートで構成できます。

スタック ポートの状態

スタック ポートは、次のいずれかの状態になります。

- ダウン：ポートの動作状態がダウンであるか、またはスタック ポートの動作状態がアップであるが、そのポート上でトラフィックを渡すことができません。
- アクティブ：スタック ポートは、スタック ポートの動作状態がアップで、そのポートでトラフィックを渡すことができ、それがスタックLAGのメンバーであるスタックLAGに追加されました。
- スタンバイ：スタック ポートの動作状態がアップで、そのポートで双方向トラフィックを渡すことができるが、そのポートをスタック LAG に追加することはできず、そのポートはトラックを送信しません。ポートがスタンバイ状態になる考えられる理由は、次のとおりです。
  - 単一のネイバーと接続するために、異なる速度のスタック ポートが使用された。

下位互換性

次のモードは、デバイスの現在のソフトウェアバージョンで拡張されています。以前のソフトウェアバージョンでこれらの機能を使用する場合は、注意が必要です。

- **スタックポート LAG**：ソフトウェアがLAGのスタックポートをサポートしているユニットが、ソフトウェアがLAGのスタックポートをサポートしていないユニットに接続されている場合、ユニットを接続しているスタックポートはスタック LAG のメンバーにはなりません。ユニットはスタックポートを介して接続され、アクティブなスタックユニットはソフトウェアを他のユニットにコピーします。コピーされるソフトウェアは、アクティブユニットになるユニットによって異なります。
- **キューモード**：このモードは、4つのQoSキューから8つのQoSキューに変更できます。4キューモードが現在のソフトウェアバージョンのデフォルトキューモードであるため、

8 キューをサポートしていなかった以前のソフトウェアバージョンからアップグレードしても問題はありません。しかし、キューモードを 8 キューに変更するときは、その新しいキューモードで必要な QoS 目標を満たすように設定を調べて調整する必要があります。キューモードの変更は、システムのリブート後に有効になります。新しいキューモードと競合するキュー関連の設定は拒否されます。

- **スタッキングモード**：ハイブリッド スタッキング モードを含むようにスタッキングモードが拡張されました。デバイスは既存のスタッキングモード（ネイティブ スタッキング モード）で起動するため、以前のソフトウェアバージョンからアップグレードしても問題はありません。ハイブリッドスタッキングモードで構成されたデバイスから、ハイブリッドスタッキングをサポートしないソフトウェアバージョンにソフトウェアをダウングレードする場合は、最初にデバイスをネイティブ スタッキング モードに構成します。

スタック LAG の物理的な制約

- スタック LAG には、同じ速度のポートを含める必要があります。
- トポロジがリング/チェーンでないスタックにユニットを接続しようとすると（たとえば、1 つのユニットを 3 つ以上のネイバー ユニットに接続しようとする - スター トポロジ）、2 つのスタック LAG のみがアクティブになり、残りのスタック ポートはスタンバイ モード（非アクティブ）に設定されます。

ポート速度の自動選択

ケーブルがポートに接続されると、スタック構成ケーブル タイプが自動的に検出されます（自動検出はデフォルト設定）。システムはスタック ケーブル タイプを自動的に特定し、そのケーブルとポートでサポートされている最高速度を選択します。

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

リンク集約

概要

Link Aggregation Control Protocol（LACP）は、IEEE（802.3az）規格に含まれており、複数の物理ポートをまとめて 1 つの論理チャネル（LAG)にすることを可能にします。LAG は、帯域幅を増大させ、ポートの柔軟性を高め、2 つのデバイス間にリンク冗長性を提供します。リンク集約を使用すると、2 つのネットワークデバイス間にある複数のイーサネットリンクを 1 つのリンクに結合できます。最も一般的な組み合わせは、スイッチの、別のスイッチ、サーバー、ネットワーク接続ストレージ （NAS）デバイス、またはマルチポート WiFi アクセスポイントへの接続などです。

ネットワークデバイスと管理機能は、複数のイーサネット接続のリンク集約グループ（LAG）を 1 つのリンクとして扱います。たとえば、仮想ローカルエリアネットワーク（VLAN）に LAG を含めることができます。同じスイッチに複数の LAG を設定することも、同じ LAG に

複数のイーサネットリンクを追加することもできます（LAG あたりのリンクの最大数はデバイスによって異なります）。

一部のネットワークデバイスは、リンク集約セットアッププロセスでのエラーの防止に役立つ Link Aggregation Control Protocol（LACP）をサポートしています。

リンク集約の利点

リンク集約には、次の利点があります。

- 信頼性と可用性の向上：LAG 内のいずれかの物理リンクがダウンした場合、トラフィックは別の物理リンクに再割り当てされます。
- 物理リソースの有効活用：物理リンク全体へのトラフィックのロードバランシングが可能です。
- 帯域幅の増加：集約された物理リンクにより、個別のリンクよりも高い帯域幅が提供されます。
- コスト効率の改善：特に新しいケーブル配線が必要である場合、物理ネットワークのアップグレードには大きな費用がかかる可能性があります。リンク集約により、新しい機器を必要とせずに帯域幅を高めることができます。

リンク集約のセットアップ

次の手順では、ネットワーク内の2つのデバイス間でリンク集約をセットアップする方法について簡単に説明します。

ステップ 1 両方のデバイスがリンク集約をサポートしていることを確認します。

ステップ 2 2 つのデバイスのそれぞれでリンク集約グループ（LAG）を設定します。

ステップ 3 各デバイスで作成した LAG のポート速度、デュプレックスモード、フロー制御、および MTU サイズの設定が同じであることを確認します。

ステップ 4 LAG のメンバーであるすべてのポートが同じ仮想ローカルエリアネットワーク (VLAN) メンバーシップを持つことを確認します。LAG を VLAN に追加する場合は、最初に LAG をセットアップし、その LAG を VLAN に追加します。個別のポートを追加しないでください。

警告 各デバイスでLAGをセットアップするまでは、複数のイーサネットケーブルを使用してデバイスを相互に接続しないでください。2 つのデバイス間に複数の接続を形成し、どちらのデバイスにもループ防止機能がない場合、ネットワークループが形成されます。ネットワークループにより、ネットワークでの通常のトラフィックが遅くなる、または停止する可能性があります。

ステップ 5 LAGを追加する各デバイスのポートをメモして、正しいポートに接続していることを確認します。ポートメンバーのポート速度、デュプレックスモード、または MTU サイズの設定が異なる場合や、LAG のメンバーではないポートを間違って接続した場合は、LAG によってアラートが生成され、設定が拒否されます。

ステップ 6 イーサネットまたはファイバケーブルを使用して、各デバイスで LAG に追加したポートを接続します。

ステップ 7 各スイッチで接続された各ポートのポート LED が緑色で点滅していることを確認します。

ステップ 8 各デバイスの管理インターフェイスで、リンクが稼働状態であることを確認します。

LAG のロードバランシングの設定

ステップ 1 **ユーザー名**と**パスワード**を入力してシスコのスイッチにログインします。[Log In] をクリックします。デフォルトでは、ユーザー名とパスワードは*cisco*ですが、既存のネットワークで作業しているため、独自のユーザー名とパスワードが必要です。代わりにそれらのログイン情報を入力してください。

ステップ 2 [Port Management] > [LAG Management] の順に移動し、[Load Balance Algorithm] オプションを選択します。[MAC Address] または [IP/MAC Address] のいずれかを選択できます。[Apply] をクリックします。

（注） デフォルトでは、[MAC Address] は、[Load Balance Algorithm] に対して選択されるオプションです。

ステップ 3 次に、画面に成功通知が表示されます。[File Operations] をクリックしてスイッチの設定をスタートアップコンフィギュレーションに保存します。

ステップ 4 [File Operations] ページが開きます。[Running Configuration] で [Source File Name] が選択され、[Startup Configuration] で [Destination File Name] が選択されていることを確認します。[Apply] をクリックして、設定を保存します

UDLD

概要

Unidirectional Link Detection（UDLD）は、単方向リンクを有効にするため、光ファイバまたはツイストペア イーサネット ケーブルを介して接続されたデバイスを有効にするレイヤ 2 プロトコルです。隣接するデバイスが送信したトラフィックをローカルデバイスが受信するにもかかわらず、ローカルデバイスから送信されたトラフィックをネイバーが受信しない場合には、常に単一方向リンクが発生します。

UDLD の目的は、ネイバーがローカル デバイスからのトラフィックを受信しないポート（単方向リンク）を検出して、そのようなポートをシャットダウンすることです。プロトコルが単方向リンクを正しく検出するには、接続されているすべてのデバイスで UDLD をサポートする必要があります。ローカル デバイスのみが UDLD をサポートしている場合、このデバイスがリンクのステータスを検出することはできません。この状況では、リンクのステータスは未定義に設定されます。ユーザは、未定義の状態でポートがシャットダウンされるようにするか、それとも単に通知がトリガーされるようにするかどうかを設定できます。

UDLD の機能

ポートで UDLD を有効にすると、次のアクションが実行されます。

- UDLD は、ポートで検出状態を開始します。
  - この状態で、UDLD は、すべてのアクティブなインターフェイスで、すべてのネイバーに定期的にメッセージを送信します。これらのメッセージには、既知のネイバーすべてのデバイス ID が含まれます。これらのメッセージは、ユーザ定義のメッセージ時間に従って送信されます。
- UDLD は、隣接するデバイスから UDLD メッセージを受信します。これらのメッセージは、有効期限（メッセージ時間の 3 倍）が切れるまでキャッシュされます。有効期限の前に新しいメッセージが受信されると、以前のメッセージの情報が新しいメッセージの情報に置き換えられます。
- 有効期限が切れると、デバイスは、受信した情報を使用して次の操作を実行します。
  - ネイバー メッセージにローカル デバイス ID が含まれている場合：ポートのリンク ステータスが双方向に設定されます。
  - ネイバー メッセージにローカル デバイス ID が含まれていない場合：ポートのリンク ステータスが単一方向に設定され、ポートがシャットダウンされます。
- 有効期限の時間内に、隣接するデバイスからの UDLD メッセージが受信されない場合、ポートのリンク ステータスが未定義になり、次のいずれかが発生します。
  - デバイスが通常の UDLD モードの場合：通知が発行されます。
  - デバイスがアグレッシブ UDLD モードの場合：ポートがシャットダウンします。

インターフェイスが双方向または未定義の状態になっている間、デバイスは、メッセージ時間（秒）ごとに定期的にメッセージを送信します。前述の手順が繰り返し実行されます。

使用上のガイドライン

シスコは、UDLD がサポートされていないか無効になっているデバイスに接続されているポートで UDLD を有効にすることを推奨しません。UDLD をサポートしていないデバイスに接続されたポートで UDLD パケットを送信すると、ポートで利点のないトラフィックの増大が発生します。

加えて、UDLD の設定時に次の点を考慮してください。

- 単一方向リンクを持つポートをシャットダウンする緊急度に従って、メッセージ時間を設定します。メッセージの時間が短いほど、より多くの UDLD パケットが送信および分析されますが、リンクが単一方向である場合、ポートがより早くシャットダウンされます。
- UDLD を銅線ポートで有効にする場合、ポートごと有効にする必要があります。UDLD をグローバルに有効にする場合、光ファイバ ポートのみで有効にできます。
- ポートをシャットダウンしない場合には、リンクが単一方向であることが明らかでない限り、UDLD モードを通常に設定します。
- 単一方向リンクと双方向リンク両方の損失を求める場合、UDLD モードをアグレッシブに設定します。

Smartport の概要

SmartPort 機能は、共通の設定を保存および共有するのに便利です。同じ SmartPort マクロを複数のインターフェイスに適用すると、インターフェイスは共通設定を共有します。Smartport マクロは、CLI（コマンドライン インターフェイス）コマンドのスクリプトです

マクロ名、またはマクロに関連付けられている SmartPort タイプによって、Smartport マクロをインターフェイスに適用できます。マクロ名による SmartPort マクロの適用は、CLI でのみ実行できます。

Smartport タイプごとに、Smartport マクロをインターフェイスに適用する 2 種類の方法があります。

- 静的 SmartPort：インターフェイスに SmartPort タイプを手動で割り当てます。その結果、対応する SmartPort マクロがインターフェイスに適用されます。
- Auto Smartport：Auto Smartport では、インターフェイスにデバイスが接続された時点で、コンフィギュレーションが適用されます。インターフェイスからデバイスが検出されると、接続デバイスの Smartport タイプに対応する Smartport マクロ（指定されている場合）が自動的に適用されます。

Smartportは、組み込み（またはユーザー定義）マクロを適用できるインターフェイスです。これらのマクロは、通信要件をサポートし、さまざまなタイプのネットワーク デバイスの機能を活用するようにデバイスを迅速に設定するための手段をもたらすように設計されています。ネットワーク アクセス要件および QoS 要件は、インターフェイスが IP phone、プリンタ、またはルータやアクセス ポイント（AP）に接続されているかどうかによって異なります。

VLAN Description

各 VLAN には、1 ～ 4094 の範囲の値を持つ VLAN ID（VID）が設定されています。VLAN のメンバーは、VLANにデータを送受信できるブリッジ型ネットワーク内のデバイスのポートです。VLAN に送信されるそのポート宛のすべてのパケットが VLAN タグを付けられていない場合、ポートは VLAN のタグなしメンバーとなります。VLAN に送信されるそのポート宛のすべてのパケットが VLAN タグを付けられている場合、ポートは VLAN のタグ付きメンバーとなります。ポートは 1 つのタグなし VLAN にのみ属することができますが、複数のタグ付き VLAN に属することができます。

VLAN アクセスモードでは、1 つのポートは、1 つの VLAN にしか属せません。ポートが全般またはトランクモードの場合、1 つまたは複数の VLAN のメンバーになれます。VLAN は、セキュリティとスケーラビリティの問題を解決するために使用されます。VLAN トラフィックはVLAN内に留まり、VLANデバイスで終了します。また、物理的な再配置を必要とせずにデバイスを概念的にリンクすることにより、ネットワーク構成を簡素化します。

VLAN タグ付きフレームの場合、4 バイトの VLAN タグが各イーサネットフレームに適用されます。タグは、1 ～ 4094 の範囲の VLAN ID と、0 ～ 7 の範囲の VLAN 優先度タグ（VPT）で構成されます。フレームが VLAN 対応デバイスに入るときに、フレーム内の 4 バイトの VLAN

タグが、VLAN に属しているものとして、分類に使用されます。フレームに VLAN タグがない、またはパケットに優先順位タグしかない場合、フレームは、フレームを受信した入力ポートで定義されている PVID（ポート VLAN ID）に基づいて VLAN に分類されます。入力のフィルタリングが有効になっていて、入力ポートがパケットの属する VLAN のメンバーではない場合、フレームは入力ポートでドロップされます。VLAN タグの VID が 0 の場合のみ、フレームは優先タグ付きと見なされます。VLAN に属するフレームは VLAN に留まります。

これは、対象 VLAN の出力ポートのメンバーにのみフレームが送信または転送されることで実現されます。VLAN の出力ポートは、タグ付きまたはタグなしのいずれかにすることができます。

出力ポートの役割は次のとおりです。

- 出力ポートが対象 VLAN のタグ付きメンバーであり、元のフレームに VLAN タグがない場合、出力ポートはフレームに VLAN タグを追加します。
- 出力ポートが対象 VLAN のタグなしメンバーであり、元のフレームに VLAN タグが付いている場合、VLAN タグはフレームから削除されます。

VLAN の役割

レイヤ 2 は、VLAN が機能する場所です。すべての VLAN トラフィック（ユニキャスト、ブロードキャスト、およびマルチキャスト）は、VLAN 内に含まれます。イーサネット MAC レイヤでは、個別の VLAN に接続されているデバイスは直接接続できません。レイヤ 3 ルータだけが、異なる VLAN からのデバイスを相互に対話できるようにします。各 VLAN が IP サブネットを表す場合、それらの間で IP トラフィックをルーティングするために IP ルータが必要です。

IP ルータは、各ポートに接続されている VLAN が 1 つだけの標準ルータである可能性があります。標準 IP ルータとの間の VLAN タグなしトラフィックが必要です。各 IP ルータのインターフェイスは 1 つまたは複数の VLAN に接続でき、VLAN 認識型 IP ルータとすることができます。VLAN 認識型 IP ルータで送受信されるトラフィックは、VLAN タグ付きまたはタグなしのいずれも可能です。

隣接する VLAN 認識型デバイスは Generic VLAN Registration Protocol（GVRP）を使用して VLAN 情報を通信します。したがって、VLAN 情報は、ブリッジ化ネットワークを介して伝達されます。デバイスで交換される GVRP 情報に基づいて、VLAN 上のデバイスは静的にも動的にも作成できます。VLAN は静的にも動的にもできますが（GVRP に基づき）、同時に両方にはできません。GVRP の詳細については、「GVRP 設定」の項を参照してください。

QinQ

QinQ は、サービス プロバイダー ネットワークと顧客ネットワーク間の分離を提供します。デバイスは、ポートベースの c タグ付きサービスインターフェイスをサポートするプロバイダーブリッジとなります。

QinQ では、デバイスは、プロバイダーネットワークに転送するパケットに、サービスタグ（S タグ）と呼ばれる ID タグを追加します。S タグはさまざまな顧客間のトラフィックを分離するために使用されますが、顧客の VLAN タグも維持されます。

顧客のトラフィックは、それがcタグ付きまたはcタグなしのいずれであっても、TPID 0x8100のSタグ付きでカプセル化されます。Sタグにより、このトラフィックはプロバイダーブリッジネットワーク内で集合体として扱われます。この場合、ブリッジ処理はSタグVID（S-VID）のみに基づいて行われます。

Sタグは、トラフィックがネットワーク サービス プロバイダーのインフラストラクチャを介して転送されている間は保持され、後に出力デバイスにより削除されます。

QinQの他の利点として、お客様のエッジ デバイスでの設定は不要です。

プライベート VLAN

プライベートVLAN機能は、ポート間でのレイヤ2の分離を提供します。つまり、IPルーティングとは異なり、ブリッジング トラフィックのレベルで、同じブロードキャスト ドメインを共有するポートが相互に通信することはできません。プライベート VLAN 内のポートはレイヤ2ネットワークの任意の場所に配置できます。よって、これらのポートは同じスイッチ上にある必要はありません。プライベートVLANは、タグなしまたは優先順位タグ付きトラフィックを受信し、タグなしトラフィックを送信するように設計されています。

次の種類のポートはプライベート VLAN のメンバーにできます。

- プロミスキャス：無差別ポートは、同じプライベート VLAN のすべてのポートと通信できます。これらのポートは、サーバとルータに接続します。
- コミュニティ（ホスト）：コミュニティ ポートは、同じレイヤ2ドメインのメンバーであるポートのグループを定義できます。これらはレイヤ 2 で他のコミュニティおよび隔離ポートから分離されます。これらのポートは、ホスト ポートに接続します。
- 隔離（ホスト）：隔離ポートは、同じプライベート VLAN 内の他の隔離ポートおよびコミュニティ ポートからレイヤ 2 で完全に分離されます。これらのポートは、ホスト ポートに接続します。

プライベート VLAN には次の種類があります。

- プライマリ VLAN：プライマリ VLAN は、無差別ポートから隔離ポートおよびコミュニティ ポートにレイヤ 2 で接続する場合に使用します。プライベート VLAN ごとに、プライマリ VLAN が 1 つだけ使用できます。
- 隔離 VLAN（セカンダリ VLAN とも呼ばれる）：隔離 VLAN は、隔離ポートがプライマリ VLAN にトラフィックを送信する場合に使用します。プライベート VLAN ごとに、隔離 VLAN が 1 つだけ使用できます。
- コミュニティ VLAN（セカンダリ VLAN とも呼ばれる）：VLAN 内のポート（コミュニティ）のサブグループを作成するには、ポートをコミュニティ VLAN に追加する必要があります。コミュニティ VLAN は、コミュニティ ポートから、無差別ポートおよび同じコミュニティのコミュニティ ポートにレイヤ 2 で接続する場合に使用します。コミュニティごとに 1 つのコミュニティ VLAN が使用でき、複数のコミュニティ VLAN が同じプライベート VLAN のシステム内で共存できます。

ホスト トラフィックは隔離 VLAN とコミュニティ VLAN 上で送信されますが、サーバとルータのトラフィックは、プライマリ VLAN 上で送信されます。

共有 MAC アドレス ラーニングは、同じプライベート VLAN のメンバーであるすべての VLAN 間に存在します（ただしスイッチは独立した VLAN ラーニングをサポートします）。これによりユニキャスト トラフィックが有効になり、ホスト MAC アドレスが隔離 VLAN およびコミュニティ VLAN により学習されるのに対し、ルータとサーバの MAC アドレスはプライマリ VLAN により学習されます。

プライベート VLAN のポートは、1 つのプライベート VLAN にのみ追加できます。アクセスまたはトランク ポートなどの他の種類のポートは、プライベート VLAN を構成する個々 の VLAN に追加できます（これらは通常の 802.1Q VLAN であるため）。

プライベート VLAN は、異なるスイッチのポート間でトランク ポートを設定し、これらをプライベート VLAN 内のすべての VLAN に追加することで、複数のスイッチ経由で拡張するように設定できます。スイッチ間のトランク ポートは、プライベート VLAN のさまざまな VLAN（プライマリ、隔離、およびコミュニティ）のタグ付きトラフィックを送受信します。

スイッチでの VLAN の設定

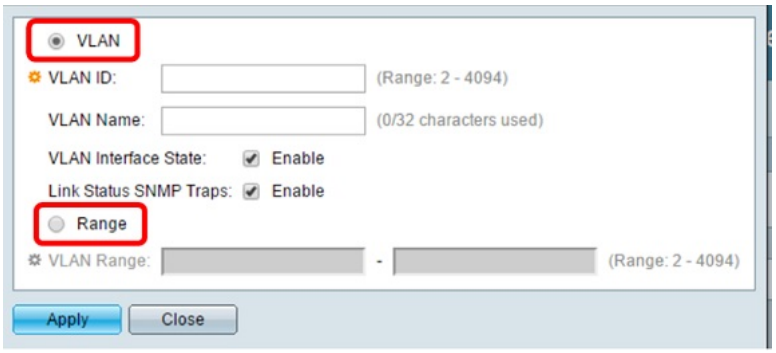
仮想ローカルエリアネットワーク（VLAN）を作成することで、スイッチ上で個別のブロードキャストドメインを設定できます。ブロードキャストドメインは、ルータなどのレイヤ 3 デバイスを使用して、互いに関連付けることができます。VLAN は、ホストの物理的な配置場所に関係なく、ホスト間でグループを形成するために主に使用されます。したがって、VLAN はホスト間にグループを形成することでセキュリティを向上させます。VLAN を作成しても、その VLAN が少なくとも 1 つのポートに手動で、または動的に接続されるまでは何の効果もありません。VLAN を設定する最も一般的な理由の 1 つは、音声用の VLAN と、データ用の VLAN を個別に設定するためです。そうすることで、同じネットワークを使用していても、両方のタイプのデータのパケットが送信されます。

VLAN の作成

ステップ 1 Web ベースのユーティリティにログインし、[VLAN Management] > [VLAN Settings] の順に選択します。

ステップ 2 [VLAN Table] エリアで、[Add] をクリックして新しい VLAN を作成します。

ステップ 3 次の図に示されているオプションのように、VLAN は 2 つの異なる方法で追加できます。目的の方法に対応するオプションボタンを選択します。



- [VLAN]：特定の VLAN を作成するには、この方法を使用します。
- [Range]：一定範囲の VLAN を作成するには、この方法を使用します。

ステップ 4 手順 3 で [VLAN] を選択した場合は、[VLAN ID] フィールドに VLAN ID を入力します。有効な範囲は 2 ～ 4094 です。

ステップ 5 [Vlan Name] フィールドに VLAN の名前を入力します。この例では、VLAN 名は「Accounting」です。最大で 32 文字を使用できます。

ステップ 6 VLAN インターフェイス状態を有効にするには、[VLAN Interface State] チェックボックスをオンにします（デフォルトでオンになっています）。有効にしないと、VLANは事実上シャットダウンされ、そのVLANを介した送受信は不可能になります。

ステップ 7 SNMP トラップの生成を有効にする場合は、[Link Status SNMP Traps] チェックボックスをオンにします。この設定はデフォルトでイネーブルになっています。

ステップ 8 手順 3 で [Range] を選択した場合は、[VLAN Range] フィールドに VLAN の範囲を入力します。有効な範囲は 2 ～ 4094 です。この例では、VLAN の範囲は 3 ～ 52 です。

（注） 一度に最大100個のVLANを作成できます。

ステップ 9 [Apply] をクリックします。

GVRP の設定

GVRP は COS スイッチでのみサポートされます。GVRP は、802.1Q トランクポートでのみ動作し、主に、トランキングスイッチ間を通過する必要がない VLAN からのトラフィックをプルーニングするために使用されます。GVRPを設定するには、次の手順を実行します。ポートが全般モードのままである状態を確保するために、GVRPに参加している各インターフェイスで、Smartport マクロ自動実行を無効にすることを強くお勧めします。

ステップ 1 目的の VLAN でスイッチを設定します。たとえば、次のように設定することができます。

- スイッチ 1 に、VLAN ID 1 をデフォルトとして割り当て、次に 300、400、および 500 を割り当てることができます。
- スイッチ 2 に、VLAN ID 1 をデフォルトとして割り当てることができます。
- スイッチ 3 に、VLAN ID 1 をデフォルトとして割り当て、次に 100 および 200 を割り当てることができます。

ステップ 2 インターフェイスで GVRP を有効にするには、全般モードで設定する必要があります。全般モードで設定しないと、スイッチは GARP メッセージを送信しません。

ステップ 3 GVRP をグローバルにイネーブルにします。デフォルトでは、スイッチに対して GVRP が有効になっていません。GVRP 動作用に 802.1Q ポートを設定する前に、まず、スイッチで GVRP を有効にする必要があります。

ステップ 4 802.1Q 動作用にポートを設定します。GVRP は、802.1Q トランキング用に設定されたポートでのみ動作します。

ステップ 5 ポートの GVRP を設定します。GVRP は、トランクの両側で正しく動作するように設定する必要があります。

ステップ 6 （任意）ポートの登録モードを設定します。デフォルトでは、GVRP ポートは **normal** 登録モードです。これらのポートは、近接スイッチからの GVRP Join メッセージを使用して、802.1Q トランクリンクで動作する VLAN をプルーニングします。相手側のデバイスが GVRP メッセージを送信できない場合やスイッチに VLAN をプルーニングさせたくない場合は、**fixed** モードを使用します。fixed モードのポートは、スイッチデータベースに存在するすべての VLAN に転送します。**forbidden** モードのポートは、VLAN 1 にのみ転送します。

音声 VLAN の設定

このトラブルシューティングのヒントは、音声 VLAN の設定に関するものです。

ステップ 1 スイッチ上で VLAN を作成します。たとえば、データ VLAN が 2 に設定され、音声 VLAN が 5 に設定されている場合は、[Auto Voice VLAN] タブで VLAN 5 を割り当てます。

ステップ 2 動作中の音声 VLAN が 5 に設定されていることを確認します。

ステップ 3 表示モードを**基本モード**から**拡張モード**に変更します。

ステップ 4 次に、[VLAN Management] の [Interface Settings] で、ポートモードを [Access] から [Trunk] に変更します。

ステップ 5 次に、[Port to VLAN Membership] で、IP フォンに接続されているポートについて、データ VLAN をタグなしとして設定し、音声 VLAN をタグ付きとして設定します。IP フォンに接続されているデスクトップおよびラップトップについても同じ手順を実行してください。

ステップ 6 [IP configuration] > [IPv4 Interface] の順に移動し、VLAN 2 と VLAN 5 の両方に IP を割り当てます。

ステップ 7 デバイスで DHCP サーバーが有効になっている場合に備えて、両方の VLAN 用に DHCP プールを作成します。（任意）

ステップ 8 [Smart port] タブに移動し、スマートポートが有効になっていることを確認します。

ステップ 9 [Device Detection] で、[IP Phone+Desktop] チェックボックスがオンになっていることを確認します。

ステップ 10 [Smartport Type] 設定に移動し、[IP Phone+Desktop] に関して [Macro] を選択します。

ステップ 11 [Edit] をクリックします。[Macro Type] で [Built-in Macro] が選択されていることを確認してください。

ステップ 12 [Macro Parameters] を変更します。

- [Parameter2] の値をデータ VLAN ID の値（今回はデータ VLAN が 2 であるため 2）に変更します。
- [Auto voice VLAN settings] で動作中の音声 VLAN が 5 と表示される場合は、[Parameter3] の値が自動的に 5 になります。

ステップ 13 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

音声 VLAN の削除

（注） 音声 VLAN を削除できず、「**VLAN xxx cannot be deleted because it is used as the agreed Voice VLAN**」というエラーメッセージが表示される場合は、**音声 VLAN** の動作が原因です。シスコのスイッチのファームウェア **2.5.5.x** 以前の場合、デフォルトでは [triggered auto voice VLAN] オプションが [enable] 設定されています。スイッチが他のスイッチから VSDP パケットを受信するか UC ルータから CDP パケットを受信すると、音声 VLAN が自動的に有効になります。

何らかの理由で**音声 VLAN** を削除する場合は、正常に削除するための一連の手順に従う必要があります。GUI を使用して、次の手順を実行してください。

ステップ 1 [VLAN Management] > [Voice VLAN] > [Properties] の順に選択し、[Dynamic Voice VLAN] を [Disable] に設定します。

ステップ 2 [VLAN Management] > [Voice VLAN] > [Properties] の画面で、[Voice VLAN Id] を [1] に設定します（これにより、セットアップで使用された音声 ID が削除され、値がデフォルトの 1 に設定されます）。

ステップ 3 [VLAN Management] > [VLAN Settings] に戻り、**音声 VLAN** として使用されていた VLAN を削除します。

（注） ただし、[Dynamic Voice VLAN] を再度有効にすると、削除した VLAN が自動的に再作成され、**音声 VLAN** として設定されます。

リンクフラッピングのトラブルシューティング

このトラブルシューティングのヒントは、Cisco Business スイッチのリンクフラッピングの問題を解決するために役立ちます。

（注） スタック構成のスイッチ間、または別のスイッチとのアップリンクを持つスイッチ間でリンクフラッピングが発生した場合は、次の手順に従って問題を解決してください。

ステップ 1 両方のスイッチが最新バージョンのファームウェアにアップグレードされていることと、両方のスイッチが同じファームウェアを実行していることを確認します。

ステップ 2 [Administration] > [Discovery-Bonjour] > [Disable] をクリックして、Bonjour プロトコルの検出を無効にします。

ステップ 3 [Port Management] > [Green ethernet] > [Properties] > [802.3 Energy Efficient Ethernet (EEE)] > [Disable] をクリックして、両方のスイッチで **EEE**（Energy Efficient Ethernet）を無効にします。

ステップ 4 [Port Management] > [Error Recovery] をクリックして、両方のスイッチで [Link Flap Prevention] を有効にします。[Link Flap Prevention] の [Enable] チェックボックスをオンにして有効にしてください。

ステップ 5 手順 1 ～ 4 を実行しても問題が解決しない場合は、**LLDP** を無効にします。[Administration] > [Discovery-LLDP Properties] > [LLDP Status] > [Disable] の順にクリックします。

手順 1 ～ 5 を実行してもリンクフラッピングを解決できない場合は、アップリンク/スタック構成に使用されているポートですべてのポートを削除します。

重要：スタック構成の場合は、スタック構成からポートを削除し、再設定する必要があります。

リンクフラップの識別

リンクフラップとは、スイッチ上の物理インターフェイスが継続的に稼働とダウンを繰り返す（1 秒間に 3 回以上、少なくとも 10 秒間）状態です。一般的な原因は通常、不良、サポート対象外、または非標準のケーブルや Small Form-Factor Pluggable（SFP）に関連しているか、その他のリンク同期に関する問題に関連しています。リンクフラップの原因は、断続的ものである場合と永続的なものである場合があります。

リンクフラップは物理的な干渉になりやすいため、ここでは、これを診断および防止するために実行できる手順について説明します。

ステップ 1 ケーブルとモニターの変更を試みます。問題が解決しない場合は、手順 2 に進みます。

ステップ 2 [Status and Statistics] > [Diagnostics] > [Copper Test] の順に移動します。

ステップ 3 ドロップダウンメニューからポートを選択し、[Copper Test] をクリックします。

ステップ 4 警告が表示されます。ポートが短時間シャットダウンされることに注意してください。[OK] を選択します。

ステップ 5 テスト結果が表示されます。「OK」と表示されるときは、多くの場合、ケーブルが原因ではありません。「OK」以外が表示される場合は、ケーブルを変更し、銅線テストを繰り返して、ケーブルが原因ではないことを確認します。

トポロジの分析

スイッチでの設定の問題ではなく物理的な問題であることを確認するには、スイッチに接続されているデバイスを分析する必要があります。次の点をチェックします。

1. スイッチに接続されているデバイスは何ですか。
   - スイッチに接続されている各デバイスを分析します。これらのデバイスで問題が発生したことはありますか。
2. どのポートが問題の原因で、どのデバイスがそれらのポートに接続されていますか。
   - 別のデバイスを接続してポートをテストし、問題が続くかどうかを確認します。
   - デバイスの別のポートが問題の原因になっているかどうかを確認します。
3. それはポートですか、それともデバイスですか。

- それがポートなのかデバイスなのかを判断することで、トラブルシューティング プロセスを続行する方法が決まります。
- それがデバイスである場合は、そのデバイスのサポート管理に連絡する必要がある場合があります。
- それがポートであると判断した場合は、問題が設定または物理的な問題に関連しているかどうかを確認します。

リンクフラップ防止の設定

リンクフラップ防止機能により、リンクフラップの発生によるスイッチおよびネットワーク動作の中断を最小限に抑えることができます。過剰なリンクフラップイベントが発生しているポートを *err-disable* に自動的に設定することにより、ネットワークトポロジが安定します。このメカニズムにより、フラッピングの根本原因をデバッグして特定するための時間も提供されます。リンクフラップおよびポートシャットダウンに関するアラートとして、Syslog メッセージまたは Simple Network Management Protocol（SNMP）トラップが送信されます。ユーザーまたはシステム管理者が明示的に有効にした場合にのみ、インターフェイスが再びアクティブになります。

ステップ 1 スイッチの Web ユーザーインターフェイス（UI）にログインします。

ステップ 2 **拡張モード**に変更します。

ステップ 3 [Port Management] > [Port Settings] の順に移動します。

ステップ 4 [Link Flap Prevention] の [Enable] チェックボックスをオンにします。[Apply] を押します。

ステップ 5 [Save] をクリックして設定を保存します。

スパニングツリー プロトコル

スパニングツリープロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークの正常な動作を実現するには、どの 2 つのステーション間でもアクティブ パスを 1 つにする必要があります。エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。

STP は、スパニングツリーアルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを 1 つ選択します。スパニングツリーアルゴリズムは、アクティブトポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチドレイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートが指定ポートの役割またはバックアップポートの役割にであるようなスイッチはルートスイッチです。少なくとも 1 つのポートに役割が指定されているスイッチは、指定スイッチを意味します。

STP は、ネットワーク上のエンドステーション間に一意のパスを作成し、それによってループをなくすことで、スイッチと相互接続リンクの配置においてツリー トポロジを提供します。

デバイスは、次のスパニング ツリー プロトコルのバージョンをサポートしています。

- 従来の STP：任意の 2 台のエンドステーション間に 1 本のパスが生成されるため、ループが解消されます。
- 高速 STP（RSTP）：ネットワークトポロジを検出し、スパニングツリーのより高速なコンバージェンスを提供します。これは、ネットワーク トポロジが自然にツリー構造化され、そのため、より高速なコンバージェンスが可能な場合に、最も効果的です。RSTP はデフォルトで有効になっています。
- 多重 STP（MSTP）：MSTP は RSTP に基づきます。レイヤ 2 ループを検出し、それに関与するポートがトラフィックを伝送するのを防ぐことで、軽減を試みます。ループはレイヤ 2 ドメイン単位で存在するため、STP ループをなくすためにポートがブロックされると、その状況が発生することがあります。トラフィックはブロックされていないポートに転送され、ブロックされているポートにはトラフィックは転送されません。これは、ブロックされたポートが常に未使用となるため、帯域幅の効率的な使用方法ではありません。MSTP は、各 STP インスタンスで個別にループを検出し、軽減できるように、いくつかの STP インスタンスを有効化することで、この問題を解決します。これにより、1 個のポートを 1 つまたは複数の STP インスタンスに対してブロックし、その他の STP インスタンスに対してはブロックしないように指定できます。異なる VLAN が異なる STP インスタンスに関連付けられている場合、それらのトラフィックは関連付けられた MST インスタンスの STP ポートの状態に基づいてリレーされます。結果として、帯域幅利用が改善されます。
- PVST+/RPVST+：（高速）Per VLAN Spanning Tree
  - PVST+ は、802.1Q STP 標準プロトコルの個別インスタンスを VLAN ごとに実行するプロトコルです。
  - Rapid PVST+ は、802.1Q RSTP 標準プロトコルの個別インスタンスを VLAN ごとに実行するプロトコルです。

    PVST/RPVST+ 動作の一環として、ポート上で定義された各 VLAN のために、個別の PVST フレームが送信されます。これにより、VLAN ごとの状態およびトポロジの維持が可能になります。

- SSTP：シスコのスイッチは、特別な共有スパニングツリープロトコル（SSTP）BPDU を使用して、PVST+ および高速 PVST+ スパニングツリートポロジ情報を交換します。これらは、SSTP BPDU をシスコの共有スパニングツリー MAC アドレスである 01-00-0C-CC-CC-CD に送信します。これらの BPDU の形式は、IEEE 標準 802.1Q の独自の拡張に基づいています。ネイティブ VLAN では、これらの BPDU はタグなしです。ポートは、複数の VLAN によってトランクモードで設定されている場合、それらの VLAN に関してタグ付けされたポートで SSTP BPDU を送信します。

スパニングツリープロトコル間の相互運用

IEEE 標準 MSTP（RSTP および STP を含む）と PVST+（および高速 PVST+）の相互運用には、2 つの主な側面があります。1 つ目は、MSTP および PVST+ を実行するスイッチとリージョンの間で共通のスパニングツリーの形成に関するものです。2 つ目は、MSTP リージョン間での PVST+ スパニングツリーのトンネリングに関するものです。

PVST+ で設定されたシスコのスイッチは、ポートで IEEE 標準 RSTP BPDU を受信すると、それらを認識し、SSTP 形式の BPDU と IEEE 標準 STP BPDU という 2 つのバージョンの BPDU をそのポートで送信します。同様に、高速 PVST+ で設定されたスイッチは、IEEE 標準 RSTP BPDU を認識し、RSTP BPDU を受信するポートで、SSTP 形式の BPDU と IEEE 標準 RSTP 形式の BPDU という 2 つのバージョンの BPDU を送信します。

MSTP と PVST+ がスパニングツリー インスタンスを VLAN にマッピングする方法には違いがあります。PVST+ はすべての VLAN に対してスパニングツリー インスタンスを作成しますが、MSTP は 1 つ以上の VLAN を各 MST インスタンスにマッピングします。PVST+ リージョンが MSTP リージョンと境界では、通常、一連の PVST+ インスタンスと一連の MST インスタンスが一致しません。そのため、PVST+ リージョンと MSTP リージョンは、単一の共通スパニングツリー インスタンス上で相互に通信する必要があります。

共通スパニングツリーを介した MSTP リージョンと PVST+ リージョンの間の相互運用は、次のように実現されます。

MST と PVST+ はどちらもループフリーのレイヤ 2 トポロジを提供しますが、それぞれが使用するアプローチは異なっています。

- MST は複数の VLAN を 1 つのインスタンスにマッピングします。このため、スパニングツリー インスタンスの数が削減されます。
- PVST+ は、スパニングツリー インスタンスごとにインスタンスを計算します。

PVST+ はインスタンス/VLAN ごとに BPDU を送信するため、VLAN 用に設定されたインスタンスによって MST に各 BPDU を個別に処理させることができます。

MST リージョンが PVST+ トポロジに接続されると、MST は PVST シミュレーションメカニズムを使用して PVST+ をシミュレートします。MST リージョンは、PVST+ スイッチに接続されているインターフェイスで PVST+ BPDU を送信（VLAN ごとに 1 つ）します。これらの BPDU はすべて、同じ情報を伝送し、同じルートブリッジをアドバタイズします。PVST+ トポロジに接続するインターフェイスは、「境界インターフェイス/ポート」と呼ばれます。PVST+ スイッチは、同じ情報を伝送する MST から各 VLAN の BPDU を受信するようになったため、ルートブリッジ、ルートポートなどを選択するときに、すべて同じ決定を行います。

MST リージョンがネットワークのルートブリッジになるようにネットワークを設定することが最も簡単です。PVST+ ドメインにルートブリッジがある場合、MST は、すべての VLAN に同じルートポートを使用します。MST リージョンにルートブリッジがある場合、異なるルートポートを使用してある程度のロードバランシングを実現するには、PVST+ スイッチで VLAN ごとのコストを変更します。

RSPAN の設定

SPAN（スイッチポートアナライザ）はポートミラーリングまたはポートモニタリングとも呼ばれ、ネットワークアナライザによる分析のためにネットワークトラフィックを選択します。シスコ スイッチ プローブ デバイスまたはその他のリモートモニタリング（RMON）プローブは、ネットワークアナライザとして使用できます。

ポートミラーリングは、1 つのデバイスポート、複数のデバイスポート、または仮想ローカルエリアネットワーク（VLAN）全体で検出されるネットワークパケットのコピーを、デバイスの別のポートのネットワークモニタリング接続に送信するネットワークデバイス機能です。この機能は、通常、侵入検知システムなど、ネットワークトラフィックのモニタリングを必要とするネットワークアプライアンスのために使用されます。データパケットは、モニタリングポートに接続しているネットワークアナライザにより、診断、デバッグ、およびパフォーマンスモニタリング用に処理されます。

リモート スイッチ ポート アナライザ（RSPAN）は、SPAN 拡張機能です。RSPAN は、ネットワーク全体にわたり複数スイッチのモニタリングを可能にし、アナライザポートをリモートスイッチ上に定義できるようにすることで、SPAN を拡張します。これは、ネットワーク キャプチャ デバイスを一元化できることを意味します。

RSPAN は、RSPAN セッションの送信元ポートからのトラフィックを RSPAN セッション専用の VLAN にミラーリングすることによって機能します。その後、この VLAN は他のスイッチにトランキングされ、RSPAN セッショントラフィックが複数のスイッチを通過できるようになります。RSPAN セッション VLAN からのトラフィックは、セッションの宛先ポートを含むスイッチの宛先ポートに単純にミラーリングされます。

各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。開始デバイスの送信元インターフェイスからのトラフィックは、リフレクタポートを介して RSPAN VLAN にコピーされます。これは設定が必要な物理ポートです。これは、RSPAN セッションを構築するためにのみ使用されます。リフレクタポートを指定する場合は「network」キーワードが必要であり、リンク上で非 RSPAN トラフィックが許可されます。

リフレクタ ポートには、次の特性があります。

- EtherChannel グループが SPAN の送信元として指定されている場合でも、EtherChannel グループに割り当てられる物理ポートにすることができます。ポートは、リフレクタ ポートとして設定されている間は、グループから削除されます。
- リフレクタ ポートとして使用されるポートは、SPAN の送信元または宛先にすることができず、一度に複数のセッションのリフレクタ ポートにすることもできません。

- すべての VLAN から認識されません。
- リフレクタ ポートではスパニングツリーが自動的にディセーブルになります。
- リフレクタポートは、すべてのモニタ対象送信元ポートで送受信されたトラフィックのコピーを受信します。

RSPAN トラフィックフロー

- 各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN を介してルーティングされます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。
- 開始デバイスの送信元インターフェイスからのトラフィックは、リフレクタポートを介して RSPAN VLAN にコピーされます。これは構成する必要がある物理ポートであり、リンクを介した他のトラフィックを許可する「network」キーワードが必要です。
- このリフレクタポートは、パケットを RSPAN VLAN にコピーするメカニズムとして機能します。
- 次に、RSPAN トラフィックは、中間デバイスのトランクポートを介して、最終的なスイッチの宛先セッションにルーティングされます。
- RSPAN VLAN は宛先スイッチによってモニタリングされ、宛先ポートにコピーされます。

RSPAN ポートメンバーシップルール

- すべてのスイッチ：RSPAN VLAN のメンバーシップはタグ付けのみが可能です。
- 開始スイッチ
  - SPAN 送信元インターフェイスは、RSPAN VLAN のメンバーになることは許可されていません。
  - リフレクタポートをこの VLAN のメンバーにすることはできません。
- 中間スイッチ
  - ミラーリングされたトラフィックの受け渡しに使用されていないすべてのポートから RSPAN メンバーシップを削除することをお勧めします。
  - 通常、RSPAN VLAN には 2 つのポートがあります。
- 最終スイッチ
  - ミラーリングされたトラフィックでは、送信元ポートが RSPAN VLAN のメンバーである必要があります。
  - RSPAN メンバーシップは、宛先インターフェイスを含む他のすべてのポートから削除する必要があります。

マルチキャスト

マルチキャストは、別々の場所にいる複数の受信者にメッセージを送信するための効率的な通信メカニズムを提供します。また、多対多および多対 1 の通信をサポートすることもできます。

マルチキャスト アプリケーションは、IP 上で User Datagram Protocol（UDP）を使用します。メッセージは送信元（「送信者」と呼ばれます）によって送信され、その情報の受信に関心のある別のデバイスがネットワーク上に存在しない場合でも送信されます（「ストリーム」と呼ばれます）。一方、受信者は、それらのメッセージを転送するようにネットワークに通知するために、特定のマルチキャストストリームに登録する必要があります。

IP マルチキャストは、ネットワーク リソース（特に、音声やビデオなどの帯域幅集約型サービス）を効率的に使用する方法です。IP マルチキャスト ルーティングにより、ホスト（ソース）は、IP マルチキャスト グループ アドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。送信側ホストは、マルチキャスト グループ アドレスをパケットの IP 宛先アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、マルチキャスト グループのメンバーに接続されたすべてのインターフェイスから着信した IP マルチキャスト パケットを転送します。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。

IP マルチキャスト ルーティングのデフォルト設定

次の表に、IP マルチキャスト ルーティングのデフォルト設定を示します。

表 *1 : IP* マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 kb/s

IGMP の概要

Internet Group Management Protocol（IGMP）は、マルチキャスト用に設計されたプロトコルです。IGMP を使用すると、ネットワーク内の異なるユーザー間でグループメンバーシップを確立できます。IGMP は、主に、ネットワーク内の異なるユーザー間でのマルチメディア ストリーミング（ビデオチャットなど）に使用されます。「スヌーピング」とは、通信において第三者が現在の接続データトラフィックをリッスンまたは観測する場合に使用される用語です。そのため、「IGMP スヌーピング」は、特にマルチキャストトラフィックをリッスンするプロ

セスを指します。IGMP スヌーピングを有効にすると、スイッチの特定ポートで登録済みのマルチキャストクライアントだけにマルチキャストトラフィックを転送できます。これにより、マルチキャストフレームは、VLAN内のすべてのユーザーではなく、VLAN内の特定のマルチキャストクライアントだけに転送されます。

マルチキャストは、1 つのホストからネットワーク内の選択されたホストにデータパケットを送信するために使用されるネットワークレイヤ技法です。下位レイヤでは、1 つのホストだけが受信する必要がある場合でも、スイッチはすべてのポートでマルチキャストトラフィックをブロードキャストします。Internet Group Management Protocol（IGMP）スヌーピングは、Internet Protocol バージョン 4（IPv4）マルチキャストトラフィックを目的のホストに転送するために使用されます。一方、マルチキャストリスナー検出（MLD）スヌーピングは、Internet Protocol バージョン 6（IPv6）マルチキャストトラフィックを目的のホストに転送するために使用されます。

IGMP が有効になっていると、IPv4 ルータとそのインターフェイスに接続されたマルチキャストホストの間で交換される IGMP メッセージが検出されます。その後、IPv4 マルチキャストトラフィックを制限するテーブルが維持され、それらのトラフィックが、受信する必要があるポートに動的に転送されます。

次の設定は、IGMP を設定するための前提条件です。

1. 仮想ローカルエリアネットワーク（VLAN）を設定します。
2. ブリッジ マルチキャスト フィルタリングを有効にします。

MLD が有効になっていると、IPv6 ルータとそのインターフェイスに接続されたマルチキャストホストの間で交換される MLD メッセージが検出されます。その後、IPv6 マルチキャストトラフィックを制限するテーブルが維持され、それらのトラフィックが、受信する必要があるポートに動的に転送されます。

IGMP_MLD プロキシ

IGMP/MLD プロキシは、簡潔な IP マルチキャスト プロトコルです。IGMP/MLD プロキシを使用して、エッジボックスなどのデバイス上のマルチキャストトラフィックを複製することにより、これらのデバイスの設計とインストールがかなり簡単になります。プロトコル独立マルチキャスト（PIM）またはディスタンス ベクター マルチキャスト ルーティング プロトコル（DVMRP）などのより高度なマルチキャストルーティングプロトコルをサポートしていないため、デバイスのコストだけではなく、動作のオーバーヘッドも削減されます。

別の利点は、コアネットワークルータのマルチキャスト ルーティング プロトコルからプロキシデバイスを独立させることができる点です。その結果、プロキシデバイスは、任意のマルチキャストネットワークで簡単にセットアップできます。

IGMP/MLD プロキシ ツリー

IGMP/MLD プロキシは、堅牢なマルチキャスト ルーティング プロトコル（PIM など）を必要としない簡潔なツリートポロジで動作します。学習グループメンバーシップとプロキシ グループ メンバーシップ情報に基づく簡潔な IPM ルーティングプロトコルを使用し、それらの情報に基づいてマルチキャストパケットを転送するには、これで十分です。各プロキシデバイス

は、アップストリーム インターフェイスとダウンストリーム インターフェイスを識別して手動で設定する必要があります。

さらに、プロキシツリートポロジのIPアドレッシング方式は、プロキシデバイスがIGMP/MLDクエリア選出で確実に選出されてマルチキャストトラフィックを転送できるように設定する必要があります。プロキシデバイスを除く他のマルチキャストルータがツリー内に存在しないようにし、より広いマルチキャスト構造にツリーのルートが接続されるようにする必要があります。

IGMP/MLD 転送を使用するプロキシデバイスは、単一のアップ ストリーム インターフェイスと 1 つ以上のダウン ストリーム インターフェイスを備えています。これらの指定は明示的に行われます。各インターフェイスのタイプを決定するプロトコルは存在しません。ダウンストリーム インターフェイスで、プロキシデバイスは IGMP/MLD のルータ部を実行し、アップストリーム インターフェイスでは、IGMP/MLD のホスト部を実行します。

転送ルールとクエリア

次のルールが適用されます。

- アップストリームインターフェイスで受信されたマルチキャストパケットは、そのパケットを要求するすべてのダウンストリームインターフェイスに転送されます（ただし、プロキシ デバイスがそのインターフェイス上のクエリアである場合のみ）。
- プロキシ デバイスは、ダウンストリーム インターフェイスでクエリアにならない場合、ダウンストリーム インターフェイスで受信されたマルチキャスト パケットをドロップします。
- ダウンストリーム インターフェイスで受信されるマルチキャスト パケットは、プロキシデバイスがそのダウンストリーム インターフェイスでクエリアとなる場合、アップストリームインターフェイスで転送されます。プロキシデバイスがダウンストリームインターフェイスでクエリアとなる場合にのみ、パケットを要求するすべてのダウンストリームインターフェイスで転送されます。

マルチキャスト転送用の IGMP スヌーピングの設定

IGMP が機能するには IGMP クエリアが必要です。マルチキャストの処理にはマルチキャストルータの方が適していますが、設定が適切に行われているかぎり、Cisco Small Business スイッチはその役割の一部を果たすことができます。

IGMP スヌーピングはマルチキャストトラフィックが送信される VLAN に結び付けられるため、サブスクライバが存在する VLAN とは異なる VLAN にマルチキャストサーバーを配置することができます。

このセットアップでは、2 つの VLAN が使用されます。マルチキャストトラフィックが発生する 1 つ目の VLAN（VLAN 115）と 2 つ目の VLAN（今回は VLAN 1）はデフォルト設定されます。

ステップ 1 この VLAN 割り当ての場合、スイッチ B（非クエリアスイッチ）は、ポート 3 を介してスイッチ A（クエリア）にアップリンク接続されます。両方のポートが、トランク 1U、115T（VLAN 1 タグなし、VLAN 115 タグ付き）として設定されます。

a) スイッチ A のポート 1 には、マルチキャストサーバーが接続されます（VLAN 115U、アクセス）。
b) スイッチ A のポート 2 には、サブスクライバが接続されます（VLAN 115U、アクセス）。
c) スイッチ B のポート 1 には、サブスクライバが接続されます（VLAN 115U、アクセス）。
d) スイッチ B のポート 2 には、サブスクライバが接続されます（VLAN 115U、アクセス）。
e) スイッチ A のポート 10 には、ルータが接続されます（VLAN 1U、115T、トランク）。

ステップ 2 スイッチが接続されるルータのポートは、トランクポート VLAN 1U、115T である必要があります。対応する IP アドレスと DHPC 設定が適切に指定されていることを確認します。

ステップ 3 スイッチのメイン設定ページに移動し、[Multicast] > [IGMP Snooping] の順に選択します。このページの場所は、スイッチのモデルによって異なります。

ステップ 4 次の [Enable] チェックボックスをオンにします。

- IGMPスヌーピングステータス
- IGMPクエリアステータス

ステップ 5 次に、VLAN 115 を選択し、[Edit] をクリックします。

ステップ 6 IGMP スヌーピングステータスの [Enable] チェックボックスをオンにして有効にします。

ステップ 7 [MRouter Ports Auto Learn] チェックボックスをオンにして有効にします。このオプションは、スイッチがクエリア（マルチキャストルータ）の場所を自動的に学習するためのものです。そのため、スイッチがクエリアとして機能している場合は、このオプションをオンにしないでください。

ステップ 8 [Immediate Leave] チェックボックスをオンにして有効にします。このオプションは、IGMP スヌーピング機能への副作用を心配することなく、有効または無効にすることができます。有効にすると、デバイスポートに送信される不要な IGMP トラフィックのブロックにかかる時間が短縮されます。

ステップ 9 [Last Member Query Counter] はデフォルト設定のままにして、ウィンドウを閉じて次の手順に進みます。

ステップ 10 スイッチのメイン設定ページに戻り、[Multicast] > [IGMP Snooping] の順に選択します。このページの場所は、スイッチのモデルによって異なります。

ステップ 11 [IGMP Querier Status] チェックボックスをオンして有効にします。このスイッチがクエリアとして機能する場合にのみ、このオプションを有効にします。それ以外の場合は、オフのままにしておいてください。今回は、クエリアを 1 つだけ設定します。

ステップ 12 次に、VLAN 115 を選択し、[Edit] をクリックします。

ステップ 13 [IGMP Querier Status] チェックボックスをオンして、スイッチがクエリアとして機能できるようにします。このスイッチをクエリアとして機能させる場合にのみ、この手順を実行してください。ほとんどのセットアップでは、必要なクエリアは 1 つだけです。

ステップ 14 [IGMP Querier Election] チェックボックスをオンにします。VLAN で複数のクエリアが使用されており、2つ目のクエリアで IGMP クエリアステータスがグローバルに有効になっている場合は、このオプションを使用することにより、この環境を管理することができます。

ステップ 15 IGM クエリアのバージョン（バージョン 2 またはバージョン 3）を選択します。バージョン 3 を選択するのはVLAN 内に送信元固有の IP マルチキャスト転送を実行するスイッチやルータがある場合であるため、ほとんどの場合はバージョン 2 を選択します。

ステップ 16 [Querier Source IP address] で [User Defined] を選択し、クエリアとして機能するスイッチの IP アドレスを選択します。

ステップ 17 スヌーピングページでの調整が完了したので、全体を機能させるためにブリッジマルチキャスト フィルタリングを有効にする必要があります。スイッチの Web UI で、[Multicast] > [Properties] の順に移動します。

ステップ 18 [Bridge Multicast Filtering Status] チェックボックスをオンにして、スイッチが IGMP スヌーピングと連携してマルチキャストを処理できるようにします。この機能が有効になっていない場合（デフォルトではオフ）、すべてのポートがマルチキャストトラフィックに使用されます。

ステップ 19 VLAN 115 または特定の VLAN を選択します。「転送方式」を選択します。ここでは、[MAC Group Address] を選択していれば、[Multicast /MAC Group Address] テーブルに MAC アドレスが表示されますが、今回は [IP Group Address] を選択しているため、[Multicast /IP Multicast Group Address] テーブルにマルチキャスト IP アドレスが表示されます。

ステップ 20 デフォルトでは、[Multicast Router Port] は [None] に設定されています。ここでは何も調整する必要がありません。非クエリアスイッチでは、クエリアデバイスへのアップリンクポートが [Dynamic] として選択されます。これを確認するには、VLAN 115 を選択し、[Go] をクリックして、[Dynamic] 行でポート 3 が選択されていることを調べてください。これは、スイッチ B はクエリアではないものの、そのアップリンクポートでクエリアを検出したことを示しています。

ステップ 21 [Multicast] > [Forward All] の順にクリックし、これが [None] に設定されていることを確認します。通常、デフォルトで [None] に設定されています。これはクエリアスイッチにも当てはまります。

ステップ 22 [Multicast] > [Unregistered Multicast] の順にクリックします。デフォルト設定では [Forwarding all] が指定されています。つまり、登録済みまたは未登録のすべてのマルチキャストトラフィックが転送されます。未登録のトラフィックを転送したくない場合は、推奨設定の [Filtering] に設定し、マルチキャスト サーバー マシンが接続されているポートについてのみ [Forwarding] 設定が選択されたままにします。

ステップ 23 動作することを確認するためにテストします。VLC をビデオ ストリーミング プログラムおよびビデオ サブスクライバ クライアントとして使用して、図のようにデバイスを接続します。VLC サーバーからビデオのストリーミングを開始し、クライアントを起動してストリームに登録します。結果は、次のとおりです。

VLC をビデオ ストリーミング プログラムおよびビデオ サブスクライバ クライアントとして使用して、図のようにデバイスを接続します。VLC サーバーからビデオのストリーミングを開始し、クライアントを起動してストリームに登録します。結果は、次のとおりです。

- マルチキャスト IP アドレスが VLAN 115 の [Multicast /IP Multicast Group Address] に正しく入力されていることを確認します。これは、クライアントがビデオストリームに正常に登録されていることを示しています。
- 複数のスイッチによるセットアップでは、クエリアとして機能していないスイッチがクエリアを正常に識別したことを確認します。非クエリアスイッチでは、クエリアデバイスへのアップリンクポートが [Dynamic] として選択されます。これを確認するには、VLAN 115 を選択し、[Go] をクリックして、[Dynamic] 行でポート 3 が選択されていることを調べてください。これは、このスイッチ B はクエリアではないものの、そのアップリンクポートでクエリアを検出したことを示しています。

ステップ 24 デフォルトでは、マルチキャストブリッジフィルタが有効になっていないかぎり、スイッチのすべてのポートでマルチキャストトラフィックが設定されます。サブスクライバが VLAN y に存在する場合、マルチキャストトラフィックが VLAN x から発信されると、上記の設定は機能しません。マルチキャスト TV を使用すると、この特別な設定に対応できます。

802_1x の概要

802.1X 認証は、未認可クライアントが一般にアクセス可能なポートから LAN に接続することを制限します。802.1X 認証はクライアント/サーバ モデルです。このモデルでは、ネットワーク デバイスが次の固有の役割を持ちます。

- クライアントまたはサプリカント
- オーセンティケータ
- 認証サーバ

ネットワーク デバイスは、ポートごとにクライアント/サプリカント、オーセンティケータ、または両方として使用できます。

クライアントまたはサプリカント

クライアントまたはサプリカントは、LAN へのアクセスを要求するネットワーク デバイスです。クライアントはオーセンティケータに接続されます。

クライアントは、認証に 802.1X プロトコルを使用する場合、802.1X プロトコルのサプリカントの部分と EAP プロトコルのクライアントの部分を実行します。

オーセンティケータ

オーセンティケータは、サプリカント ポートの接続先となる、ネットワーク サービスを提供するネットワーク デバイスです。ポートでは次の認証モードがサポートされています。

- 単一ホスト：ポートごとに単一のクライアントを受け入れる、ポートベースの認証をサポートします。
- 複数ホスト：ポートごとに複数のクライアントを受け入れる、ポートベースの認証をサポートします。
- 複数セッション：ポートごとに複数のクライアントを受け入れる、クライアントベースの認証をサポートします。

次の認証方式がサポートされます。

- 802.1X ベース：すべての認証モードでサポートされます。
- MAC ベース：すべての認証モードでサポートされます。
- Web ベース：マルチセッション モードでのみサポートされます。

802.1X ベース認証では、オーセンティケータが 802.1X メッセージ（EAPOL パケット）から EAP メッセージを抽出し、RADIUS プロトコルを使用してそれらを認証サーバに渡します。

MAC ベース認証または Web ベース認証では、オーセンティケータ自体が、ネットワーク アクセスを求めるクライアントの代わりにソフトウェアの EAP クライアントの部分を実行します。

オープンアクセス

802.1x 環境で、オープン（モニタリング）アクセス機能は、実際の認証失敗と、設定ミスやリソース不足のために発生する失敗を区別するために役立ちます。オープンアクセスを使用することにより、システム管理者は、ネットワークに接続しているホストの設定上の問題を容易に把握し、不適切な状態をモニターして、これらの問題を修正できるようになります。

オープンアクセスがインターフェイスで有効になっている場合、スイッチは RADIUS サーバーの失敗をすべて成功と見なし、認証結果にかかわらず、インターフェイスに接続しているステーションのネットワークへのアクセスを許可します。通常の動作では、認証が有効になっているポート上のトラフィックは認証と認可が正常に完了するまでブロックされますが、オープンアクセスにより、その動作が変更されます。

認証のデフォルトの動作では、Extensible Authentication Protocol over LAN（EAPoL）を除くすべてのトラフィックがブロックされます。一方、オープンアクセスでは、認証（802.1X ベース、MAC ベース、または Web ベース）が有効になっている場合でも、すべてのトラフィックに対して無制限のアクセスを許可するオプションが管理者に提供されます。

RADIUS アカウンティングが有効になっている場合、認証試行をログに記録し、監査証跡を使用して、ネットワークに接続しているユーザやシステムを把握できます。

オーセンティケータの概要

ポート管理認証状態

ポート管理状態により、クライアントがネットワークへのアクセス権を付与されるかどうかが決まります。

次の値が有効です。

- force-authorized-Port 認証は無効で、ポートはスタティック設定に従い、認証を行わずにすべてのトラフィックを送信します。スイッチは、802.1X EAPOL 開始メッセージを受信すると、EAP 成功メッセージを格納した 802.1X EAP パケットを送信します。これは、デフォルトの状態です。
- force-unauthorized-Port 認証は無効で、ポートはゲスト VLAN および非認証 VLAN 経由ですべてのトラフィックを送信します。スイッチは、802.1X EAPOL 開始メッセージを受信すると、EAP 失敗メッセージを格納した 802.1X EAP パケットを送信します。
- auto-Enables 802.1x 認証は、設定済みのポートホストモードおよびポートに設定されている認証方式に従って有効になります。

ポート ホスト モード

ポートに設定できるポートホストモードは次のとおりです。

- [Single-Host Mode]：許可されたクライアントが存在する場合にポートが許可されます。1つのポートでは1つのホストのみ認可されます。ポートが未承認でゲストVLANがイネーブルの場合、タグなしトラフィックはゲスト VLAN に再マッピングされます。タグ付きトラフィックは、ゲスト VLAN または非認証 VLAN に属していないかぎりドロップされます。ポートでゲスト VLAN が有効になっていない場合、非認証 VLAN に属しているタグ付きトラフィックだけがブリッジされます。

  ポートが認可されると、認可済みホストからのトラフィックは、タグなしのものもタグ付きのものも、スタティック VLAN メンバーシップ ポート設定に基づいてブリッジされます。他のホストからのトラフィックはドロップされます。許可ホストからのタグなしトラフィックが、認証プロセス中に RADIUS サーバによって割り当てられた VLAN に再マッピングされるようにユーザが指定できます。タグ付きトラフィックは、RADIUS割り当て VLAN か非認証 VLAN に属していないかぎりドロップされます。

- [Multi-Host Mode]：許可されたクライアントが少なくとも 1 つ存在する場合にポートが許可されます。ポートが認可されておらず、ゲスト VLAN が有効になっている場合、タグなしトラフィックはゲスト VLAN に再マッピングされます。タグ付きトラフィックは、ゲスト VLAN または非認証 VLAN に属していないかぎりドロップされます。ポート上でゲスト VLAN が有効になっていない場合、認証されていない VLAN に属するタグ付きトラフィックだけがブリッジされます。

  ポートが認可されると、そのポートに接続されたすべてのホストからのトラフィックは、タグなしのものもタグ付きのものも、スタティック VLAN メンバーシップ ポート設定に基づいてブリッジされます。ユーザは、認可済みポートからのタグなしトラフィックが、認証プロセス中に、RADIUSサーバによって割り当てられているVLANに再マッピングされるように指定できます。タグ付きトラフィックは、RADIUS 割り当て VLAN か非認証 VLAN に属していないかぎりドロップされます。

- [Multi-Sessions Mode]：シングルホストおよびマルチホストモードとは異なり、マルチセッションモードのポートには認証ステータスがありません。このステータスは、ポートに接続している各クライアントに割り当てられます。非認証 VLAN に属しているタグ付きトラフィックは、ホストが認可されているどうかにかかわらず、常にブリッジされます。

  非認証 VLAN に属していない未認可ホストからのトラフィックは、タグ付きのものもタグなしのものも、ゲスト VLAN が VLAN で定義されていて有効になっている場合はゲストVLANに再マッピングされ、ゲストVLANがポートで有効になっていない場合はドロップされます。ユーザは、認可済みポートからのタグなしトラフィックが、認証プロセス中に、RADIUSサーバによって割り当てられているVLANに再マッピングされるように指定できます。タグ付きトラフィックは、RADIUS 割り当て VLAN か非認証 VLAN に属していないかぎりドロップされます。

複数の認証方法

スイッチで複数の認証方式が有効になっている場合は、次の認証方式の階層が適用されます。

- 802.1X 認証：最上位
- Web ベース認証
- MAC ベース認証：最下位

複数の方式を同時に実行できます。1 つの方式が正常に完了すると、クライアントが認可されて、優先順位の低い方式は停止され、優先順位の高い方式は続行されます。

同時に実行されている認証方式のいずれかが失敗すると、他の方式が続行されます。

優先順位の低い認証方式で認証されたクライアントに対して別の認証方式が正常に完了すると、新しい認証方式の属性が適用されます。新しい方式が失敗する場合、クライアントは古い方式で認可されたままになります。

802.1xベース認証

802.1x ベースのオーセンティケータは、透過的な EAP メッセージを 802.1x サプリカントと認証サーバーの間でリレーします。サプリカントとオーセンティケータの間で交換された EAP メッセージは802.1x メッセージ内にカプセル化され、オーセンティケータと認証サーバーの間で交換された EAP メッセージは RADIUS メッセージ内にカプセル化されます。

MAC ベースの認証

MAC ベース認証は、802.1X のサプリカント機能を持たない装置（プリンタおよび IP Phone など）へのネットワークアクセスを可能にする、802.1X 認証に代わるものです。MAC ベース認証は、接続装置の MAC アドレスに基づき、ネットワークアクセスを許可または拒否します。この場合、スイッチは、次のように、クライアントの MAC アドレスであるユーザー名とパスワードで EAP MD5 機能をサポートします。

Web ベース認証

スイッチを介したネットワークへのアクセスを要求するエンドユーザーは、Webベース認証を使用して認証されます。これにより、スイッチに直接接続されているクライアントを、ネットワークへのアクセス権が与えられる前に、キャプティブポータルメカニズムを使用して認証できます。

Web ベース認証はクライアントベースの認証であり、レイヤ 2 とレイヤ 3 の両方においてマルチセッションモードでサポートされます。この認証方式がポートごとに有効になっている場合、各ホストはネットワークにアクセスするためにそのホスト自体を認証する必要があります。したがって、有効になっているポートで認証されるホストと認証されないホストが存在する可能性があります。

ポートで Web ベース認証が有効になっている場合、スイッチは、ARP、DHCP、および DNS パケットを除き、未認可クライアントからのすべてのトラフィックをドロップします。スイッチにより、これらのパケットは転送されることが許可されます。そのため、未認可クライアントでも IP アドレスを取得し、ホスト名またはドメイン名を解決することができます。

未認可クライアントの IPv4 の HTTP/HTTPS パケットは、スイッチの CPU にルーティングされます。エンドユーザーがネットワークアクセスを要求すると、Webベース認証がポートで有効

な場合は、要求されたページが表示される前にログインページが表示されます。ユーザーはユーザー名およびパスワードを入力する必要があります。これらは、EAPプロトコルを使用して RADIUS サーバーによって認証されます。認証が成功すると、ユーザーに通知されます。

この時点でユーザーのセッションが認証されます。セッションが使用されている間は、開いたままです。指定された時間内に使用されない場合、セッションは終了します。この時間間隔は「待機時間」と呼ばれ、システム管理者が設定します。セッションが期限切れになると、ユーザー名とパスワードが失われ、ゲストは新しいセッションを開始するためにそれらを再入力する必要があります。

非認証 VLAN とゲスト VLAN

非認証 VLAN とゲスト VLAN は、サプリカント デバイスまたはポートを認証および認可する必要のないサービスへのアクセスを提供します。

ゲスト VLAN は、未認可クライアントに割り当てられる VLAN です。ゲスト VLAN、および 802.1x 認証プロパティで非認証にする 1 つ以上の VLAN を設定できます。

非認証 VLAN は、認可済みデバイス/ポートと未認可デバイス/ポートの両方によるアクセスを許可する VLAN です。非認証 VLAN には次の特性があります。

- スタティック VLAN である必要があり、ゲスト VLAN またはデフォルト VLAN にはできません。
- メンバー ポートは、タグ付きメンバーとして手動で設定する必要があります。
- メンバー ポートは、トランク ポートまたは一般的なポートである必要があります。アクセス ポートは非認証 VLAN のメンバーにはできません。

ゲスト VLAN（設定されている場合）は次の特性を持つスタティック VLAN です。

- 既存のスタティック VLAN から手動で定義する必要があります。
- ゲスト VLAN を音声 VLAN または非認証 VLAN として使用することはできません。

ホスト モードとゲスト VLAN

ゲスト VLAN を使用する場合、ホスト モードは次のように機能します。

- シングルホストおよびマルチホストモード：未認可ポートに着信する、ゲスト VLAN からのトラフィックは、タグなしのものもタグ付きのものも、ゲスト VLAN を介してブリッジされます。他のすべてのトラフィックは拒否されます。認証されていない VLAN からのトラフィックは、VLAN を介してルーティングされます。
- レイヤ 2 のマルチセッションモード：未認可クライアントから着信する、非認証 VLAN に属していないトラフィックは、タグなしのものもタグ付きのものも、TCAMルールを使用してゲスト VLAN に割り当てられ、ゲスト VLAN を介してブリッジされます。認証されていない VLAN からのタグ付きトラフィックは、VLAN を介してルーティングされます。

  このモードは、ポリシーベース VLAN と同じインターフェイスでは設定できません。

- レイヤ 3 のマルチセッションモード：このモードはゲスト VLAN をサポートしていません。

RADIUS VLAN 割り当てまたはダイナミック VLAN 割り当て

このオプションが [Port Authentication] ページで有効になっている場合、RADIUS サーバーは認可済みクライアントにVLANを割り当てることができます。これは、RADIUS割り当てVLAN、またはダイナミック VLAN 割り当て（DVA）と呼ばれます。このガイドでは「RADIUS 割り当て VLAN」という用語を使用しています。

ポートがマルチセッションモードで、RADIUS割り当てVLANが有効な場合、デバイスはこのポートを認証プロセス中に追加して、RADIUSサーバーによって割り当てられたVLANのタグなしメンバーとします。タグなしパケットが認証および許可済みのデバイスもしくはポートから発信されたものである場合、そのパケットは、割り当て済み VLAN に所属するものとして分類されます。

（注） 複数セッション モードでは、デバイスがレイヤ 2 システム モードの場合にのみ、RADIUS VLAN 割り当てがサポートされます。

DVA 対応ポートでデバイスの認証および認可を行う場合は、次の点に注意してください。

- RADIUSサーバーは、デバイスを認証し、デバイスにVLANを動的に割り当てる必要があります。[Port Authentication] ページで、[RADIUS VLAN Assignment] フィールドを [static] に設定できます。これにより、ホストをスタティック設定に基づいてブリッジすることが可能になります。
- tunnel-type (64) = VLAN (13)、tunnel-media-type (65) = 802 (6)、および tunnel-privategroup-id = VLAN ID のように RADIUS 属性を指定した RADIUS サーバーにより、DVA がサポートされる必要があります。

RADIUS 割り当て VLAN 機能が有効になっている場合、ホスト モードの動作は次のようになります。

- シングルホストおよびマルチホストモード：RADIUS 割り当て VLAN に属しているトラフィックは、タグなしのものもタグ付きのものも、この VLAN を介してブリッジされます。非認証 VLAN に属していないその他のすべてのトラフィックは破棄されます
- フルマルチセッションモード：クライアントから着信する、非認証 VLAN に属していないトラフィックは、タグなしのものもタグ付きのものも、TCAMルールを使用してRADIUS割り当て VLAN に割り当てられ、その VLAN を介してブリッジされます。
- レイヤ 3 システム モードの複数セッション モード

このモードは、RADIUS 割り当て VLAN をサポートしていません。

次の表に、認証方式とポートモードに応じたゲスト VLAN および RADIUS VLAN 割り当てのサポートを示します。

表 *2: VLAN* および *RADIUS VLAN* 割り当て

認証方式	シングルホスト	マルチホスト	マルチセッション	
			L3 のデバイス	L2 のデバイス
802.1X	†	†	N/S	†
MAC	†	†	N/S	†
Web	N/S	N/S	N/S	N/S

凡例

†：ポートモードはゲスト VLAN および RADIUS VLAN 割り当てをサポートします

N/S：ポートモードは認証方法をサポートしません。

違反モード

シングルホストモードでは、認可済みポートで未認可ホストがインターフェイスにアクセスしようとしたときに実行するアクションを設定できます。これは、[ホストおよびセッション認証] ページで行います。

次のオプションを使用できます。

- restrict：MAC アドレスがサプリカント MAC アドレスではないステーションがインターフェイスへのアクセスを試みると、トラップが生成されます。トラップ間の最短時間は 1 秒です。これらのフレームは転送されますが、送信元アドレスは不明のままです。
- protect：サプリカントアドレスではない送信元アドレスを持つフレームは廃棄されます。
- shutdown：サプリカントアドレスではない送信元アドレスを持つフレームを拒否し、ポートを閉じます。

SNMP トラップを、設定可能な最小の時間間隔で送信するようにデバイスを設定することもできます。seconds を 0 にした場合、トラップは無効になります。最小時間を指定しない場合、制限モードではデフォルトで 1 秒に設定され、その他のモードでは 0 に設定されます。

待機時間

認証失敗情報交換後、ポート（シングルホストモードまたはマルチホストモード）またはクライアント（マルチセッションモード）は、待機時間中に認証を試行できません。シングルホストモードまたはマルチホストモードの場合、この期間はポートごとに定義され、マルチセッションモードの場合、この期間はクライアントごとに定義されます。待機時間の間、スイッチは認証要求を受け付けず、開始もしません。

802.1x ベース認証と Web ベース認証のみがこの期間の対象です。待機時間に入る前に許可されるログインの試行回数を指定することもできます。0 の値は、ログインの試行回数が無制限であることを示します。[Port Authentication] ページで、待機時間の長さとログインの最大試行回数を設定できます。

モードの動作

次の表に、さまざまな状況で認証トラフィックと非認証トラフィックがどのように処理されるかを示します。

	非認証 トラフィック				認証トラフィック		
	ゲスト **VLAN** あり		ゲスト **VLAN** なし		**RADIUS VLAN** あり		**RADIUS V**
	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
シングルホスト	フレームはゲスト VLAN に再マッピングされます	フレームはゲスト VLAN または非認証 VLAN に属していないかぎりドロップされます	フレームはドロップされます	フレームは非認証 VLAN に属していないかぎりドロップされます	フレームは RADIUS 割り当て VLAN に再マッピングされます	フレームは RADIUS VLAN または非認証 VLAN に属していないかぎりドロップされます	フレームタティッ VLAN 設基づいてリッジさす
マルチホスト	フレームはゲスト VLAN に再マッピングされます	フレームはゲスト VLAN または非認証 VLAN に属していないかぎりドロップされます	フレームはドロップされます	フレームは非認証 VLAN に属していないかぎりドロップされます	フレームは RADIUS 割り当て VLAN に再マッピングされます	フレームは RADIUS VLAN または非認証 VLAN に属していないかぎりドロップされます	フレームタティッ VLAN 設基づいてリッジさす
ライト マルチセッション	N/S	N/S	フレームはドロップされます	フレームは非認証 VLAN に属していないかぎりドロップされます	N/S	N/S	フレームタティッ VLAN 設基づいてリッジさす

	非認証 トラフィック				認証トラフィック		
	ゲスト VLAN あり		ゲスト VLAN なし		RADIUS VLAN あり		RADIUS VLA
	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
フル マルチセッション	フレームはゲスト VLAN に再マッピングされます	フレームは非認証 VLAN に属していないかぎりゲスト VLAN に再マッピングされます	フレームはドロップされます	フレームは非認証 VLAN に属していないかぎりドロップされます	フレームは RADIUS 割り当て VLAN に再マッピングされます	フレームは非認証 VLAN に属していないかぎり RADIUS VLAN に再マッピングされます	フレームはタティック VLAN 設定基づいてブリッジされます

DHCPv4 のタイプと相互作用

DHCPv4 スヌーピング

DHCP スヌーピングは、誤った DHCP 応答パケットの受信を防ぎ、DHCP アドレスをログに記録するセキュリティ機能です。これは、デバイスのポートを信頼できるまたは信頼できないに分類することによって実現されます。

信頼できるポートは、DHCP サーバーに接続していて、DHCP アドレスの割り当てが許可されているポートです。信頼できるポートで受信した DHCP メッセージは、デバイスをパススルーできます。DHCP アドレスの割り当てが許可されていないポートは、信頼できないポートと呼ばれます。ポートを信頼できると宣言するまで、デフォルトでは信頼できないと見なされます。

DHCPv4 リレー

DHCP リレーは、DHCP サーバに DHCP パケットをリレーします。

レイヤ 2 およびレイヤ 3 における DHCPv4

レイヤ 2 システムモードで、デバイスは、DHCP リレーが有効になっている VLAN から受け取った DHCP メッセージをリレーします。レイヤ 3 システムモードで、デバイスは、IP アドレスのない VLAN から受け取った DHCP シグナルも送信できます。IP アドレスのない VLAN で DHCP リレーを有効にすると、Option 82 が自動的に挿入されます。この挿入は単一の VLAN で行われ、Option 82 のグローバル管理状態には影響しません。

透過型 DHCP リレー

外部 DHCP リレーエージェントが使用される透過型 DHCP リレーの場合は、次の手順を実行します。

- DHCP スヌーピングを有効にします。
- Option 82 の挿入を有効にします。
- DHCP リレーを無効にします。

通常の DHCP リレーの場合は、次の手順を実行します。

- DHCP リレーを有効にします。
- Option 82 の挿入を有効にする必要はありません。

Option 82

Option 82（DHCP リレーエージェント情報オプション）は、ポートおよびエージェント情報を中央 DHCP サーバーに渡して、割り当てられた IP アドレスがネットワークに物理的に接続されている場所を識別します。

Option 82 の主な目的は、DHCP サーバーが IP アドレスを受け取る最適な IP サブネット（ネットワークプール）を決定できるようにすることです。

デバイス上では、以下のオプション 82 設定が利用可能です。

- [DHCP Insertion]：Option 82 情報を持たないパケットに Option 82 情報を追加します。
- [DHCP Pass through]：信頼できないポートからの Option 82 情報を含む DHCP パケットを転送または拒否します。信頼できるポートでは、Option 82 情報が含まれている DHCP パケットは常に転送されます。

DHCP リレー、DHCP スヌーピング、および Option 82 モジュールによるパケットフローを次の表に示します。

発生する可能性のあるさまざまなシナリオがあります。

- DHCP クライアントと DHCP サーバーの両方が同じ VLAN にある。このシナリオでは、一般的なブリッジは、DHCP クライアントと DHCP サーバーの間で DHCP メッセージを渡します。
- DHCP クライアントと DHCP サーバーの両方が異なる VLAN にある。この場合、DHCP リレーのみが、DHCP クライアントと DHCP サーバーの間の DHCP メッセージのブロードキャストを実行可能であり、実際にそれを実行します。正規のルータがユニキャスト DHCP パケットを送信するため、IP アドレスのない VLAN 上で DHCP リレーが有効である場合、またはデバイスがルータ（レイヤ 2）でない場合には、外部ルータが必要になります。

DHCP リレーによってのみ、DHCP サーバーに DHCP メッセージが転送されます。

DHCPv4 スヌーピング、DHCPv4 リレーおよび Option 82 間の相互作用

次の表に、DHCP スヌーピング、DHCP リレー、および Option 82 のさまざまな組み合わせを使用した場合のデバイスの動作について説明します。DHCP スヌーピングが有効になっておらず、DHCP リレーが有効になっているときの DHCP 要求パケットの処理方法について以下で説明します。

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着
Option 82 の挿入が無効	Option 82 なしでパケットが送信されます	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 ブリッジを挿入：Option 82 が挿入されない	リレー：パケットを破棄 ブリッジ：元の Option 82 と一緒にパケットが送信されます
Option 82 の挿入が有効	リレー：Option 82 と一緒に送信 ブリッジ：Option 82 は送信されません	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 と一緒に送信 ブリッジ：Option 82 は送信されません	リレー：パケットを破棄 ブリッジ：元の Option 82 と一緒にパケットが送信されます

DHCP スヌーピングと DHCP リレーの両方が有効になっているときの DHCP 要求パケットの処理方法について以下で説明します。

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着
Option 82 の挿入が無効	Option 82 なしでパケットが送信されます	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 を挿入 ブリッジ：Option 82 を挿入しない	リレー：パケットを破棄 ブリッジ：元の Option 82 と一緒にパケットが送信されます

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
Option 82 の挿入が有効	リレー：Option 82 と一緒に送信 ブリッジ：Option 82 を追加 （ポートが信頼できる場合は、DHCP スヌーピングが有効でない場合のように動作します）	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 と一緒に送信 ブリッジ：Option 82 を追加 （ポートが信頼できる場合は、DHCP スヌーピングが有効でない場合のように動作します）	リレー：パケットを破棄 ブリッジ：元の Option 82 と一緒にパケットが送信されます

次に、DHCP スヌーピングが無効になっているときの DHCP リレーパケットの処理方法について説明します

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着
Option 82 の挿入が無効	Option 82 なしでパケットが送信されます	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 を破棄 ブリッジ：Option 82 なしでパケットが送信されます	リレー： 1. 応答の発信元がデバイスの場合、パケットは Option 82 なしで送信 2. 応答の発信元がデバイスではない場合、パケットは破棄されます。 ブリッジ：元の Option 82 と一緒にパケットが送信されます

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
Option 82 の挿入が有効	Option 82 なしでパケットが送信されます	リレー：Option 82 なしのパケットを送信 ブリッジ：Option 82 ありのパケットを送信	リレー：Option 82 を破棄 ブリッジ：Option 82 なしでパケットが送信されます	リレー：Option 82 なしのパケットを送信 ブリッジ：Option 82 ありのパケットを送信

次に、DHCP スヌーピングと DHCP リレーの両方が有効になっているときの DHCP 応答パケットの処理方法について説明します。

	IP アドレスのある DHCP リレー VLAN		IP アドレスのない DHCP リレー VLAN	
	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着	Option 82 なしでパケットが到着	Option 82 と一緒にパケットが到着
Option 82 の挿入が無効	Option 82 なしでパケットが送信されます	元の Option 82 と一緒にパケットが送信されます	リレー：Option 82 を破棄 ブリッジ：Option 82 なしでパケットが送信されます	リレー： 1. 応答の発信元がデバイスの場合、パケットは Option 82 なしで送信 2. 応答の発信元がデバイスではない場合、パケットは破棄されます。 ブリッジ：元の Option 82 と一緒にパケットが送信されます
Option 82 の挿入が有効	Option 82 なしでパケットが送信されます	Option 82 なしでパケットが送信されます	リレー：Option 82 を破棄 ブリッジ：Option 82 なしでパケットが送信されます	Option 82 なしでパケットが送信されます

IPv6 管理インターフェイス

IPv6（インターネット プロトコル バージョン 6）は、パケット交換インターネット操作用のネットワーク層プロトコルです。IPv6は、最も幅広く使用されているインターネットプロトコルである IPv4 に代わるものとして作成されました。アドレスサイズが 32 ビットから 128 ビットに増加するため、IPv6 では IP を割り当てる際の柔軟性が増します。FE80::9C00:876A:130B またはFE80:0000:0000:0000:0000:9C00:876A:130B は省略形の例で、一連のゼロは省略して「::」に置き換えることができます。

IPv4 しか使用できないネットワーク上で他の IPv6 ノードに接続するには、途中でマッピングする技術が必要です。このトンネリング技術を使用すれば、IPv6にしか対応していないホストでも IPv4 サービスに接続でき、孤立した IPv6 ホストおよびネットワークが IPv4 インフラストラクチャをまたいで IPv6 ノードに接続できます。

ISATAP または手動メカニズムがトンネリングに使用されます（「IPv6 トンネル」を参照）。IPv4 ネットワークは仮想 IPv6 ローカルリンクとして扱われ、トンネリングを経由して、各 IPv4 アドレスからリンクローカル IPv6 アドレスへのマッピングが行われます。IPv6 Ethertype は、デバイスが IPv6 フレームを認識するために使用されます。

DoS防御

サービス妨害（DoS）攻撃は、デバイスをユーザーがアクセスできない状態にしようとするハッカーの行為です。

DoS 攻撃では、デバイスが外部の通信要求でオーバーロード状態になり、正当なトラフィックに応答できないようになります。

この攻撃では通常、デバイスの CPU がオーバーロードになります。

Secure Core Technology（SCT）

このデバイスは、DoS 攻撃に抵抗する方法の 1 つとして SCT を採用しています。デバイスの SCT はデフォルトで有効になっていて、無効にすることはできません。シスコデバイスは、エンドユーザー（TCP）トラフィックに加えて、管理トラフィック、プロトコルトラフィック、およびスヌーピングトラフィックを処理します。SCT を使用することで、デバイスは、受信するトラフィック量に関係なく、管理およびプロトコルトラフィックを受信して処理できます。これは、CPU に対する TCP トラフィックを制限することで実現されます。

他の機能との相互作用はありません。

DoS 攻撃の種類

DoS 攻撃には、次の種類のパケットやその他の戦略が関係している可能性があります

- TCP SYN Packets：このパケットには不正な送信者アドレスが含まれていることがよくあります。各パケットは接続要求として扱われ、TCP/SYN-ACK パケット（確認応答）を送り返して、送信者アドレスからのパケット（ACK パケットへの応答）を待機することで、サーバーでハーフオープン接続が生じる原因となります。しかし、送信者アドレスは正し

くないため、応答が受信されることはありません。このようなハーフオープン接続により、デバイスで使用可能な接続が一杯になり、正当な要求に応答できなくなります。

- [TCP SYN-FIN Packets]：新しい TCP 接続を確立するために SYN パケットが送られます。TCP FIN パケットは接続を終了するために使用されます。1 つのパケット内に SYN と FIN の両方のフラグが設定されることは決してありません。結果として、これらのパケットはデバイスへの攻撃を示している可能性があるため、ブロックする必要があります。
- Martian アドレス（Martian Addresses）：Martian アドレスは、IP プロトコルの観点からは不正なアドレスです。
- ICMP 攻撃：不適切な形式の ICMP パケットまたは膨大な数の ICMP パケットが攻撃の標的に送られると、システムクラッシュが発生する可能性があります。
- IP フラグメンテーション：重複する、サイズが大きすぎるペイロードを含む細切れの IP フラグメントをデバイスが受信します。このため、TCP/IP フラグメンテーションの再アセンブリコード内のバグが原因で、さまざまなオペレーティングシステムがクラッシュすることがあります。
- Stacheldraht ディストリビューション：攻撃者はハンドラに接続します。ハンドラはゾンビエージェントにコマンドを発行する侵害を受けたシステムで、それにより DoS 攻撃を可能にします。攻撃者は、ハンドラを介してエージェントを侵害します。自動ルーチンを使用して、攻撃対象のリモートホストで実行中のリモート接続を承認するプログラムの脆弱性をエクスプロイトします。各ハンドラは、最大 1,000 のエージェントを操ることができます。
- Invasor トロイの木馬：トロイの木馬により、攻撃者はゾンビエージェントをダウンロードできます（トロイの木馬にゾンビエージェントが含まれていることもあります）。攻撃者は、リモートホストからの接続をリッスンするプログラムの欠陥をエクスプロイトする自動化ツールを使用してシステムにアクセスすることもできます。このシナリオでは、Web サーバーとして機能するデバイスを主に問題にしています。
- Back Orifice トロイの木馬：これは、Back Orifice ソフトウェアを使用してトロイの木馬をインストールするトロイの木馬のバリエーションです。

DoS 攻撃に対する防御

サービス妨害（DoS）防御機能は、このような攻撃に対抗しているシステム管理者を次の方法で支援します。

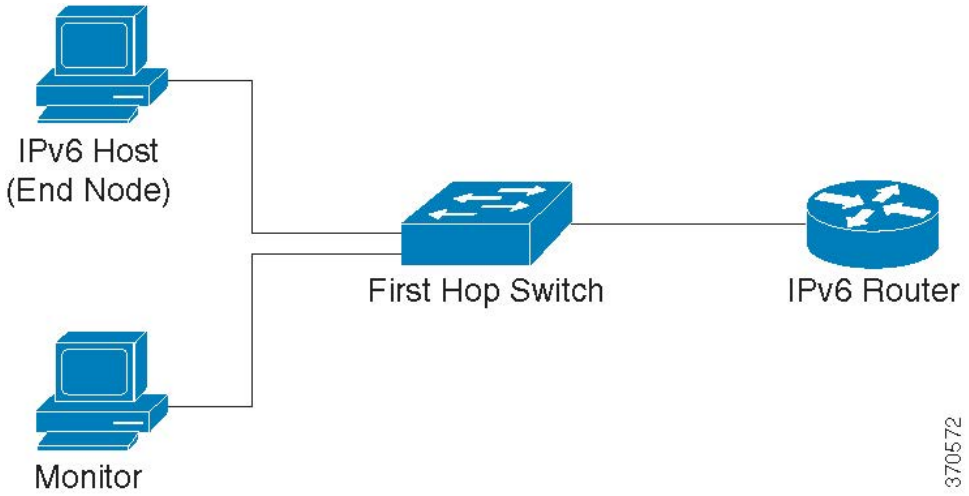
- TCP SYN 保護の有効化。この機能が有効になっている場合、SYN パケット攻撃の特定時にレポートが発行され、攻撃されたポートを一時的にシャットダウンできます。SYN 攻撃は、1 秒あたりの SYN パケットの数がユーザ設定のしきい値を超えた場合に特定されます。
- SYN-FIN パケットのブロック。
- 予約済み Martian アドレスを含むパケットのブロック。
- 特定のインターフェイスからの TCP 接続の防止およびパケットのレート制限。

- 特定の ICMP パケットのブロックの設定。
- 特定のインターフェイスからのフラグメント化された IP パケットの破棄。
- Stacheldraht ディストリビューション、Invasor トロイの木馬、および Back Orifice トロイの木馬からの攻撃の拒否。

IPv6 ファースト ホップ セキュリティ

IPv6 FHS は、IPv6 対応ネットワークでのリンク操作を保護するように設計された一連の機能です。これは、ネイバー探索プロトコルと DHCPv6 メッセージに基づいています。

この機能では、レイヤ 2 スイッチは（下に示すように）、複数の異なるルールに従って、ネイバー探索プロトコルメッセージ、DHCPv6 メッセージ、およびユーザーデータのメッセージをフィルタ処理します。



IPv6 ファースト ホップ セキュリティの個別かつ独立したインスタンスは、その機能が有効になっている各 VLAN で実行されます。

表 *3*：略語

名前	説明
CPA メッセージ	認証パス アドバタイズメント メッセージ
CPS メッセージ	認証パス請求メッセージ
DAD-NS メッセージ	重複アドレス検出ネイバー要請メッセージ
FCFS-SAVI	先入先出 - 発信元アドレス検証の改善
NA メッセージ	ネイバー アドバタイズメント メッセージ

名前	説明
NDP	ネイバー探索プロトコル
NS メッセージ	ネイバー要請メッセージ
RA メッセージ	ルータ アドバタイズメント メッセージ
RS メッセージ	ルータ要請メッセージ
SAVI	発信元アドレス検証の改善

IPv6 ファースト ホップ セキュリティのコンポーネント

IPv6 ファースト ホップ セキュリティには、次の機能があります。

- IPv6 ファースト ホップ セキュリティの共通機能
- RA ガード
- ND インスペクション
- ネイバー バインド整合性
- DHCPv6 ガード
- IPv6 ソース ガード

これらのコンポーネントは、VLAN で有効または無効にできます。

機能ごとに、VLAN default と port default という名前の 2 つの空の事前定義済みポリシーが存在します。最初のポリシーは、ユーザー定義ポリシーに接続されていない各 VLAN に接続され、2 番目のポリシーは、ユーザー定義ポリシーに接続されていない各インターフェイスと VLAN に接続されます。ユーザーはこれらのポリシーに明示的に接続できません。

IPv6 ファースト ホップ セキュリティのパイプ

IPv6 ファースト ホップ セキュリティが VLAN で有効になっている場合、スイッチは次のメッセージをトラップします。

- ルータ アドバタイズメント（RA）メッセージ
- ルータ要請（RS）メッセージ
- ネイバー アドバタイズメント（NA）メッセージ
- ネイバー要請（NS）メッセージ
- ICMPv6 リダイレクト メッセージ
- 認証パス アドバタイズメント（CPA）メッセージ
- 認証パス請求（CPS）メッセージ

• DHCPv6 メッセージ

トラップされたRA、CPA、およびICMPv6リダイレクトメッセージは、RAガード機能にルーティングされます。RA ガードはこれらのメッセージを検証し、不正なメッセージを破棄し、正当なメッセージを ND インスペクション機能に転送します。ND インスペクションはこれらのメッセージを検証し、不正なメッセージを破棄し、正当なメッセージを IPv6 ソースガード機能にルーティングします。

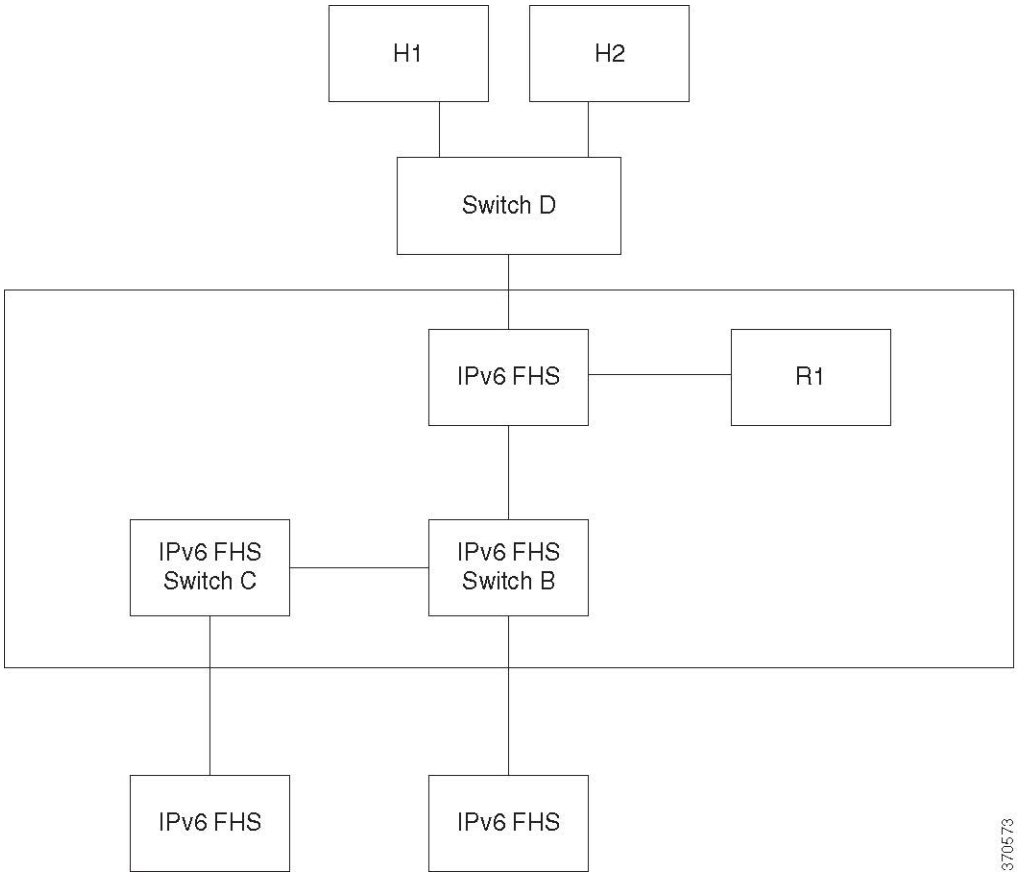
トラップされたDHCPv6メッセージは、DHCPv6ガード機能にルーティングされます。DHCPv6ガードはこれらのメッセージを検証し、不正なメッセージを破棄し、正当なメッセージをIPv6ソースガード機能に渡します。

トラップされたデータメッセージは、IPv6 ソースガード機能にルーティングされます。ネイバーバインドテーブルを使用して、IPv6ソースガードは受信メッセージ（トラップされたデータメッセージ、ND インスペクションからの NDP メッセージ、および DHCPv6 ガードからの DHCPv6メッセージ）を検証し、不正なメッセージをドロップし、正当なメッセージを転送します。ネイバーバインド整合性では、受信メッセージ（NDP および DHCPv6 メッセージ）からネイバーを取得し、それらをネイバーバインドテーブルに保存します。

静的エントリは手動で追加することもできます。アドレスを学習したら、NBI機能はフレームを転送します。NDインスペクション機能は、トラップされたRS、CPSNSおよびNAメッセージも受信します。ND インスペクションはこれらのメッセージを検証し、不正なメッセージを破棄し、正当なメッセージを IPv6 ソースガード機能に転送します。

IPv6 ファースト ホップ セキュリティの境界

IPv6 ファースト ホップ セキュリティ スイッチは、境界を形成することで、信頼できるエリアを信頼できないエリアから分離することができます。境界内のすべてのスイッチはIPv6ファーストホップセキュリティをサポートし、境界内のホストとルータは信頼できるデバイスです。たとえば、下の図のスイッチ B とスイッチ C は、保護されたエリア内の内部リンクです。



ネイバーバインドポリシー設定画面の device-role コマンドで、境界を指定します。各 IPv6 ファースト ホップ セキュリティ スイッチは、エッジによって分割されたネイバーをバインドします。この方法により、バインドエントリは IPv6 ファースト ホップ セキュリティ デバイスに分散されて、境界を形成します。その後、IPv6 ファースト ホップ セキュリティ デバイスは、各デバイスですべてのアドレスのバインドを設定せずに、境界の内部にバインド整合性を提供できます。

ルータ アドバタイズメント ガード

ルータ アドバタイズメント（RA）ガードは、トラップされた RA メッセージを処理する最初の FHS 機能です。RA ガードは、次の機能をサポートしています。

- 受信した RA、CPA、および ICMPv6 リダイレクト メッセージのフィルタリング。RA ガードは、ロールがルータではないインターフェイスで受信された RA および CPA メッセージを破棄します。
- 受信した RA メッセージの検証。RA ガードは、インターフェイスに接続されている RA ガードポリシーに基づくフィルタリングを使用して RA メッセージを検証します。

メッセージが検証に合格しないと、ドロップされます。FHS 共通コンポーネントのロギング パケット ドロップ設定が有効になっている場合は、レートが制限された SYSLOG メッセージが送信されます。

ネイバー探索インスペクション

ネイバー探索（ND）インスペクションは、次の機能をサポートしています。

- 受信したネイバー探索プロトコルメッセージの検証
- 出力フィルタリング

メッセージ検証

インターフェイスに接続されている ND インスペクションポリシーに基づいて、ND インスペクションはネイバー探索プロトコルメッセージを検証します。[ND Inspection Settings] ページで、このポリシーを定義できます。

メッセージがポリシーで定義されている検証に合格しない場合、メッセージはドロップされ、代わりにレート制限 SYSLOG メッセージが送信されます。

出力フィルタリング

ND インスペクションは、ホストインターフェイスとして設定されているインターフェイスでの RS および CPS メッセージの転送をブロックします。

ネイバー バインド整合性

ネイバー バインド（NB）整合性では、ネイバーのバインドが確立されます。NB 整合性の個別かつ独立したインスタンスは、その機能が有効になっている各 VLAN で実行されます。

アドバタイズされた IPv6 プレフィックスの学習

NB 整合性は、RA メッセージでアドバタイズされた IPv6 プレフィックスを学習し、ネイバープレフィックス テーブルに保存します。プレフィックスは、割り当てられたグローバル IPv6 アドレスの検証に使用されます。デフォルトでは、この検証は無効になっています。これを有効にすると、アドレスは [Neighbor Binding Settings] ページのプレフィックスと照らし合わせて検証されます。アドレス検証に使用されるスタティックプレフィックスは、[Neighbor Prefix Table] ページで追加できます。

グローバル IPv6 アドレスの検証

NB 整合性は、次の検証を実行します。

- NS または NA メッセージのターゲット アドレスがグローバル IPv6 アドレスの場合は、RA プレフィックス テーブルで定義されているプレフィックスのいずれかに属している必要があります。

- DHCPv6 サーバーから提供されたグローバル IPv6 アドレスは、IPv6 プレフィックスリストで定義されているプレフィックスのいずれかに属している必要があります。

メッセージが検証に合格しない場合、メッセージはドロップされ、レート制限 SYSLOG メッセージが送信されます。

ネイバー バインド テーブルのオーバーフロー

新しいエントリを作成する空き領域がない場合は、エントリは作成されず、SYSLOGメッセージが送信されます。

ネイバーのバインドの確立

IPv6 ファースト ホップ セキュリティ スイッチは、次のメソッドを使用してバインド情報を検出および記録できます。

- NBI-NDP メソッド：スヌープされたネイバー探索プロトコル メッセージから IPv6 アドレスを学習
- NBI-DHCP メソッド：スヌープされた DHCPv6 メッセージから IPv6 アドレスを学習
- NBI 手動メソッド：手動設定を使用

IPv6アドレスは、ホストのネットワーク接続のリンク層プロパティにバインドされます。このプロパティは「バインドアンカー」と呼ばれ、ホストの接続に使用されるインターフェイス識別子（if Index）とホストの MAC アドレスで構成されています。

IPv6 ファースト ホップ セキュリティ スイッチは、境界インターフェイスのみでバインドを確立します。バインド情報は、ネイバーバインドテーブルに保存されます

NBI-NDP メソッド

使用される NBI-NDP メソッドは、RFC6620 で指定されている FCFS-SAVI メソッドに基づいていますが、次の違いがあります。

- リンク ローカル IPv6 アドレスのバインドのみをサポートする FCFS SAVI とは異なり、NBI-NDP はさらにグローバル IPv6 アドレスのバインドをサポートします。
- NBI-NDP は、NDP メッセージから学習した IPv6 アドレスのみを対象とした IPv6 アドレスバインドをサポートします。データ メッセージの発信元アドレス検証は、IPv6 ソース アドレス ガードによって提供されます。
- NBI-NDP では、アドレス所有権の証明は先着順の原則に基づいています。特定の発信元アドレスを要求する最初のホストが、さらに通知があるまでそのアドレスの所有者になります。ホストの変更は承認されないため、新しいプロトコルを必要とせずにアドレスの所有権を確認する方法を見つける必要があります。このため、NDP メッセージから IPv6 アドレスを最初に学習するたびに、スイッチはアドレスをインターフェイスにバインドします。この IPv6 アドレスを含む以降の NDP メッセージを、同じバインドアンカーに照らし合わせてチェックすることで、発信元が送信元 IP アドレスを所有していることを確認できます。

IPv6 ホストが L2 ドメインにローミングするか、またはその MAC アドレスを変更した場合は、このルールの例外が発生します。この状況では、ホストは引き続き IP アドレスの所有者ですが、関連付けられているバインドアンカーが変更された可能性があります。この状況に対処するために、NBI-NDP は、以前のバインド インターフェイスに DAD-NS メッセージを送信することにより、ホストに引き続き到達可能かどうかを検証します。以前に記録されたバインド アンカーでホストに到達できない場合、NBI-NDP は新しいアンカーが有効であると見なし、バインドアンカーを変更します。以前に記録されたバインドアンカーを使用してホストに引き続き到達可能な場合、バインドインターフェイスは変更されません。

ネイバーバインドテーブルのサイズを減らすために、NBI-NDP は境界インターフェイスのみでバインドを確立し（「IPv6 ファースト ホップ セキュリティの境界」を参照）、NS および NA メッセージを使用して、内部インターフェイス経由でバインド情報を配布します。NBI-NDP ローカルバインドを作成する前に、デバイスは関連するアドレスを照会する DAD-NS メッセージを送信します。あるホストが NA メッセージでそのメッセージに応答した場合、DAD-NS メッセージを送信したデバイスは、そのアドレスのバインドが別のデバイスに存在すると推測し、そのアドレスのローカル バインドを作成しません。DAD-NS メッセージへの応答として NA メッセージを受信しなかった場合、ローカルデバイスは、そのアドレスのバインドが他のデバイスに存在しないと推測し、そのアドレスのローカル バインドを作成します。

NBI-NDP は、ライフタイム タイマーをサポートしています。タイマーの値は、[Neighbor Binding Settings] ページで設定できます。このタイマーは、バインドされた IPv6 アドレスが確認されるたびに再起動されます。タイマーが期限切れになった場合、デバイスは短い間隔で最大 2 つの DAD-NS メッセージを送信してネイバーを検証します。

NBI-DHCP メソッド

NBI-NDP メソッドは、SAVI Solution for DHCP（draft-ietf-savi-dhcp-15、2012 年 9 月 11 日）で指定されている SAVI-DHCP メソッドに基づいています。

NBI-NDP と同様に、NBI-DHCP は、拡張性のために境界バインドを提供します。NBI-DHCP メソッドと NBI-FCFS メソッドには、次の違いがあります。NBIDHCP は DHCPv6 メッセージで発表された状態に従います。そのため、NS/NA メッセージで状態を配布する必要はありません。

NB 整合性ポリシー

他の IPv6 ファースト ホップ セキュリティ機能の動作と同じように、インターフェイスでの NB 整合性の動作は、インターフェイスに接続されている NB 整合性ポリシーで指定されます。これらのポリシーは、[Neighbor Binding Settings] ページで設定されます

DHCPv6 ガード

DHCPv6 ガードでは、トラップされた DHCPv6 メッセージが処理されます。DHCPv6 ガードは、次の機能をサポートしています。

- 受信したDHCPv6メッセージのフィルタリング。DHCPガードは、ロールがクライアントであるインターフェイスで受信されたDHCPv6メッセージを破棄します。インターフェイスロールは [DHCP Guard Settings] ページで設定されます。
- 受信したDHCPv6メッセージの検証。DHCPv6ガードは、インターフェイスに接続されているDHCPv6ガードポリシーに基づくフィルタリングを使用してDHCPv6メッセージを検証します。

メッセージが検証に合格しないと、ドロップされます。FHS共通コンポーネントのロギングパケットドロップ設定が有効になっている場合は、レートが制限されたSYSLOGメッセージが送信されます。

IPv6 ソース ガード

ネイバーバインド整合性（NB整合性）が有効になっている場合、IPv6ソースガードは、有効になっているかどうかに関係なく、NDPおよびDHCPv6のメッセージの送信元IPv6アドレスを検証します。NB整合性とIPv6ソースガードがどちらも有効になっている場合、IPv6ソースガードはTCAMを設定して、どのIPv6データフレームを転送、ドロップ、またはCPUにトラップする必要があるかを指定し、トラップされたIPv6データメッセージの送信元IPv6アドレスを検証します。NB整合性が有効になっていない場合、IPv6ソースガードは有効になっているかどうかに関係なくアクティブ化されません。

TCAMに新しいルールを追加する空き領域がない場合、TCAMオーバーフローカウンタが増加し、インターフェイス識別子、ホストのMACアドレス、およびホストのIPv6アドレスが含まれるレート制限SYSLOGメッセージが送信されます。IPv6ソースガードは、ネイバーバインドテーブルを使用して、受信したIPv6メッセージの送信元アドレスを検証します。ただし、検証なしで渡される次のメッセージを除きます。

- RSメッセージ（送信元IPv6アドレスが未指定のIPv6アドレスに等しい場合）。
- NSメッセージ（送信元IPv6アドレスが未指定のIPv6アドレスに等しい場合）。
- NAメッセージ（送信元IPv6アドレスがターゲットアドレスに等しい場合）。

IPv6ソースガードは、送信元IPv6アドレスが未指定のIPv6アドレスに等しい他のすべてのIPv6メッセージをドロップします。IPv6ソースガードは、境界に属する信頼できないインターフェイスのみで実行されます。

IPv6ソースガードは、次の場合に入力IPv6メッセージをドロップします。

- ネイバーバインドテーブルにIPv6アドレスが含まれていない場合。
- ネイバーバインドテーブルにIPv6アドレスが含まれているが、別のインターフェイスにバインドされている場合。

IPv6ソースガードは、不明な送信元IPv6アドレスのDAD_NSメッセージを送信することにより、ネイバーリカバリプロセスを開始します

-

攻撃からの保護

この項では、IPv6 ファースト ホップ セキュリティで提供される攻撃からの保護について説明します

IPv6 ルータ スプーフィングに対する保護

IPv6 ホストは、受信した RA メッセージを次の目的で使用できます。

- IPv6 ルータの検出
- ステートレス アドレスの設定

悪意のあるホストは、RA メッセージを送信して、自身を IPv6 ルータとしてアドバタイズし、ステートレス アドレス設定用の偽造プレフィックスを提供する可能性があります。RA ガードは、IPv6 ルータを接続できないすべてのインターフェイス用のホスト インターフェイスとしてインターフェイス ロールを設定することにより、このような攻撃からの保護を実現します。

IPv6 アドレス解決スプーフィングに対する保護

悪意のあるホストは、NA メッセージを送信して、特定の IPv6 アドレスを持つ IPv6 ホストとして自身をアドバタイズする可能性があります。NB 整合性は、次の方法でこのような攻撃からの保護を提供します。

- 特定の IPv6 アドレスが未知の場合は、内部インターフェイスのみにネイバー要請（NS）メッセージが転送されます。
- 特定の IPv6 アドレスが既知の場合は、IPv6 アドレスがバインドされているインターフェイスにのみ NS メッセージが転送されます。
- ネイバー アドバタイズメント（NA）メッセージは、ターゲット IPv6 アドレスが別のインターフェイスにバインドされている場合はドロップされます。

IPv6 重複アドレス検出スプーフィングに対する保護

IPv6 ホストは、特別な NS メッセージ（重複アドレス検出ネイバー要請（DAD_NS）メッセージ）を送信することによって、割り当てられている各 IPv6 アドレスに対して重複アドレス検出を実行する必要があります。

悪意のあるホストは、DAD_NS メッセージに対する応答を送信して、特定の IPv6 アドレスを持つ IPv6 ホストとして自身をアドバタイズする可能性があります。NB 整合性は、次の方法でこのような攻撃からの保護を提供します。

- 特定の IPv6 アドレスが未知の場合は、内部インターフェイスにのみ DAD_NS メッセージが転送されます
- 特定の IPv6 アドレスが既知の場合は、IPv6 アドレスがバインドされているインターフェイスにのみ DAD_NS メッセージが転送されます。
- NA メッセージは、ターゲット IPv6 アドレスが別のインターフェイスにバインドされている場合はドロップされます。

DHCPv6 サーバ スプーフィングに対する保護

IPv6 ホストは、DHCPv6 プロトコルを次の目的で使用できます。

- ステートレス情報の設定
- ステートレス アドレスの設定

NBD キャッシュ スプーフィングに対する保護

IPv6 ルータは、IPv6 アドレスをラスト ホップ ルーティング用の MAC アドレスにマップするネイバー探索プロトコル（NDP）キャッシュをサポートしています。悪意のあるホストは、ラストホップ転送用に異なる宛先 IPv6 アドレスを含む IPv6 メッセージを送信して、NBD キャッシュのオーバーフローを引き起こす可能性があります。

NDP 実装の組み込みのメカニズムでは、ネイバー探索キャッシュ内で許容される不完全状態のエントリの数が制限されます。これにより、ハッカーによるテーブルのフラッディングに対する保護が実現されます。

セキュア センシティブ データ管理

セキュアセンシティブデータ（SSD）は、パスワードやキーなどのデバイス上の機密データの保護を可能にするアーキテクチャです。パスワード、暗号化、アクセス制御、およびユーザー認証を使用して、機関で機密データを管理するための安全なアプローチを作成します。

この機能は、構成ファイルを保護し、構成プロセスを保護し、SSD ゼロタッチ自動構成を容易にするように拡張されています。

SSD は、ユーザー資格情報および SSD ルールに基づいて暗号化された機密データやプレーンテキストの機密データへのアクセスの許可/拒否、機密データを含むコンフィギュレーションファイルの改ざんからの保護により、デバイスの機密データ（パスワードやキーなど）を保護します。

さらに、SSD では、機密情報を含むコンフィギュレーションファイルをセキュアにバックアップおよび共有することができます。

ユーザーは機密データに必要な保護のレベルを、プレーンテキストの機密データを保護しないレベルから、デフォルトパスフレーズに基づく暗号化による最小限の保護、ユーザー定義のパスフレーズに基づく暗号化による強力な保護まで、選択できます。

認証され承認されたユーザーのみに機密データへの読み取り権限が付与され、これは SSD の規制に従って行われます。ユーザー認証プロセスを通じて、デバイスはユーザーに対する管理アクセスを認証および承認します。SSD を使用しているかどうかにかかわらず、管理者は、ローカル認証データベースを使用して認証プロセスの安全性を確保したり、ユーザー認証プロセスで使用される外部認証サーバーへの通信の安全性を確保したりすることが推奨されます。

要約すると、SSD は、SSD 規則、SSD 属性、およびユーザー認証を使用して、デバイス上の機密データを保護します。また、デバイスの SSD 規則、SSD 特性、ユーザー認証構成はすべて、SSD が保護する重要なデータです。

SSD 管理

SSD管理は、機密データをどのように処理および保護するかを指示する一連のセットアップパラメータで構成されます。SSD 構成パラメータは、SSD によって保護される機密情報です。

SSD 構成はすべて、適切な権限を持つ人だけがアクセスできる SSD ページから行います。

SSDルール

SSD規則により、管理チャネルのユーザーセッションに割り当てられる読み取りアクセス許可とデフォルトの読み取りモードが定義されます。SSD 規則が属するユーザーおよび SSD 管理チャネルは、独自のIDを提供します。同じユーザーだが異なるチャネルに対応する異なるSSD規則が存在することがあります。逆に、同じチャネルだが異なるユーザーに対応する異なる規則が存在することがあります。

読み取りアクセス許可は、次のような機密データを表示する方法を指定します。暗号化された形式のみ、プレーンテキスト形式のみ、暗号化された形式とプレーンテキスト形式の両方、または機密データへのアクセス許可なし。SSD規制は機密データとして分類されているため、保護されています。

デバイスでサポートできる SSD 規則は合計 32 個あります。デバイスにより、ユーザーアイデンティティ/クレデンシャルおよびユーザーの機密データへのアクセスで経由する管理チャネルのタイプに最も一致するSSD規則のSSD読み取りアクセス許可がユーザーに付与されます。

すべてのデバイスには、一連のデフォルト SSD 規則が含まれています。SSD 規則は、管理者がいつでも追加、削除、変更できます。

デフォルトの SSD ルール

デバイスは、次のファクトリー デフォルトの規則を保持しています。

ルール キー		規則アクション	
ユーザ	チャネル	読み取り権限	デフォルト読み取りモード
レベル 15	セキュア XML SNMP	Plaintext Only	Plaintext
レベル 15	セキュア	Both	Encrypted
レベル 15	非セキュア	Both	Encrypted
すべて（All）	非セキュア XML SNMP	Exclude	Exclude
すべて（All）	セキュア	Encrypted Only	Encrypted
すべて（All）	非セキュア	Encrypted Only	Encrypted

デフォルトの規則を変更することはできますが、削除することはできません。SSDデフォルト規則を変更した場合は、それらを復元できます。

セキュア シェル

セキュアシェル（SSH）は、SSH クライアント（デバイス）と SSH サーバー間でデータのセキュアな送信を可能にするネットワークプロトコルです。

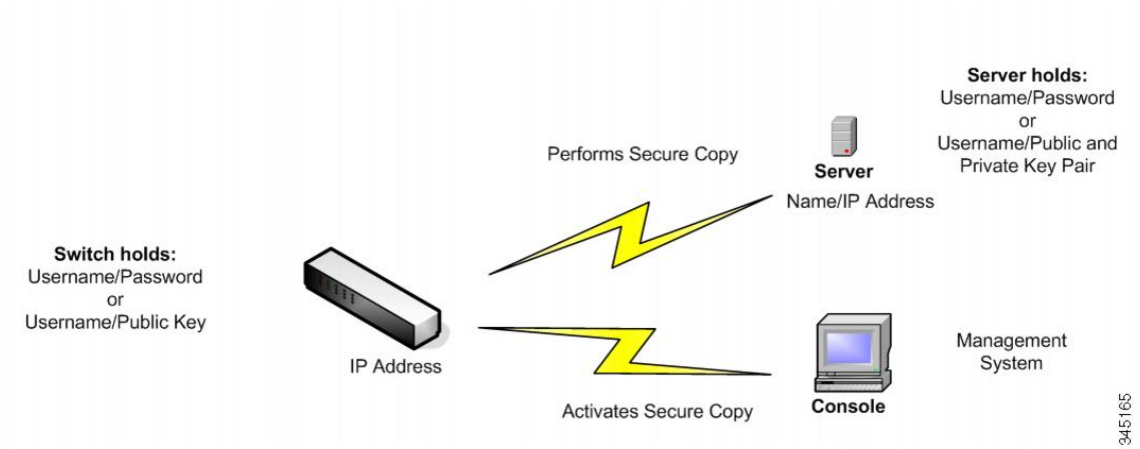
SSH クライアントは、中央の SSH サーバーに保持されているさまざまなシステムファイルを持つ1つ以上のスイッチで構成されるネットワークの管理を支援します。SSHプロトコルを使用してネットワークを通じて構成ファイルを転送するアプリケーションであるセキュアコピー（SCP）により、ユーザー名/パスワードなどの機密データが盗まれないことが保証されます。セキュアコピー（SCP）は、ファームウェア、ブートイメージ、設定ファイル、言語ファイル、およびログファイルを中央SCPサーバーからデバイスへ安全に転送するための方法です。

SSH に関しては、デバイスで実行されている SCP が SSH クライアント アプリケーションであり、SCP サーバが SSH サーバ アプリケーションとなります。

ファイルが TFTP または HTTP を介してダウンロードされる場合、データ転送は保護されません。ファイルがSCPを介してダウンロードされる場合、データはセキュアチャネル経由でSCPサーバーからデバイスへ送信されます。この安全なチャネルを作成するには、ユーザーがアクティビティを実行する権限を持っていることを確認するため、認証が必要です。この項目ではサーバーの操作について説明しませんが、認証情報は、デバイスと SSH サーバーの両方に、ユーザーが入力する必要があります。

次の図は、SCP 機能を利用できる一般的なネットワーク構成を示しています。

一般的なネットワーク構成



QoS

QoS（Quality of Service）は、さまざまなアプリケーション、データフロー、またはユーザーのパフォーマンスを保証するために、1 つまたは複数のタイプのトラフィックに他よりも高い優先度を割り当てます。QoS では、ネットワーク上に存在するさまざまな変数を調べることで、問題への対処方法が決定されます。

QoS が対処する問題

- 遅延：宛先ネットワークへの理想的なパフォーマンスを発揮できないルート。このような遅延により、VoIP などの一部のアプリケーションでエラーが発生する可能性があります。
    - QoS を使用する最大の理由は、リアルタイム アプリケーション（RTA）への対応です。
- パケットのドロップ：バッファが一杯になり、パケットが時間内に処理されないと、それらのパケットがドロップされます。競合のあるリンクでは、QoS がトラフィックに優先度を割り当てるため、重要度の低いトラフィックのパケットがドロップされます。
- エラー：パケットはさまざまな理由で破損しますが、TCP を使用しているため、ACK を受信するまで再送信が継続され、再送信と遅延が発生します。
- ジッター：パケットが宛先に到達するパスは複数存在する可能性があり、最適パスが使用されない場合があります。この変動により、「ジッター」と呼ばれる遅延が発生します。ジッターは 30 ミリ秒未満にする必要があります。また、パケット損失は 1% 以下にする必要があります。
- 順不同配信：パケットはさまざまなパスを使用して宛先に到達するため、受信するアプリケーションでパケットの並べ替えに予期以上の時間がかかり、遅延やドロップが発生する場合があります。QoS は、予測可能性のレベルに関する要件を持つアプリケーションが、必要な帯域幅を受け取ることを保証します。

QoS のメカニズム

- 分類：QoS のクラス指向のメカニズムによってサポートされます。
- 輻輳管理：各インターフェイスのキューイングメカニズムでパケットの送信に優先順位を付けるために使用されます。
- ポリシング：パケットをドロップまたはマークダウンすることによってレート制限を適用するために使用されます。
- シェーピング：バッファを使用してパケットを遅延させることによってレート制限を適用するために使用されます。

QoS の一般パラメーターを設定を設定するには、次の手順に従います。

ステップ 1 [QoS プロパティ] ページで信頼モードを選択し、QoS を有効にします。次に、[インターフェイス設定] ページで、ポートに対する QoS を有効にします。

ステップ 2 [QoS プロパティ] ページで、各インターフェイスにデフォルトの CoS または DSCP プライオリティを割り当てます。

ステップ 3 [キュー] ページで、各出力キューに対してスケジュール方式（完全優先または WRR）と WRR 帯域割り当て率を設定します。

ステップ 4 [DSCP 値のキューへのマッピング] ページで、各 IP DSCP/TC 値に出力キューを割り当てます。デバイスが DSCP 信頼モードになっている場合、着信パケットは、その DSCP/TC 値に基づいて出力キューに格納されます。

ステップ 5 各 CoS/802.1p プライオリティに出力キューを割り当てます。デバイスが CoS/802.1 信頼モードになっている場合、すべての着信パケットは、パケットの CoS/802.1p プライオリティに基づいて出力キューに格納されます。この作業は [CoS/802.1p 値のキューへのマッピング] ページで行います。

ステップ 6 次のページで、帯域幅とレート制限を設定します。

a) [キューあたりの出力シェーピング] ページで、各キューに対する出力シェーピングを設定します。

b) [帯域幅] ページで、各ポートに対する入力レート制限と出力シェーピング レートを設定します。

QoS の機能とコンポーネント

QoS 機能は、ネットワークのパフォーマンスを最適化する目的で使用されます。

QoS を使用すると、次のことが可能です。

- 次の属性に基づいて着信パケットをトラフィック クラスに分類する。
  - デバイス設定
  - 入力インターフェイス
  - パケット内容
  - これらの属性の組み合わせ

QoS には、以下のことが含まれます。

- トラフィック分類：着信パケットのそれぞれを、パケットの内容やポートに基づいて、特定のトラフィック フローに属するものとして分類します。分類は ACL（アクセス制御リスト）によって行われ、ACL の条件を満たすトラフィックだけが CoS または QoS 分類の対象になります。
- ソフトウェア キューへの割り当て：着信パケットが転送キューに割り当てられます。パケットは特定のキューに送信され、それらのパケットが属しているトラフィック クラスの機能として処理されます。
- その他のトラフィック クラス処理属性：QoS 機構が各種のクラス（帯域幅管理など）に適用されます。

QoS モード

選択されている QoS モードは、システム内のすべてのインターフェイスに適用されます。

- 基本モード：サービス クラス（CoS）。

  同じクラスのトラフィックはすべて、同じように処理されます。具体的には、着信フレーム内で示されている QoS 値に基づいて、出力ポート上の出力キューを決定するという 1 つの QoS アクションが実行されます。この QoS 値は、レイヤ 2 においては VLAN Priority Tag（VPT）802.1p 値となり、レイヤ 3 においては、IPv4 の場合は Differentiated Service Code Point（DSCP）値、IPv6 の場合はトラフィック クラス（TC）値となります。デバイスが基本モードで動作している場合、外部デバイス上で割り当てられたこの QoS 値が信頼されます。外部デバイス上で割り当てられた、パケットの QoS 値によって、そのパケットのトラフィック クラスと QoS が決定されます。

- 拡張モード：フローごとのサービス品質（QoS）。

  拡張モードの場合、フローごとの QoS は、クラス マップやポリサーで構成されます。

  - クラス マップはフローのトラフィックの種類を定義し、1 つ以上の ACL が含まれています。ACL に合致するパケットは、フローに属します。

  - ポリサーは、設定されている QoS をフローに適用します。フローの QoS 設定に含められるのは、出力キュー、DSCP または CoS/802.1p 値、およびアウト オブ プロファイル（超過）トラフィックに対するアクションです。

- 無効モード：このモードでは、すべてのトラフィックが単一のベスト エフォート キューにマッピングされるため、特に優先されるトラフィックのタイプはありません。

アクティブになるのは一度に 1 つのモードだけです。システムが QoS 拡張モードで動作するように設定されているときには、QoS 基本モードの設定値はアクティブになりません。その逆も同じです。

モードが変更されると、次のことが発生します。

- QoS 拡張モードからその他のモードに変更される場合、ポリシー プロファイル定義とクラス マップが削除されます。インターフェイスに直接適用されている ACL は、適用された状態のままになります。

- QoS 基本モードから拡張モードに変更される場合、基本モードでの QoS 信頼モードの設定は保持されません。

- QoS が無効にされた場合、シェーパーとキューの設定（WRR/SP 帯域幅の設定）はデフォルト値にリセットされます。

その他のすべてのユーザ設定は、そのまま維持されます。

SNMP

SNMP は、マネージャとエージェント間の通信のメッセージ フォーマットを提供するアプリケーションレイヤプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および管理情報ベース（MIB）で構成されます。SNMP マネージャは、CiscoWorks などのネットワーク管理システム（NMS）に統合できます。エージェントおよび MIB は、スイッチに常駐します。スイッチに SNMP を設定するには、マネージャとエージェントの関係を定義します。

SNMP は、通常、ルータの管理に関連付けられていますが、さまざまなタイプのデバイスの管理に使用できることを理解することが重要です。スイッチは SNMP エージェントとして機能し、SNMPv1、v2、v3 をサポートします。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイスパラメータやネットワーク データの保存場所である MIB から値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

SNMP バージョン

インターネット技術標準化委員会（IETF）は、SNMP を含むインターネットトラフィックを制御する標準プロトコルの定義を担当しています。IETF は、IP レルムに存在する多くのプロトコルの仕様である Requests for Comments（RFC）を公開しています。これらのドキュメントは、まず、標準化提案として標準化過程に入り、次に、ドラフトステータスに移行します。最終ドラフトが最終的に承認されると、その RFC に標準ステータスが与えられますが、完全に承認された標準は一般に思われているほど多くありません。他にも「歴史的」と「実験的」という 2 つの標準化過程の分類があり、それぞれ、「より新しい RFC によって置き換えられたドキュメント」と「まだ標準になるには準備不足であるドキュメント」が含まれます。次のリストには、現在のすべての SNMP バージョンとそれぞれの IETF ステータスが含まれています。

- SNMP バージョン 1（SNMPv1）は、SNMP プロトコルの最初のバージョンです。これは RFC 1157 で定義されており、歴史的 IETF 標準です。SNMPv1 のセキュリティの基盤であるコミュニティストリングは、単なるパスワード（プレーンテキストストリング）にすぎません。この文字列を認識するすべての SNMP ベースアプリケーションに、デバイスの管理情報へのアクセスが許可されます。SNMPv1 には基本として 3 つのコミュニティ（読み取り専用、読み取り/書き込み、トラップ）があります。SNMPv1 は歴史的標準ですが、今でも多くのベンダーがサポートする主要な SNMP 実装であることに注意してください。
- SNMP バージョン 2（SNMPv2）は、多くの場合、コミュニティストリングベースの SNMPv2 と呼ばれます。

- SNMP バージョン 3（SNMPv3）は、最新バージョンの SNMP です。ネットワーク管理上の主な役割はセキュリティです。管理対象エンティティ間の強力な認証およびプライベート通信のサポートが追加されています。

システムへのアクセスを制御するには、コミュニティエントリのリストが定義されます。各コミュニティエントリは、コミュニティストリングおよびそのアクセス権限で構成されます。適切な権限および正しい操作を持つコミュニティを指定するSNMPメッセージにのみ、システムは応答します。

SNMPエージェントは、デバイスの管理に使用される変数のリストを維持します。これらの変数は、管理情報ベース（MIB）で定義されます。

表 *4 : SNMP* のバージョンとセキュリティ レベル

バージョン	レベル	認証	暗号化
SNMPv1	noAuthNoPriv	コミュニティストリング	未対応
SNMPv2C	noAuthNoPriv	コミュニティストリング	未対応
SNMPv3	noAuthNoPriv	Username	未対応
SNMPv3	authNoPriv	Message Digest 5（MD5）またはSecure Hash Algorithm（SHA）	未対応
SNMPv3	authPriv（暗号化ソフトウェアイメージが必要）	MD5 または SHA	データ暗号規格（DES）または Advanced Encryption Standard（AES）

（注） その他のバージョンにはセキュリティの脆弱性があるため、SNMPv3を使用することをお勧めします。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。

- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリートポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS がスイッチにアクセスするには、NMS のコミュニティ ストリング定義が、スイッチ上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致していなければなりません。

コミュニティ ストリングの属性は、次のいずれかです。

- Read-Only（RO）：許可された管理ステーションに、コミュニティ ストリングを除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- Read-Write（RW）：許可された管理ステーションに、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ ストリングに対するアクセスは許可しません。
- クラスタを作成すると、コマンド スイッチがメンバ スイッチと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドスイッチ上で最初に設定された RW および RO コミュニティストリングにメンバスイッチ番号（*@esN*、*N* はスイッチ番号）を追加し、これらのストリングをメンバスイッチに伝播します。

サポートされている MIB

Management Information Base（MIB）は定義の集合であり、これらによって管理対象デバイス内の管理対象オブジェクトのプロパティが定義されます。サポート対象 MIB の一覧を表示するには、次の URL に移動し、Cisco MIBS として列挙されたダウンロード エリアに移動します：

http://www.cisco.com/cisco/software/navigator.html

SNMP を介したスイッチポートモードの設定

スイッチで SNMP を介してスイッチポートモードを設定するには、次の手順を実行します。

ステップ 1 コンソールポート経由でスイッチに接続し、スイッチを工場出荷時のデフォルトにリセットします。

ステップ 2 SNMP を有効にして、読み取りおよび書き込み権限のコミュニティ名を設定します。

ステップ 3 任意の MIB ブラウザ（MG-Soft など）で、vlanPortModeState を選択して右クリックします。

ステップ 4 次に、[Set] を選択します。

ステップ 5 [Select Table Instance(s)] が表示されます。このテーブルには、インターフェイス ID に対応するインスタンス ID と、スイッチポートに対応する [Value] 列の値が含まれます。

例：

インスタンス 1 は GigabitEthernet 1/0/1 インターフェイスに対応します。

例：

インスタンス 3 は GigabitEthernet 1/0/3 インターフェイスに対応します。

[Value] は、インターフェイスのスイッチポートモードがアクセスされていることを示します。

全般モード	10	プライベート - VLAN プロミスキャスモード	13
アクセス モード	11	プライベート - VLAN ホストモード	14
トランク モード	12	カスタマー	15

ステップ 6 [Instance 3] を選択し、GigabitEthernet 1/0/3 インターフェイスのスイッチポートモードを [General] に変更します。

ステップ 7 次に、トランクモードについて手順を繰り返します。

SNMP を介した VLAN の作成または追加

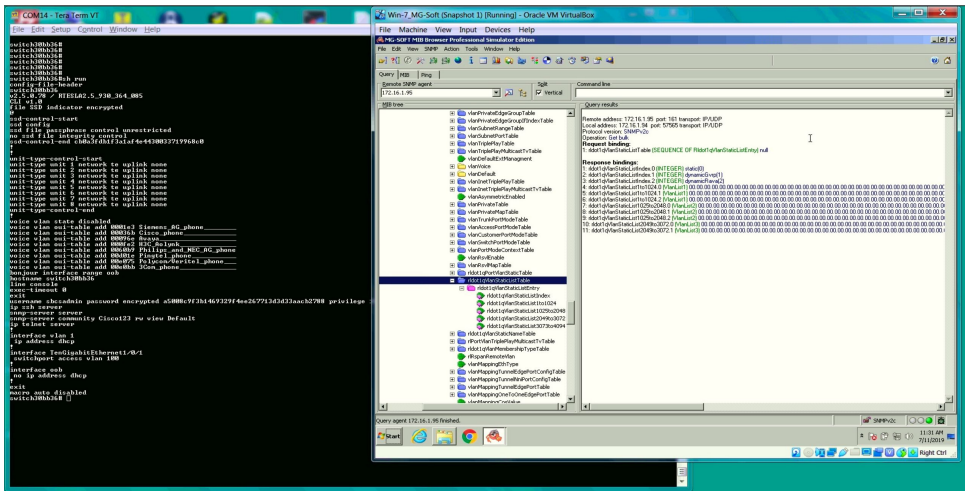
スイッチで VLAN を作成または追加するには、次の手順を実行します。

ステップ 1 コンソールポート経由でスイッチに接続し、スイッチを工場出荷時のデフォルトにリセットします。

ステップ 2 SNMP を有効にして、読み取りおよび書き込み権限のコミュニティ名を設定します。

ステップ 3 show run コマンドを実行します。

ステップ 4 任意の MIB ブラウザ（この例では MG-Soft）で、rldot1qVlanStaticListTable MIB コンテナを選択し、Get Bulk 操作を実行します。



ステップ 5 上のスライドを参照して、VLAN を作成または追加します。

a) VLAN 2 ～ 14、16 を追加します。

b) [rldot1qVlanStaticList1to1024] を選択します。

c) [Set] 操作ウィンドウを開きます。

d) VLAN 値をオクテット形式 "# 0x7F 0xFD で設定します。

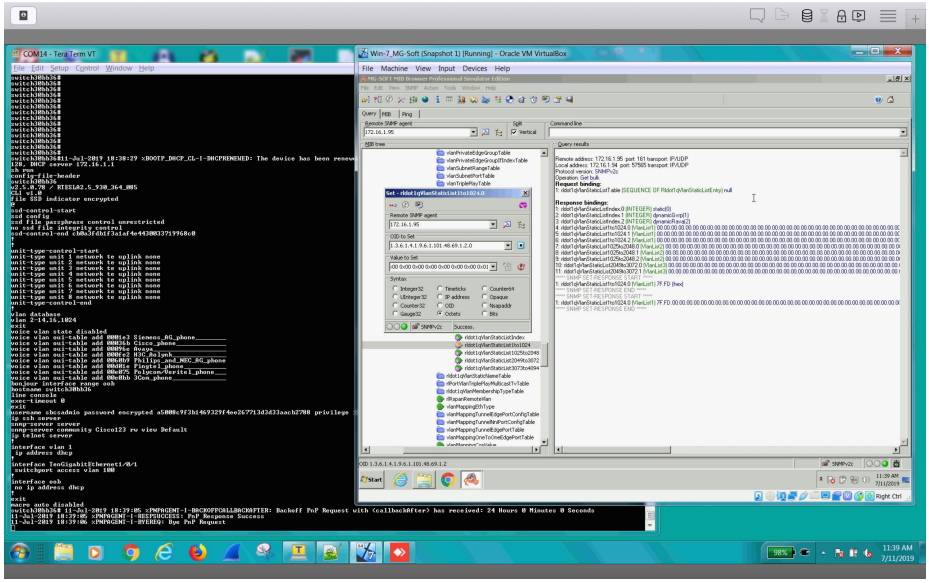
例：

VLAN ID。1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

オクテットビット：0 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1

オクテット（16 進数）：7 F F D

ステップ 6 [Set] をクリックして VLAN を追加します。



ステップ 7 VLAN 1024 を追加する場合は、次の手順を実行します。

a) [Set] 操作ウィンドウを開いた状態で、[Value to Set] をクリックしてアイコンを更新します。このフィールドが “rldot1qVlanStaticList1to1024 で更新されます。
b) フィールド内を最後のオクテットまで右にスクロールして、1024 番目のビット値を 1 に設定します。
c) [Set] をクリックします。

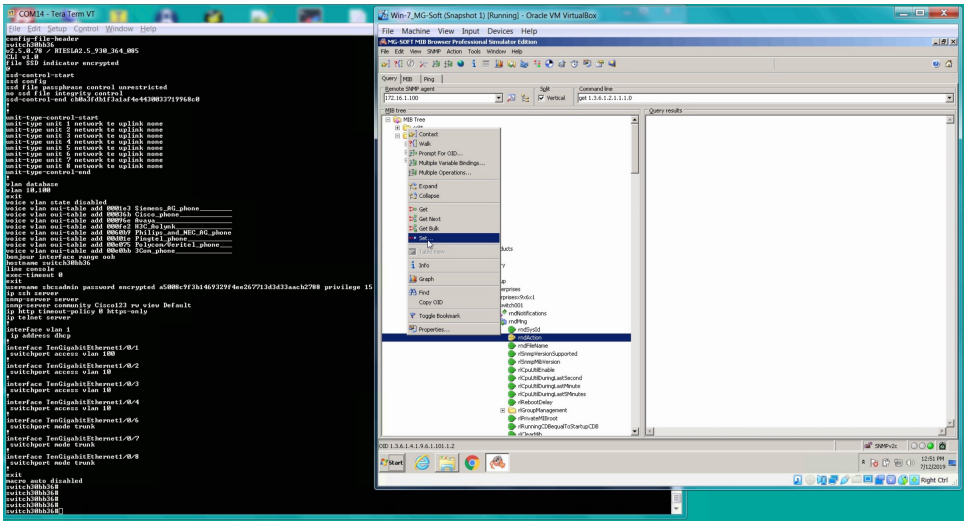
4 つの分かりやすい VLAN のリストがあります。

- rldot1qVlanStaticList1to1024
- rldot1qVlanStaticList1025to2048
- rldot1qVlanStaticList2049to3072
- rldot1qVlanStaticList3073to4094

SNMP 経由の再起動リセット

スイッチを工場出荷時のデフォルト設定にリセットするには、次の手順を実行します。

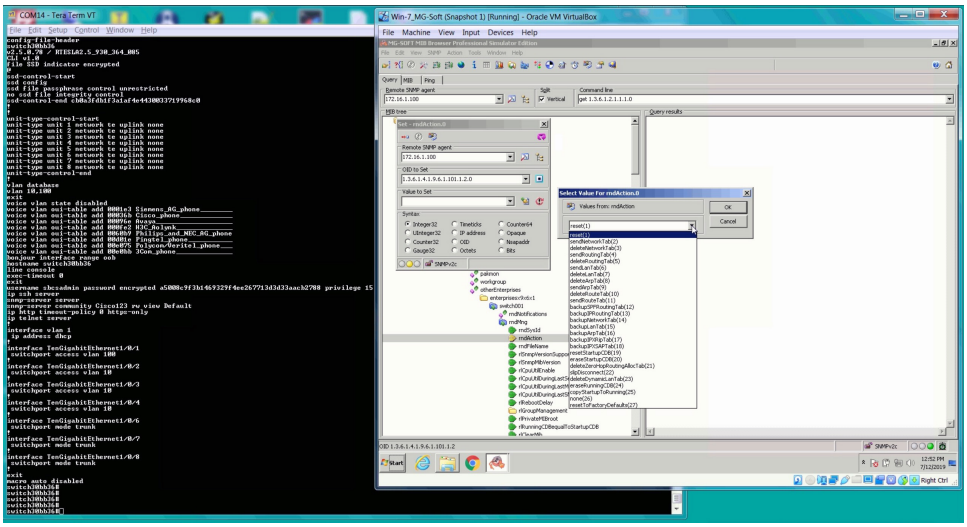
ステップ 1 コンソールポート経由でスイッチに接続し、スイッチを工場出荷時のデフォルトにリセットします。
ステップ 2 SNMP を有効にして、読み取りおよび書き込み権限のコミュニティ名を設定します。
ステップ 3 設定を保存します。
ステップ 4 show コマンドを実行します。
ステップ 5 任意の MIB ブラウザ（この例では MG-Soft）で、rndAction MIB を選択します。
ステップ 6 右クリックし、[Set] を選択します。



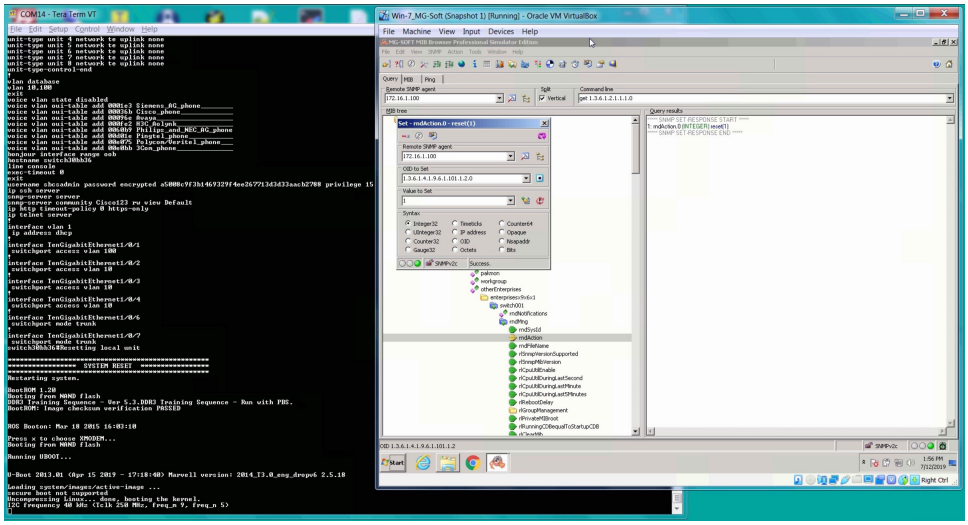
ステップ 7 [Value to Set] フィールドの横に 2 つのアイコンがあります。

a) [Select From Value List] をクリックします。
b) ドロップダウンリストから [Reset] 選択し、[OK] をクリックします。

c) 次に、[Set] をクリックします。



d) スイッチの再起動後、ユーザー名とパスワードでログインし、[resetTo Factory Default(27)] を選択して手順を繰り返します。再起動後、新しいユーザー名とパスワードを作成する必要があります。



翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。